Поліпшення позиції України відбулося через ухвалення законодавчих актів у галузі кібербезпеки та кіберзахисту.

Міністерство цифрової трансформації України та Державна служба спеціального зв'язку та захисту інформації проводять роботу щодо посилення захисту від кіберзлочинності через оновлення та реформування законодавчої бази, вдосконалення механізму кіберзахисту органів державної влади, їх інформаційно-телекомунікаційних систем, проведення аналізу стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Але сучасний розвиток цифрових технологій відбувається дуже швидко і сприяє поширенню кіберзлочинності, на відміну від наявного нормативно-правового законодавства, яке спрямоване на врегулювання цього виду економічної злочинності.

До основних нормативно-правових документів та законів щодо інформаційної безпеки України належать: Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про національну безпеку України» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

Бібліографічні посилання

1. Report To The Nations. 2020 Global Study On Occupational Fraud And Abuse. URL: https://www.acfe.com/report-to-the-nations/2021/#download (дата звернення: 10.10.2021).

Рижков Е. В.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ВИКОРИСТАННЯ ІНФОТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАХИСТУ ЕКОНОМІКИ

Україна переживає черговий процес реформування своєї правоохоронної сфери. На цей раз зміни стосуються органів, підрозділів та служб, призначенням яких є протидія економічним злочинам [1]. Етап характеризується стрімким вдосконаленням злочинних схем та їх переходом у віртуальний інформаційний простір. При цьому неухильно зростає

кількість випадків використання під час вчинення економічних злочинів сучасних інформаційно-телекомунікаційних технологій [2]. Особливу небезпеку в контексті появи нових видів злочинів у сфері економіки становить поява віртуальних форм розрахунків із використанням криптовалют. Більшість фінансових операцій, учасниками яких є як фізичні, так і юридичні особи, сьогодні відбувається за допомогою Інтернету. Електронні системи кредитно-фінансових установ і банків, як потенційні об'єкти злочинного посягання, а також активне користування цими системами фізичними особами, стали природною причиною виникнення, існування та збільшення економічних злочинів з використанням сучасних інфотелекомунікаційних технологій.

Водночас більшість методик щодо протидії економічним злочинам, які за останні роки були напрацьовані відповідними оперативними підрозділами Національної поліції та Служби безпеки України, нереалізовані через ліквідацію останніх у зв'язку зі створенням Бюро економічної безпеки України [3].

Тактика отримання економічної інформації оперативного характеру зумовлена як специфікою завдань відповідних підрозділів, так і особливостями економічної інформації, що становить оперативний інтерес, що відрізняють її від оперативної інформації про злочини загальнокримінальної спрямованості.

Отримання інформації, що утворюється під час використання сучасних інформаційно-телекомунікаційних технологій, передбачає застосування спеціальних технічних засобів та дотримання певного процесуального порядку, що забезпечує її доказове значення. Процесуальною формою пізнавальної діяльності негласного характеру під час розслідування кримінального правопорушення є негласні слідчі (розшукові) дії (далі – НСРД), які згідно з ч. 2 ст. 246 КПК проводяться у випадках, якщо відомості про злочин та особу-злочинця неможливо отримати в інший спосіб. НСРД «зняття інформації з транспортних телекомунікаційних мереж» (ст. 263 КПК) та «зняття інформації з електронних інформаційних систем» (ст. 264 КПК) в частині дій, що проводяться на підставі ухвали слідчого судді, проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів [4].

Незалежно від тяжкості злочину проводиться установлення місцезнаходження радіоелектронного засобу без розкриття змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження (ст. 268 КПК), а також зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України) [5].

Зазначене положення цілком кореспондується з вимогами Закону

України «Про телекомунікації», в ч. 4 ст. 39 якого передбачено, що оператори телекомунікацій зобов'язані за власні кошти закуповувати та встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [6].

Треба додати, що оператори телекомунікацій під час виконання своїх службових обов'язків мають доступ до інформації про персональні дані, переміщення (місцезнаходження), контакти (особисті зв'язки) користувачів тощо, яка може бути цінною під час розслідування економічних злочинів.

Наприклад, операторами систем мобільного зв'язку оброблюються (приймається, реєструється, зберігається тощо) такі відомості: 1) розрахункові дані – відомості, на основі яких системами операторів здійснюється облік наданих послуг і наступні розрахункові операції з абонентами; абонентські номери, що беруть участь у з'єднанні, отриманні послуг (MSISDN); вид послуги, напрям з'єднання тощо; час початку, завершення та тривалість з'єднання, надання послуги тощо; телекомунікаційні картки, що використовувалися для розрахунків із оператором; 2) службові дані – відомості суто технічного характеру, що забезпечують функціонування систем операторів і терміналів щодо надання та споживання послуг, підтримки з'єднання тощо: міжнародний ідентифікаційний номер рухомого абонента (IMSI); міжнародний ідентифікаційний номер терміналу (IMEI); постійне місцезнаходження споживача відносно підсистеми базових станцій (BSS) оператора [7, с. 7].

Тому важливим і актуальним завданням для фахівців по боротьбі з економічною злочинністю є виявлення метаслідів, а особливо слідів метадезінформування у сфері економічної діяльності, утворених внаслідок використання інформаційно-телекомунікаційних технологій.

Автоматизовані комп'ютерні системи оперують у своїй роботі інформацією в бінарному вигляді, багаторазово змінюючи її форму та зміст. Саме через те, що інформація не є матеріальним об'єктом, а лише може бути матеріально зафіксована у різній формі, класичне розуміння слідів та процесу слідоутворення, у розрізі злочинів, що вчиняються в інформаційно-телекомунікаційній мережі, не є співвідносним. При цьому визначальна роль у процесі слідоутворення в комп'ютерній мережі належить процесу інкапсуляції – важливому інструменті об'єктно-орієнтованого програмування, що обмежує доступ до компонентів (методів і властивостей), які становлять об'єкт, та робить їх приватними (доступними лише всередині об'єкта).

Під час вчинення економічного злочину за допомогою застосування

інформаційно-телекомунікаційних технологій відбувається зміна матеріального стану елементів телекомунікаційної системи мобільного зв'язку або Інтернет, що утворює системи електронних слідів-відображень, придатних до сприйняття за допомогою відповідних програмно-технічних засобів. Це вказує на корисну властивість телекомунікаційних систем (мереж) щодо фіксації обліково-звітних даних про факт передачі та зміст переданої телекомунікаційними мережами інформації у формі електронного документа, завдяки чому цей процес можна назвати унікальним способом виявлення, попередження та припинення сучасних способів учинення злочинів у сфері економіки.

Зазначені технології мають перевагу в отриманні фахівцями по боротьбі з економічною злочинністю криміналістично значущої інформації під час оперативно-розшукового документування та розслідування кримінальних правопорушень, а тому повинні використовуватись під час виявлення, попередження та припинення злочинів цими підрозділами за конкретними напрямами, зумовленими виконанням завдань кримінального провадження, згідно з визначеною КПК процедурою шляхом зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем, а також встановлення контролю за місцезнаходженням злочинців з урахуванням специфіки протидії злочинам економічної спрямованості [8, с. 204].

З урахуванням термінів запуску нового державного органу (мінімум до одного року) та фактичною ліквідацією вказаних попередників маємо тимчасову відсутність в державі ефективно працюючих правоохоронних структур щодо протидії економічній злочинності.

За вказаних обставин питання вдосконалення підготовки відповідних кадрів, проведення прикладних наукових досліджень, організація спеціалізованих науково-практичних заходів та запозичення міжнародного досвіду є вкрай актуальними та перспективними [9].

Ефективний запуск Бюро економічної безпеки України можна здійснити шляхом використання в його діяльності наукомістких інноваційних методик, інформаційно-аналітичних продуктів, сучасних інформаційно-телекомунікаційних технологій та обов'язковим запровадженням кримінального аналізу на етапах оперативно-розшукового документування та розслідування кримінальних проваджень.

Бібліографічні посилання

1. Бюро економічної безпеки: коли запрацює новий орган і чим він відрізняється від фіскалів. URL: https://biz.ligazakon.net/analitycs/205046_byuro-ekonomchno-bezpeki-koli-zapratsyu-noviy-organ--chim-vn-vdrznyatsya-vd-fskalv
2. Всесвітнє дослідження економічних злочинів та шахрайства 2020. URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf
3. Закон України Про Бюро економічної безпеки України. URL: https://ukurier.gov.ua/media/files/2021-4/1_P6-10.pdf

4. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. *Голос України*. 2012. № 90–91.
5. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Міністерства фінансів України, Адміністрації Державної прикордонної служби України, Міністерства юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1687/5.
6. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.
7. Сулацький Д. В., Маркарян Г. О. Відомості щодо наданих телекомунікаційних послуг як предмет інформаційної безпеки людини та джерело оперативно значимої інформації : науково-практ. рекомендації. Донецьк : ДЮІ МВС України, 2011. 28 с.
8. Рижков Е. В. Отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки за допомогою сучасних інфотелекомунікаційних технологій. *Митна справа. Науково-аналітичний журнал*. Одеса. 2014. № 2 (92). Ч. 2. К. 2. С. 194–205.
9. Рижков Е. В. Інформаційні технології як засіб підготовки фахівців з економічної безпеки правоохоронних органів. *Економічна та інформаційна безпека: проблеми та перспективи* : матеріали Всеукр. науково-практ. конф. (27 квітня 2018 р., м. Дніпро). Дніпро : Дніпропетр. державний ун-т внутр. справ. 2018. С. 176–178.
10. Рыжков Э. В., Бортэ Г. Р., Охрименко С. А., Чобан Г., Шквир В. Д. Вызовы цифровой экономики. *Landmarks and Challendgts of the Sosial-Ekonomic Development* : Internetional Symposium (24–25 мая 2018 г., бухарест, Румыния). С. 497–504.

Рижкова С. А., старший викладач
кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

AMBER ALERT В УКРАЇНІ: СИСТЕМА ОПЕРАТИВНИХ СПОВІЩЕНЬ ПРО ЗНИКЛИХ ДІТЕЙ ЗА ДОПОМОГОЮ FACEBOOK

Відповідно до статистичних даних МВС України з початку 2021 року органи та підрозділи Національної поліції зареєстрували понад 12 тисяч звернень про зниклих дітей, з них – 98 % дітей були знайдені протягом доби [1]. Окрім позитивної динаміки щодо оперативного встановлення місцезнаходження зниклої дитини, органами та підрозділами Національної поліції у 2 % випадків, які мають найвищий ступінь загрози життю та здоров'ю дитини, є такі, що потребують залучення та допомоги населення в районі, де саме зникла дитина.

У контексті зазначеного науковий та практичний інтерес має впровадження системи пошуку зниклих дітей AMBER Alert за допомогою