САМОЙЛЕНКО ОЛЕНА АНАТОЛІЇВНА

Національний університет «Одеська юридична академія»,
професор кафедри криміналістики,
доктор юридичних наук, доцент

СТАУРСЬКА ОЛЕКСАНДРА МИКОЛАЇВНА

Національний університет «Одеська юридична академія»,
аспірант кафедри криміналістики

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ: ІННОВАЦІЙНІ ЗАСОБИ КРИМІНАЛІСТИЧНОЇ ПРОФІЛАКТИКИ

Традиційно в криміналістичній літературі профілактика злочинів зводиться до оснащення суб'єкта виявлення та розслідування технічними та організаційними можливостями протидії злочинам, а також забезпечення процесуального документування результатів розслідування шляхом умілого використання тактичних і методичних рекомендацій криміналістики. Останнє власно виступає надійним та доступним засобом подолання можливих спроб протидії розслідуванню з боку зацікавлених осіб. Враховуючи темпи інформатизації сучасного суспільства та зумовлене цим закономірне збільшення рівня злочинності у кіберпросторі, не можна залишитись осторонь питань протидії кібрзлочинам в цілому та інноваціям у сфери криміналістичної профілактики кіберзлочинів зокрема.

В цілому складність механізму вчинення конкретного виду кіберзлочину зумовлюється певними чинниками, зокрема: 1) терміном реагування на звернення та повідомлення про кіберзлочини; 2) рівнем кібербезпеки держави; 3) ступенем «комп'ютерної безграмотності» потенційних жертв злочинів; 4) темпами усунення недоліки в роботі правоохоронних органів. В цьому сенсі звернемо увагу на запропоновані Національною поліцією України профілактичні заходи спрямовані на протидію кібрзлочинам.

Особливо важливим в цілях профілактики кіберзлочинів є зменшення часу реакції Національної поліції України на вхідну інформацію про кримінальне правопорушення. Тому в 2017 році на базі Департаменту кіберполіції було створено цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються в Інтернет [1]. За допомогою цієї технології громадяни отримують необхідну допомогу від працівників кіберполіції не пізніше ніж за три години після надходження звернення [1]. Важливо зауважити, що у випадку надходження до «call-центру» інформації, що не відноситься до компетенції кіберполіції, вона автоматично перенаправляється до іншого підрозділу поліції.

Високий рівень кібербезпеки України планується досягти шляхом створення спеціалізованих підрозділів кібербезпеки у кожному державному органі та установі. Також надання партнерами інформаційно-

консультативної підтримки та застосування міжнародної кооперації дозволить вдосконалити механізм протидії існуючим та потенційним загрозам кібербезпеки, зокрема глобальним. Саме тому 25 вересня 2020 року Міністерство внутрішніх справ спільно із Міністерством цифрової трансформації України цифри, Радою національної безпеки і оборони України та ГК «Нафтогаз України» на першій конференцію щодо цифрової трансформації держави презентували створення на базі Глобального центру взаємодії в кіберпросторі інтеграційного майданчика, який повинен об'єднати усіх ключових гравців та забезпечить максимальну ефективність української системи безпечного кіберпростору, та як логічний наслідок – посилення системи Національної безпеки України.

На зниження ступеню «комп'ютерної безграмотності» потенційних жертв злочинів впливатиме діяльність Національної поліції з виявлення та прогнозування можливих кіберзагроз, у тому числі з використанням штучного інтелекту.

Згідно із нещодавно схваленою Кабінетом Міністрів України Концепцією розвитку штучного інтелекту в Україні, штучний інтелект – це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [2]. Серед напрямків впровадження технологій штучного інтелекту слід звернути увагу на сферу освіти, кібер- та інформаційної безпеки. Для досягнення мети Концепції у сфері освіти планується забезпечити виконання такого завдання як поширення цифрової грамотності серед школярів та абітурієнтів (застосування цифрових інструментів для розв'язання прикладних задач, пошук інформації в Інтернеті, захист персональних даних, медіаграмотність, цифрова гігієна тощо); у сфері кібербезпеки – розробити та впровадити у практику правоохоронних органів інноваційні системи кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання. Отже, мова йде по суті про активне впровадження у практику правоохоронних органів інформаційно-аналітичних комплексів, що об'єднуватимуть в єдиному інформаційному просторі основні та найсучасніші методи і методики аналізу та аналітичного пошуку в реальному часі.

Так, наприклад, сьогодні активно впроваджується в практику роботи Головних управлінь Національної поліції в областях України відеоаналітична платформа «Vezha» [3], будучи спрямованою на розпізнавання об'єктів, номерних знаків транспорту, обличчя людини вона прискорить процес отримання, обробки та зберігання даних, користуватися якими зможе кожний поліцейський в своїй роботі задля забезпечення громадської безпеки та пошуку розшукуваних осіб та транспорту в місті та області.

Впровадження інтелектуальної системи кримінального аналізу «RICAS» дозволяє значно підвищити ефективність і результативність розкриття злочинів по гарячих слідах і нерозкритих раніше злочинів. Цей інформаційно-аналітичний комплекс об'єднує в єдиному просторі методи і методики кримінального аналізу та аналітичного пошуку. RICAS дозволяє виконувати наступні види аналізу: аналіз кримінального стану; аналіз загального профілю; аналіз конкретного розслідування; порівняльний аналіз; аналіз групової злочинності; аналіз особливостей профілю; аналіз розслідувань [4]. По-суті цей комплекс дозволяє суттєво підвищити якість та своєчасності управлінських рішень керівників підрозділів Національної поліції, що позитивно впливатиме й на темпи усунення недоліки в роботі правоохоронних органів в цілому.

Отже, профілактика кіберзлочинів криміналістичними засобами та методами зводиться сьогодні не тільки до вивчення причин та умов вчинення злочинів та узагальнення останніх, а також й до розробки та використання засобів, прийомів та методів, спрямованих на ускладнення злочинної діяльності у кіберпросторі та полегшення виявлення вчинюваних у кіберпросторі злочинів і розкриття злочинів.

Список використаної літератури:

1. Кіберполіція впровадила нові шляхи оперативного реагування на кіберзлочини, URL: https://www.kmu.gov.ua/news/250050267
2. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінета міністрів України від 2 грудня 2020 р. за № 1556-р URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
3. Офіційний портал Вінницької обласної державної адміністрації. Впровадження штучного інтелекту. URL: http://www.vin.gov.ua/news/ostanni-novyny/34089-vpershe-v-ukraini-hu-natsionalnoi-politsii-u-vinnytskii-oblasti-zaprovadzhuie-v-svoiu-robotu-bezpekovyi-proiekt-vezha-v-osnovi-iakoho-lezhyt- vykorystannia-shtuchnoho-intelektu
4. Про допомогу штучного інтелекту у запобіганні та виявленні злочинів URL: https://nure.ua/pro-dopomogu-shtuchnogo-intelektu-u-zapobiganni-ta-vijavlenni-zlochiniv

Ключові слова: кіберзлочини, криміналістичні засоби, криміналістична профілактика.

Ключевые слова: киберпреступления, криминалистические средства, криминалистическая профилактика.

Key words: cybercrimes, forensic tools, forensic prevention.