Недостатні ресурси. Кіберполіція може стикатися з обмеженими ресурсами, включаючи фінанси та кваліфікований персонал. Боротьба з кіберзлочинністю вимагає великих витрат на технічні засоби та підвищення кваліфікації персоналу.

Порушення приватності. Проведення розслідування та збір інформації в інтересах безпеки може порушувати приватність громадян і піддається критиці з точки зору прав людини.

Інформаційна війна і дезінформація. Кіберзлочинці можуть використовувати кібератаки для поширення дезінформації та впливу на громадську думку, що створює загрозу для демократичних процесів.

Вирішення цих проблемних питань вимагає постійної оновлення стратегій, технологій та законодавства, а також збільшення міжнародної співпраці та удосконалення навичок персоналу. Кіберполіція повинна бути готовою відповідати на нові виклики та адаптуватися до зростаючої складності кіберзлочинності.

ВИКОРИСТАННЯ МЕТОДУ OSINT ПІД ЧАС ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент
заступник декана з навчально-методичної роботи факультету № 4 (Кіберполіції) Харківський національний університет внутрішніх справ
ORCID: http://orcid.org/0000-0002-7755-3071
onischenko1980@gmail.com

На факультеті № 4 ХНУВС здійснюється підготовка фахівців за спеціальністю 125 «Кібербезпека та захист інформації». Серед пріоритетних напрямків організації освітнього процесу варто відмітити практичну орієнтованість підготовки фахівців за даною спеціальністю, що реалізується за рахунок тісної співпраці зі стейкхолдерами – практичними підрозділами Національної поліції України, які у межах укладених договорів про співпрацю надають практичні завдання та кейси для вирішення курсантами під час відпрацювання навичок поліцейської діяльності у кіберсфері.

Для організації співпраці з практичними підрозділами у 2013 році в ХНУВС було створено Навчально-тренувальний центр протидії кіберзлочинності та моніторингу кіберпростору, який у 2023 році набув назву навчально-тренувальний центр пошукової та аналітичної роботи у кіберсфері (далі – «Кіберцентр»).

Робота Кіберцентру спрямована на відпрацювання тактики і техніки роботи правоохоронних органів у кіберсфері. До виконання завдань Кіберцентру залучені науково-педагогічні працівники кафедри протидії кібербзлочинності факультету № 4 та курсанти університету, які виявили бажання набуття практичних навичок поліцейської діяльності у кіберсфері.

Діяльність кіберцентру ґрунтується на використанні методу OSINT (Open source intelligence) – технологія добування і використання військової, політичної, економічної та іншої безпекової інформації з відкритих джерел. Первинна інформація з відкритих джерел після її аналітико-синтетичної переробки стає цінними даними, що представляють слідчий або оперативний інтерес для підрозділів Національної поліції України.

ДЖЕРЕЛА OSINT розділяють на 6 категорій інформаційного потоку:

- ЗМІ: газети, журнали, радіо та телебачення;

- Інтернет, онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube та інші відеохостинги, вікі-довідники та вебсайти соціальних медіа (наприклад, Facebook, Twitter, Instagram тощо). Ці джерела випереджають безліч інших джерел через своєчасність та легкість доступу;

- державні дані, публічні урядові звіти, телефонні довідники, прес-конференції, вебсайти та виступи офіційних посадових осіб. Ці джерела є офіційними і публічно доступними, отже можуть використовуватися відкрито і вільно;

- професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів та наукових праць;

- комерційні дані, комерційні зображення, фінансові та промислові оцінки, бази даних;

- так звана «сіра» література: технічні звіти, препринти, патенти, робочі та ділові документи.

Серед основних завдань Кіберцентру:

- моніторинг мережі Інтернет за завданнями практичних підрозділів Національної поліції України;
- допомога у розшуку безвісти зниклих дітей та осіб, які переховуються від органів державної влади;
- набуття знань і навичок поліцейської діяльності у кіберсфері.

Кіберцентр тісно взаємодіє з підрозділами Національної поліції України:

- Департаментом кіберполіції;
- Департаментом інформаційно-аналітичної підтримки;
- Департаментом боротьби з наркозлочинністю;
- Департаментом кримінального аналізу;
- Ювенальної превенції.

Взаємодія з підрозділи кримінального аналізу здійснюється шляхом підготовки дайджестів та аналітичних довідок за поставленими кураторами завданнями, зокрема пов'язаних з дією правового режиму воєнного стану. Зокрема за наданими вхідними даними із використанням технологій OSINT створюються профілі військовослужбовців РФ та ДНР/ЛНР, які брали участь у військових діях на території України.

Співпраця Кіберцентру з підрозділами кримінального розшуку полягає у підготовці довідок (аналітичних звітів) з орієнтуючою інформацією (наприклад, дані про осіб, які переховуються від органів державної влади – слідства й суду, та використовують мережу Інтернет). Ми неодноразово й ефективно брали участь у операціях «Розшук», під час яких здобували інформацію з відкритих джерел в мережі Інтернет про осіб, які переховуються від органів державної влади.

Співпраця Кіберцентру з підрозділами ювенальної превенції полягає у пошуку безвісти зниклих дітей через мережу Інтернет (встановлення кола спілкування дітей та їх можливого місця перебування шляхом аналізу сторінок у соціальних мережах та встановлення IP-адрес пристроїв зниклої дитини).

За час роботи центру було надано допомогу у пошуку 22 дітей.

Силами працівників Кіберцентру проводиться пошук та фіксація наступних даних, наявних в мережі Інтернет:

- про незаконний продаж підроблених документів та грошей;
- про торгівлю зброєю, боєприпасами, вибухівкою тощо;
- про розповсюдження наркотичних речовин та прекурсорів;
- про діяльність в мережі Інтернет радикально та екстремістськи налаштованих груп осіб та їх активних учасників щодо проведення заходів, які можуть викликати суспільний резонанс;
- про проведення мітингів, маршів, протестів та інших масових заходів;
- про продаж пристроїв, які служать для незаконного заволодіння транспортними засобами (код-граббери, різноманітні «глушилки» тощо);
- щодо вчинення кібератак, зламів вебресурсів, розповсюдження протиправного контенту та шкідливого програмного забезпечення – комп'ютерних вірусів та експлойтів;
- пошук інформації, щодо осіб, які здійснюють сепаратистську та іншу протиправну діяльність.

Кіберцентр активно проводить заходи превентивного, просвітницького та профорієнтаційного характеру, під час яких їхніх учасників інформують про способи захисту від хакерських атак та видів шахрайських дій, що вчиняються з використанням кіберпростору, особливо враховуючи той факт, що на сьогоднішній день чи не у кожної людини є сторінка в тій чи іншій соціальній мережі або електронна пошта, а зловмисники часто використовують дані, отримані злочинним шляхом з цих сторінок в своїх злочинних цілях.

Структурно роботу OSINT можна представити у вигляді низки етапів або фаз, які безперервно повторюються, утворюючи циклічне коло: «Первинна постановка завдання – Збір інформації – Оцінка – Обробка (узагальнення) – Аналіз – Поширення (підготовка звіту, дайджесту, аналітичної довідки) – Повторна оцінка» і далі по колу.

Для автоматизації збирання відомостей з відкритих джерел на національному рівні застосовуються різноманітні засоби автоматизації, наприклад:

- Octoparse (www.octoparse.com) для вилучення вебданих;
- Microsoft Defender Threat Intelligence – платформа, яка накопичує інформацію про різні мережні ресурси та надає можливість її структурованої обробки і аналізу;
- Hunchly (hunch.ly) та Kuiper (github.com/DFIRKuiper/Kuiper) – використовується з метою автоматизації процесу накопичення та обробки даних та здійснення взаємного обміну відповідними відомостями з колегами та керівництвом.

Окремі програмні інструменти активно застосовуються під час аналізу здобутої інформації, наприклад:

- MS Excel – для аналізу ступеня небезпеки організованих злочинних угруповань
- IBM i2 Analysts Notebook – для аналізу фінансових транзакцій;
- Gephi – для мережного аналізу груп в Telegram;
- Pajek – для мережного аналізу великих даних з соціальних мереж;
- Maltego – для аналізу результатів криміналістичної розвідки (FORINT) та розвідки з відкритих джерел (OSINT).

З метою закріплення теоретичних знань та набуття практичних навичок щодо використання комп'ютерних технологій для документування воєнних злочинів було розроблено 5 навчальних квестів:

1. Проведення радіотехнічної розвідки на місці події.
2. Розпізнавання обличчя особи, яка підозрюється у вчиненні воєнного злочину.
3. Встановлення місця перебування дитини за її установчими даними.
4. Картографування небезпечних зон на деокупованій території.
5. Ідентифікація особи, яка вчиняє шахрайські дії стосовно тимчасово-переміщених осіб.

Отже, використання методу OSINT під час підготовки фахівців з кібербезпеки є вкрай важливим та необхідним напрямом діяльності закладу вищої освіти як з боку освітнього процесу, так і практичної складової, що дозволить сформувати знання та навички у курсантів, які безумовно знадобляться їм під час службової діяльності у підрозділах Національної поліції України.

ШЛЯХИ УДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ ДОКТРИНИ КІБЕРБЕЗПЕКИ

Безуглий Леонід Анатолійович
кандидат юридичних наук
головний спеціаліст відділу координації
первинної професійної підготовки та
професійного навчання Управління освітньої
діяльності Департаменту освіти, науки та спорту МВС

В Україні досягнуто значний прогрес у створенні системи захисту кіберпростору. Відповідна нормативно-правова база вже розроблена та впроваджена. Визначено основні функції й повноваження суб'єктів системи кібербезпеки. Тривають роботи зі створення нових