МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2023

Безпека інформаційних технологій

МАТЕРІАЛИ

XII Міжнародної науково-технічної конференції

2-4 травня 2023
м. Ужгород (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 жовт. 2023 р. К.: НАУ, 2023. 140 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека, а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Національний авіаційний університет
- ДВНЗ «Ужгородський національний університет»
- Казахський національний педагогічний університет ім. Абая
- Кафедра безпеки інформаційних технологій НАУ
- Кафедра твердотільної електроніки та інформаційної безпеки УжНУ
- Наукова школа “Кібербезпека” НАУ
- ГО “Асоціація спеціалістів кібербезпеки”
- ТОВ «Безпека інформаційних систем «Дельта»
- Редакція наукового журналу «Безпека інформації»
- Редакція наукового журналу «Захист інформації»

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Співголови	**Максим ЛУЦЬКИЙ**, д.т.н., проф., ректор Національного авіаційного університету
	Володимир СМОЛАНКА, д.м.н., проф., ректор ДВНЗ «Ужгородський національний університет»
Заступники співголов	**Олександр Корченко,** д.т.н., проф., зав. каф. БІТ НАУ
	Василь РІЗАК, д.ф.-м.н., проф., зав. каф. ТЕІБ УжНУ
Відповідальні секретарі	**Юлія ХОХЛАЧОВА**, к.т.н., доц., доц. каф. БІТ НАУ
	Михайло ПРИГАРА, к.т.н., доц. каф. ТЕІБ УжНУ
	Марина ПОГОРЕЛОВА, асистент каф. БІТ НАУ

Члени програмного комітету

Микола КАРПІНСЬКИЙ, д.т.н., проф.,
Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)
Станіслав РАЙБА, д.т.н., проф.,
Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)
Бахитжан АХМЄТОВ, д.т.н., проф.,
Казахський національний педагогічний університет ім. Абая (м. Алмати, КАЗАХСТАН)
Геворг МАРҐАРОВ, к.т.н., доц.,
Державний інженерний університет Вірменії (м. Єреван, ВІРМЕНІЯ)
Володимир МОХОР, д.т.н., проф. чл.-кор. НАН України,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, НАН України (м. Київ, УКРАЇНА)
Олена ТИМОШЕНКО, д.ф.н. проф.,
Європейський Університет (м. Київ, УКРАЇНА)
Євген ВАСІЛІУ, д.т.н., проф.,
Державний університет інтелектуальних технологій і зв'язку (м. Одеса, УКРАЇНА)
Василь ЦУРКАН, ктн. доц.,
Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" (м. Київ, УКРАЇНА)

- створити красивий звіт. У тому числі налаштований безпосере-дньо для ваших потреб. Наприклад, щоденний звіт про інциденти, щотиж-невий звіт TOP-10 порушників, звіт з працездатності пристроїв і т. д.;

- відстежувати події, що спровоковані пристроя-ми / серверами / критично важливими системами, створювати відповідні оповіщення для зацікавлених осіб;

- зібрати доказову базу з приводу інцидентів;

- надати звіт про події в мережі без надання доступу до самої мережі, тобто адміністратор з відділу захисту інформації може відстежува-ти поведінку користувачів при тому, що не матиме ніякої можливості ознайомитися з конфіденційною інформацією власника аккаунту.

Загалом може скластися таке хибне враження, що SIEM-система є панацеєю для запобігання будь-яких загроз, але це не так. Ця система мо-же відстежувати всі події в мережі, проте не може виконувати якихось дій крім створення попередження для адміністраторів цієї мережі, а адміністратор вже спираючись на отриманий звіт приймає рішення про подальші дії. Та все ж таки ця система може відстежувати поведінку користувачів та спираючись на статистику подій вирішити, чи потрібно адміністратору звернути більше уваги тому чи іншому користувачу. Причиною тому мо-же бути як нетипова для користувача поведінка, так і певні маркери в повідомленнях, що можуть вказувати на можливу діяльність користувача, що пов'язана з тероризмом, розповсюдженням наркотичних речовин тощо.

До того ж система SIEM лише аналізує отримані дані і працює тим краще, чим більше до неї надходить інформації з різних джерел (IDS/IPS, DLP, маршрутизатори, сервери тощо) в вигляді логів.

Література

1. Кримінальний Кодекс України, ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах(комп'ютерах), автоматизованих системах, комп'ютерних мережах, або зберігається на носіях такої інформації, вчиненні особою, яка має право доступу до неї».

2. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/Slyusar V.I. Blockchain technology in future multi-domain operations.

3. Методи виявлення інцидентів/Ukrainian Information Security journal. http://jrnl.nau.edu.ua/index.php/ZI/article/view/8798.

4. Кассето О. What is UBA, UEBA, & SIEM? Security Management Terms Defined [Електронний ресурс] / Оріон Кассето. https://www.exabeam.com/siem/uba-ueba-siem-security-management-terms-defined-exabeam/.

5. Incident Response Automation and Security Orchestration with SOAR. https://www.exabeam.com/siem-guide/incident-response-and-automation/.

УДК 004.056.53

ВИЯВЛЕННЯ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ЗА РАХУНОК ПОЄДНАННЯ МЕТОДІВ ЛОКАЛІЗАЦІЇ ЗА РІВНЕМ ПОЛЯ ТА АКУСТИЧНОГО ЗВ'ЯЗУВАННЯ

Павло Павловський, Дмитро Присяжний, Віталій Гудзь

Вінницький національний технічний університет

prepod@vntu.net, dimpris@gmail.com

Проаналізовано існуючі методи захисту інформації від витоку акустичним каналом, а також методи та засоби захисту від закладних пристроїв. Доведено доцільність поєднання методів локалізації за рівнем поля та акустичного зв'язування з метою мінімізації часових витрат на виявлення радіозакладних пристроїв. Обґрунтовано необхідність розроблення пристрою, який буде виконувати функції кількох пристроїв водночас, що визначає не лише його функціональну, але й економічну доцільність.

Найпоширеніший метод витоку інформації – через технічні канали витоку інформації (ТКВІ). Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки. Тобто, технічним каналом витоку інформації є фізичний шлях носія інформації від його джерела до противника. Одним із найбільш поширених ТКВІ є акустичний. Акустичний канал витоку інформації вважають найпоширенішим, тому що у будь-якій ситуації, чи то під час проведення нарад, переговорів, чи то інших подій, люди природнім способом, а саме вголос, висловлюють свої думки, ідеї чи просто важливу інформацію. Разом із цим, завжди існувало поняття конкурент чи опонент, тобто ті особи, яким знання цієї інформації може принести користь. Одним із способів підслуховування розмов – є встановлення у приміщенні, де буде відбуватись розмова, закладних пристроїв (ЗП). Такий тип ТКВІ є найбільш «простим», саме тому він дуже часто використовується. Тому актуальним є розроблення пристрою, який буде здійснювати захист від витоку інформації таким каналом.

Один із таких засобів є пристрій, що здійснює пошук радіозакладних пристроїв. Принцип його роботи базується на пошуку радіовипромінювань та реагуванню на них. Пропонується покращити можливості виявлення радіозакладних пристроїв шляхом поєднання трьох пристроїв у один, що, у свою чергу, дозволяє не лише більш точно локалізувати несанкціонований пристрій, але й отримати певну інформацію про нього. Для досягнення цієї мети пропонується поєднати в один пристрій індикатор поля, частотомір та демодулятор. Частотомір – це електровимірювальний прилад, що призначений для вимірювання частот різних періодичних коливань, електричних або механічних. Такі пристрої поділяються на вібраційні, електромеханічні, резонансні та цифрові. Принцип дії цифрових частотомірів полягає в підрахунку кількості періодів вимірюваних коливань за певний проміжок часу. Цифровий частотомір складається з формуючого пристрою, що перетворює синусоїдальну напругу вимірюваної частоти у послідовність однополярних імпульсів; тимчасового селектора імпульсів, що відкривається на певний проміжок часу; електронного лічильника, який відраховує кількість імпульсів на виході селектора; та цифрового індикатора. Демодуляція сигналу –

процес, виділення інформаційного сигналу з модульованого коливання високої частоти. Демодулятор – пристрій, що здійснює розподіл сигналу на інформаційний та несучий (які утворюються у процесі модуляції сигналів). Це дає змогу відкинути несучий сигнал і працювати лише з інформаційним, тобто процес демодуляції сигналу, який передає закладний пристрій, дозволить отримати детальну інформацію про закладний пристрій, та яку інформацію він передає. Пропонується комбінувати ці всі пристрої у одне технічне рішення. Таке поєднання дозволяє мінімізувати час, оскільки для пошуку закладних пристроїв потрібно буде використовувати лише один пристрій, який виконуватиме функції трьох пристроїв. Запропонований пристрій дозволяє здійснити пошук закладних пристроїв, частотомір відобразити користувачеві частоту, на якій працює даний «шпигунський» пристрій, а демодулятор зчитати та відфільтрувати інформацію, що випромінює закладний пристрій.

Такий підхід уможливлює не лише отримання синергічного ефекту від застосування такого комплексного пристрою, а також знизити його собівартість порівняно з ринковою вартістю трьох окремих його складових-пристроїв. Базою для запропонованого пристрою пропонується мікроконтролер Arduino UNO, оскільки дана платформа є найбільш гнучкою, зручною у використанні та має невелику вартість.

Пошук здійснюється шляхом планомірного обходу приміщення з рухом уздовж стін і обстеженням меблів та інших розташованих у ньому предметів. При обході антену необхідно орієнтувати у різні площини, роблячи плавні, повільні повороти основного блоку для пошуку максимального рівня сигналу. Антену приладу доцільно тримати на відстані не більше 20-25 см від обстежуваних поверхонь та предметів. При відсутності обмежень на використання методу акустичного зв'язування динамік вбудованого гучномовця приладу слід орієнтувати у бік обстежуваних поверхонь і предметів.

УДК 544.171.44:004

ВИГОТОВЛЕННЯ ТА ВЛАСТИВОСТІ НАНОШАРІВ АЗОТИСТИХ ОСНОВ НУКЛЕЇНОВИХ КИСЛОТ ДЛЯ МОЛЕКУЛЯРНОЇ КРИПТОГРАФІЇ

Наталія Попович[1], Наталія Цуд[2], Катеріна Велтруска[2],
Владімір Матолін[2], Василь Різак[1]
[1]Ужгородський національний університет,
nataliyai.popovych@uzhnu.edu.ua,
[2]Карлов університет в Празі (Чеська Республіка),
veltrusk@mbox.troja.mff.cuni.cz

Криптографія - одна з найстаріших наук, які займаються вивченням методів захисту даних від несанкціонованих доступу та дій, які можуть призвести до