КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.182198
УДК 336.71:004.056

Глухов Сергій Іванович
Доктор технічних наук, професор
Завідувач кафедри військово-технічної підготовки факультету
післядипломної освіти Військового інституту
Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID 0000-0002-4918-3739
gluhov1971@ukr.net

Собчук Андрій Валентинович
доктор філософії
доцент кафедри інформаційної та кібернетичної безпеки
Навчально-науковий інститут Захисту інформації
Державний університет телекомунікацій, Київ, Україна
ORCID 0000-0003-3250-3799
anri.sobchuk@gmail.com

Ровда Володимир Володимірович
аспірант
Державний університет інформаційно-комунікаційних технологій
ORCID 0009-0001-9987-6787
volodymyr.rovda@gmail.com

Половінкін Миколай Ігорович
аспірант
Державний університет інформаційно-комунікаційних технологій
ORCID 0009-0009-5242-567X
navarrokain@gmail.com

Пономаренко Віталій Валерійович
аспірант навчально-наукового інституту захисту інформації
Державний університет інформаційно-комунікаційних технологій
ORCID 0000-0002-6567-4247
Ur_suviator @ukr.net

МЕТОД ВИЯВЛЕННЯ ВИТОКУ ІНФОРМАЦІЇ ЗА ВІДХИЛЕННЯМ ТРАФІКУ З ІНФОРМАЦІЙНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Анотація. У роботі проведено аналіз методів виявлення витоку мовної інформації. Проведений аналіз показав відсутність єдиного науково методичного апарату або автоматизованих програмних комплексів для забезпечення оперативного здійснення аналізу трафіку. Тому робота присвячена актуальної тематиці виявлення витоку інформації за відхиленням трафіку з інформаційної мережі зв'язку. Пропонується удосконалений метод забезпечення оперативного здійснення аналізу трафіку та інформування про підозрілу ситуацію. Ситуацію яка потребує подальшого детального аналізу трафіку автоматизованими програмними комплексами або відповідними спеціалістами. Розроблений метод дозволяє здійснювати інформування, у реальному часі, відповідальних спеціалістів, про можливий виток інформації, якій базується на аналізі відхилення характеру трафіку з елементів інформаційної мовної мережі. Відхилення, характеру трафіку з елементів параметрів мережі вимірюються відносно звичного трафіку телефонної або мовної мережі відносно цих параметрів. Проводиться порівняльний аналіз звичайного трафіка з трафіком у реальному часі. Наведений метод додатково удосконалює методику. Удосконалення проведено за рахунок використання практичних рекомендації щодо сталих коефіцієнтів, розрахунків. Ці коефіцієнти для удосконаленого методу обирались розрахунковим та емпіричним шляхом,

що дозволяє значно скоротити реакцію системи оцінки трафіку, системи яка використовує розроблену методику для виявлення можливого витоку мовної інформації

Ключові слова: відхилення трафіку; метод; модель; прогнозування; інформаційні технології; стійкість; запізнення; конфіденційність; доступність; неправдива інформація; персональні дані.

ВСТУП

Згідно з дослідженнями всесвітньої Асоціації по контролю за порушеннями на телекомунікаційних мережах (Communications Fraud Control Association, CFCA), втрати від порушень в телекомунікаційній галузі складали 74,4–90 млдр. долл. Це приблизно на 57% більше цифри, одержаної в дослідженнях CFCA трирічної давності [1]. Порушення на телекомунікаційних мережах це дії, абонентів, операторів телекомунікацій чи сторонніх осіб, які направленні на одержання несанкціонованого доступу до мовної інформації та телекомунікаційних послуг за більш низькою ставкою або без оплати. Експерти CFCA нараховують близько 200 видів порушень на телекомунікаційних мережах. Найбільш поширеними порушеннями зі сторони абонентів є стороннє підключення до абонентської лінії з метою отримання мовної інформації, здійснення довготривалих міжнародних розмов, організація несанкціонованих переговорних пунктів [2]. Зі сторони сторонніх осіб порушенням є використання апаратно-програмного забезпечення для отримання несанкціонованого доступу до мовної інформації, міжнародного трафіку з мережі Інтернет та завершення його на телекомунікаційній мережі загального користування під виглядом місцевого, що призводить до втручання в роботу засобів зв'язку, підміни інформації про виклик. Зі сторони операторів найбільш поширеним є несанкціоноване прослухування розмов, перенаправлення вхідного міжміського та міжнародного трафіку на мережу загального користування під виглядом місцевого. Зловживання призводять до втрати репутації, доходів, скарг абонентів та порушення функціонування телекомунікаційних мереж.

Боротьба із зловживаннями на телекомунікаційних мережах значною мірою спирається на аналіз даних про послуги та дані, що їх містять розрахункові системи з абонентами та операторами [3]. Виявлення підозрілих дій абонентів та їх аналіз є основним принципом дії сучасних систем захисту проти порушень (Fraud Managment System, FMS). Ключовими критеріями ефективності FMS є швидкість роботи, гнучкість налагодження алгоритмів, які забезпечують виявлення та аналіз інцидентів та наявність стандартизованих інтерфейсів для інтеграції з платформами білінгу та системою управління взаємодією з клієнтами (Customer Relationship Management System, CRM).

АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ ТА ПОСТАНОВКА ПРОБЛЕМИ

Завданням щодо забезпечення оперативного здійснення аналізу трафіку зв'язку з метою виявлення каналів витоку інформації присвячено значну кількість публікацій.

Так у роботі[4] розглядаються питання аналізу трафіку зв'язку з технічними параметрами, які можуть тільки показувати та у де яких випадках зберігати панорами сигналів в мережі зв'язку. Завдання аналізу трафіку зв'язку, особливо на предмет витоку інформації вони у взагалі не вирішують.

У роботах [5], [6] представлені результати дослідження захищеності мереж SS7. Стандарт Signaling System 7, які використовується для обміну службовою інформацією

між мережевими пристроями в телекомунікаційних мережах. Здійснюється аналіз, який свідчить про те, що у той час, коли розроблявся цей стандарт, доступ до мережі SS7 мали лише оператори фіксованого зв'язку, тому безпека не була пріоритетним завданням. Сьогодні мережа вже не є в тій же мірі ізольованою, тому зловмисник, який тим чи іншим шляхом отримав до неї доступ, має можливість використовувати недоліки безпеки для того, щоб прослуховувати мовну інформацію абонентів, читати SMS, викрадати гроші з рахунків, обходити системи тарифікації або впливати на функціонування мобільної мережі. Однак проблеми безпеки, методи захисту мережи не розглядаються та реальні способи захисту не пропонуються.

У роботах [7] – [9] розглядається розвиток мобільного зв'язку за останнє десятиліття. Відзначається, що стався величезний прогрес в області бездротового зв'язку і особливо в області стільникових мереж 4G. Проте, потрібно кілька років, щоб повністю перейти на системи 4G, і вже почалася робота над технологіями 5G і їх проблемами. Проблеми безпеки базуються на шифруванні інші проблеми захисту мереж не розглядаються.

У роботах [10], [11] говориться, що ефективна робота співробітників — одна з головних умов успіху компанії. Але саме співробітники можуть нанести велику шкоду безпеки інформації. Без забезпечення належного контролю в середньому до третини робочого часу може витрачатися на відвідування ресурсів, ніяк не пов'язаних з роботою. Саме тому важливо налаштувати контроль інтернет-трафіку та використовувати лічильник трафіку. У цих роботах захист та належний контроль за телефонним мобільним зв'язком не знайшов належного розгляду та опису.

Таким чином найбільш критичними є виявлення витоку інформації за відхиленням трафіку з інформаційної мережі зв'язку за рахунок: порушення порядку маршрутизації міжміських та міжнародних викликів, виявлення активності абонентських номерів по вихідному місцевому трафіку, активності операторів по вхідному місцевому трафіку, схожу на роботу шлюзів для завершення вхідного міжміського та міжнародного трафіку, виявлення змін у активності абонентських номерів, які можуть бути свідченням стороннього підключення до абонентської лінії або дій абонента, що потенційно призводять до скарг, несплата за послуги та списання заборгованості. Автоматизований аналіз даних про послуги повинен бути оперативним.

З проведеного аналізу наукової літератури можливо зробити висновок, що універсальних пристроїв або автоматизованих програмних комплексів для забезпечення виявлення витоку інформації, оперативного здійснення аналізу трафіку та передачі інформації автоматизованими комплексами або відповідними спеціалістами практично немає. Тому тема розробки методів виявлення витоку інформації за відхиленням трафіку з інформаційної мережі зв'язку, відхилення трафіку, що є підозрілими та потребує подальшого детального аналізу автоматизованими комплексами або відповідними спеціалістами, методу інформування відповідальних спеціалістів актуальною і дуже важливою.

Мета статті. Підвищення ефективності виявлення каналів витоку мовної інформації з за рахунок використання розробленого методу виявлення витоку інформації за параметрами відхиленням трафіку з інформаційної мережі зв'язку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Робота механізмів виявлення порушень заснована на обробці записів про зареєстровані в мережі події CDR (Call Detail Record). Система протидії шахрайству вишукує в них невідповідності певним умовам або не відповідності заданому шаблону, характеристики поведінки абонента. Коли модуль виявлення знаходить одну з аномалій, він генерує повідомлення з попередженням.

До типових перевірок по умові для систем FMS можна віднести такі, як:

1. Неіснуюча нумерація (номеру сторони що викликає «А»);
2. Перевірка авторизації, тимчасового блокування номеру «А»;
3. Відповідність заданому шаблону;
4. Перевірка «чорних та білих списків»;
5. Номери абонентів «А» або «Б» що найчастіше повторюються;
6. Перевірка на тривалість з'єднання;
7. Перевірка підозрілих викликів від абонентів «А» на входження до переліку абонентів «Б» яким найчастіше надходять виклики із закордону;
8. Зміни інтенсивності сигнального та інформаційного навантаження.

Пошук по заданому шаблону опирається на шаблони трафіку який створюється для кожного оператора телекомунікацій. Різниця яка виникає між наявним сигнальним та інформаційним трафіком та шаблоном свідчить про можливе порушення. Додаткове застосування шаблонів полягає в складанні профілю абонента (оператора телекомунікацій) зловмисника та пошук відповідності такому профілю серед існуючих абонентів (операторів телекомунікацій). Профілі можуть мати в своєму складі такі характеристики, як:

- активність у денний час;
- активність у вечірній час;
- активність у нічний час;
- об'єми вихідного трафіку на мобільні телефони;
- об'єми вихідного трафіку на фіксовані місцеві номери (включаючи часто використовувані номери);
- об'єми вихідного трафіку на фіксовані номери в інших містах (включаючи часто використовувані номери);
- об'єми вихідного трафіку на фіксовані номери в інших країнах (включаючи часто використовувані номери);
- номерний діапазон оператора;
- середня кількість з'єднань за проміжок часу;
- середній об'єм трафіку за проміжок часу;
- середня тривалість з'єднань;
- кількість унікальних номерів;
- характерні напрямки.

Найбільш критичними для витоку мовної інформації є: порушення порядку маршрутизації міжміських та міжнародних викликів, виявлення активності абонентських номерів по вихідному місцевому трафіку, активності операторів по вхідному місцевому трафіку, схожу на роботу шлюзів для завершення вхідного міжміського та міжнародного трафіку, виявлення змін у активності абонентських номерів, які можуть бути свідченням стороннього підключення до абонентської лінії або дій абонента. Автоматизований аналіз даних про послуги повинен бути оперативним. Таким чином, на даному етапі є актуальним

ISSN 2663 - 4023

розробка методу, призначеного для здійснення аналізу трафіку та інформування про ситуації, що є підозрілими та потребують подальшого детального аналізу автоматизованими комплексами або відповідними спеціалістами.

Основними завданнями при розробці методу будуть:

1. Налагодження профілю елементів телекомунікаційної мережі зв'язку;
2. Забезпечення автоматичного аналізу, класифікації даних, пошуку відхилень параметрів телекомунікаційної мережі від параметрів звичайного профілю;
3. Створення алгоритму виявлення відхилень, який ґрунтується на особливостях порушень, що створюють динамічний у часі вплив на мережу, викликаючи аномальні явища;
4. Розробка графічного відображення змін кількісних характеристик за певний проміжок часу;
5. Оцінка відповідності параметрів аномалій (неіснуючий номер, велика тривалість виклику та ін.) до характерних для даного типу значень;
6. Оцінка аномалій на ступінь імовірності порушення для визначення пріоритету реагування;
7. Розробка інформування про виявленні відхилення та події;
8. Розробка зручного інтерфейсу оператора.

Блок схема виявлення, яке ґрунтується на особливостях порушень, можливо представити на рис.1.

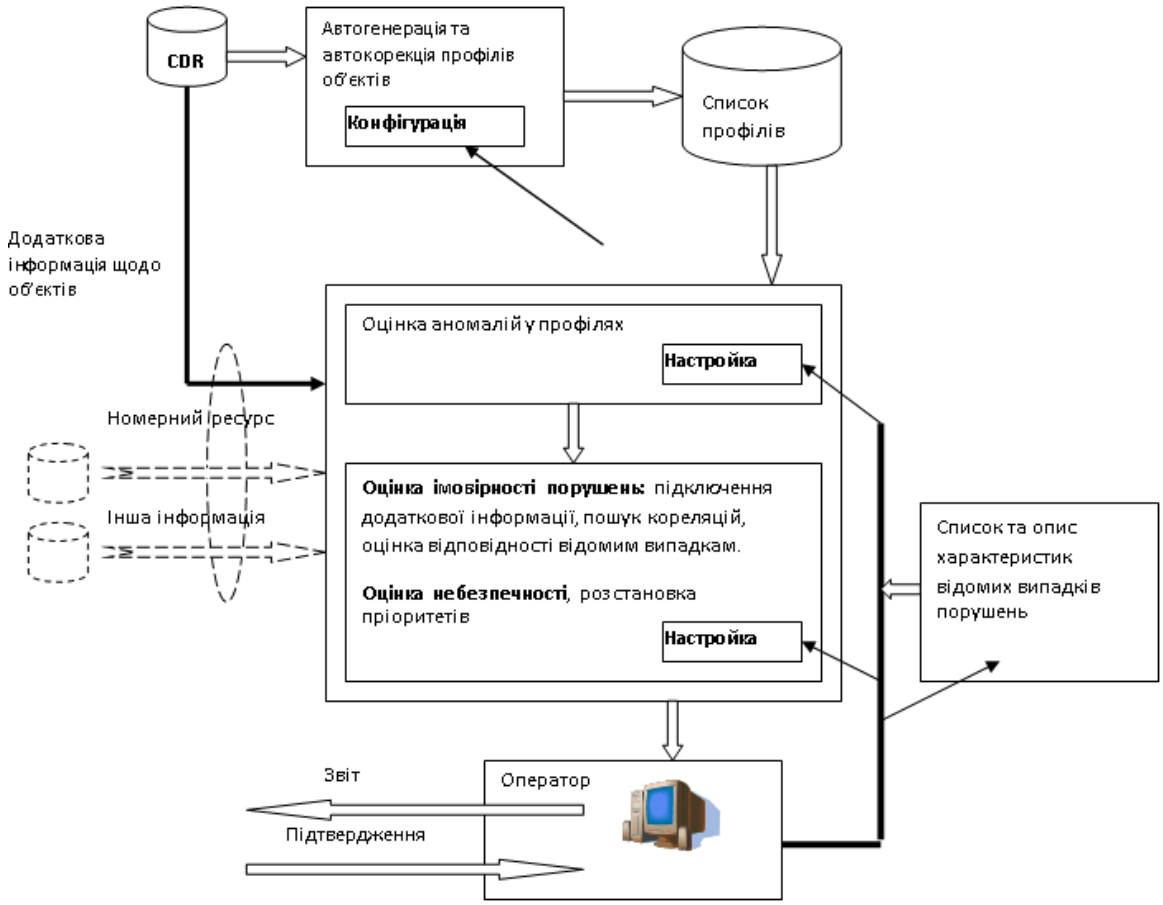

Рис.1. Блок схема виявлення оцінок аномалій профілів для виявлення порушень

Для оцінки кількісних характеристик об'єкта та динаміки змін у часі пропонується використовувати метод експонентних середніх значень з різними коефіцієнтами згладжування:

$$Q_t = (1-k)Q_{t-\Delta t} + kq_{\Delta t}, \quad (1)$$

де Q — експонентне середнє значення; q — новий вимір; k — коефіцієнт згладжування; Δt — інтервал між вимірами.

У формулі використовується постійний інтервал вимірів. Корекція профілю при кожному виклику складна, оскільки в цьому випадку коефіцієнт згладжування є складною експонентною функцією від інтервалу виміру. Однак особливості параметрів дозволяють використовувати більш прості формули.

Оптимальна кількість середніх значень і величин коефіцієнтів згладжування для кожного параметра можуть бути отримані дослідним шляхом. Для початку передбачається використовувати для кожного параметра три значення з коефіцієнтами k = 0.3; 0.05 і 0.005 з орієнтацією на добовий інтервал вимірів.

Для всіх використовуваних нижче параметрів і коефіцієнтів представлені значення, які можна використовувати при розробці, але при одержанні практичних результатів ці значення можуть бути змінені оператором. Крім того, використання деяких параметрів профілю й розрахунків аномальності може виявитися неможливим або недоцільним, а інші необхідно буде додати.

Трафік будемо оцінювати як середньодобову кількість секунд з'єднань:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \text{ якщо } \Delta t < 86400 \quad (2)$$

та

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{ якщо } \Delta t \geq 86400, \quad (3)$$

де T — тривалість з'єднань у секундах; Δt — час між закінченнями (початками) попереднього і нового виклику в секундах.

Для аналізу передбачаються такі типи трафіку:

- вихідний місцевий;
- вихідний міжміський;
- вихідний міжнародний;
- вхідний.

Інтенсивність потоку викликів пропонуємо оцінювати як середньодобова кількість спроб з'єднань:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \text{ якщо } \Delta t < 86400 \quad (4)$$

та

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{ якщо } \Delta t \geq 86400, \quad (5)$$

де T — тривалість з'єднань у секундах; Δt — час закінченнями (початками) попереднього й нового виклику в секундах.

Передбачається оцінка інтенсивності потоку викликів:

- вхідних;
- вихідних;
- ефективних.

Розподіл трафіку по типу часу оцінюється як середньодобова кількість секунд з'єднань для робочого часу:

- робочий час — 1й–5й день тижня з 8:30 до 17:30;
- неробочий час — 1й–5й день тижня з 0:00 до 8:30 і з 17:30 до 24:00;
- 6й–7й день тижня з 0:00 до 24:00.

Розподіл трафіку за часом доби будемо оцінювати як середньодобова кількість секунд з'єднань у денний період:

- денний час із 7:00 до 24:00;
- нічний час із 0:00 до 7:00.

Сигнальний трафік оцінюється як середня кількість байт сигнальної інформації на один виклик:

$$Q_t = (1-k)Q_{t-\Delta t} + kB, \tag{6}$$

де B — кількість байт сигнальної інформації у виклику.

Нестабільність стійких мережних параметрів об'єкта оцінюється по їхній зміні від виклику до виклику. Для всіх параметрів можливе використання однієї характеристики.

Для кожного виклику:

$$Q_t = LQ_{n-1} + \sum h_i, \tag{7}$$

де h_i — рівні інкременту для параметрів, значення яких відрізняються в попередніх і наступних викликах; L — коефіцієнт, що враховує застарілу інформацію L = 0,9.

Інші значення параметрів (якщо є в CDR):

- доступ (ISDN, non ISDN) h = 10;
- категорія абонента, що викликає h = 5;
- наявність або відсутність взаємодії сигналізації при встановленні з'єднання h = 8;
- неприпустима локалізація абонента, що викликає (відповідність адреси припустимому шаблону) h = 200;
- неприпустима категорія абонента, що викликає h = 100.

Необхідно передбачити можливість розширення й зміни подібних параметрів у майбутньому, а також використання різних характеристик для різних груп параметрів.

Додаткові коефіцієнти:

- $K2_{norm}$ постійний додатковий коефіцієнт, що дозволяє знижувати або підвищувати чутливість до аномалій при оцінці. Може змінюватися тільки оператором;
- $K2_t$ тимчасовий додатковий коефіцієнт, що дозволяє знижувати або підвищувати чутливість до аномалій при оцінці. Може змінюватися тільки оператором, але згодом автоматично прагнути до нормального значення.

Після кожного виклику тимчасовий додатковий коефіцієнт визначається:

$$K2_t = (1-k)K2_{t-\Delta t} + kK2_{norm}, \tag{8}$$

де Δt — час між закінченнями(початками) попереднього й наступного викликів у секундах; $K2_{norm}$ — нормальне значення; k — коефіцієнт згладжування, k = 0,05.

Нормальні значення для додаткових коефіцієнтів: $K1_{norm}$=100, $K2_{norm}$=100.

Оцінку аномального поводження об'єкта проведемо за таким методом:

Аномальність у поводженні об'єкта оцінюється по загальному рейтингу, як середнє визначеної аномалії з урахуванням додаткових коефіцієнтів.

ISSN 2663 - 4023

$$A_{pr} = \frac{(\sum A) * K1 * K2}{(\sum C) * K1_{norm} * K2_{norm}}. \quad (9)$$

де K1 — постійний додатковий коефіцієнт; K2 — тимчасовий додатковий коефіцієнт.

При створення об'єкта у поле T заноситься час початку спостереження, у поле K2 — знижене значення для стабілізації характеристик, в інші поля — значення, прийняті за умовчанням.

Для визначенні аномалій застосуємо такий спосіб:

При визначенні аномалій використовуються загальні для усіх об'єктів коефіцієнти та параметри:

C — ваговий коефіцієнт, враховує вплив кожної аномалії на загальний рейтинг;

m — параметр, що компенсує високу невизначеність у профілях об'єктів з низьким трафіком.

Трафік (A1, A2, A3, A4):

$$A(0.3) = C(0.3) * \frac{|Q(0.3) - Q(0.05)}{Q(0.05) + m}, A(0.05) = C(0.05)\frac{Q(0.05) - Q(0.005)}{Q(0.05) + m}. \quad (10)$$

Для визначення аномалій потрібно задати параметри трафіка, задаємо загальні для усіх об'єктів коефіцієнти та параметри табл.1 та табл. 2:

Таблиця 1

Задані вагові коефіцієнти визначення аномалій

$C_1(0.3)$	$C_1(0.05)$	$C_2(0.3)$	$C_2(0.05)$	$C_3(0.3)$	$C_3(0.05)$	$C_4(0.3)$	$C_4(0.05)$
1	**3**	**20**	**60**	**100**	**300**	**1**	**3**

Таблиця 2

Задані параметри визначення аномалій

m_1	m_2	m_3	m_4
200	**100**	**80**	**200**

Тривалість з'єднання будемо обчислювати, таким чином:

Вихідний трафік:

$$Q_{tout} = Q_1 + Q_2 + Q_3; m_{tout} = m_1 + m_2 + m_3 \quad (11)$$

Вихідні виклики:

$$A5(0.3) = C5(0.3) * \left[\left|\frac{(Q_{Tout}(0.3) + m_{Tout}) * (Q5(0.05) + m_5)}{(Q5(0.3) + m_5) * (Q_{Tout}(0.05) + m_{Tout})} - 1\right|\right], \quad (12)$$

$$A5(0.05) = C5(0.05) * \left[\left|\frac{(Q_{Tout}(0.05) + m_{Tout}) * (Q5(0.005) + m_5)}{(Q5(0.05) + m_5) * (Q_{Tout}(0.005) + m_{Tout})} - 1\right|\right]. \quad (13)$$

Вхідні виклики:

$$A6(0.3) = C6(0.3) * \left[\left|\frac{(Q4(0.3) + m_4) * (Q6(0.05) + m_6)}{(Q6(0.3) + m_6) * (Q4(0.05) + m_4)} - 1\right|\right], \quad (14)$$

ISSN 2663 - 4023

$$A6(0.05) = C6(0.05) * \left[\left| \frac{(Q4(0.05) + m_4) * (Q6(0.005) + m_6)}{(Q6(0.05) + m_6) * (Q_4(0.005) + m_4)} - 1 \right| \right]. \quad (15)$$

Для визначенні тривалості з'єднання потрібно задати параметри трафіка, за розробленою методикою загальні для усіх об'єктів коефіцієнти та параметри надані у табл. 3:

Таблиця 3

Задані параметри визначення тривалості з'єднання

$C_5(0.3)$	$C_5(0.05)$	$C_6(0.3)$	$C_6(0.05)$	$m_5(0.3)$	$m_6(0.05)$
3	**10**	**3**	**10**	**5**	**5**

За розробленою методикою ефективність будемо визначати:

Загальна кількість викликів: $Q_{Nall} = Q5 + Q6; m_{Nall} = m_5 + m_6$

$$A7(0.3) = C7(0.3) * \left[\left| \frac{Q7(0.3) + 0.45 * m_{Nall}}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} \right| \right], \quad (16)$$

$$A7(0.05) = C7(0.05) * \left[\left| \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q7(0.005) + 0.45 * m_{Nall}}{Q_{Nall}(0.005) + m_{Nall}} \right| \right]. \quad (17)$$

де C7(0.3) = 3 та C10(0.05) = 10

Розділ по типу часу будемо виконувати таким чином:

Загальний трафік: $Q_{Tall} = Q_{Tout} + Q4; m_{Tall} = m_{Tout} + m_4$.

$$A8(0.3) = C8(0.3) * \left[\left| \frac{Q_{Tall}(0.3) - k_1(d,h) * Q8(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right| \right], \quad (18)$$

де $k_1(d,h)$, $k_2(d)$ — коефіцієнти, які враховують помилку експонентного усереднення (d — день тижня, h — година).

Коефіцієнти, які враховують помилку експонентного усереднення наведені у табл. 4 та табл. 5.

Таблиця 4

Коефіцієнти помилки експонентного усереднення

d=1		d=2		d=3		d=4		d=5	
h	$k_1(d,h)$	**h**	$k_1(d,h)$	**h**	$k_1(d,h)$	**h**	$k_1(d,h)$	**h**	$k_1(d,h)$
0	1.470	0	1.151	0	0.992	0	0.900	0	0.842
1	1.489	1	1.165	1	1.004	1	0.911	1	0.853
2	1.507	2	1.180	2	1.017	2	0.923	2	0.863
3	1.527	3	1.195	3	1.030	3	0.934	3	0.874
4	1.546	4	1.210	4	1.043	4	0.946	4	0.885
5	1.565	5	1.226	5	1.056	5	0.958	5	0.897
6	1.585	6	1.241	6	1.069	6	0.970	6	0.908
7	1.605	7	1.257	7	1.083	7	0.982	7	0.919
8	1.626	8	1.273	8	1.097	8	0.995	8	0.931
9	1.529	9	1.216	9	1.056	9	0.962	9	0.903

Таблиця 5

Коефіцієнти помилки експонентного усереднення

d	1	2	3	4	5	6	7
k₂(d)	1.031	1.008	0.988	0.970	0.952	1.003	1.055

$$A8(0.05) = C8(0.05) * \left[\left| \frac{Q_{Tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{Tall}(0.05) + m_{Tall}} - \frac{Q_{Tall}(0.005) - Q8(0.005)}{Q_{Tall}(0.005) + m_{Tall}} \right| \right] \quad (19)$$

де C8(0.3) = 5 та C8(0.05) = 15.

Розподіл за часом доби ми обчислюємо за виразом:

$$A9(0.3) = C9(0.3) * \left[\left| \frac{Q_{Tall}(0.3) - k_3(h) * Q9(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right| \right], \quad (20)$$

$$A9(0.05) = C9(0.05) * \left[\left| \frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.005)}{Q_{Tall}(0.005) + m_{Tall}} \right| \right], \quad (21)$$

де $k_3(h)$ — коефіцієнт, що враховує помилку експонентного усереднення (h — година).

Таблиця 6

Коефіцієнт помилки експонентного усереднення

h	0	1	2	3	4	5	6	7
k₃(h)	0.9709	0.9832	0.9956	1.0082	1.0210	1.0339	1.0470	1.0408

h	8	9	10	11	12	13	14	15
k₃(h)	1.0347	1.0288	1.0230	1.0173	1.0118	1.0064	1.0012	0.9960

h	16	17	18	19	20	21	22	23
k₃(h)	09910	0.9861	0.9813	0.9766	0.9720	0.9675	0.9630	0.9587

Для розробленої методики C9(0.3) = 8; C9(0.05) = 24.

Сигнальний трафік ми будемо визначати за виразами:

$$A10(0.3) = C10(0.3) * \left[\left| \frac{Q10(0.3)}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} \right| \right], \quad (22)$$

$$A10(0.05) = C10(0.05) * \left[\left| \frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q10(0.005)}{Q_{Nall}(0.005) + m_{Nall}} \right| \right] \quad (23)$$

Коефіцієнт C10(0.3) = 20, коефіцієнт C10(0.05) = 60.

Стійкість параметра мережі, будемо визначати, за виразом

$$A_{11} = W \quad (24)$$

Подальшій обробці можуть піддаватися не всі об’єкти, а тільки об’єкти з найвищим загальним рейтингом аномальності. Достатньо обробляти близько 1% від загальної кількості.

Оцінка імовірності порушення, на відміну від існуючих методів , буде визначатися з урахуванням додаткових факторів. Крім високого рівня аномальності профілю об'єкта додатковими факторами, що підвищують можливість виявлення шахрайства при оцінці, є:

- кореляція подій аномальних об'єктів — збіг унікальних адрес у записах викликів об'єктів за останній час (2–3 доби);
- відповідність профілю об'єкта відомого випадку порушення, збіг специфічної для цього відомого випадку інформації про виклик (напрямок, адресація) за останній час;
- невідповідність профілю об'єкта типовому профілю абонентського обліку. (Можливо тільки при наявності доступу до бази абонентського обліку, не обов'язково на перших етапах розробки, однак необхідно передбачити таку можливість у майбутньому).

Визначення ймовірності порушення

$$P = MAX\left(\frac{A}{A+a} MAX\left(P_{known}\right) P_{subbase}\right), \tag{25}$$

де $\frac{A}{A+a}$ — імовірність порушення, певна по аномальності поводження; a — аномальність при 50% імовірності. Значення ***a*** може бути отримано дослідним шляхом.

Спочатку можна використовувати: a = 20;

$$A = A_{pr} + \sum A_{cor.pr.}, \tag{26}$$

де $A_{cor.pr}$ — аномальність об'єкта, у якого спостерігається кореляція у викликах (при перевірці необхідно виключати збіг по популярних адресах: спецслужби, серійні модемні пули і т.д.), якщо кореляція не визначена — $A_{cor.pr} = 0$;

$P_{subbase}$ — імовірність шахрайства, що оцінена по невідповідності профілю об'єкта типовому профілю у відповідності до абонентського обліку.

P_{known} — імовірність відомого типу порушення (визначається для кожного відомого типу). Методика визначення ймовірності відомого типу порушення може бути також побудована на відповідності характерних аномалій у профілі спостережуваного об'єкта і профілю об'єкта, що порушує на момент виявлення, а також кореляції у викликах по адресах або префіксах. Більш точно методику можна визначити тільки після накопичення достатньої кількості дослідних результатів.

Оцінка ступеня небезпеки шахрайства за розробленою методикою буде розраховуватися наступним чином.

Оцінка ступеня небезпеки необхідна для випадків, які вимагають першочергового втручання. Їх можна розглянути як дію імовірності порушення на збиток або недоотриманий дохід:

$$\Delta Q(0.3) = | Q(0.3) - Q(0.05) |, \tag{27}$$

$$\Delta Q(0.05) = | Q(0.05) - Q(0.005) |. \tag{28}$$

$$D = P * \begin{pmatrix} \Delta Q1(0.3) + k_2 * \Delta Q2(0.3) + k_3 * \Delta Q3(0.3) + L * (\Delta Q1(0.05) + \\ + k_2 * \Delta Q2(0.05) + k_3 * \Delta Q3(0.05)) \end{pmatrix}, \tag{29}$$

де k_2, k_3 — коефіцієнти, що враховують середню різницю в тарифах.

Вони будуть приймати значення k_2 = 15, k_3 = 250, L = 3.

РЕКОМЕНДАЦІЇ ЩО ДО ПРАКТИЧНОГО ЗАСТОСУВАННЯ РОЗРОБЛЕНОЇ МЕТОДИКИ

Особливістю функціонування та відзнакою розробленої методики буде наступне:

1. Особливість при створення профілів об'єктів:
   - Для кожної групи з'єднувальних ліній і для кожного напрямку заняття каналу, описується перелік припустимих адрес вихідної сторони, перелік неконтрольованих адрес вихідної сторони, списки об'єктів, які мають більше ніж одну адресу у відповідному списку адрес;
   - Якщо при обробці виклику запис інформації про профіль об'єкта не знайдено, він повинен бути генерований автоматично.
2. Специфічне формування профілю:

Якщо відбулася втрата в Системі інформації про виклики за будь-який період, для запобігання збоїв у формуванні інформації про профілі об'єктів, необхідно перевірити ще раз всі об'єкти, використовуючи нульові значення трафіку на початок періоду й відновити інформацію в профілях на момент закінчення.

З метою зручності використання, інтерфейси користувача і методи роботи з ними мають бути ідентичними як для Системи в цілому. Але додатково потрібно враховувати наступне:

1. Підсистема повинна містити засоби активного інформування користувачів про події, що потребують уваги, за допомогою формування екранних повідомлень в клієнтській частині системи, у тому числі при старті клієнтської частини, якщо подія трапилась і не була висвітлена раніше.
2. Передбачити можливість графічного відображення характеристик профілю об'єктів.
3. Передбачити можливість організації додаткових перевірок, з легкою зміною правил, які використовуються при аналізі за допомогою редактору правил.

ВИСНОВКИ

Проведене дослідження довело відсутність науково методичного апарату, універсальних пристроїв або автоматизованих програмних комплексів для забезпечення оперативного здійснення аналізу трафіку з метою виявлення витоку мовної інформації та передачі інформації відповідним спеціалістам. У зв'язку з чим у роботі розроблено метод виявлення витоку інформації за відхиленням трафіку з інформаційної мережі зв'язку. Розроблений метод забезпечує оперативне здійснення аналізу трафіку та інформування про ситуації, що є підозрілими та потребують подальшого детального аналізу відповідними спеціалістами.

Розроблений метод дозволяє здійснювати у реальному часі інформування відповідальних спеціалістів, про відхилення характеру трафіку з елементів мережі. Відхилення характеру трафіку з елементів параметрів мережі вимірюються від звичного трафіку інформаційної мережі відносно саме цих параметрів.

Наведена методика враховує практичні рекомендації, що до сталих коефіцієнтів, розрахунків. Ці коефіцієнти у досліджені обрані розрахунковим та емпіричним шляхом. Запропоновані сталі коефіцієнти та використання розробленої методиці підвищує ефективність виявлення відхилення інформаційного трафіку на 9% у порівнянні з існуючими методиками. Що доводить адекватність наукового дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Atassi, A., & Khalil, H. (1999). A separation princi ple for the stabilization of class of nonlinear systems. *IEEE Trans. Automat. Control. 44(9),* 1672–1687.
2. Tao, G., & Ioannou, P. (1993). Model reference adaptive control for plants with unknown relative degree. *IEEE Trans. Automat. Control. 38(6),* 976–982.
3. Лаптєв, О. (2019). Порівняний аналіз методів розпізнавання сигналів радіозакладних пристроїв на основі частотних перетворень. *Телекомунікаційні та інформаційні технології, 3,* 71–83.
4. Лаптєв, О., Савченко, В., Савченко, В., Мацько, О., Кізяк, Я., & Лазаренко, С. (2019). Мультиагентна технологія пошуку цифрових радіозакладних пристроїв на основі кластеризації за методом бджолиної колонії. *Журнал Захист інформації, 21(3),* 194–202.
5. Laptev, A., et al. (2019). The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. *International Journal of Advanced Research in Science, Engineering and Technology, 6(7),* 10101–10105.
6. Лаптєв, О., Собчук, В., Саланди, И., & Сачук, Ю. (2019). Математична модель структури інформаційної сеті на основі нестаціонарної ієрархічної та стаціонарної гиперсети. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, 64,* 124–132.
7. Kapustian, O., et al. (2022). Approximate Optimal Control for a Parabolic System with Perturbations in the Coefficients on the Half-Axis. *Axioms, 11(4), 175.* https://doi.org/10.3390/axioms11040175
8. Korchenko, A.O., et al. (2021). Development of a method for construction of linguistic standards for multicriterial evaluation of honeypot efficiency. *Eastern-European journal of enterprise technologies, 1(2) (109),* 14–23. https://doi.org/10.15587/1729-4061.2021.225346
9. Svynchuk, O. Et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2),* 1–14. https://doi.org/10.3390/fractalfract5020031
10. Laptiev, O., et al. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1),* 48–54.
11. Laptiev, O., et al. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1),* 15–21.
12. Laptiev, O., et al. (2021). Improved model of estimating economic expenditures on the information protection system in social networks. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(12),* 19–28. https://doi.org/10.28925/2663-4023.2021.12.1928
13. Laptiev, O., et al. (2022). Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1).* https://doi.org/10.17762/ijcnis.v13i1.4902
14. Barabash, O., et al. (2021). Comprehensive Methods of Evaluation of Distance Learning System Functioning. *International Journal of Computer Network and Information Security (IJCNIS), 13(3),* 62–71. https://doi.org/10.5815/ijcnis.2021.03.06
15. Laptiev, O., et al. (2022). The method of spectral analysis of the determination of random digital signals. *International Journal of Communication Networks and Information Security (IJCNIS), 13(2).* https://doi.org/10.17762/ijcnis.v13i2.5008
16. Laptieva, T. (2021). Algorithm for determining the measure of existence of unreliable information in the conditions of information conflict. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(14),* 15–25. https://doi.org/10.28925/2663-4023.2021.14.1525
17. Nakonechnyi, V., et al. (2022). Improving the method of detecting and clustering sources of false information. *Scientific technologies, 54(4),* 105–111. https://doi.org/10.18372/2310-5461.54.16747
18. Laptieva, T., Lukova-Chuiko, N. (2022). Improvement of the method of detection of false information based on the method of expert evaluation "Delphi". *Scientific technologies, 55(3),* 193–199. https://doi.org/10.18372/2310-5461.55.16901
19. Zamrii, I., et al. (2022). Algorithm of control and prediction of functional stability of complex information and technical systems. *Telecommunications and information technologies, 1(74),* 4–15.
20. Laptiev, S. (2022). An improved method of protecting personal data from attacks using social engineering algorithms. *Electronic specialized scientific publication "Cybersecurity: education, science, technology", 4(16),* 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

21. Laptiev, S., & Tolupa, S. (2022). The methodology for evaluating the functional stability of the protection system of special networks. *Information technologies, cyber security, 55(3),* 178–183. https://doi.org/10.18372/2310-5461.55.16900
22. Korolkov, R., & Laptiev, S. (2022). Realistic simulation of a “war driving” attack on a wireless network. *Electronic specialized scientific publication “Cybersecurity: education, science, technology”, 2(18),* 99–107. https://doi.org/10.28925/2663-4023.2022.18.99107

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Sergey Gluhov
Doctor of Technical Science, professor
Head of the Department of Military and Technical Training
of the Faculty of Postgraduate Education of the Military Institute,
Taras Shevchenko National University of Kyiv
ORCID 0000-0002-4918-3739
gluhov1971@ukr.net

Andrii Sobchuk
PhD
Associate Professor of the Department of Information and Cyber Security
Educational and Scientific Institute of Information Protection
State University of Information and Communication Technologies
ORCID 0000-0003-3250-3799
anri.sobchuk@gmail.com

Volodymyr Rovda
PhD student
State University of Information and Communication Technologies
ORCID 0009-0001-9987-6787
volodymyr.rovda@gmail.com

Mykola Polovinkin
PhD student
State University of Information and Communication Technologies
ORCID 0009-0009-5242-567X
navarrokain@gmail.com

Vitaly Ponomarenko
PhD student of the educational and scientific institute of information protection,
State University of Information and Communication Technologies
ORCID 0000-0002-6567-4247
Ur_suviator@ukr.net

METHOD OF DETECTION OF INFORMATION LEAKAGE BY REJECTING TRAFFIC FROM THE INFORMATION COMMUNICATION NETWORK

Abstract. In the work, an analysis of the methods of detecting the leakage of language information was carried out. The analysis showed the absence of a single scientific methodical apparatus or automated software complexes to ensure the operational implementation of traffic analysis. Therefore, the work is devoted to the topical topic of information leakage detection based on the deviation of traffic from the information communication network. An improved method of providing operational traffic analysis and informing about a suspicious situation is proposed. A situation that requires further detailed traffic analysis by automated software complexes or relevant specialists. The developed method allows informing, in real time, the responsible specialists about a possible leak of information, which is based on the analysis of the deviation of the nature of the traffic from the elements of the information speech network. Deviations, the nature of the traffic from the elements of the network parameters are measured relative to the usual traffic of the telephone or voice network relative to these parameters. A comparative analysis of normal traffic with real-time traffic is carried out. This method further improves the methodology. The improvement was carried out due to the use of practical recommendations regarding constant coefficients, calculations. These coefficients for the improved method were chosen by calculation and empirically, which allows to significantly reduce the response of the traffic estimation system, a system that uses the developed methodology to detect possible leakage of language information.

Keywords: traffic deviation; method; model; forecasting; information technology; resilience; delay; privacy; availability; false information; personal data..

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Atassi, A., & Khalil, H. (1999). A separation princi ple for the stabilization of class of nonlinear systems. *IEEE Trans. Automat. Control. 44(9),* 1672–1687.
2. Tao, G., & Ioannou, P. (1993). Model reference adaptive control for plants with unknown relative degree. *IEEE Trans. Automat. Control. 38(6),* 976–982.
3. Laptev, O. (2019). Comparative analysis of methods of recognition of signals of radio equipment based on frequency transformations. *Telecommunications and information technologies: a scientific journal, 3,* 71–83.
4. Laptev, O., et al. (2019). Multi-agent technology for finding digital radio beacons based on bee colony clustering. *Journal of Information Protection, 21(3),* 194–202.
5. Laptev, A., et al. (2019). The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. *International Journal of Advanced Research in Science, Engineering and Technology, 6(7),* 10101–10105.
6. Laptiev, O., et al. (2019). Mathematical model of the information network structure based on non-stationary hierarchical and stationary hypernet. *Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University, 64,* 124–132.
7. Kapustian, O., et al. (2022). Approximate Optimal Control for a Parabolic System with Perturbations in the Coefficients on the Half-Axis. *Axioms, 11(4), 175.* https://doi.org/10.3390/axioms11040175
8. Korchenko, A.O., et al. (2021). Development of a method for construction of linguistic standards for multicriterial evaluation of honeypot efficiency. *Eastern-European journal of enterprise technologies, 1(2) (109),* 14–23. https://doi.org/10.15587/1729-4061.2021.225346
9. Svynchuk, O. Et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2),* 1–14. https://doi.org/10.3390/fractalfract5020031
10. Laptiev, O., et al. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1),* 48–54.
11. Laptiev, O., et al. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1),* 15–21.
12. Laptiev, O., et al. (2021). Improved model of estimating economic expenditures on the information protection system in social networks. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 4(12),* 19–28. https://doi.org/10.28925/2663-4023.2021.12.1928
13. Laptiev, O., et al. (2022). Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. *International Journal of Communication Networks and Information Security (IJCNIS), 13(1).* https://doi.org/10.17762/ijcnis.v13i1.4902
14. Barabash, O., et al. (2021). Comprehensive Methods of Evaluation of Distance Learning System Functioning. *International Journal of Computer Network and Information Security (IJCNIS), 13(3),* 62–71. https://doi.org/10.5815/ijcnis.2021.03.06
15. Laptiev, O., et al. (2022). The method of spectral analysis of the determination of random digital signals. *International Journal of Communication Networks and Information Security (IJCNIS), 13(2).* https://doi.org/10.17762/ijcnis.v13i2.5008
16. Laptieva, T. (2021). Algorithm for determining the measure of existence of unreliable information in the conditions of information conflict. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", 2(14),* 15–25. https://doi.org/10.28925/2663-4023.2021.14.1525
17. Nakonechnyi, V., et al. (2022). Improving the method of detecting and clustering sources of false information. *Scientific technologies, 54(4),* 105–111. https://doi.org/10.18372/2310-5461.54.16747
18. Laptieva, T., Lukova-Chuiko, N. (2022). Improvement of the method of detection of false information based on the method of expert evaluation "Delphi". *Scientific technologies, 55(3),* 193–199. https://doi.org/10.18372/2310-5461.55.16901
19. Zamrii, I., et al. (2022). Algorithm of control and prediction of functional stability of complex information and technical systems. *Telecommunications and information technologies, 1(74),* 4–15.
20. Laptiev, S. (2022). An improved method of protecting personal data from attacks using social engineering algorithms. *Electronic specialized scientific publication "Cybersecurity: education, science, technology", 4(16),* 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

21. Laptiev, S., & Tolupa, S. (2022). The methodology for evaluating the functional stability of the protection system of special networks. *Information technologies, cyber security, 55(3),* 178–183. https://doi.org/10.18372/2310-5461.55.16900
22. Korolkov, R., & Laptiev, S. (2022). Realistic simulation of a "war driving" attack on a wireless network. *Electronic specialized scientific publication "Cybersecurity: education, science, technology", 2(18),* 99–107. https://doi.org/10.28925/2663-4023.2022.18.99107