



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ



НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»



ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ
ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО ТЕХНІЧНОГО
УНІВЕРСИТЕТУ УКРАЇНИ «КИЇВСЬКИЙ
ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

*До п'ятнадцятої річниці від дня заснування
ІСЗЗІ КПІ ім. Ігоря Сікорського*

МАТЕРІАЛИ
науково-практичної конференції
“ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ
ТА КІБЕРБЕЗПЕКА: НОВІ ВИКЛИКИ, НОВІ ЗАВДАННЯ”

24–25 листопада 2021 року



Київ – 2021

УДК 621

Матеріали науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. – 316 с.

У матеріалах науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” опубліковано тези доповідей, в яких досліджуються питання аналізу і узагальнення нових теоретичних і практичних результатів у сферах криптографічного та технічного захисту інформації, кібербезпеки та кіберзахисту, телекомунікацій, комп’ютерних наук та інформаційних технологій, технічної експлуатації систем і засобів спеціального зв’язку, управління інформаційною безпекою, а також досліджуються питання підготовки фахівців з відповідних спеціальностей у закладах вищої освіти.

РЕЦЕНЗЕНТИ:

Пучков О.О.	к.філос.н., професор
Конюшок С.М.	к.т.н., доцент
Рома О.М.	д.т.н., с.н.с.
Криховецький Г.Я.	к.т.н., с.н.с.
Єрохін В.Ф.	д.т.н., професор
Романенко В.П.	к.т.н., доцент
Субач І.Ю.	д.т.н., доцент
Іванченко С.О.	д.т.н., професор

Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 3 від 17.11.2021).

Куліков В.М., к.т.н., доцент; Чепчиков Д.В. ПІДСИСТЕМА УПРАВЛІННЯ ПАРОЛЯМИ	261
Ланде Д.В., д.т.н., професор; Болдох М.О. ДЕАНОНІМІЗАЦІЯ КОРИСТУВАЧА МЕРЕЖІ ІНТЕРНЕТ ЗА ДОПОМОГОЮ OSINT	262
Ланде Д.В., д.т.н., професор; Нагорний Д.О. РОЗРОБКА МЕТОДІВ ТА ЗАСОБІВ ДОБУВАННЯ ІНФОРМАЦІЇ ІЗ СОЦІАЛЬНИХ МЕРЕЖ	263
Ланде Д.В., д.т.н., професор; Гладун О.Я., к.т.н., доцент; Рибак О.О. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЧНОГО ФОРМУВАННЯ ОНТОЛОГІЧНИХ МОДЕЛЕЙ НА БАЗІ КОНТЕНТУ МЕРЕЖІ ІНТЕРНЕТ	264
Ланде Д.В., д.т.н., професор; Собко А.В. МОДЕЛЮВАННЯ І ВІЗУАЛІЗАЦІЯ МЕРЕЖ НА ОСНОВІ ФОРМАТУ JSON	266
Мігін С.В. Пікуза О.О. МЕТОДИКА ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В МЕСЕНДЖЕРІ TELEGRAM ЗА ВИЗНАЧЕНИМИ ПАРАМЕТРАМИ	267
Мігін С.В. Раківський Д.Ю. МЕТОДИКА КОНТРОЛЮ ДОТРИМАННЯ ПРАВИЛ ПОЛІТИКИ БЕЗПЕКИ КОРИСТУВАЧАМИ ТЕЛЕГРАМ ЧАТУ УСТАНОВИ	268
Рябцев В.В., к.т.н., доцент; Завальна Р.С.; Малацьковський В.В. МОДУЛЬ КОНТРОЛЮ ЗНАНЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДТРИМКИ ПРОФЕСІЙНОГО НАВЧАННЯ	269
Рябцев В.В., к.т.н., доцент; Зюзін І.О.; Кирилова Є.В. СИМУЛЯЦІЯ ПРОГРАМНО-АПАРАТНИХ СИСТЕМ ЗАСОБАМИ Н5Р	271
Рябцев В.В., к.т.н., доцент; Іскрич Є.О. МЕТОДОЛОГІЯ АВТОМАТИЗОВАНОГО ДОСЛІДЖЕННЯ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ.....	273

Соболев А.М., к.т.н.; Ланде Д.В., д.т.н., професор РОЗПОДІЛЕНІ ІНТЕЛЕКТУАЛЬНІ АГЕНТИ ДОБУВАННЯ КОНТЕНТУ ІЗ СОЦІАЛЬНИХ МЕРЕЖ	274
Соколов В.В., к.т.н., доцент; Мацей С.О. СПОСІБ ПРЕДСТАВЛЕННЯ ДІАГРАМ UML ДЛЯ АВТОМАТИЧНОЇ ГЕНЕРАЦІЇ ВИХІДНОГО КОДУ ПРОГРАМ	276
Соколов В.В., к.т.н., доцент; Савойський Г.С. УМОВНІ ТА ЦИКЛІЧНІ СХЕМИ МЕТАМОРФОЗУ АКТИВНИХ ДИНАМІЧНИХ СПОЛУК ОБ'ЄКТІВ	277
Субач І.Ю., д.т.н., доцент; Жилін А.В., к.т.н., доцент; Коротаєв С.О.; Волошин Г.В. МЕТОДИКА ВИЯВЛЕННЯ ТА АНАЛІЗУ БЕЗФАЙЛОВИХ АТАК	278
Субач І.Ю., д.т.н., доцент; Жилін А.В., к.т.н., доцент; Кубрак В.О.; Приверт Д.В. МОДЕЛЮВАННЯ КІБЕРАТАК ДЛЯ ПОБУДОВИ ПЛАТФОРМИ КІБЕРНАВЧАНЬ ТАКТИЧНОГО РІВНЯ	280
Субач І.Ю., д.т.н., доцент; Євдоченко Л.О., к. держупр.; Микиток А.В. ФУНКЦІОНАЛЬНА МОДЕЛЬ СИТУАЦІЙНОГО ЦЕНТРУ З КІБЕРБЕЗПЕКИ	282
Успенський О.А., к.т.н., доцент; Бачинський М.В. ВИБІР ПАРАМЕТРІВ МОНІТОРИНГУ В СИСТЕМІ ВИЯВЛЕННЯ АТАК	284
Успенський О.А., к.т.н., доцент; Беза Т.О. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СТЕГОСИСТЕМИ З АУДІОКОНТЕЙНЕРОМ	285
Успенський О.А., к.т.н., доцент; Восмерик М.І. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖИВИХ АТАК	287
Цуркан В.В., к.т.н., доцент; Біловицька І.А. ОБ'ЄКТНО-ОРІЄНТОВАНА МОДЕЛЬ ВИЗНАЧЕННЯ КАТЕГОРІЇ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	288
Цуркан В.В., к.т.н., доцент; Волошин Д.В. АНАЛІЗ СПОСОБІВ РЕВЕРС-ІНЖИНІРИНГУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	289

ДЕАНОНІМІЗАЦІЯ КОРИСТУВАЧА МЕРЕЖІ ІНТЕРНЕТ ЗА ДОПОМОГОЮ OSINT

Анотація. Розглянуто принцип розвідки за відкритими джерелами. Представлено основні етапи деанонімізації користувача за допомогою OSINT.

Summary. The principle of open source intelligence is considered. The main stages of deanonymizing the user using OSINT are presented.

Ключові слова: OSINT, особисті дані, об'єкт зацікавленості, мережа Інтернет, деанонімізація.

З кожним роком все більше людей починають використовувати засоби і сервіси глобальної мережі Інтернет не лише для звичайного перегляду розважальних фільмів чи особистого листування, але й для віддаленого навчання, роботи та ведення активного «онлайн-життя», при цьому залишаючи багато особистої інформації у відкритому доступі, чи то у вигляді резюме із вказанням конкретних даних (номер телефону, місце проживання, місця проходження навчання та попередні посади, які займали), чи то розповідь автобіографії з певними деталями під час ведення власного блогу.

Такий змістовний виклад особистої інформації у відкритому доступі полегшує процес деанонімізації за допомогою OSINT. OSINT (розвідка за відкритими джерелами) проводиться шляхом збору та аналізу публічно доступної інформації, що публікується в джерелах, які не мають обмежень доступу.

В загальному, виокремлюють такі основні етапи проведення OSINT:

- 1) окреслення даних, які вже відомі про об'єкт зацікавленості (користувача) та визначення того, що саме необхідно дізнатися;
- 2) пошук доступних джерел даних;
- 3) знаходження та аналіз даних із доступних джерел;
- 4) створення звіту про об'єкт зацікавленості.

Висновки. Розвідка за відкритими джерелами стала одним із основних перспективних напрямків та методів деанонімізації об'єктів зацікавленості. Проте, обізнаність звичайних користувачів про необхідність приховування особистих даних зростає, а тому і постає необхідність у створенні нових методологій проведення OSINT.