УДК 342:343.346.8

Леонід Володимирович МОГІЛЕВСЬКИЙ,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ АНАЛІЗУ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ

Сучасний світ стрімко вривається в епоху Четвертої промислової революції і, відповідно, в епоху докорінних змін у всіх сферах життєдіяльності, і в кримінальному світі в тому числі. Все доступніше і потужніше стають технологічні інструменти, використання яких надає суспільству принципово нові можливості, але в руках злочинців можуть заподіяти дуже великої шкоди.

Як мінімум останні 15-20 років боротьба з тероризмом ведеться на основі упереджувальної концепції, а боротьба зі злочинністю - на основі караючої концепції. Це обумовлено, як правило, істотно різними масштабами наслідків для суспільства. В контексті цієї концепції якщо стає відомо про скоєний терористичний акт, а потім винні в ньому караються, це все одно говорить про провал розвідслужб і правоохоронців. У зв'язку з цим в останні роки в ряді країн, в першу чергу в США, Великобританії здійснюються спроби перебудувати боротьбу зі злочинністю за образом і подобою боротьби з тероризмом. З 2016 року нью-йоркська поліція, ФБР і Офіс директора національної розвідки розробили і прийняли Третю стратегію боротьби з ОЗ. Суть її полягає в максимальному використанні даних для випереджаючого реагування на загрози.

У даний час відомий лише один спосіб вирішення цього завдання - побудова поліцейської діяльності не тільки на штабному, а й на оперативному рівнях на основі інтелектуального аналізу і прогнозу різнорідних даних. Головним в цій перебудові є перехід від реактивної до проактивної поліцейської позиції. Це, в свою чергу, вимагає наявності у поліцейських надійних предикативних методів, що дозволяють з достатнім ступенем релевантності не стільки розслідувати вже скоєні, скільки прогнозувати злочини на етапі їх підготовки. Це завдання набуває все більшої актуальності у країнах розвиненої демократії, в яких потреби розвідувальної діяльності поліції конфліктують з зако-

нодавчими нормами, які традиційно суворо захищають право недоторканності приватного життя. В цих обставинах особливо актуальними є можливості автоматичного (суто програмно-технічними засобами, без участі людини) дослідження соціальних мереж, як легального джерела цінної розвідувальної інформації.

У доповіді Європолу 2016 р. «Соціальні мережі: як з ними працювати правоохоронцям» вказується: «Згідно з даними, отриманими від правоохоронних органів країн ЄС, наукових доповідей і власними дослідженнями, не менше 70% членів високотехнологічних ОЗУ, в першу чергу кіберкріміналу, становить молодь у віці від 18 до 25 років. Ця демографічна група сформувалася як особистості вже в епоху інтернету. Для них немає чіткої і однозначної межі між фізичним і віртуальним. Планшет або смартфон є таким же звичним інструментом, як блокнот або ручка для більш старших поколінь».

Згідно з даними спільного дослідження Стенфордського, Джорджтаунського університетів, Університету Техніон в Єрусалимі і Цюрихського технологічного університету «Інтернет-залежності: міфи і реальність» більш ніж дві третини молоді відчувають інтернет-залежності. Вони не можуть в інтервалі більш ніж сім хвилин жодного разу не звернутися до комунікатора, месенджера, e-mail тощо. В тому ж дослідженні вказується, що більш ніж для 4/5 молодих людей не просто звичною, а єдино нормальною моделлю поведінки є безперервне викладання в соціальні мережі візуальної, текстової та іншої інформації про своє проведення часу. Приблизно половина обстежених робить це навіть тоді, коли з міркувань безпеки або внаслідок можливих колізій з законом викладати такого роду інформацію було б не треба.

Наведені вище відомості дозволяють зробити висновок, що вперше в історії правоохоронні органи мають справу зі злочинцями, які не в поодиноких випадках, а масово залишають сліди своєї злочинної діяльності, повідомляють про зв'язки, знайомства, звички і т. п. Це робить соціальні мережі воістину неоціненним джерелом інформування для правоохоронців.

Аналіз соціальних мереж став одним з головних напрямків в програмі SECILE (Безпека Європи і боротьба з тероризмом: вплив, легітимність і ефективність). Також аналіз соціальних мереж вставлений як окремий блок в програму загальноєвропейського відеоспостереження - INDECT (Інтелектуальна інформаційна система, що підтримує спостереження,

пошук і виявлення небезпеки в контекстному транзакційному і відео-средовищі для забезпечення безпеки громадян у мегаполісах). Уже в 2016 р. аналіз соціальних мереж як пріоритетний напрямок вказано у найважливішій темі Європолу CAPER (Збір, обробка, аналіз, прогноз та звітність по інтегрованій інформації для попередження терактів). Найважливішою розробкою в рамках CAPER стало створення прототипу системи ePOOLICE (Раннє розпізнавання загроз організованої злочинності на основі сканування інформаційного середовища).

У 2007-2011 рр. була створена і почала функціонувати комп'ютерна система поліції Нідерландів. Система використовує великі сховища даних, що включають кілька компонентів: загальнонаціональна поліцейська база даних, поєднана з базами даних Європолу та Європейської Комісії; сховище електронної документації голландської поліції на всіх рівнях - від міністерства до первинних поліцейських управлінь. Третій блок комп'ютерної системи поліції включає в себе потужну систему сканування інтернету, і, в першу чергу, соціальних мереж і соціальних медіа. Голландський уряд в звіті за 2016 р. вказав, що використання системи дозволило в рамках встановлених бюджетних обмежень більш ніж на 17% за період з 2013 по 2016 рр. знизити число серйозних і організованих злочинів на території Нідерландів. За винятком Голландії, в країнах ЄС подібних систем в даний час немає. У той же час подібні системи експлуатуються не тільки ФБР, але і поліціями ряду штатів.

Досягненням голландської системи стало раннє розпізнавання загрози здійснення терористичних актів у Франції і в Бельгії. Голландська система моніторить Twitter та інші платформи в масштабах Бенілюксу, Німеччини, Франції та Великобританії. На жаль, французькі та бельгійські правоохоронні органи належним чином не оцінили попередження голландських колег і не вжили запобіжних дій.

Транснаціональна злочинність не має фізичних кордонів, тому боротьба з нею може вестися тільки на загальноєвропейському рівні, тому для європейських правоохоронців немає іншого шляху, як співпрацювати в аналізі та прогнозуванні організованої злочинності, розвивати загальні технології і здійснювати спільні багатосторонні практичні операції. В цьому ж руслі повинні рухатися і правоохоронні структури України як на штабному так і на оперативному рівні, особливо підрозділі таких департаментів: Департамент стратегічних розслідувань (у складі кримінальної поліції), Департамент кримінального аналізу (у складі

кримінальної поліції), Департамент кіберполіції (у складі кримінальної поліції), Департамент превентивної діяльності, Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми (у складі кримінальної поліції), Департамент протидії наркозлочинності (у складі кримінальної поліції).

Одержано 12.04.2020