КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.9
DOI https://doi.org/10.32838/TNU-2707-0581/2022.1/12

Бугера О.І.
Національний транспортний університет

СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ВИКОРИСТАННЯ НОВІТНІХ ІНТЕРНЕТ-ТЕХНОЛОГІЙ ДЛЯ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

У статті досліджено сучасний стан та проблеми використання інтернет-технологій для запобігання злочинності. Наголошено, що кримінологічні засади використання інтернет-технологій для запобігання злочинності полягають у задіянні суб'єктами запобіжної діяльності у системі заходів на загальнонаціональному, спеціально-кримінологічному та індивідуальному рівнях новітніх інформаційно-комунікаційних технологій з метою збору, зберігання, аналізу кримінологічно значимої інформації, прогнозування злочинності та протидії процесам її детермінації. З'ясовано, що основними проблемами, що перешкоджають ефективному використанню новітніх інтернет-технологій для запобігання злочинності в Україні, є такі: недостатній рівень технологічного оснащення правоохоронних органів; відсутність достатньої кількості фахівців, насамперед кримінологів-аналітиків, які б володіли необхідними методиками у сфері новітніх інформаційних технологій; недосконалість законодавчого забезпечення; недостатній рівень впровадження результатів кримінологічних досліджень та ін. Доведено, що ефективне запобігання злочинності в умовах активного розвитку інтернет-технологій можливе шляхом забезпечення на основі наукових досліджень постійної технологічної переваги правоохоронних органів над злочинцями, які використовують технологічний прогрес зі злочинною метою. Встановлено, що проведення досліджень з проблем використання інтернет-технологій для запобігання злочинності є сучасною тенденцією розвитку кримінологічної науки та сприяє підвищенню рівня ефективності запобіжної діяльності правоохоронних органів. Для законодавчого забезпечення цього процесу доцільним є розроблення та прийняття Стратегії запобігання злочинності з використанням інтернет-технологій та відповідного Плану заходів з її реалізації з відображенням шляхів вирішення проблем щодо технологічного переоснащення правоохоронних органів, підвищення професійного рівня їх працівників, створення баз даних кримінологічної інформації та забезпечення їх функціонування.

Ключові слова: *запобігання злочинності, кримінологічні засади, інтернет-технології, Стратегія запобігання злочинності, законодавче забезпечення.*

Постановка проблеми. Інтенсивний розвиток новітніх технологій у сфері комунікацій, глобальні інтеграційні процеси, становлення інформаційного суспільства викликають пильну увагу до можливостей впливу на індивідуальну і масову свідомість, актуалізують проблему правового регулювання суспільних відносин у галузі інформаційної політики. Практика правозастосування, законодавчі ініціативи значно відстають за часом від правової реальності, тому актуальними розробками сьогодні є дослідження у галузі «правова діяльність – інфотехнології». Особливо це стосується «високих», «нових», «критичних» технологій [1, с. 6].

Впровадження сучасних інформаційних технологій у сфері економіки, управління, кредитно-банківській діяльності, стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет і спрощення доступу до неї широкого кола користувачів через персональні комп'ютери зумовило також поширення високотехнологічних злочинів – злочинів, пов'язаних з використанням високих інформаційних технологій [2, с. 302].

Отже, актуальним у найближчій перспективі є формування кримінологічних засад використання новітніх інформаційних технологій для запобігання злочинності. Тобто ідеться про якісні зміни у роботі суб'єктів запобіжної діяльності на основі високотехнологічних підходів до вирішення цього питання. Також важливим є законодавче забезпечення ефективності цього процесу.

Аналіз останніх досліджень і публікацій. Питання використання сучасних інтернет-технологій для запобігання та протидії злочинності, розслідування злочинів прямо чи опосередковано розглядали у своїх наукових працях такі вчені, як В.О. Біляєв, Р.І. Благута, М.В. Карчевський, В.В. Клюс, А.В. Мовчан, С.В. Пеньков, П.С. Романько, С.А. Сумський, В.В. Шендрик, І.А. Юрій. Водночас технологічні досягнення (зокрема, на основі можливостей мережі Інтернет), що можуть бути задіяні для запобігання злочинності, потребують постійного моніторингу та наукового обґрунтування щодо їх використання з точки зору кримінологічної науки.

Метою статті є дослідження сучасного стану та проблем використання новітніх інтернет-технологій для запобігання злочинності та формування рекомендацій щодо удосконалення законодавства з цього питання.

Виклад основного матеріалу. Інтернет-технології – це комунікаційні, інформаційні та інші технології і сервіси, ґрунтуючись на яких здійснюється певна діяльність в мережі Інтернет [3]. Загалом сфера високих інформаційних технологій розглядається як сукупність галузей людської діяльності, інформаційні процеси в яких реалізуються методами автоматизованої обробки даних на основі використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних мереж. При цьому злочини у сфері високих інформаційних технологій слід розглядати як злочинні дії, в якості засобів і знарядь учинення яких використовувалися методи автоматизованої обробки інформації, засновані на використанні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. До найбільш характерних рис злочинності у сфері високих інформаційних технологій можна віднести такі: високу технічну озброєність злочинців; високий рівень латентності; використання в якості знарядь злочину інформаційних і телекомунікаційних технологій; електронне середовище як місце вчинення злочину; транскордонність; організований характер [2, с. 302–304].

Відповідно до звіту Національної поліції України про результати роботи у 2020 році [4] впродовж звітного року було зареєстровано понад 5 тисяч кіберзлочинів, у яких вдалося оперативно затримати 106 фігурантів кримінальних проваджень. Шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, розповсюдження комп'ютерних вірусів, онлайн-торгівля наркотиками та зброєю, викрадення інформації – це далеко не повний перелік злочинів, які розкриває кіберполіція. Крім того, у кіберполіції у 2020 році запрацювала сервісна служба. Вона створена для надання громадянам консультацій з питань кібербезпеки. За 9 місяців її роботи надійшло понад 100 тисяч дзвінків та понад 40 тисяч електронних звернень. Загалом протягом 2020 року поліція зареєструвала понад 335 тисяч кримінальних правопорушень, з яких було розкрито майже 164 тисячі. Пріоритетом у роботі поліції залишається протидія організованій злочинності, бо саме ці устатковані кримінальні елементи глобально впливають на криміногенну ситуацію в країні. У 2020 році поліція знешкодила 353 організованих групи (у 2019 році – 275). До кримінальної відповідальності притягнуто майже півтори тисячі учасників цих груп, які скоїли понад 3,5 тисяч злочинів, 500 осіб узято під варту.

Отже, існує нагальна необхідність в удосконаленні заходів щодо запобігання злочинності на основі технологічного переоснащення правоохоронних органів. При цьому високотехнологічні підходи до запобігання злочинності є сучасною тенденцією розвитку кримінологічних досліджень у світі за принципом «технологічні інновації повинні бути максимально використані суб'єктами запобіжної діяльності та одночасно зводити до мінімуму можливість використання цих інновацій зі злочинною метою». Зокрема, використання сучасних інформаційно-комунікаційних технологій (зокрема, інтернет-технологій) надає суттєві переваги поліції у практичній роботі щодо підвищення рівня оперативного реагування, здійснення кримінологічного аналізу інформації та прогнозування злочинності, забезпечення кібербезпеки тощо.

У Стратегії кібербезпеки України [5] вказується, що XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз зростає. Ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту протягом найближчого десятиліття посилюватиметься. Зростає технічний рівень реалізації кіберзагроз,

постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики щодо їхньої протидії. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору і передбачаючи нові можливості для цифровізації всіх сфер суспільного життя. Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі.

Також у Стратегії боротьби з організованою злочинністю [6] вказується, що з метою наукового забезпечення боротьби з організованою злочинністю передбачається, зокрема, проведення інженерно-технічних робіт, дослідно-конструкторських розробок, а також створення апаратних і програмних комплексів для виконання завдань щодо боротьби з організованою злочинністю. При цьому одним з пріоритетів розвитку системи кадрового забезпечення державних органів, що беруть участь у боротьбі з організованою злочинністю, є підвищення рівня спеціалізації, фахової підготовки та перепідготовки кадрів, діяльність яких безпосередньо пов'язана з протидією організованій злочинності.

Необхідно зазначити, що кримінологічні засади використання інтернет-технологій для запобігання злочинності полягають у задіянні суб'єктами запобіжної діяльності у системі заходів на загальнонаціональному, спеціально-кримінологічному та індивідуальному рівнях сучасних інформаційно-комунікаційних технологій з метою збору, зберігання, аналізу кримінологічно значимої інформації, прогнозування злочинності та протидії процесам її детермінації, ресоціалізації потенційних злочинців. Основними інтернет-технологіями щодо запобігання злочинності є такі: технології великих даних (Big Data Technologies), технології Інтернету речей (Internet of Things Technologies), хмарні технології (Cloud Technologies), технологія QR-кодів (QR code technology) та ін.

Серед високотехнологічних розробок, які вже практично використовуються для протидії злочинності, можна виділити такі: обробку кримінологічних даних з використанням технологій великих даних для прогнозування злочинності та створення інтернет-карт злочинів в онлайн-режимі; використання віртуальної реальності для відтворення окремих епізодів злочину та дорожньо-транспортних пригод; підвищення рівня аналізу кримінологічної інформації патрульними поліцейськими з використанням хмарних технологій; використання технології сканування QR-кодів для підвищення рівня комунікації як в системі правоохоронних органів (в т. ч. і для контролю процесу патрулювання житлових кварталів або певної території), так і з громадськістю з питань запобігання злочинності (зокрема, для оперативного повідомлення громадянами інформації в онлайн-режимі про вчинені злочини або щодо осіб, що знаходяться у розшуку).

Як показує зарубіжний досвід, у практичній діяльності правоохоронних органів також передбачається використання технологій Інтернету речей. Ідеться про таке: методику розпізнавання обличчя за допомогою камер високої роздільної здатності з використанням штучного інтелекту; роботизовані комплекси для усунення терористичних загроз, забезпечення візуального та аудіоспостереження за потенційно небезпечними ситуаціями та для вирішення інших оперативних задач; використання безпілотних літальних апаратів (дронів) для отримання інформації з місця злочину, проведення пошуково-рятувальних робіт, моніторингу натовпу тощо (деякі з найскладніших моделей дронів можуть бути оснащені програмним забезпеченням для тепловізійних зображень або 3D-картографування) [7].

Загалом використання дронів як елементу Інтернету речей, оснащених тепловізорами, дозволяє вести ефективний нагляд навіть уночі. При цьому спроможність оптичних камер дронів надвисокої роздільної здатності дозволяє робити високоякісні фото і відео, на яких можна розглянути найдрібніші деталі, наприклад, автомобільні номери на машині злочинця або навіть татуювання на його руці. Одним з найбільш перспективних напрямів використання дронів є охорона правопорядку в неблагополучних районах сучасних мегаполісів, куди звичайному поліцейському небезпечно заходити без прикриття спецназу. Передбачається, що в майбутньому дрони,

оснащені нелетальною зброєю, допомагатимуть поліцейським під час припинення масових вуличних заворушень [8].

Основними проблемами, що перешкоджають ефективному використанню новітніх інтернет-технологій для запобігання злочинності в Україні, є такі: недостатній рівень технологічного оснащення правоохоронних органів; відсутність достатньої кількості фахівців, зокрема кримінологів-аналітиків, які б володіли необхідними методиками у сфері новітніх інформаційних технологій; недосконаліть законодавчого забезпечення; недостатній рівень впровадження результатів кримінологічних досліджень та ін.

З огляду на це необхідно погодитись з О.М. Бандуркою та О.М. Литвиновим щодо уповільнення розвитку кримінології. Така ситуація стала, на думку авторів, наслідком дії кількох чинників. По-перше, тривалий час лави кримінологів недостатньо поповнюються вченими, здатними забезпечити новий виток у розвитку цієї науки, запропонувати нові ідеї, змінити усталені підходи до вирішення наукових проблем. По-друге, сучасні кримінологічні дослідження здебільшого базуються на поглядах, вироблених старою школою, їх відрізняє консервативність і статичність. Нові досягнення в суміжних галузях знань (технічних, природних) важко приймаються і використовуються в кримінології. По-третє, кримінологія відхилилася від свого первісного призначення – вивчення причин і умов злочинності та розробки програм боротьби з нею з метою подальшої практичної реалізації [9, с. 26].

Отже, доцільність розширення кримінологічних досліджень з питань формування кримінологічних засад щодо використання інтернет-технологій для запобігання злочинності визначається, зокрема, загальними процесами цифровізації економіки та суспільства, переходом до активного використання інноваційних інформаційно-комунікаційних технологій у практичній роботі суб'єктів запобіжної діяльності у розвинених країнах світу.

Зокрема, на чотирнадцятому конгресі Організації Об'єднаних Націй із попередження злочинності та кримінального правосуддя (м. Кіото, 7–12 березня 2021 р.) була прийнята Кіотська Декларація, що окреслює шляхи вирішення проблем у цих сферах на період до 2030 року. У Декларації, зокрема, вказується на загрозливі тенденції поширення транснаціональної організованої злочинності. При цьому злочинці все частіше використовують новітні технології (у тому числі й на основі мережі Інтернет) для здійснення своєї незаконної діяльності, створюючи безпрецедентні виклики щодо запобігання злочинності. Отже, передбачається посилення координації та міжнародного співробітництва з питань запобігання та протидії кіберзлочинності. Також вказується на необхідність постійного технологічного переоснащення правоохоронних органів для підвищення рівня запобіжної діяльності [10].

Висновки. Отже, можна зробити висновок, що ефективне запобігання злочинності в умовах активного розвитку інтернет-технологій можливе у разі постійної технологічної переваги правоохоронних органів над злочинцями, які використовують технологічний прогрес зі злочинною метою. Тобто ідеться про високотехнологічний підхід до запобігання злочинності, що є сучасною тенденцією розвитку кримінологічної науки та забезпечує підвищення рівня ефективності запобіжної діяльності правоохоронних органів шляхом використання інформаційно-комунікаційних технологій для збору, обміну, аналізу, зберігання, картографування кримінологічної інформації, прогнозування злочинності, розроблення заходів щодо її запобігання на загальносоціальному, спеціально-кримінологічному, індивідуальному рівнях. Для законодавчого забезпечення цього процесу доцільним є розроблення та прийняття Стратегії запобігання злочинності з використанням інтернет-технологій та відповідного Плану заходів з її реалізації з відображенням шляхів вирішення проблем щодо технологічного переоснащення правоохоронних органів, підвищення професійного рівня їх працівників, створення баз даних кримінологічної інформації та забезпечення їх функціонування.

Список літератури:

1. Синєокий О.В. Високотехнологічне інформаційне право України : навчальний посібник. Харків : Право, 2010. 360 с. URL: http://library.nlu. edu.ua/poln_text/posibniki_2011/Posib_Sineokiy_2010.pdf (дата звернення: 10.01.2022).

2. Бутузов В.М. Співвідношення понять «комп'ютерна злочинність» і «злочинність у сфері високих інформаційних технологій». *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. Вип. 23. С. 302–307. URL: http://nbuv.gov.ua/UJRN/boz_2010_23_36 (дата звернення: 10.01.2022).

3. Сучасні інтернет-технології. URL: https://sites.google.com/site/internettehnologiiecom/sucasni-internet-tehnologiie (дата звернення: 10.01.2022).

4. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf (дата звернення: 10.01.2022).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 10.01.2022).

6. Про схвалення Стратегії боротьби з організованою злочинністю : Розпорядження Кабінету Міністрів України від 16 вересня 2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text (дата звернення: 10.01.2022).

7. Fritsvold E. 10 Innovative Police Technologies. URL: https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/ (дата звернення: 10.01.2022).

8. Высокотехнологичная борьба с преступностью. URL: https://www.dronarium.com.ua/uslugi/specsluzhby/ (дата звернення: 10.01.2022).

9. Бандурка О.М., Литвинов О.М. Про кримінологічні інновації та деякі невтішні результати їх упровадження (с. 25–27). *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації* : збірник тез доповідей науково-практичної конференції, м. Харків, 16 квітня 2021 р. Харків : ХНУВС, 2021. 464 с. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/10418/Zlochynnist%20i%20protydiia%20yii%20v%20umovakh%20synhuliarnosti_2021.pdf?sequence=1&isAllowed=y (дата звернення: 10.01.2022).

10. Kyoto declaration on advancing crime prevention, criminal justice and the rule of law: towards the achievement of the 2030 agenda for sustainable development. URL: https://www.unodc.org/documents/commissions/Congress/21-02815_Kyoto_Declaration_ebook_rev_cover.pdf (дата звернення: 10.01.2022).

Bugera O.I. CURRENT STATUS AND PROBLEMS OF USING THE LATEST INTERNET TECHNOLOGIES TO PREVENT CRIME

The article examines the current state and problems of using Internet technologies to prevent crime. It is emphasized that the criminological principles of using Internet technologies to prevent crime are to involve the subjects of preventive activities in the system of measures at the national, special criminological and individual levels of the latest information and communication technologies to collect, store, analyze criminologically relevant information, predict crime and counteracting the processes of its determination. The main Internet technologies for crime prevention are: big data technologies, Internet of Things technologies, cloud technologies; QR-code technology, etc. It was found that the main problems hindering the effective use of the latest Internet technologies to prevent crime in Ukraine are: insufficient level of technological equipment of law enforcement agencies; lack of a sufficient number of specialists, first of all, criminologists-analysts, who would have the necessary methods in the field of the latest information technologies; imperfection of legislative support; insufficient level of implementation of criminological research results, etc. It is proved that effective crime prevention in the conditions of active development of Internet technologies is possible by providing on the basis of scientific research a permanent "technological advantage" of law enforcement agencies over criminals who use technological progress for criminal purposes. It is established that conducting research on the problems of using Internet technologies to prevent crime is a current trend in the development of criminological sciences and, accordingly, contributes to improving the effectiveness of law enforcement prevention activities. To ensure the legislative support of this process, it is advisable to develop and adopt a Strategy for the Prevention of Crime with the Use of Internet Technologies and a corresponding Action Plan to reflect ways to solve problems of technological re-equipment of law enforcement agencies, improve the professional level of their employees. functioning.

Key words: *crime prevention, criminological principles, Internet technologies, crime prevention strategy, legislative support.*