

УДК 343.1+004

Віталій Вікторович НОСОВ,

кандидат технічних наук, доцент,

професор кафедри кібербезпеки факультету № 4

Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0002-7848-6448>

ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ В АСПЕКТІ ЗАСТОСУВАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ У РОЗСЛІДУВАННЯХ КІБЕРЗЛОЧИНІВ

Одним із напрямів діяльності Національної поліції України є боротьба із кіберзлочинністю. Так, у 2015 році у складі Національної поліції України було створено міжрегіональний територіальний орган – Департамент кіберполіції, основною місією якого є здійснення оперативно-розшукової діяльності для забезпечення впровадження державної політики у сфері протидії кіберзлочинності та здійснення інформаційно-аналітичного забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції [1].

У рамках проекту «Кібербезпека і протидія кіберзлочинності» координатором проектів ОБСЄ в Україні Харківський національний університет внутрішніх справ був залучений для чотиримісячного навчання і двотижневого підвищення кваліфікації інспекторів і спеціальних агентів Департаменту кіберполіції.

Враховуючі, що підрозділи Департаменту кіберполіції беруть участь і сприяють іншим підрозділам поліції у попередженні та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання комп'ютерних систем, комп'ютерних мереж і мереж електрозв'язку, було складені відповідні плани підготовки кіберполіцейських.

Під час складання планів підготовки було взято за основу:

- програму курсів Центру з розслідування кібербезпеки і кіберзлочинності Дублінського університетського коледжу;
- програму курсів Європейської групи з навчання і освіти в області кіберзлочинності;
- стратегію Ради Європи «Підготовка правоохоронних органів» 2014 року;
- вітчизняні напрацювання.
- У результаті було складено плани навчання, до яких увійшли два цикли:
- універсальної поліцейської підготовки;
- ☑️ дисципліни спеціалізації.

Курс «Кібербезпека» намагається розкрити технології вчинення кримінальних правопорушень у кіберпросторі, а курс «Цифрова криміналістика» фокусується на технології збирання цифрових слідів злочинної поведінки, які можуть стати у встановленому законом порядку джерелом доказів. Для визначення детального змісту курсу «Цифрова криміналістика» було взято до уваги, що збирання доказів (цифрових слідів) у загальному випадку складається із:

- виявлення або відшукування цифрових слідів;
- фіксації або закріплення цифрових слідів;
- вилучення цифрових слідів – дій, що забезпечують можливість їх використання, приєднання до справи та дослідження;
- збереження цифрових слідів.

Теоретична частина курсу «Кібербезпека» структурно спирається на курс Certified Ethical Hacker від EC-Council, а практичні завдання виконуються у середовищах операційних систем Kali Linux, Windows, CentOS. Метою курсу є дати базові знання про різні види атак в комп'ютерних системах і мережах, способи організації та захисту від них.

Передбачалось набуття компетенцій слухачами за такими темами:

- основні відомості про кібербезпеку;
- встановлення, налаштування і використання операційної системи Kali Linux;

- проведення пасивного збору інформації із доступних сервісів мережі Інтернет, побудова та аналіз зв'язків між частинами отриманої інформації;
- проведення активного збору інформації про мережу;
- застосування механізмів захисту мережі від збору інформації, сканування та проникнення;
- застосування криптографічних сервісів;
- аналіз трафіку в комп'ютерних мережах;
- перехоплення сесій передачі даних в комп'ютерних мережах;
- оцінка безпеки безпроводних мереж;
- вразливості операційних систем;
- технологія створення шкідливого програмного забезпечення;
- аналіз атаки переповнення буферу;
- оцінка безпеки веб-серверів та веб-застосунків;
- вивчення атак «відмова в обслуговуванні»;
- вивчення атак «SQL-ін'єкції»;
- технології соціальної інженерії.

Теоретична частина курсу «Цифрова криміналістика» у загальному вигляді спирається на окремі модулі курсу Computer Hacking Forensic Investigator від EC-Council, а практична частина використовує розроблені задачі і збірки довідкових даних для цифрової криміналістики (Computer Forensic Reference Data Sets, CFReDS) від Національного інституту стандартів і технології США.

Курс «Цифрова криміналістика» з огляду на обмеженість часу ознайомлює із:

- поняттям цифрових слідів;
- криміналістичним дослідженням ОС Windows;
- концепцією збору даних та створення дублікатів носіїв даних;
- технічними особливостями огляду засобів комп'ютерної техніки, виявлених на місці події;
- відновленням видалених файлів і логічних розділів носіїв даних;
- криміналістичним дослідженням комп'ютерної мережі, журналів аудиту і трафіку мережі;
- криміналістичним дослідженням безпроводних атак;
- криміналістичним дослідженням атак на веб.

У ході розробки і викладання курсу «Цифрова криміналістика» зібрані доступні електронні книжки, публікації та посилання на ресурси, які пов'язані із цифровою криміналістикою і можуть бути використані у практичній діяльності кіберполіції.

Означені дисципліни за відзивами спеціальних агентів і інспекторів Департаменту кіберполіції або надали необхідні для їх професійної діяльності спеціальні знання або їх суттєво систематизували.

Список бібліографічних посилань

1. Департамент кіберполіції Національної поліції України // Національна кіберполіція : тимчас. веб-сайт. URL: <https://www.npu.gov.ua/uk/publish/article/1816252> (дата звернення: 10.02.2017).

Одержано 07.11.2017

УДК 343.222

Олександр Володимирович ОЛІШЕВСЬКИЙ,

кандидат юридичних наук, старший викладач

кафедри кримінального права і кримінології факультету № 1

Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0003-1102-0675>

ВСТАНОВЛЕННЯ МОЖЛИВОСТІ ОЦІНКИ СУСПІЛЬНОЇ НЕБЕЗПЕЧНОСТІ ОСОБИ

Відповідно до ст. 48 КК України, особу, яка вперше вчинила злочин невеликої або середньої тяжкості, крім корупційних злочинів, може бути звільнено від кримінальної відповідальності, якщо буде визнано, що на час кримінального провадження внаслідок зміни обстановки вчинене нею діяння втратило суспільну небезпечність або ця особа перестала бути суспільно