DOI: 10.18372/2225-5036.30.18608

ТЕСТОВА КОНФІГУРАЦІЯ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ДЛЯ ВІДПРАЦЮВАННЯ НАВИЧОК ІЗ ПОШУКУ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Михайло Шелест, Тарас Петренко
Сергій Семендяй, Владислав Нороха

Національний університет «Чернігівська політехніка»

ШЕЛЕСТ Михайло Євгенович, д.т.н., професор
Рік та місце народження: 1954 рік, м. Ромни, Україна.
Освіта: Національний університет «Львівська політехніка».
Посада: професор кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: інформаційна безпека, оцінювання вразливосте, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографія, підручники, навчально-методичні посібники та деклараційні патенти.
E-mail: michel3141@gmail.com.
Orcid ID: 0000-0001-7110-4876.

ПЕТРЕНКО Тарас Анатолійович, к.т.н.
Рік та місце народження: 1983, с. Пороги, Україна.
Освіта: Чернігівський державний технологічний університет (зараз НУ "Чернігівська політехніка").
Посада: доцент кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: інформаційна безпека, адміністрування операційних систем, архітектура комп'ютерних систем, інтелектуальні системи в кібербезпеці.
Публікації: понад 30 наукових, навчальних та методичних робіт.
E-mail: 4650364@gmail.com.
Orcid ID: 0000-0001-5571-3815.

СЕМЕНДЯЙ Сергій Матвійович, старший викладач
Рік та місце народження: 1972 рік, Чернігівська обл., Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут».
Посада: ст. викладач кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: захист інформації, електроніка, радіотехніка.
Публікації: наукові статті, навчальний посібник, тези та матеріали доповідей на конференціях.
E-mail: serhii_semendiai@icloud.com.
Orcid ID: 0000-0002-7751-5956.

НОРОХА Владислав Олександрович, студент
Рік та місце народження: 2001 рік, м. Чернігів, Україна.
Освіта: Національний університет «Чернігівська політехніка», 2022 рік.
Посада: студент кафедри кібербезпеки та математичного моделювання
Наукові інтереси: захист інформації, комп'ютерні науки, технологія OSINT.
Публікації: тези та матеріали доповідей на конференціях.
E-mail: vnoroha@gmail.com.
Orcid ID: 0009-0005-1140-3061.

Анотація. *Тема дослідження визначається надзвичайною актуальністю у зв'язку зі швидким розвитком цифрових технологій та збільшенням загроз для конфіденційності даних. Зростаюча кількість кіберзлочинів і поширення великих обсягів інформації підкреслюють необхідність навчання майбутніх фахівців із кібербезпеки навичкам виявлення технічних каналів витоку інформації (ТКВІ). У контексті динамічного кіберпростору, де зловмисники постійно вдосконалюють технічні методи атак, постановка проблеми полягає в необхідності готовності майбутніх фахівців до виявлення та ефективної протидії ТКВІ. Їхні навички стають*

ключовими для збереження конфіденційності, цілісності та доступності інформації в цифровому середовищі. Аналіз останніх досліджень вказує на важливість розгляду пристроїв пошуку каналів витоку інформації та комплексів технічного захисту інформації. Навчальний посібник [12] розглядає загальні положення щодо створення таких комплексів. Необхідність створення спеціалізованих лабораторій для відпрацювання навичок у сфері ТКВІ залишається недослідженою частиною загальної проблеми.

***Ключові слова**: витік інформації, закладні пристрої, засоби виявлення ТКВІ, ОІД.*

Постановка проблеми

В сучасному цифровому світі актуальність дослідження та навчання майбутніх фахівців із кібербезпеки в області пошуку технічних каналів витоку інформації (ТКВІ) беззаперечно зростає. Швидкий розвиток цифрових технологій та загрози для конфіденційності даних створюють необхідність у глибокому розумінні технічних аспектів витоку інформації та ефективному виявленні та захисті цільових об'єктів від кібератак.

У контексті динамічного кіберпростору, де зловмисники неперервно вдосконалюють технічні методи атак, важливість навичок майбутніх фахівців полягає в їхній готовності до виявлення та ефективної протидії технічним каналам витоку інформації. Ці навички та знання стають ключовими для забезпечення конфіденційності, цілісності та доступності інформації в умовах сучасного цифрового середовища.

Постановка проблеми вказує на необхідність розвитку методів виявлення та протидії технічним каналам витоку інформації в умовах постійних кіберзагроз. Відзначається, що навички, які формуються в процесі навчання майбутніх фахівців у лабораторіях кібербезпеки, можуть стати дієвим підґрунтям для їхньої успішної професійної діяльності.

Аналіз останніх досліджень та публікацій

Аналіз останніх досліджень та публікацій доводить значущість вивчення пристроїв пошуку каналів витоку інформації та створення комплексів технічного захисту інформації. Однак, не дивлячись на широке покриття теоретичних матеріалів, деякі аспекти, зокрема, створення спеціалізованих лабораторій для практичного відпрацювання навичок, залишаються недослідженими.

Мета та постановка завдання

Мета статті полягає в розробці та відтворенні тестової конфігурації об'єкта інформаційної діяльності в лабораторії кібербезпеки. Це спрямовано на вдосконалення навичок майбутніх фахівців із пошуку технічних каналів витоку інформації та підготовку їх до викликів сучасного кіберпростору.

Виклад основного матеріалу дослідження

До початку роботи з обладнанням, слід ознайомитись з базовою літературою про канали витоку інформації [10-12], та обладнання, що використовуються під час обстеження ОІД [1-9]. Методика, що використовується для виявлення каналів витоку інформації, складається із кількох етапів.

Етап перший – це візуальний огляд приміщення. Під час такого огляду можуть бути виявленні закладні пристрої різних цільових застосувань.

Другий етап – обстеження кімнати на наявність прихованих камер за допомогою детектора прихованих камер, які не були виявлені під час візуального огляду, або вмонтовані в декор чи меблі.

Третій етап – обстеження приміщення за допомогою детектора цифрових сигналів на наявність передавальних пристроїв через Bluetooth-канал, які не були виявленні під час візуального огляду приміщення.

Четвертий етап – це обстеження приміщення за допомогою пошукового комплексу на наявність несанкціонованих точок доступу Wi-Fi, які не були виявленні під час візуального огляду приміщення.

П'ятим етапом є обстеження приміщення на наявність GPS-трекерів, які не були виявленні під час візуального огляду приміщення.

Шостий етап – це обстеження кімнати за допомогою локатора нелінійних переходів, на наявність закладних пристроїв, що містять напівпровідникові компоненти.

Сьомий етап – створення звіту про обстеження та утилізація знайденого обладнання.

Тестування методу виявлення каналів витоку інформації

Було розроблено метод виявлення технічних каналів витоку інформації із застосуванням конкретного обладнання, такого як багатофункціональний пошуковий прилад ANDRE, детектор цифрових радіокомунікацій PROTECT 1207i, детектор прихованих камер WEGA-i та локатор нелінійних переходів.

Дане обладнання дозволяє виявляти закладні пристрої, що створюють технічні канали витоку інформації, такі як приховані камери, Wi-Fi та Bluetooth-жучки тощо.

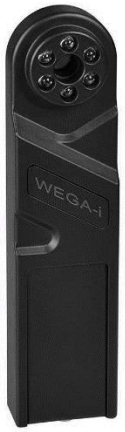

Рис. 1. Пристрій WEGA-i

В якості тестового середовища було обрано приміщення лабораторії кібербезпеки, через зручність проводити там експерименти з виявлення ТКВІ та знаходження закладних пристроїв, що працюють через мережі мобільного зв'язку, Wi-Fi-мережі, Bluetooth-з'єднання – це приховані камери, радіомікрофони, GPS-трекери.

Нульовим етапом буде вимкнення всіх доступних радіопередавальних пристроїв, щоб знизити рівень сторонніх завад.

Спочатку будемо шукати приховані камери. Такі пристрої можуть бути непомітними при зовнішньому огляді приміщення, тому для пошуку ми використаємо детектор прихованих камер WEGA-і (рис. 1). Слід зазначити, що приховані камери можуть бути вмонтовані в меблі, вентиляцію, та інші непримітні місця. Також важливою складовою під час пошуку є розуміння, яка саме інформація потрібна зловмисникам. Слід ретельно оглянути місця, де підписуються документи, проводяться конференції тощо.

Для контрольного тестування використовуватимемо камери відеоспостереження в лабораторії та встановимо додатково кілька смартфонів з включеною відеозйомкою. За допомогою WEGA-і шукаємо «приховані камери» (рис. 2).

Рис. 2. Застосування WEGA-і

Наступним етапом обстеження буде перевірка на наявність Bluetooth-з'єднань та передачі координат через GPS. Для цієї задачі використаємо детектор цифрових радіокомунікацій PROTECT 1207i (рис. 3). Попередньо потрібно вимкнути всі зайві джерела радіовипромінювань.

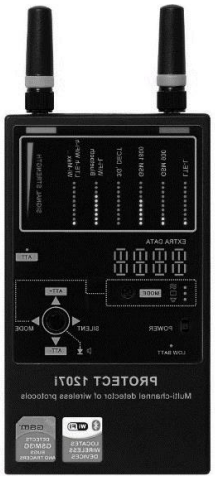

Рис. 3. Детектор бездротових протоколів PROTECT 1207i

Для контрольного тестування приладу розмістимо телефони з увімкненим GPS та встановленим Bluetooth-з'єднаннями до навушників, що знаходяться поза межами нашого ІОД (рис. 4). Також для перевірки використаємо передачу геоданих через Telegram, а це передача за стандартом LTE. Таким чином під час обстеження лабораторії виявимо два пристрої з включеним Bluetooth-з'єднанням (рис. 5).

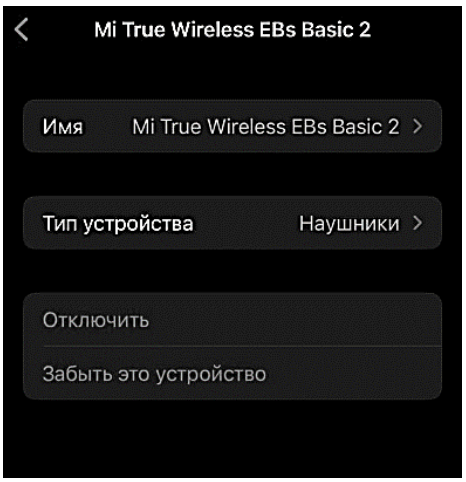

Рис. 4. Налаштування закладного пристрою

Рис. 5. Застосування PROTECT 1207i

Наступним етапом буде обстеження на наявність закладних пристроїв, що працюють через Wi-Fi мережі. Для цього буде використовуватись багатофункціональний пошуковий прилад ANDRE (рис. 6).

Рис. 6. Прилад ANDRE

Для контрольного тестування декілька телефонів будуть підключені до окремої Wi-Fi мережі лабораторії (MicroTik-KBMM-UP) та сховані в приміщенні лабораторії (рис.7). У якості іншого закладного пристрою, імітуючого приховані радіомікрофони, використовуватиметься хакерська радіостанція HackRF One, налаштована да довільну частоту передачі. За допомогою приладу ANDRE буде обстежено приміщення та знайдено всі «закладні пристрої» (рис. 8).

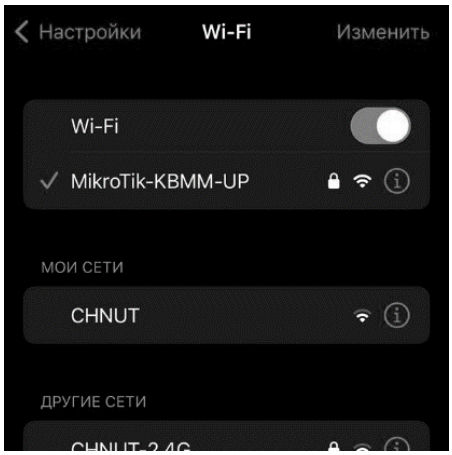

Рис. 7. Налаштування закладного пристрою

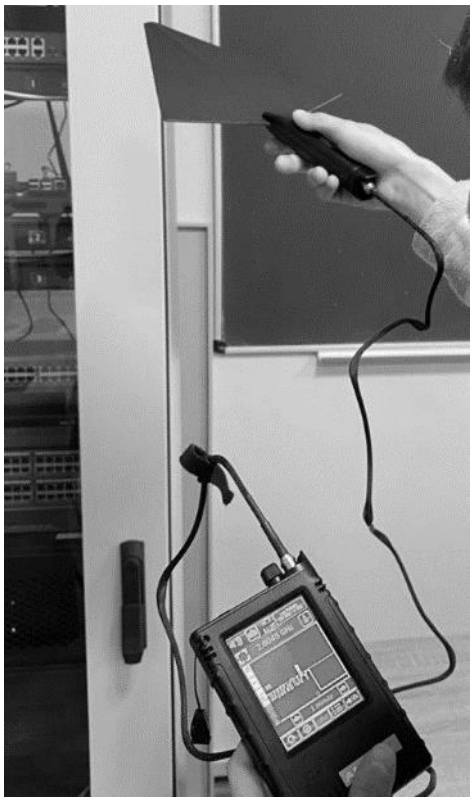

Рис. 8. Застосування багатофункціонального пошукового приладу ANDRE

Наступним етапом є обстеження приміщення за допомогою локатора нелінійних переходів (рис. 9). Для обстеження нашого ОІД на предмет невиявлених закладних пристроїв, проходимо по всій площі поверхонь приміщення зигзагом, або спіраллю. У якості закладного пристрою виступає мобільний телефон, попередньо прихований нами у приміщенні. Пам'ятаємо, що прилад також може реагувати і на оксиди металів – це буть хибні спрацювання на які не слід звертати увагу. Під час обстеження кімнати нелінійний локатор упевнено спрацював на прихований мобільний телефон і таким чином його було виявлено.

Рис. 9. Локатор нелінійних переходів

Підсумком проведеного експерименту є повне обстеження імітаційного ОІД (лабораторії кібербезпеки) та успішне виявлення всіх закладних пристроїв, які створювали загрозу витоку інформації. Відповідно до вимог НД ТЗІ 2.7-011-2012 складаємо учбовий «Акт за результатами проведення робіт з виявлення закладних пристроїв» (рис. 10) [11].

АКТ
за результатами проведення робіт з виявлення закладних пристроїв

на Лабораторія кафедри КБММ, ЧНТУ, м. Чернігів, вулиця Шевченка, 95, 1 корпус, 110 кабінет
(назва ОІД, де проводились роботи, назва організації-замовника, до якої належить ОІД, адреса організації-замовника)

Рис. 10. Приклад заповнення Акту

Також в акті прописуються наступні пункти:

– характеристика приміщення: це опис приміщення, включаючи його призначення, розташування на поверсі, розміщення вікон і дверей, інформація про суміжні приміщення тощо;

– мета і основні завдання робіт із виявлення закладних пристроїв на об'єкті інформаційної діяльності;

– спосіб проведення робіт із виявлення закладних пристроїв (вказується, чи робота була відкритою чи прихованою);

– склад пошукової групи: інформація про осіб, які брали участь у проведенні робіт;

– технічні засоби, прилади та обладнання, включаючи пошукову апаратуру, що використовувалися під час робіт з виявлення закладних пристроїв, із зазначенням заводських номерів;

– перелік тестових сигналів активації закладних пристроїв, які застосовувалися під час робіт;

– перелік проведених робіт із виявлення закладних пристроїв на об'єкті і їх результати;

– перелік предметів, на які були нанесені спеціальні захисні знаки, інформація щодо цих знаків. Якщо цих предметів багато, перелік можна додати до Акта у вигляді окремого додатка;

– загальний висновок щодо результатів робіт із виявлення закладних пристроїв на об'єкті інформаційної діяльності. Якщо були виявлені закладні пристрої, надається детальна інформація щодо їх місцезнаходження, функціонального призначення, технічних характеристик, ознак демаскування та способів їх виявлення;

– заходи, які були вжиті відносно виявлених закладних пристроїв, включаючи інформацію про час і спосіб повідомлення Служби безпеки України про їх виявлення, нейтралізацію можливих шляхів витоку інформації і подання інформації до Адміністрації Держспецзв'язку [11].

Дана тестова конфігурація об’єкта інформаційної діяльності дає можливість ознайомитись із роботою засобів виявлення технічних каналів витоку інформації, відпрацювати навички із пошуку закладних пристроїв та оформлення документації за результатами обстежень.

Висновки. Загальний аналіз сучасного цифрового оточення підкреслює зростаючу актуальність вивчення та підготовки майбутніх фахівців із кібербезпеки до пошуку технічних каналів витоку інформації (ТКВІ). Швидкий розвиток цифрових технологій та поширення кіберзагроз визначають необхідність у глибокому розумінні технічних аспектів витоку інформації для забезпечення конфіденційності, цілісності та доступності інформації.

Постановка проблеми вказує на важливість розвитку навичок, які дозволять майбутнім фахівцям ефективно виявляти та протидіяти технічним каналам витоку інформації. Навчання у лабораторіях кібербезпеки стає ключовим елементом формування цих навичок та знань, що може забезпечити їхню успішну професійну кар'єру. Аналіз останніх досліджень підкреслює важливість вивчення пристроїв пошуку каналів витоку інформації та розробки комплексів технічного захисту. Водночас, наголошується на необхідності дослідження аспектів, пов'язаних із створенням спеціалізованих лабораторій для практичного відпрацювання отриманих навичок, які залишаються поки що недослідженими. Зазначена мета статті, а саме розробка тестової конфігурації об’єкта інформаційної діяльності в лабораторії кібербезпеки, свідчить про прагматичний підхід до вирішення визначених завдань та підготовки майбутніх фахівців до викликів сучасного кіберпростору. Результати досліджень можуть сприяти ефективній інтеграції отриманих знань у професійну практику та вдосконаленню стратегій захисту від кібератак.

Список літератури

[1]. Детектор прихованих камер [Електронний ресурс] / Режим доступу до ресурсу: https://www.das-ua.com / katalog / obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii / detector-skrytyx-kamer-wegai/.

[2]. Детектор цифрових радіокомунікацій PROTECT 1207i [Електронний ресурс] / Режим доступу до ресурсу: https://www.das-ua.com/katalog/obladnannya - dlya - viyavlennya - kanaliv-vitoku-informacii / detektor - cifrovyx-radiokommunikacij-protect-1207i/.

[3]. Багатофункціональний пошуковий прилад Andre [Електронний ресурс] / Режим доступу до ресурсу: https: // www.das-ua.com / katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/mnogofunkcionalnyj-poiskovyj-pribor-andre/.

[4]. Захист провідних комунікацій та мереж мобільного зв’язку [Електронний ресурс] / Режим доступу до ресурсу: https://kvirin.com/tech_info_protect/2/protection/496/.

[5]. Технічні канали витоку інформації [Електронний ресурс] / Режим доступу до ресурсу: https://studfile.net/preview/5652242/.

[6]. Тепловізори [Електронний ресурс] / Режим доступу до ресурсу: https://yug.com.ua/uk/apparatnie-uctroictva/teplovizoryi/.

[7]. Тепловізори [Електронний ресурс] / Режим доступу до ресурсу: https://hunterstore.com.ua/ua/g4175418-teplovizory.

[8]. Детектор жучків iProtech Protect 1207i [Електронний ресурс] / Режим доступу до ресурсу: https://ibughunter.com.ua/protect-1207-ru/.

[9]. Детектори прихованих пристроїв [Електронний ресурс] / Режим доступу до ресурсу: https://glushilki.in.ua/product-category/detektor_zhuchkov/.

[10]. Захист від вібро-акустичних каналів витоку інформації [Електронний ресурс] / Режим доступу до ресурсу: https://glushilki.in.ua/product-category/zashhita_peregovorov/.

[11]. НД ТЗІ 2.7-011-2012 [Електронний ресурс]/ Режим доступу до ресурсу: https://tzi.com.ua/ downloads/2.7-011-2012.pdf.

[12]. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. [Електронний ресурс] / Режим доступу до ресурсу: https://ela.kpi.ua/jspui/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf.

УДК 004.056.5

Shelest M., Petrenko T., Semendyay S., Norokha V. Test configuration of the object of information activity for practicing skills in finding technical channels of information leakage

Abstract: *The research topic is of utmost relevance due to the rapid development of digital technologies and the increase in threats to data privacy. The growing number of cybercrimes and the proliferation of large amounts of information highlight the need to train future cybersecurity professionals to identify technical channels of information leakage (TKVI). In the context of dynamic cyberspace, where attackers are constantly improving technical methods of attack, the problem statement lies in the need for future specialists to be ready to detect and effectively counteract TKVI. Their skills become key to maintaining the confidentiality, integrity, and availability of information in the digital environment. The analysis of recent studies indicates the importance of considering devices for searching channels of information leakage and complexes of technical protection of information.*

Keywords: *information leakage, embedded devices, tools for detecting information leakage channels, OID.*

Шелест Михайло Євгенович, професор кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Michael Shelest, Professor of the Department of Cybersecurity and Mathematical Modeling, Chernihiv Polytechnic National University.

Петренко Тарас Анатолійович, доцент кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Taras Petrenko, Associate Professor of the Department of Cybersecurity and Mathematical Modeling, Chernihiv Polytechnic National University.

Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Serhii Semendyay, Senior Lecturer at the Department of Cybersecurity and Mathematical Modeling, Chernihiv Polytechnic National University.

Нороха Владислав Олександрович, студент кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Vladyslad Norokha, student of the Department of Cybersecurity and Mathematical Modeling, Chernihiv Polytechnic National University.

Отримано *19 лютого 2024 року,* затверджено редколегією *1 квітня 2024 року*