

УДК 343.97

Андрій Васильович МИКИТЧИК,

кандидат юридичних наук,
доцент кафедри кримінології та кримінально-виконавчого права
Національної академії внутрішніх справ (м. Київ)

ЗАХОДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Активний розвиток комунікаційних мереж, інформаційних технологій і масової комп'ютеризації призвели до еволюційних змін кримінального середовища не тільки на рівні окремих держав, а й у всьому світовому співтоваристві. Відсутність належного соціального контролю призвела до того, що мережа Інтернет практично безкарно стала використовуватися злочинцями як місце і основний засіб вчинення різних протизаконних посягань, як традиційних (шахрайств, крадіжок), так і інших – викрадень та продажу конфіденційної інформації, вимагань, «геймерських» шахрайств, а так само поширення предметів і послуг, які були виключені з легального обігу (наркотичних засобів, дитячої порнографії). Особливу небезпеку становлять кіберекстремізм і крайня його форма – кібертероризм, тобто дії з дезорганізації роботи інформаційних систем, що створюють небезпеку загибелі людей, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків, якщо вони вчинені з метою порушення громадської безпеки, залякування населення або здійснення впливу на прийняття рішень державними органами, а також погроза вчинення зазначених дій з тією ж метою.

Запобігання кіберзлочинності є однією з найбільш актуальних і складних кримінологічних проблем. Висока латентність, зростання числа кіберзлочинів, вдосконалення інформаційних технологій, що створюють нові можливості вчинення злочинів, вимагають кардинально інших підходів запобігання злочинів що вчиняються у віртуальному просторі та створюють загрози для глобальних інформаційних мереж і суспільства в цілому.

Досліджуючи кіберзлочинність в Україні можливо дійти наступних висновків, а саме:

- кіберзлочинність є різновидом злочинності, яка існує нарівні з насильницькою, корисливою, корупційною, екологічною та іншими видами;
- тісно взаємопов'язана з іншими видами злочинності, оскільки злочини в сфері комп'ютерних технологій доволі часто виступають способом вдосконалення інших кримінальних правопорушень (крадіжка, вимагання, шахрайство та ін.);
- має високотехнологічний характер, що викликано використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп'ютерних пристроїв, носіїв комп'ютерної інформації та інше, які виступають знаряддями і засобами вчинення кримінальних правопорушень;
- мають високий ступінь латентності, яка становить від декількох десятків до декількох тисяч відсотків з різних видів злочинних діянь, що обумовлено різними об'єктивними факторами (небажання жертв комп'ютерних злочинів звертатися до правоохоронних органів, неочевидність комп'ютерних злочинів для більшості населення в силу їх вчинення у віртуальному середовищі, складність виявлення комп'ютерних злочинів за відсутності необхідної кількості фахівців в правоохоронних органах та ін.);
- носить високоорганізований характер і тісно взаємопов'язана з організованою злочинністю, так як значна кількість кіберзлочинів (DDoS-атаки, Е-банкінг, фішинг, створення ботів та ін.) вчиняється злочинними групами;
- має «професійний» характер, так як особи, які вчиняють кіберзлочини мають злочинну спеціалізацію, не вчиняючи інших видів злочинних діянь; отримують злочинний дохід (прибуток) в результаті злочинної діяльності; мають необхідні знання, вміння, навички в сфері ІТ-технологій для вчинення злочину; дотримуються певних правил, законів, понять і термінології, що дозволяють їм спілкуватися, обмінюватися досвідом і знаходити однодумців;
- характеризується транскордонністю, так як кіберпростір існує поза державними кордонами і будучи загальнодоступним, дозволяє злочинцю, що знаходиться на території однієї держави, вчиняти злочинні дії щодо осіб, які перебувають в іншій державі;
- носить транснаціональний характер, так як кіберзлочинці в силу своєї приналежності до комп'ютерного «андеграунду» для отримання злочинних доходів та спрощення вчинення злочинних діянь на території двох і більше держав змушені, незалежно від національності, об'єднуватися в міжнародні злочинні групи [1, с. 356];

– знаходиться в стані динамічного розвитку, що обумовлено постійним вдосконаленням існуючих і створенням нових ІТ-технологій, залученням до інформаційних відносин нових учасників, розширенням кіберпростору за рахунок збільшення числа користувачів мережі Інтернет, мобільних комп'ютерних пристроїв, переходом до електронного документообігу все більшої кількості організацій, підприємств, установ;

– отримала риси економічної злочинності, так як більшість кіберзлочинів відбувається в банківсько-фінансовому або корпоративному секторі (інтернет-банкінг, банківський фішинг, кібервимагання та ін.), а діяльність злочинців спрямована на вилучення доходів (прибутку);

– трансформується в злочинність політичного характеру, що пов'язано з активізацією протиправної діяльності в кіберпросторі представників хакерського руху, спецслужб і силових структур зарубіжних держав, міжнародних екстремістських і терористичних організацій (DDoS-атаки на урядові сайти, кібершпіонаж щодо інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше.

Аналіз стану і криміногенного комплексу кіберзлочинності дозволяє сформулювати висновок про те, що запобігання їй повинно ґрунтуватися на таких основних підходах:

Міжнародний підхід передбачає консолідацію зусиль правоохоронних органів різних держав, а також створення спеціальних органів і підрозділів по боротьбі з кіберзлочинністю. Особливості кіберзлочинності з усією очевидністю свідчать про неможливість ефективного протистояння їй в межах окремих держав, без активного міжнародного співробітництва.

Правовий підхід пов'язаний з удосконаленням правових механізмів національного та міжнародного законодавства, що передбачає відповідальність за кіберзлочини. Оскільки на сьогоднішній день жодна держава не може захистити себе від кіберпосягань приймаючи правові заходи тільки на національному рівні, вбачається необхідним організація і реалізація комплексної програми запобігання кіберзлочинності, що включає: гармонізацію кримінального законодавства про кіберзлочини; розробку на міжнародному рівні і імплементацію в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах; міжнародне співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; дієвий механізм вирішення юрисдикційних питань в кіберпросторі.

Таким чином, міжнародне співробітництво є ключовим моментом в ліквідації правового вакууму, який існує між розвитком інформаційних технологій і реагуванням на них законодавцем.

Технічний підхід передбачає запобігання кіберзлочинам за рахунок реалізації заходів технічного характеру, що забезпечують безпеку в інформаційній сфері, а також формування матеріально-технічної бази підрозділів по боротьбі з кіберзлочинністю, виходячи з принципу «найсучасніша техніка».

Організаційний підхід має на меті розробку і запровадження в практику, удосконалених організаційно профілактичних заходів. Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій, і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян.

Запобігання кіберзлочинності має включати в себе заходи віктимологічної профілактики – підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації. Актуальними є поглиблені віктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант кіберзлочинності, характеристик окремих типів особистості кіберзлочинців, а також різних аспектів забезпечення кібербезпеки.

Таким чином, проведений аналіз дає підстави зробити висновок про те, що проблема запобігання кіберзлочинності є багатогранною і лежить не тільки у законодавчій сфері, а і в технічній і технологічній.

Список бібліографічних посилань

1. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. Київ : Скіф, 2012. 728 с.

2. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 172–177.

3. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.

Одержано 14.03.2019

УДК 343.96:351.741

Тетяна Василівна МИРОНЮК,

кандидат юридичних наук,

доцент кафедри кримінології та кримінально-виконавчого права

Національної академії внутрішніх справ (м. Київ)

ПРОБЛЕМНІ ПИТАННЯ РЕАЛІЗАЦІЇ ПОЛІЦЕЙСЬКОГО ПІКЛУВАННЯ ЩОДО ПСИХІЧНОХВОРИХ ОСІБ

Законодавчі новели, які впроваджуються в процесі реформування, в нашій державі – є безумовно необхідними, оскільки мають за мету покращити рівень діяльності тих органів, служб і установ, що служать на користь суспільства, захищають права та свободи громадян.

Так, поліцейська реформа розпочалася з прийняття закону України «Про національну поліцію», в якому передбачені правові інститути діяльності поліції, що безумовно покликані забезпечити належний та необхідний захист прав громадян. Серед таких інститутів слід виокремити, до цього не існуючого в практиці поліції, інституту «поліцейське піклування».

Одним із видів поліцейського піклування визначено піклування щодо особи, яка підозрюється у втечі з психіатричного закладу чи спеціалізованого лікувального закладу, де вона утримувалася на підставі судового рішення, та особи, яка має ознаки вираженого психічного розладу і створює реальну небезпеку оточуючим або собі. На нашу думку, саме ця категорія осіб на сьогодні потребує особливої уваги з боку держави та суспільства. Сьогодні існує ряд невирішених питань як на законодавчому так і організаційному рівнях, які впливають на належне забезпечення реалізації даного заходу.

Разом з цим, поліцейське піклування відноситься до одного з превентивних поліцейських заходів. Застосовуючи превентивні заходи, поліцейські тим самим створюють необхідні умови, для неухильного дотримання законів, виявлення і припинення різних правопорушень, відвернення можливості посягання на суспільні відносини, які охороняються правом.

Так, за статистичними даними 1,2 млн українців (тобто більше 3 % всього населення країни) страждає на психічні розлади, цей показник з кожним роком зростає. Україна займає перше місце в Європі за кількістю психічних розладів майже 2 млн наших співвітчизників щороку стають пацієнтами психіатричних лікарень. «За оцінками фахівців, від різноманітних нервових розладів страждає кожен третій українець» [1]. За прогнозами Всесвітньої організації охорони здоров'я, до 2020 року психічні розлади увійдуть до першої п'ятірки хвороб (за [1]).

Найпоширенішою причиною розладів психіки в Україні є вживання алкоголю і наркотиків. На другому місці – розлади, пов'язані із травмами мозку або церебральною дисфункцією. До таких хвороб, зокрема, відносяться хвороба Альцгеймера, судинна деменція та інші. Третє місце – група з розумовою відсталістю всіх ступенів. Четверта за кількістю зареєстрованих хворих в Україні група налічує шизофренії і шизоафективних розладів. На п'ятому місці – невротичні, пов'язані зі стресом, і соматоформні розлади [2]. Наприклад, депресії, тривожні розлади, фобії, obsesивно-компульсивні розлади та інші. До них схильні, в першу чергу люди, які часто знаходяться у стресових ситуаціях: наприклад, заробітчани, шахтарі і військові. Згідно з дослідженнями Дніпропетровської медичної академії МОЗ, після знаходження в зоні АТО 25 % бійців скаржилися на підвищену агресивність, 12 % – на нав'язливі спогади про пережите, 10 % – на нічні кошмари і 2–3 % – на головний біль і погіршення пам'яті [1]. Звичайно в статистиці враховані лише ті люди, які проходили стаціонарне, амбулаторне або консультативне лікування в установах Міністерства охорони здоров'я. Справжня кількість людей із тими чи іншими порушеннями психічного здоров'я може істотно відрізнятись від офіційних даних [2].