СЛУЖБА БЕЗПЕКИ УКРАЇНИ
ІНСТИТУТ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ НАЦІОНАЛЬНОГО ЮРИДИЧНОГО УНІВЕРСИТЕТУ ІМЕНІ ЯРОСЛАВА МУДРОГО

ЗАСОБИ АНАЛІТИЧНОЇ РОЗВІДКИ. ОСНОВИ РОБОТИ В I2 ANALYST'S NOTEBOOK

Навчально-практичний посібник

Харків
«Право»
2024

УДК 004.62:355.401
З-36

Авторський колектив:

Адам Даль, кандидат юридичних наук;
Сергій Наумюк, кандидат юридичних наук, доцент;
Євгеній Рибинський, доктор філософії в галузі права;
Андрій Ханькевич, кандидат юридичних наук, професор;
Владислав Шендрик, доктор юридичних наук, професор, заслужений юрист України

Рецензенти:

Іван Калабашкін, співробітник Служби безпеки України, кандидат юридичних наук;
Наталія Свиридюк, провідний науковий співробітник наукової лабораторії з правового забезпечення стратегічних комунікацій Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, доктор юридичних наук, професор

Рекомендовано до видання
Вченою радою Інституту Служби безпеки України Національного юридичного університету імені Ярослава Мудрого
(протокол № 3 від 11.03.2024)

З-36 **Засоби** аналітичної розвідки. Основи роботи в i2 Analyst's Notebook : навч.-практ. посіб. / [А. Даль, С. Наумюк, Є. Рибинський та ін.] ; Служба безпеки України, Ін-т Служби безпеки України Нац. юрид. ун-ту ім. Ярослава Мудрого. – Харків : Право, 2024. – 306 с.

ISBN 978-617-8518-09-7

Навчально-практичний посібник підготовлений відповідно до програми навчальної дисципліни «Основи аналітичної розвідки», яка викладається для здобувачів вищої освіти спеціальностей 262 «Правоохоронна діяльність» та 081 «Право».

Призначений для користувачів спеціального програмного забезпечення i2 Analyst's Notebook, таких як здобувачі вищої освіти, метою навчання яких є набуття знань і навичок, необхідних у подальшій професійній діяльності; співробітників аналітичних підрозділів, слідчих та оперативних працівників, які цікавляться питаннями опрацювання значних масивів даних і потенційними перевагами, які пропонує i2 Analyst's Notebook; керівників організацій та установ, які хочуть дізнатися більше про те, як їхні команди можуть використовувати програму найбільш ефективно.

УДК 004.62:355.401

ISBN 978-617-8518-09-7

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ, ПОЗНАЧКИ, ПОЯСНЕННЯ

i2 ANB	– спеціальне програмне забезпечення i2 Analyst's Notebook
ScrSh	– зображення, отримане шляхом технічного захвату частини екрану монітору (Screenshot)
ЛКМ	– ліва клавіша миші
ПКМ	– права клавіша миші
→	– послідовність виконання дій в вікнах програми
Icon (Значок)	– для зручності сприйняття та відмежування простого тексту від назв спеціальних команд, підписів до кнопок і термінів програми i2 Analyst's Notebook поруч із англійським текстом у дужках зі всіх великих літер наводиться пояснювальний переклад українською мовою.
Користувач	– особа, яка проводить аналітичне дослідження розвідувальних даних за допомогою можливостей програми i2 Analyst's Notebook

ВСТУП

Шановні колеги!

Роль інформаційно-аналітичної діяльності у системі забезпечення національної безпеки важко переоцінити. Вона є вагомим і необхідним елементом та сучасним інструментом у механізмі захисту національних інтересів України, що зумовлено передусім неконтрольованим розвитком усіх процесів і явищ у сфері економіки, політики та суспільного життя. Діяльність будь-яких правоохоронних структур сьогодні потребує хоча б мінімального прогнозування розвитку, захисту від ризиків, небезпек та викликів.

У сфері діяльності Служби безпеки України аналітична розвідка визначає ефективність взаємодії всіх наявних засобів і сил під час виконання поставлених перед ними завдань із захисту інтересів держави.

У зв’язку із цим особливої важливості набуває розробка і використання програм реалізації науково-технічних досягнень, поширення можливостей їх використання під час проведення розвідувальної, контррозвідувальної та оперативно-розшукової діяльності.

Різноманітність і складність діяльності структурних підрозділів Служби безпеки України у сучасних умовах об'єктивно обумовлюють застосування сучасних інформаційних технологій, серед яких чинне місце займають продукти опрацювання великих інформаційних масивів.

Сучасні комп'ютерні технології відкривають нові можливості для вилучення цільової інформації шляхом очищення оперативних даних, аналізу трафіку телефонних з’єднань, банківських транзакцій, розшифрування відеозображень, ідентифікації за голосом, за портретом, за смисловим змістом тексту, за відбитками пальців тощо. Комп'ютерне опрацювання текстів і документів дає змогу їх структурувати і виділяти значущі для інтересів спеціальних служб об'єкти.

Ключовою ланкою дедалі більшою мірою стають комп'ютерні технології наповнення й аналізу інформації, отриманої із відкритих джерел, що дають змогу виявляти латентні кримінальні зв'язки і на основі синтезу здобутих даних виходити як на конкретних виконавців, так і на організаторів протиправних дій, давати прогноз розвитку подій на різні проміжки часу.

У цьому сенсі, підготовлений навчально-практичний посібник "Засоби аналітичної розвідки. Основи роботи в i2 Analyst's Notebook" безсумнівно є корисним для практичних працівників, що займаються питаннями аналітичної розвідки.

Актуальність навчально-практичного посібника має особливе значення, оскільки він є першим повним ілюстрованими виданням в Україні із опанування можливостей і вивчення алгоритмів роботи з найбільш затребуваною аналітичної програмою i2 Analyst's Notebook фірми i2 Group.

Змістовна частина матеріалу має чітку структуру і надає зрозумілі пояснення основних концепцій та функцій програмного забезпечення i2 Analyst's Notebook.

Особливо цінною є практична спрямованість навчально-посібника, яка дозволить не лише ознайомитися з теоретичними аспектами аналітичної розвідки, але й випробувати свої навички у практичній роботі, що значно підвищить ефективність та професійну компетентність співробітників СБУ.

Ми впевнені, що цей навчально-практичний посібник стане неоціненним ресурсом для будь-якої правоохоронної структури, яка цікавиться підвищенням якості своєї аналітичної роботи. Ще раз висловлюємо велику подяку авторам за їхню відмінну роботу та відданість розвитку сфери розвідувальної аналітики.

Василь МАЛЮК, кандидат юридичних наук,
голова Служби безпеки України, генерал-лейтенант

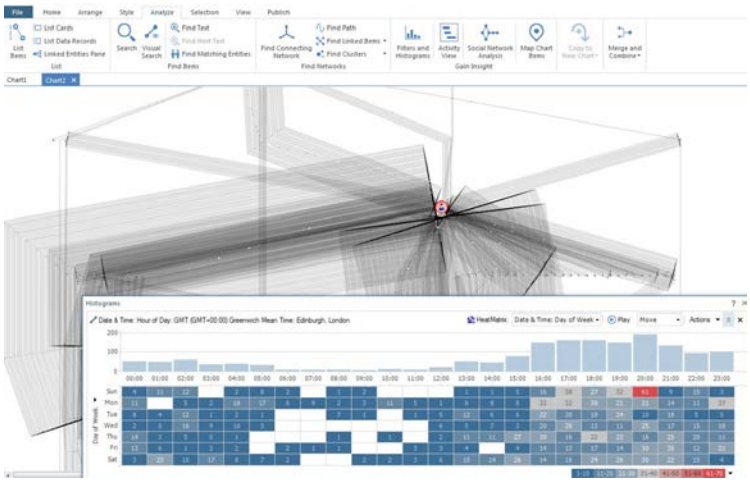
ОГЛЯД МОЖЛИВОСТЕЙ I2 ANALYST'S NOTEBOOK

Під час виконання завдань, покладених на оперативні підрозділи та слідчі органи, часто виникає ситуація, коли в силу наявності великої кількості інформації стає складним вилучити з них сенс в інтересах кримінального судочинства.

i2 Analyst's Notebook (далі – i2 ANB) — це спеціалізоване програмне забезпечення, перевірене багатьма спеціальними службами, слідчими та оперативними підрозділами у всьому світу.

Права на розповсюдження програми i2 Analyst's Notebook належать I2 Group – світовому лідеру у розробці програмного забезпечення для аналізу розвідувальних даних. I2 Group, заснована в Кембриджі (Великобританія) в 1990 році, має більш ніж 30-річний досвід допомоги користувачам у вирішенні складних аналітичних завдань. Продукти I2 Group були перевірені в незліченній кількості реальних операцій, і їм довіряють 4 500+ користувачів у більш ніж 140 країнах. i2 Group є частиною корпорації Harris Computer Corporation.

I2 ANB надає широкі можливості візуального аналізу які допомагають швидко перетворити складні набори розрізненої інформації у високоякісну, практичну аналітику. Він призначений для допомоги аналітичним працівникам, та іншим, хто займається аналізом розвідувальних даних, виявляти, прогнозувати та запобігати злочинним, терористичним та шахрайським діям.



I2 ANB підтримує динамічний процес людського мислення та пропонує безпрецедентну візуальну аналітику, надає багаті можливості візуального аналізу, які допомагають швидко перетворювати складні набори різнорідної інформації у високоякісний, ефективний інтелектуальний продукт, покликаний допомогти аналітикам, оперативним працівникам та слідчим, які займаються аналізом розвідувальних даних, виявляти, прогнозувати та запобігати протиправній діяльності як окремих осіб, так і їх груп.

I2 ANB дозволяє користувачам оперативно зіставляти як структуровану, так і неструктуровану інформацію у потужному середовищі візуального аналізу та допомагає оперативно створювати цілісну картину подій у просторі і часі.

Інтуїтивно зрозумілий, сучасний інтерфейс скорочує час освоєння програми, дозволяє працівникам і організаціям швидко скористатися перевагами підвищення продуктивності. Гнучка модель оброблення даних і середовище візуалізації у поєднанні з широким спектром інструментів візуального аналізу полегшують розуміння складних інформаційних процесів. Інтегрований аналіз соціальних мереж також забезпечує більш глибоке розуміння соціальних зв'язків і структур у мережах, що становлять інтерес для правоохоронних органів та спецслужб.

Отримані в ході детального аналізу даних результати можуть бути надані у вигляді інтуїтивно зрозумілих візуалізацій. Нескладні для розуміння схеми (інформаційні моделі) можуть стати фундаментом для планування, підготовки та проведення оперативно-розшукових, розвідувальних і контррозвідувальних заходів, і, зрештою, сприятимуть своєчасному і точному прийняттю управлінських, оперативних і процесуальних рішень.

Потенційними перевагами програмного забезпечення i2 ANB є:

- ✓ скорочення часу, потрібного для створення повноцінної, практичної аналітики на основі комплексного використання програмних інструментів під час опрацювання розрізнених даних;
- ✓ швидке перетворення даних у зрозумілі візуалізації для аналізу складних сценаріїв;
- ✓ об'єднання всієї наявної інформації для створення моделі цілісної розвідувальної картини;
- ✓ проведення якісного аналізу широкого спектру типів даних за допомогою гнучкого інструментарію для моделювання та візуалізації даних;
- ✓ надання можливості поглибленого розуміння аналітичних продуктів для більш ефективного використання наявних ресурсів організації з метою вирішення поставлених завдань.

i2 ANB підтримує динамічний процес людського мислення і пропонує:

- ✓ унікальну візуальну аналітику, що визначає зв'язки, закономірності та ключові дані, які в іншому випадку могли бути пропущеними;
- ✓ допомагає знайти відповіді на ключові питання «хто, чому, що, де і коли» за допомогою широкого спектру інструментів візуального аналізу;
- ✓ поєднує асоціації, часові та геопросторові аспекти даних з багатовимірним аналізом;
- ✓ швидко виокремлює ключових осіб і зв'язки, а також їхні зв'язки з ключовими подіями за допомогою аналізу основних зв'язків можливостей аналізу зв'язків;
- ✓ полегшує розуміння критично важливих часових рамок подій або закономірностей протиправної діяльності за допомогою потужних інструментів часового аналізу;
- ✓ визначає потенційно важливих посередників між, на перший погляд не пов'язаними між собою, об'єктами в мережі.

Програма дозволяє:

- ✓ поглибити розуміння діяльності складних злочинних, терористичних та шахрайських мереж;
- ✓ краще зрозуміти структуру, ієрархію та «спосіб дій» складних мереж, ієрархію та «modus operandi» зазначених мереж за допомогою інтегрованих інструментів їх аналізу;
- ✓ сприяти процесу прийняття рішень та забезпечення найкращого використання ресурсів для проведення оперативних заходів зі спостереження, впливу, дезорганізації та нейтралізації протиправних мереж.

Самостійне оволодіння інструментами i2 ANB забезпечує:

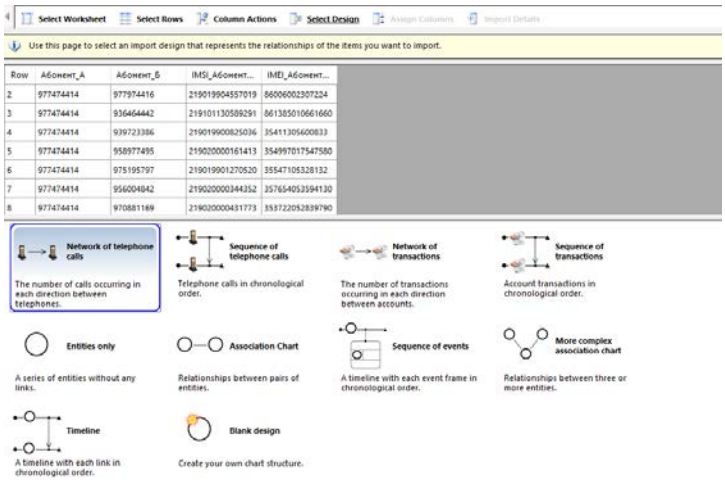
- ✓ суттєве підвищення продуктивності оперативних працівників та слідчих;
- ✓ усуває потребу в розгортанні додаткових професійних послуг інших людей;
- ✓ скорочує час на оптимізацію аналізу та завершення діяльності з генерації розвідувальних продуктів завдяки швидкому розгортанню потужних засобів візуального аналізу за допомогою сучасного користувацького інтерфейсу.

До основних переваг програми можна віднести такі:

Гнучкий збір даних. I2 ANB пропонує низку методів для швидкого збору різноманітної інформації, з якою аналітики, слідчі та оперативні співробітники стикаються щодня. Такий гнучкий підхід до збору даних дозволяє користувачам вводити широкий спектр типів даних. Приклади містять записи телефонних з’єднань, фінансові транзакції, журнали IP-адрес комп'ютерів і дані мобільної криміналістики, і це лише деякі з них.

Збір даних в i2 ANB дозволяє користувачам швидко імпортувати структуровані дані за допомогою візуального імпортера в стилі майстра; спростити ручне введення даних за допомогою інтуїтивно зрозумілого режиму перетягування; підключатися до доступних ресурсів інформації та робити запити до них за допомогою численних опцій розширення програми.

Візуальний імпорт структурованих даних. Користувачі i2 ANB можуть легко імпортувати дані зі структурованих файлів даних за допомогою візуального імпортера у режимі «майстра».



Імпорт специфікацій з файлів табличного стилю в i2 ANB, дозволяє швидко створювати схеми. Введення табличних даних у візуальне середовище i2 Analyst's значно збільшує потенціал виявлення ключової інформації, що допомагає виявити зв'язки і взаємозалежності або комунікації і товарні потоки в мережі, які в іншому випадку залишилися б прихованими.

Специфікації імпорту в i2 ANB задають спосіб інтерпретації даних у вихідному файлі. Вони точно визначають, які елементи даних мають бути використані для сутностей і зв'язків, а також вказують, як додаткові дані мають бути внесені до схеми у вигляді карток або атрибутів. Крім того, деталізується, як має бути побудована кінцева вихідна схема.

Специфікації імпорту можна зберігати та поширювати. Дані одного формату, як для окремих осіб, так і для груп аналітиків, можна швидко імпортувати та візуалізувати. Використання таких специфікацій дозволяє отримувати дані, готові до аналізу, з мінімальними зусиллями і без повторення роботи.

Навчальне видання

Даль Адам Лаврентійович
Наумюк Сергій Анатолійович
Рибинський Євгеній Ігорович
Ханькевич Андрій Миколайович
Шендрик Владислав Володимирович

ЗАСОБИ АНАЛІТИЧНОЇ РОЗВІДКИ. ОСНОВИ РОБОТИ В I2 ANALYST'S NOTEBOOK

Навчально-практичний посібник

Видається в авторській редакції

Підписано до друку 15.08.2024. Формат 60×84/8.
Ум. друк. арк. 35,6. Обл.-вид. арк. 13. Тираж 100 пр. Зам. № 160

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20, (063) 254-50-84
Вебсайт: https://pravo-izdat.com.ua
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт»,
вул. Весніна, 12, Харків, 61023, Україна
Тел. (057) 717-25-44
Свідоцтво суб'єкта видавничої справи ДК № 5748 від 06.11.2017