МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

факультет № 4

кафедра протидії кіберзлочинності

МЕТОДИЧНІ МАТЕРІАЛИ

до семінарських занять

з навчальної дисципліни **Поліцейська діяльність у кіберсфері**

вибіркових компонент освітньої програми першого рівня вищої освіти
081 Право (поліцейські)

м. Харків
2023 рік

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
Тема № 1 **Засадничі принципи протидії кіберзлочинності та інструментарій поліції у кіберсфері**	**90**	**8**	**8**	**28**		**46**	**Залік**
Всього за семестр № 7:	**90**	**8**	**8**	**28**	**0**	**46**	

2. Методичні вказівки до практичного навчання

Семінарське заняття. Об’єкти та суб’єкти протидії кіберзлочинності

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.
Час проведення __2 год__. Місце проведення: навчальна аудиторія_____.
(кількість годин) (полігон, комп’ютерний клас, лабораторія, лінгафонний кабінет)

Навчальні питання:
1. Поняття кіберпростору.
2. Поняття кіберзлочинів.
3. Конвергенція організованої злочинності та кіберпростору.
4. Суб’єкти протидії кіберзлочинності.

Література, методичне та матеріально-технічне забезпечення занять

1. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.12.2018).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.

3. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.08.20123).

4. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 12.06.2017).

5. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.

Додаткова

6. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

Інформаційні ресурси в інтернеті

7. cyberpolice.gov.ua

Хід проведення заняття

1. Курсанти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
    Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету;
12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.
14. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

Семінарське заняття. Організаційно-правові засади протидії кіберзлочинності

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.
Час проведення __2 год__. Місце проведення: навчальна аудиторія_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Навчальні питання:
1. Заходи у сфері матеріального кримінального права, передбачені Конвенцією «Про кіберзлочинність».
2. Юрисдикція щодо кіберзлочинів, передбачена в Конвенції «Про кіберзлочинність».
3. Міжнародне співробітництво країн-учасниць у сфері боротьби з кіберзлочиністю відповідно до Конвенції «Про кіберзлочинність».
4. Зміст допомоги, яку надає цілодобова контактна мережа у боротьбі з кіберзлочинністю.
5. Типова структура організованого злочинного угруповання у кіберсфері, визначеного ФБР.
6. Схеми шахрайства з кредитними картками.
7. Несправжні Інтернет-аукціони.
8. Пошук та використання «розривів» (похибок) в програмах.
9. Піраміди та листи по ланцюжку.
10. Кіберсквоттинг.
11. Крадіжка послуг.
12. Схема Pump&Dump.

Література, методичне та матеріально-технічне забезпечення занять

Основа

1. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.08.2020).
2. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
3. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html (дата звернення: 10.08.2023).

Додаткова

4. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

Інформаційні ресурси в інтернеті

5. cyberpolice.gov.ua

Хід проведення заняття

1. Курсанти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
    Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету;
12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.
14. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

Семінарське заняття. Міжнародний досвід протидії кіберзлочинності

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.
Час проведення __2 год__. Місце проведення: навчальна аудиторія_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Навчальні питання:

1. Органи протидії кіберзлочинності в різних країнах.
2. Протидія злочинності з використанням комп'ютерних технологій у російському законодавстві та в теорії оперативно-розшукової діяльності.
3. Інструменти здійснення оперативно-розшукових заходів через кіберпростір у США.
4. Зміст онлайнової секретної операції в США.
5. Правила онлайнових розслідувань США.
6. Боротьба з кіберзлочинністю у ФРН та загальний порядок здійснення проникнення за допомогою технічних засобів у інформаційно-технічні системи, що використовуються підозрюваним.
7. Використання комп'ютерних технологій в оперативно-розшуковій діяльності Великої Британії та КНР.

Література, методичне та матеріально-технічне забезпечення занять

Основна

1. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.
2. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.
3. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
4. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2023).
5. 互联网信息服务管理办法（国务院令第292号）. URL: http://www.gov.cn/gongbao/content/2000/content_60531.htm (дата звернення: 03.08.2023).

Додаткова

6. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

Інформаційні ресурси в інтернеті

7. cyberpolice.gov.ua

Порядок проведення заняття

1. Курсанти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
    Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету;
12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.
14. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

Семінарське заняття. Програмні засоби кримінального аналізу

Навчальна мета заняття: ознайомитися з роботою програмних пакетів Maltego та i2.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows XP або вище.

Завдання, які потрібно виконати, **підкреслено**

Сучасна правоохоронна діяльність характеризується необхідністю обробки та аналізу великих масивів даних. Нерідко доводиться обробляти дані телефонного білінгу правопорушників, файли протоколів відповідних транзакцій та активності в мережі Інтернет. З цією метою може бути використано спеціалізоване програмне забезпечення. У якості прикладів в даному контексті можна назвати Datasploit, i2, Maltego, Splunk. Система Datasploit (https://github.com/upgoingstar/datasploit) буде корисною для збирання та аналізу інформації про домен, електронну пошту тощо, Splunk (https://www.splunk.com) – для збирання та аналізу машинних даних, наприклад, лог-файлів. Програма Maltego у безкоштовному виконанні (https://www.maltego.com/) цілком може бути застосована для роботи з невеликим обсягом даних, у той час як i2 (www.ibm.com/software/products/ru/analysts-notebook) орієнтована на роботу з так званими «big data».

Розглянемо на прикладі роботу застосувань Maltego та i2.

Maltego

Програма Maltego має декілька версій. Серед них варто звернути увагу на умовно-безкоштовні Maltego CE та Maltego CaseFile. Перша призначена для аналізу даних онлайн, друга – для роботи з локальними файлами. Мова інтерфейсу програми – англійська.

Для використання означених версій Maltego їх потрібно завантажити з сайту виробника, після чого зареєструватися та авторизуватися у програмі.

Сам процес використання програми є доволі зрозумілим навіть пересічному користувачу. Спочатку потрібно обрати відповідну методику аналізу. Після одержання попереднього результату його можна деталізувати із застосуванням інших методів наведених у випадаючому списку в меню Run View. На рис. 1 наведено приклад аналізу за базовим методом Footprint L1 сайту mini-house.kh.ua із наступним більш детальним аналізом на предмет наявності асоційованих з ним електронних поштових адрес та їх даних (зокрема методу To Email addresses [using Search Engine]). Вказаний аналіз проводився у програмі Maltego CE.

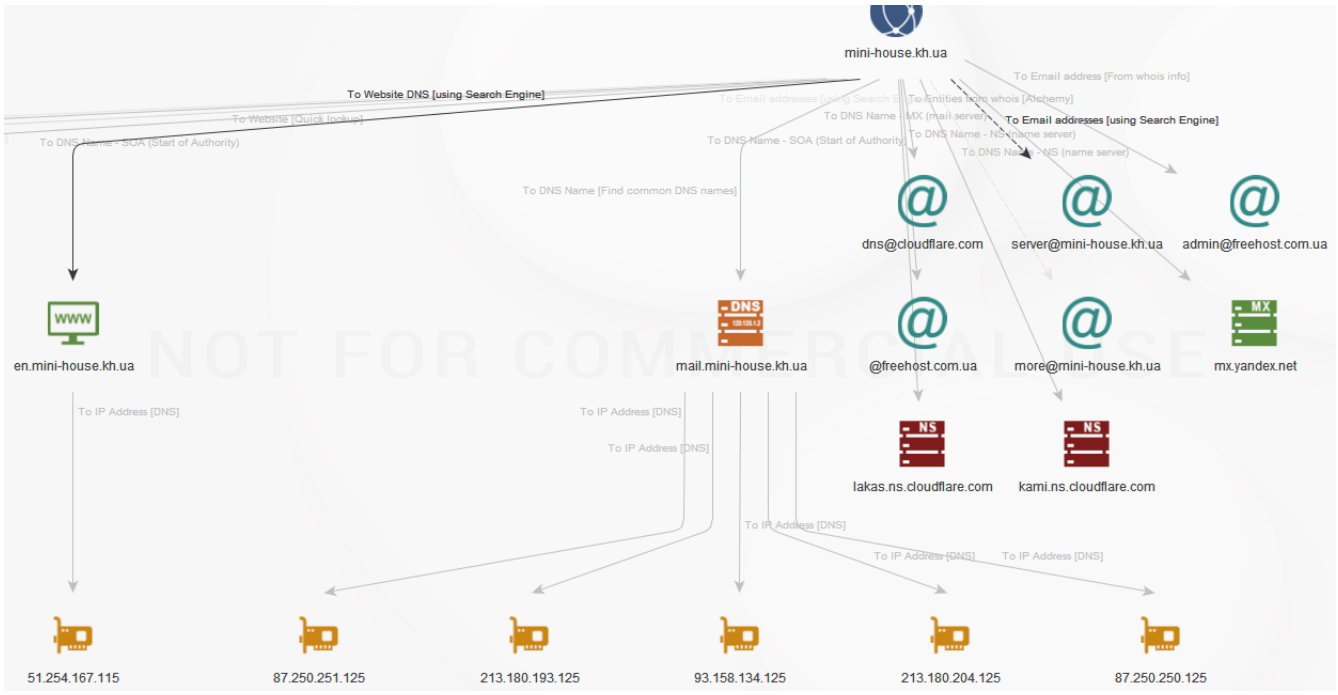

Рис. 1. Результат аналізу сайту

Якщо потрібно аналізувати дані з локальних файлів, можна скористатися програмою Maltego CaseFile.

Для імпорту відповідних даних слід у розділі Import обрати Import Graph from Table (рис. 2), після чого визначити поля таблиці, які будуть аналізуватися (рис. 3).

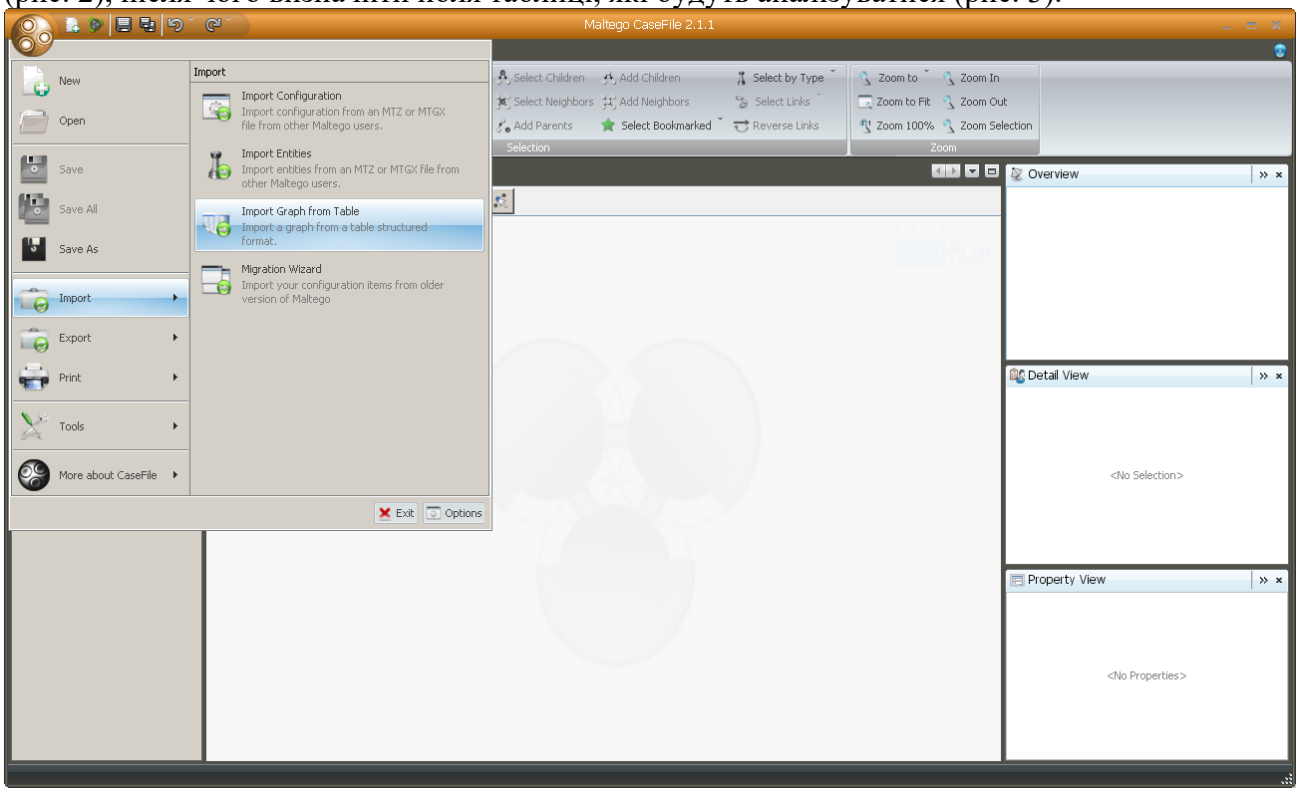

Рис. 2. Імпорт локальних даних до програми Maltego CaseFile

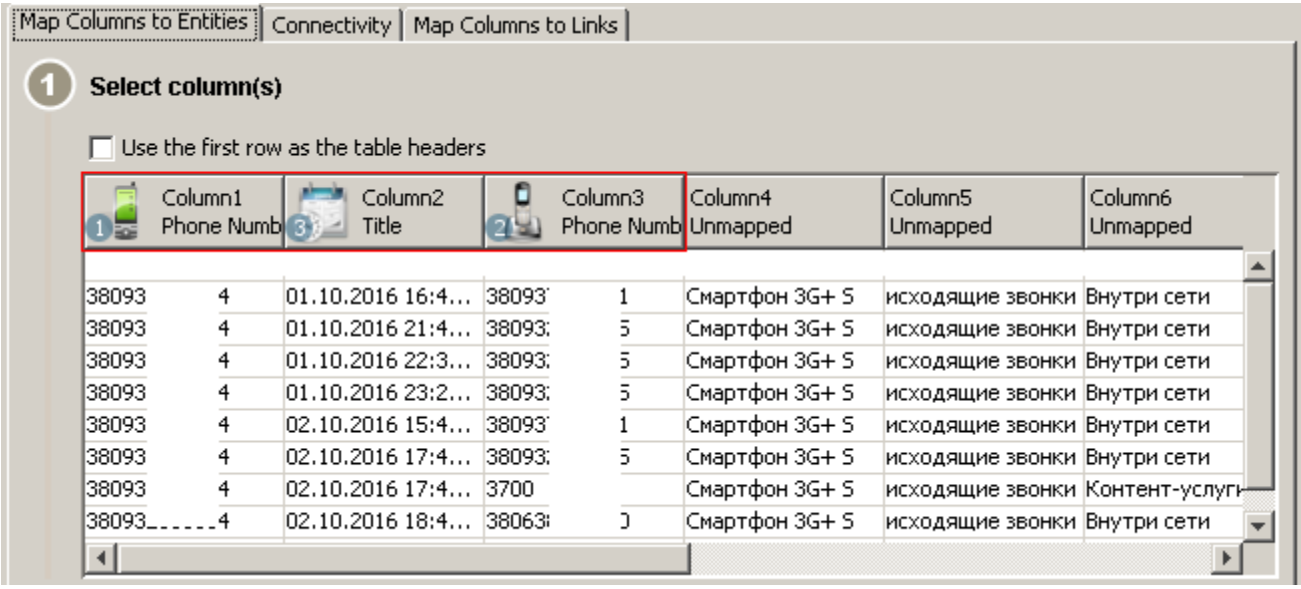

Рис. 3. Визначення даних для аналізу

У результаті аналізу одержуємо відповідний граф (рис. 4), форма якого може бути змінена.

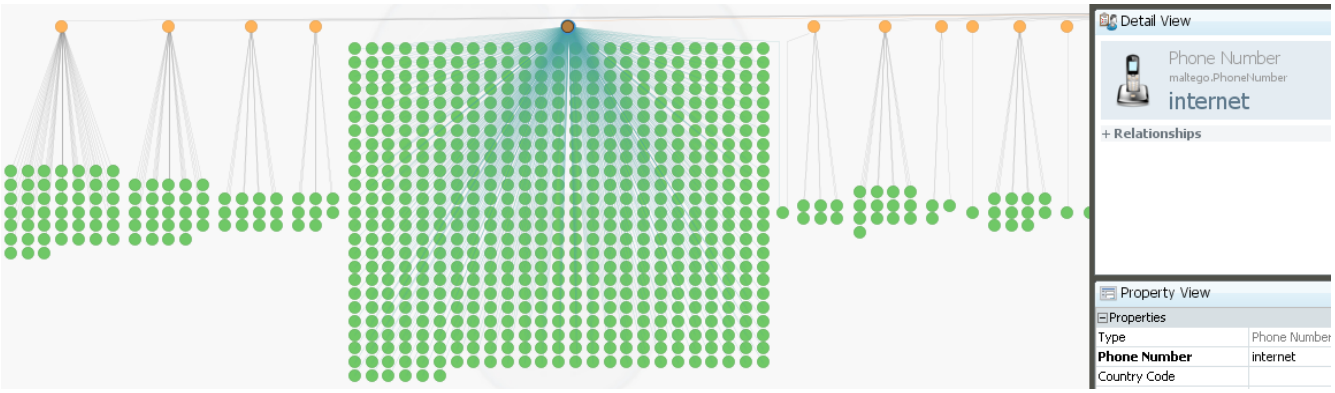

Рис. 4. Результати аналізу

У даному випадку на графіку жовтими точками позначено конкретний номер або назву послуги, а зеленим – дати та час, коли відбувалися відповідні дії. У випадку проведення реального аналізу самі дані для аналізу можна конкретизувати та змінювати, щоб у кінцевому випадку одержати більш візуально значущу інформацію про конкретну особу, подію або групу подій. На рис. 5, наприклад, наведено фрагмент діаграми аналізу шахрайської схеми, яка відбувалася з використанням мережі Інтернет.

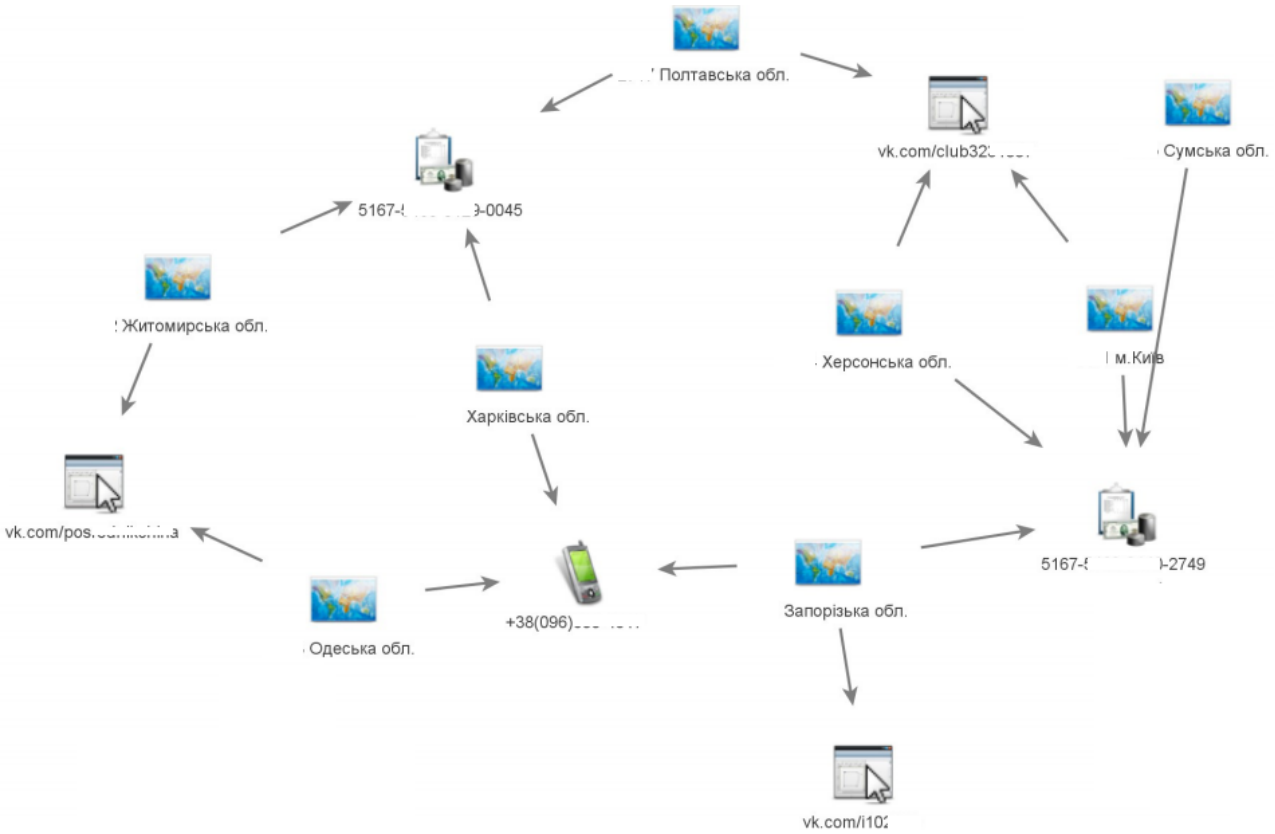

Рис. 5. Фрагмент діаграми

Сформовані у програмі Maltego діаграми та інші результати аналізу можуть бути збережені у вигляді звітів.

IBM i2

Для роботи з великим масивами даних вельми корисним представляється програмний комплекс IBM i2, зокрема IBM i2 Analyst's Notebook. Порядок роботи з даною програмою так само, як і у попередньо наведеному випадку, є візуально зрозумілим. Хоча велика кількість інструментів та налаштувань передбачає необхідність базових знань роботи з програмою.

У якості прикладу роботи застосування можна навести аналіз даних про рух коштів на картковому рахунку. Під час імпорту файлу з відповідними відомостями (рис. 6) обираємо необхідні стовпці для аналізу, вид графу тощо.

Включить выделенную строку (строки) | Исключить выделенную строку (строки) | Задать строку заголовка

Строка	1	2	3	4	5	6	7
1	Выписка по ва...						
2	Дата	Время	Категор			Сумма в валют...	Валюта карты
3	01.11.2016	17:20	Прочее			3 475,53	грн
4	30.10.2016	20:22	Выдача наличных	Карта для вып...	Снятие наличн...	- 300,00	грн
5	29.10.2016	20:19	Кафе, бары, ре...	Карта для вып...	Ресторан: BUR...	- 44,00	грн
6	29.10.2016	09:15	Выдача наличных	Карта для вып...	Снятие наличн...	- 50,00	грн
7	27.10.2016	19:44	Пополнение мо...	Карта для вып...	Пополнение мо...	- 51,00	грн
8	25.10.2016	21:56	Переводы	Карта для вып...	Перевод с карт...	497,00	грн
9	23.10.2016	20:01	Выдача наличных	Карта для вып...	Снятие наличн...	- 200,00	грн
10	21.10.2016	19:44	Пополнение мо...	Карта для вып...	Пополнение мо...	- 16,00	грн
11	20.10.2016	12:16	Переводы	Карта для вып...	Перевод на кар...	-1 000,00	грн
12	19.10.2016	21:23	Прочее	Карта для вып...	Пополнение на...	497,50	грн

Показать данные в Проводнике
Исключить выделенную строку (строки)

Рис. 6. Імпорт даних

У результаті одержуємо граф для візуального аналізу (рис. 7), з використанням якого можна наочно спостерігати рух коштів по карті.

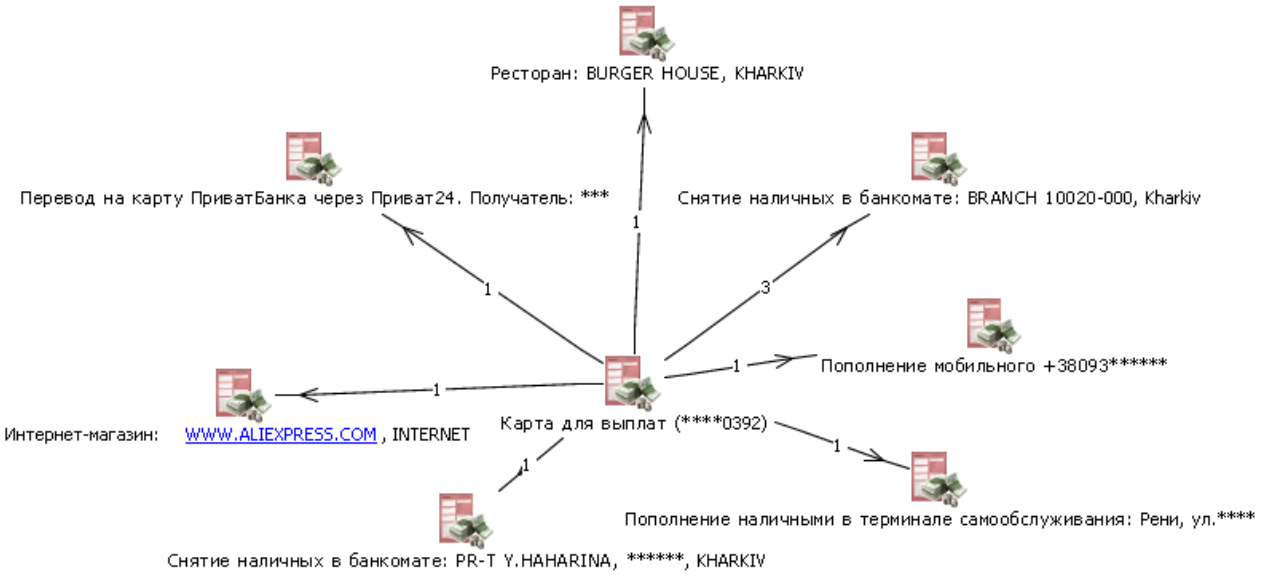

Рис. 7. Граф простого аналізу

Відповідний граф аналізу можна зробити більш інформативним (рис. 8).

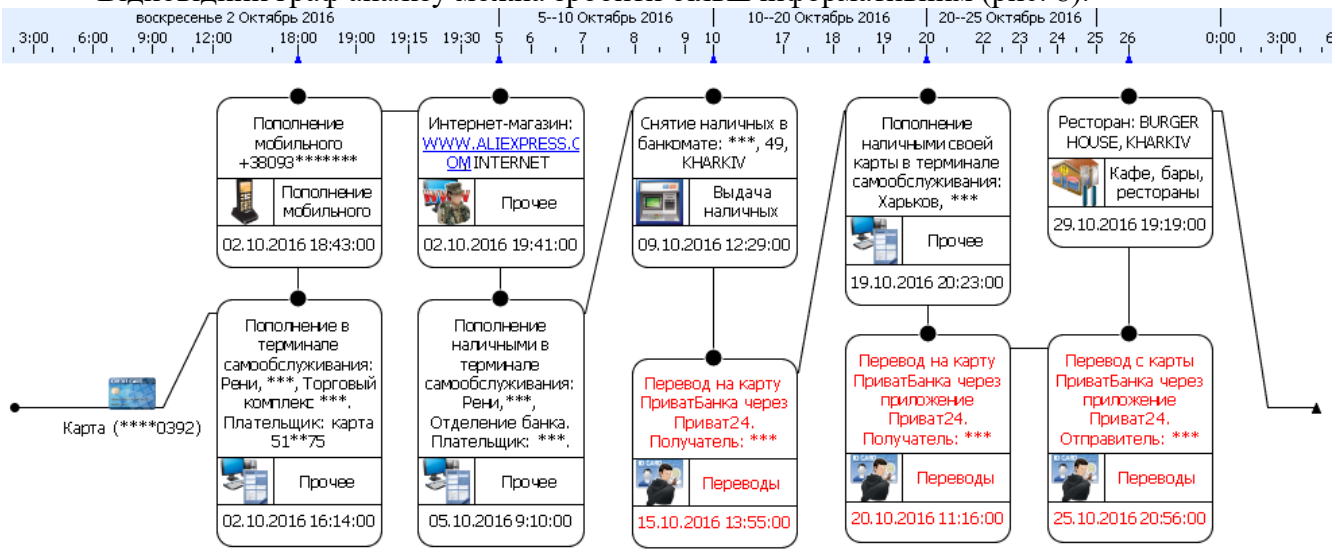

Рис. 8. Більш інформативна часова діаграма

Для того, щоб збудувати наведену часову діаграму, з використанням інструментів імпорту було видалено зайві символи у полях дати та часу, а потім обрано відповідну ним форму виведення.

1. З використанням програми Maltego CE здійснити аналіз даних з визначеного сайту.

2 З використанням електронних сервісів мобільного зв'язку та онлайн-банкінгу сформувати файли деталізації. Проаналізувати сформовані файли у програмному забезпеченні Maltego CaseFile та IBM i2 Analyst's Notebook. Порівняти одержані результати.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Апетик А. М., Дьякова А. Д., Ковальова О. В., Козлова А. Г., Манжай О. В., Мердова О. М., Мілорадова Н. А., Пашко Н. А., Юртаєва К. В., Філоненко В. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ: ГО Волонтер, 2023.
2. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
3. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
4. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.
5. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
6. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
8. Реєстр методик проведення судових експертиз. URL: http://rmpse.minjust.gov.ua (дата звернення: 13.02.2023).
9. Особливості розслідування кримінальних правопорушень, пов'язаних із доведенням до самогубства неповнолітніх із використанням соціальних мереж в Інтернеті: науково-методичні рекомендації / О.В. Манжай, В.В. Кікінчук, В.В. Корнієнко, В.С. Гнатенко, О.М. Рвачов. Х. : ХНУВС, 2022. 57 с.
10. Методика розслідування створення та поширення контенту з вмістом дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій: науково-методичні рекомендації / С.О. Книженко, О.В. Салманов, О.В. Манжай, В.В. Кікінчук, В.В. Романюк. Х. : ХНУВС, 2022. 68 с.
11. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів: науково-методичні рекомендації / В.В. Кікінчук, Т.П. Матюшкова, А.В. Піддубна, О.В. Манжай, В.В. Носов. Х. : ХНУВС, 2022. 69 с.
12. Носов В. В., Манжай І. А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1(80). С. 93-100 (DOI: 10.32631/pb.2021.1.13).
13. Носов В. В., Манжай О. В., Панченко Є. В. Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень. *Право і безпека*. 2022. № 4(87). pp. 108-124 (DOI: https://doi.org/10.32631/pb.2022.4.09).
14. Носов В. В., Манжай О. В., Ковтун В.О. Техніко-криміналістичні та організаційні аспекти роботи з криптовалютою Monero. *Право і безпека*. 2023. № 3(90). С. 102-125 (DOI: https://doi.org/10.32631/pb.2023.3.9).
15. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) ; Чинний від 2019-01-01. Київ : УкрНДНЦ, 2018. VI, 31 с. : рис., табл. (Національний стандарт України).

16. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.05.2022).

17. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.

18. Про електронні комунікації : Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.

Допоміжна

19. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.

20. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.

21. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.

22. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.

23. The Attorney General’s Guidelines for Domestic FBI Operations. September 29, 2008.

24. The Attorney General’s Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.

Інформаційні ресурси в Інтернеті

25. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.05.2023).

26. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 10.05.2023).

27. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.05.2023).

28. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.05.2023).

29. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.05.2023).

30. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.05.2023).

31. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2023).

32. cyberpolice.gov.ua.

33. hackthebox.eu.

34. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.05.2023).

35. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.05.2023).

36. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.05.2023).