КРИМИНОЛОГИЯ

УДК 343.97

ОСНОВНІ КОНЦЕПТУАЛЬНІ ПІДХОДИ ЩОДО ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

Олена БУГЕРА,
кандидат юридичних наук, доцент,
доцент кафедри права
Київського національного лінгвістичного університету

АНОТАЦІЯ

Статтю присвячено дослідженню основних концептуальних підходів щодо використання мережі Інтернет для запобігання злочинності. Здійснено аналіз вітчизняного законодавства та міжнародного досвіду з цього питання. Обґрунтовано доцільність використання мережі Інтернет для запобігання злочинності за такими напрямами: Інтернет-картографування кримінологічної інформації; моніторинг соціальних Інтернет-мереж; застосування можливостей Інтернету речей; підвищення рівня правової культури суспільства з використанням можливостей мережі Інтернет, формування спеціалізованих інформаційних баз даних; забезпечення комунікації між працівниками правоохоронних органів та громадськістю. Обґрунтовано доцільність законодавчого закріплення Концепції щодо використання мережі Інтернет для запобігання злочинності.

Ключові слова: мережа Інтернет, злочинність, попередження, концептуальні підходи, законодавство.

MAIN CONCEPTUAL APPROACHES TO USE THE INTERNET TO PREVENT CRIME

Olena BUHERA,
Candidate of Law Sciences, Associate Professor,
Associate Professor at the Department of Law
of Kiev National Linguistic University

SUMMARY

The article is devoted to the study of the main conceptual approaches to the use of the Internet for crime prevention. The analysis of domestic legislation and international experience on this issue is carried out. The expediency of using the Internet to prevent crime in the following areas has been substantiated: Internet-mapping of criminological information; monitoring of social Internet networks; application of possibilities of the Internet of things; raising the level of the legal culture of society using the possibilities of the Internet, creating specialized information databases; providing communication between law enforcement officials and the public. The expediency of legislative consolidation of the Concept on the use of the Internet to prevent crime.

Key words: Internet network, crime, prevention, conceptual approaches, legislation.

Постановка проблеми. Ефективність вирішення проблем запобігання злочинності в сучасному інформаційному світі передбачає здійснення відповідних кримінологічних досліджень із метою розроблення відповідних концептуальних підходів та формування практичних рекомендацій для правоохоронних органів. При цьому в Стратегії сталого розвитку «Україна – 2020» указується, що метою державної політики у сфері реформи правоохоронної системи є корегування завдань та функцій правоохоронних органів, упровадження нових засад проходження служби, нових критеріїв оцінки роботи правоохоронців для підвищення рівня захисту прав і свобод людини, а також інтересів суспільства і держави від протиправних посягань [1].

Відповідно до ст. 2 Закону України «Про національну безпеку», до фундаментальних національних інтересів України належить сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення [2]. При цьому забезпечення цього зростання залежить також від ефективності виконання державою функцій щодо запобігання злочинності.

Актуальність теми дослідження. Необхідно зазначити, що протягом 2017 року в Україні обліковано 523,9 тис. кримінальних правопорушень. Із загальної кількості зафіксованих правоохоронними органами кримінальних проявів 41% є тяжкими та особливо тяжкими. Протягом 2017 року обліковано 1 633 очевидні умисні вбивства і замахи на вбивство, 2 228умисні тяжкі тілесні ушкодження, 259 згвалтувань і замахів на згвалтування. Кількість крадіжок становила 261,3 тис., шахрайств – 37,1 тис., грабежів – 18,1 тис., розбоїв – 3 тис., хабарництва – 2,7 тис. [3].

Наведена статистика вказує на необхідність здійснення правоохоронними органами відповідної запобіжної діяльності на новому якісному рівні. При цьому сучасною тенденцією розвитку кримінологічної науки щодо розроблення концептуальних підходів запобігання злочинності є використання можливостей мережі Інтернет.

Стан дослідження. Питання використання можливостей мережі Інтернет для запобігання злочинності

досліджено недостатньо. Водночас окремі проблеми використання соціальних Інтернет-мереж для запобігання злочинності, картографування кримінологічно значимої інформації, підвищення рівня правової культури з використанням мережі Інтернет та інформатизації в галузі кримінології досліджували такі вчені, як К.А. Автухов, Н.О. Андріїв, А.М. Бабенко, В.С. Батиргареєва, В.Д. Гавловський, О.Ф. Гіда, Д.І. Голосніченко, В.В. Галунько, С.В. Горова, О.М. Джужа, А.П. Закалюк, О.В. Каплій, Г.П. Клімова, О.В. Косолап, Н.В. Кушакова, О.В. Минькович-Слободяник, Є.В. Орлов, В.А. Пересадько, Н.В. Теремцова, О.Ю. Юрченко та інші.

Метою та завданням статті є дослідження основних концептуальних підходів щодо використання мережі Інтернет для запобігання злочинності.

Виклад основного матеріалу. Розроблення загальної стратегії протидії злочинності – це завдання державної влади в контексті визначення України правовою державою. Кримінологія має грати вирішальну роль у реалізації цього завдання, чим, безперечно, може продемонструвати своє суспільне і державне значення та потребу в ній. У межах певної стратегії визначаються концептуальні засади (концепції) вирішення окремих актуальних проблем. Кримінологічна концепція визначається у разі виникнення нової складної проблеми у сфері протидії злочинності. Її завдання – окреслити цю проблему, розкрити її сутність, природу, чинники, суспільну небезпечність, концептуально вказати напрями й засоби розв'язання, необхідну для цього систему забезпечення. Таким чином, у концепції предмет розгляду, як правило, вужчий, на відміну від стратегії, але сфера його висвітлення більш глибока та багатобічна [4, с. 261, 289].

Необхідно зазначити, що концептуальні підходи щодо боротьби з певними видами злочинів були відображені у відповідних Концепціях. Так, відповідно до Концепції боротьби з корупцією на 1998–2005 роки, боротьба з корупцією повинна здійснюватися на таких основних принципах: наукової обґрунтованості; входження до міжнародної системи боротьби з корупцією та розвитку всебічного співробітництва з іноземними державами [5].

Відповідно до Концепції державної політики у сфері боротьби з організованою злочинністю, інформаційне та наукове забезпечення боротьби з організованою злочинністю має включати надання засобам масової інформації відомостей для об'єктивного інформування населення України про проблеми боротьби з організованою злочинністю і корупцією; сприяння в отриманні іноземними громадянами необхідної для захисту прав інформації про органи та систему боротьби з організованою злочинністю і корупцією в Україні; створення умов для залучення громадських та інших організацій, засобів масової інформації до поширення інформації про діяльність організованих злочинних угруповань; обмін інформацією, що стосується боротьби з організованою злочинністю, на міжвідомчому та міждержавному рівнях [6].

При цьому світовою тенденцією в стратегії попередження злочинності є тенденція впровадження в цей процес технологічних інновацій із метою переоснащення всієї правозахисної системи, насамперед це стосується використання можливостей мережі Інтернет. Наприклад, у США інноваційні технології призначені для попередження злочинності та переоснащення поліції поділяють на так звані „HARD Technology" – «важкі технології», які стосуються вдосконалення рівня фізичного захисту громадян і поліцейських, підвищення рівня комп'ютеризації патрульних автомобілів, використання дистанційних датчиків для контролю і аналізу різних ситуацій і „SOFT Technology" – «легкі технології», які передбачають упровадження інформаційних технологій для створення спеціалізованих баз даних, картографування кримінологічно значимої інформації, моніторингу інформації в мережі Інтернет та ін. [7].

Загалом, досвід США вказує на те, що суттєві успіхи у боротьбі зі злочинністю залежать від низки факторів, зокрема від поєднання профілактичної та просвітницької кампанії з посиленням кримінальної репресії – так звана політика «нульової толерантності» до будь-яких правопорушень. Вагоме антикриміногенне значення в США має також широке залучення громадськості до протидії злочинності у різних формах [8].

Необхідно зазначити, що Розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки та затверджено план заходів щодо її реалізації. У Концепції вказується, що за умов системного державного підходу цифрові технології будуть значно стимулювати розвиток відкритого інформаційного суспільства – одного з істотних факторів розвитку демократії в країні, підвищення продуктивності, економічного зростання, а також підвищення якості життя громадян України. При цьому цифровізація – це насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично забезпечує інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір.

Одним із базових принципів цифровізації є створення цифрових інфраструктур, що забезпечить розширення доступу громадян до глобального інформаційного середовища та знань. Ще у 2011 році вільний доступ до Інтернету визнано ООН фундаментальним правом людини (цифровим правом). При цьому Національний план розвитку широкосмугового доступу до Інтернету повинен містити відповідні показники покриття широкосмуговим доступом до Інтернету території країни; технічні вимоги до самих послуг широкосмугового доступу до Інтернету; моделі використання наявних у державі фізичних інфраструктур (автомобільні та залізничні магістралі, газопроводи, лінії електропередачі) із метою розвитку телекомунікаційних мереж; відповідні ініціативи та проекти з організації надання послуг широкосмугового доступу до Інтернету для територій, громад, домоволодінь та соціальної інфраструктури (насамперед заклади освіти, медицини, культури).

Важливим є також те, що Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки передбачає створення цифрового робочого місця – віртуального еквівалента фізичного робочого місця, котрий вимагає належної організації, користування та управління, оскільки має стати запорукою підвищеної ефективності працівників та створення для них більш сприятливих умов праці. В умовах цифрової економіки робочі місця перестають бути прив'язаними до фізичних місць. Вони стають «цифровими», віртуальними, мобільними, тобто такими, що не потребують постійного перебування працівника на робочому місці. Концепція «цифрових робочих місць» поширюється надзвичайно швидко у бізнес-середовищі та позитивно сприймається більшістю працівників, яким подобаються гнучкі способи роботи, можливість працювати вдома, на відпочинку, тобто з будь-якого місця.

Загалом, цифрофізація здатна удосконалити низку сфер життєдіяльності людини. Життя людини та її безпека, правопорядок та громадський спокій є пріоритетними завданнями сучасної України. Загострення криміногенної ситуації та антитерористична операція на Сході країни вимагають створення надсучасної системи запобігання надзвичайним ситуаціям, протидії тероризму, «інтелектуальних» заходів безпеки громадян та критичної інфраструк-

тури міст та селищ. Використання цифрових технологій повинно запровадити новий рівень координації діяльності оперативних, чергових, диспетчерських та муніципальних служб, відповідальних за громадську безпеку та повсякденну життєдіяльність місцевих громад, а також запровадити механізми швидкого реагування відповідних служб із метою усунення наслідків правопорушень та надзвичайних ситуацій.

Окремої уваги потребує напрям безпеки, пов'язаний із контролем та спостереженням за дорожнім рухом. Кількість дорожньо-транспортних пригод можна потенційно зменшити втричі за умов використання технологій та значного світового досвіду щодо зменшення аварійності на дорогах. Моніторинг небезпечних перехресть та транспортних магістралей, паркувальних майданчиків, автоматичної фіксації порушень правил дорожнього руху, керування інфраструктурою світлофорів потребують упровадження цифрових технологій, відповідних систем, програмного забезпечення. Завдяки отриманню та аналізу інформації, яка надходить із систем відеоспостереження, дорожніх контролерів, телеметрії, датчиків та інших спеціалізованих засобів, забезпечується оперативне реагування на аварії та управління ситуаціями.

Можливе також використання цифровізації у сфері охорони здоров'я. При цьому медицина трансформується: періодична діагностика стає онлайн-діагностикою, Інтернет речей дозволяє за допомогою датчиків та сенсорів здійснювати постійний моніторинг стану здоров'я людини, оператори медичних і супутніх послуг та інфраструктури стають учасниками цифрових платформ – усе це впливає на якість, ефективність та функціональність системи медичної допомоги та супроводу громадян.

Також потенціали соціальних, мобільних, хмарних технологій, технологій аналізу даних, Інтернету речей (окремо та в сукупності) здатні призвести до трансформаційних змін у державному управлінні та зробити державний сектор ефективним, реактивним, ціннісним. Є позитивні приклади використання цифрових технологій, наприклад, у сфері державних закупівель та реєстрації майнових прав із використанням технології блокчейн.

Необхідно зазначити, що наступним етапом цифровізації виробництв та промисловості є Індустрія 4.0 – оновлена концепція «розумного виробництва», що ототожнюється з «четвертою промисловою революцією» та появою кіберфізичних систем. В Індустрії 4.0 головну роль відіграють такі технології та концепти, як Інтернет речей, «великі дані» (big data), «предиктивна аналітика», хмарні та туманні обчислення, «машинне навчання», машинна взаємодія, штучний інтелект, робототехніка, 3D-друк, доповнена реальність [9].

Визначаючи основні концептуальні підходи щодо використання мережі Інтернет для запобігання злочинності, можна висловити думку що сутність підходів пов'язана з технологічними можливостями мережі Інтернет, станом розвитку інформаційних технологій, а також із необхідністю підвищення рівня ефективності запобіжних заходів. Загалом, концептуальними підходами щодо використання мережі Інтернет для запобігання злочинності можуть бути такі: Інтернет-картографування кримінологічної інформації; моніторинг соціальних Інтернет-мереж; технологічне переоснащення правоохоринних органів шляхом використання сучасних Інтернет-технологій і можливостей Інтернету речей; підвищення рівня правової культури суспільства з використанням можливостей мережі Інтернет та ін.

Необхідно зазначити, що картографування кримінологічної інформації – це спосіб візуалізації на карті різноманітних правопорушень, який використовується аналітиками для аналізу злочинів і конкретизації специфіки скоєння. Необхідно зазначити, що це ключовий компонент поліцейської статистики і кримінологічного аналізу. Картографування злочинів використовує геоінформаційну систему (далі – ГІС), що дозволяє аналітикам виявляти гарячі точки вчинення злочинів на карті (поряд з іншими даними, недоступними без картографічної візуалізації правопорушень). Використовуючи ГІС, кримінологи можуть здійснювати кореляційний аналіз таких статистичних даних, як демографічні, інформація щодо розміщення шкіл, ринків, ломбардів, місць торгівлі зброєю, стан освітленості вулиць та ін., що дозволяє краще зрозуміти глибинні кореневі причини вчинення злочинів і допомогти правозахисним установам боротися з цими проблемами. Уперше спосіб комп'ютерного моделювання даних злочинів із накладенням на карти був здійснений у Чикаго в 1986 році, коли Департамент поліції виграв грант для втілення кримінальної картографії у життя. Згодом цю ініціативу перейняли інші великі міста США [10].

На підставі вищевикладеного можна зробити висновок, що для підвищення рівня запобігання злочинності у сучасних умовах розвитку інформаційного забезпечення суспільства необхідно внести доповнення до ст. 5 Закону України «Про Національну програму інформатизації» щодо картографування кримінологічної інформації та забезпечення доступу до неї через мережу Інтернет усіх зацікавлених сторін.

Важливим є також те, що соціальні Інтернет-мережі для запобігання злочинності використовуються вже тривалий час правоохоронцями багатьох держав. Правоохоронці намагаються використовувати нові технології, зокрема ті, що отримані завдяки наявності соціальних мереж, для виявлення, розкриття, розслідування та попередження злочинів. Ними здійснюється постійний моніторинг підозрілих блогів, чатів, сайтів тощо з метою отримання оперативно вагомої для правоохоронців інформації. Сьогодні соціальні мережі широко використовуються правоохоронними органами зарубіжних країн засобом для зв'язків із громадськістю, зокрема з метою отримання криміналістично значимої інформації. У контексті сучасного стану протиправного використання соціальних мереж, прогнозованого зростання у найближчому майбутньому кількості та суспільної небезпеки реальних і потенційних загроз, що виходять із кібернетичного простору, можна констатувати, що створення ефективної системи протидії таким деструктивним явищам і локалізації відповідних загроз можливе лише через безпосереднє використання правоохоронними органами нашої держави (у взаємодії з компетентними органами інших зарубіжних країн) специфічних можливостей соціальних мереж. Ідеться про те, що правоохоронці мають постійно використовувати у своїй діяльності соціальні мережі (як засоби і знаряддя для виявлення, розкриття та попередження злочинів). Сьогодні в Україні не існує законодавства, яке б здійснювало нормативно-правове регулювання такої діяльності загалом та спеціальних методів «дослідження цільової аудиторії» зокрема. При цьому одним із достатньо ефективних засобів припинення протиправної діяльності, тобто забезпечення прав і свобод громадян, повинен стати так званий «правоохоронний моніторинг», функцію якого законодавець має покласти (із відповідним визначенням компетенції) на правоохоронні органи, наділені правом здійснення оперативно-розшукової діяльності [11, с. 277, 280].

Загалом, Інтернет активно змінює наше життя, тому уявити сучасний світ без соціальних мереж стає не зовсім можливо. На початок 2017 року соціальні мережі охопили понад 2 мільярди користувачів. Найбільшу популярність сьогодні отримав Facebook з аудиторією понад 1,59 мільярда постійних користувачів [12].

Однією із сучасних тенденцій розвитку кримінологічної науки є дослідження, пов'язані з можливістю застосування Інтернету речей для запобігання злочинності. При цьому Інтернет речей (Internet of Things, IoT) – це концепція мережі, що складається із взаємопов'язаних фізичних пристроїв, які мають вбудовані «давачі», а також програмне забезпечення, що дозволяє здійснювати передання й обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію функції програмування та ідентифікації, а також вони дозволяють виключити необхідність участі людини за рахунок використання інтелектуальних інтерфейсів. Набуває поширення також термін "Internet of Everything" (IoE) – всеосяжний Інтернет. Загалом, основною концепцією Інтернету речей є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильника, кондиціонера, автомобіля, велосипеда і навіть кросівок. Усі ці об'єкти (речі) повинні бути оснащені вбудованими «здавачами» (сенсорами), які мають можливість обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею і виконувати різні дії залежно від отриманої інформації. Прикладом упровадження такої концепції є система «розумний будинок» або «розумна ферма». Уже зараз Інтернету речей приділяється увага на найвищому рівні; починаючи з 2009 року, в Брюсселі (за підтримки Єврокомісії) проходять конференції Annual Internet of Things, на яких виступають із доповідями єврокомісари, науковці та керівники провідних IT-компаній. За прогнозами аналітиків, найближчим часом очікується справжній «бум» Інтернету речей. Тому передбачається, що до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів [13].

Отже, розвиток Інтернету речей є загальносвітовою тенденцією, що створює нові умови функціонування людського суспільства. Технологічні можливості Інтернету здатні забезпечити виконання різних завдань: від якісного підвищення побутових умов людини до використання у сфері штучного інтелекту. Безперечно, кримінологічна наука не може стояти осторонь цих процесів. На нашу думку, доцільним є концептуальне обґрунтування використання можливостей Інтернету речей для запобігання злочинності. При цьому використання Інтернету речей для запобігання злочинності можливе шляхом формування комплексної системи збирання кримінологічно значимої інформації та її аналізу з використанням звукових датчиків, відеокамер, безпілотних літальних апаратів та інших технологічних елементів. Важливим є також вирішення проблем правового регулювання Інтернету речей та формування відповідної законодавчої бази.

Важливим є також те, що одним із шляхів підвищення рівня правової культури суспільства є використання можливостей мережі Інтернет. При цьому значення Інтернету в суспільних відносинах (як майданчика для комунікації) постійно зростає. Це загальносвітовий процес. Необхідно підкреслити, що Інтернет став більш важливим джерелом інформації, ніж періодичні друковані засоби масової інформації [14, с.228–229]. Особливо актуальним є використання можливостей мережі Інтернет для підвищення рівня правової культури – дієвого засобу запобігання злочинності на загальносоціальному рівні.

Висновки. Отже, враховуючи міжнародний досвід, основними концептуальними підходами щодо використання мережі Інтернет для запобігання злочинності можуть бути такі: Інтернет-картографування кримінологічної інформації; моніторинг соціальних Інтернет-мереж; застосування можливостей Інтернету речей; підвищення рівня правової культури суспільства з використанням можливостей мережі Інтернет; формування спеціалізованих інформаційних баз даних; забезпечення комунікації між працівниками правоохоронних органів та громадськістю. При цьому доцільним є розроблення та законодавче закріплення Концепції щодо використання мережі Інтернет для запобігання злочинності.

Список використаної літератури:

1. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12 січня 2015 року № 5/2015. URL: http://zakon5.rada.gov.ua/laws/show/5/2015 (дата звернення: 17.07.2018).

2. Про національну безпеку України: Закон України від 21 червня 2018 року№ 2469-VIII / Голос України. № 122 (6877). 7 липня 2018 року.

3. Істратенко І.М. Стан злочинності у 2017 році (за даними Генеральної прокуратури України). URL: http://www.ukrstat.gov.ua/druk/publicat/kat_u/publzlochin_u.htm (дата звернення: 17.07.2018).

4. Закалюк А.П. Курс сучасної української кримінології: теорія і практика: У 3 кн. К.: видавничий Дім «Ін Юре». 2008. Кн. 3: Практична кримінологія. 320 с.

5. Про Концепцію боротьби з корупцією на 1998-2005 роки: Указ Президента України від 24 квітня 1998 року № 367/98. URL: http://zakon5.rada.gov.ua/laws/show/367/98 (дата звернення: 17.07.2018).

6. Про Концепцію державної політики у сфері боротьби з організованою злочинністю: Указ Президента України від 21 жовтня 2011 року № 1000/2011. URL: http://zakon2.rada.gov.ua/laws/show/1000/2011 (дата звернення: 17.07.2018).

7. Byrne J., Gary Marx G. Technological Innovations in Crime Prevention and Policing. URL: https: //www.ncjrs.gov/App/Publications/abstract.aspx?ID=260054 (дата звернення: 03.07.2018).

8. Тимчук О.Л. Окремі аспекти стратегії протидії злочинності в Україні та США. Право і суспільство. 2015. № 5(3). С. 162–168. URL: http://inter.criminology.onua.edu.ua/?p=22345 (дата звернення: 03.07.2018).

9. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: http://zakon2.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення: 03.07.2018).

10. Кримінальна картографія. URL: https://uk.wikipedia.org/wiki/Кримінальна картографія (дата звернення 03.07.2018).

11. Гавловський В.Д. Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 2 (28). С. 271–282.

12. Попова Т.М. Соціальні мережі, кібератаки та гібридні війни. URL: https://www.radiosvoboda.org/a/28598299.html (дата звернення 03.07.2018).

13. Інтернет речей. URL: https://uk.wikipedia.org/wiki/Інтернет_речей (дата звернення 03.07.2018).

14. Каплій О.В. Інтернет-видання ЗМІ як новий вид традиційних ЗМІ: поняття та сучасний стан конституційно-правового регулювання. Актуальні проблеми держави і права. 2011. Вип. 61. С. 227–235.

ІНФОРМАЦІЯ ПРО АВТОРА

Бугера Олена Іванівна – кандидат юридичних наук, доцент, доцент кафедри права Київського національного лінгвістичного університету

INFORMATION ABOUT AUTHOR

Buhera Olena Ivanivna – Candidate of Law Sciences, Associate Professor, Associate Professor at the Department of Law of Kiev National Linguistic University

sib22@ukr.net