САМОЙЛЕНКО ОЛЕНА АНАТОЛІЇВНА

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

СТАУРСЬКА ОЛЕКСАНДРА МИКОЛАЇВНА

Національний університет «Одеська юридична академія», аспірантка кафедри криміналістики

КОМПЛЕКС ПРОБЛЕМ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ В УКРАЇНІ: ПРИКЛАДНИЙ АСПЕКТ

26 серпня 2021 року Указом Президента України № 447 /2021 було введено нову Стратегію кібербезпеки України, яка вперше отримала назву «Безпечний кіберпростір – запорука успішного розвитку країни», вона містить параграфи присвячені не тільки засадам подальшої розбудови національної системи кібербезпеки України, її пріоритетним стратегіям та цілям цієї сфери, а також параграф, в якому визначені результати реалізації першої Стратегії кібербезпеки України від 15 березня 2016 року, зокрема й щодо протидії кіберзлочинам. Так, стан реалізації першої Стратегії був оцінений як такий, що не перевищує 40 відсотків від запланованого результату.

Аналізуючи наявні повні річні звіти за останні три роки, а також сучасний стан забезпечення в Україні безпечного, стабільного і надійного кіберпростору можна сформулювати такі положення.

По-перше, питома вага обліковуваних НП України кіберзлочинів порівняно із загально кримінальною злочинністю є незначною, але прослідковується тенденція до її збільшення. При цьому спостерігається неоднакова динаміка розвитку різних видів кіберзлочинів. Тож, збір, оброблення, узагальнення та аналіз інформації з метою протидії кіберзлочинності повинні відбуватися не тільки в умовах дотримання високого рівні звітно-реєстраційної дисципліни, а також адекватного відображення структури кіберзлочинності.

По-друге, на кінець звітних років суттєво зменшується кількість кримінальних правопорушень, по яким досудове розслідування закінчується. При цьому показники ефективності діяльності Департаменту кіберполіції Національної поліції України свідчать про щорічне збільшення навантаження на підрозділи кіберполіції, що свідчить про необхідність розроблення стандартів, спрямованих на збільшення ефективності системи документування кіберзлочинів.

По-третє, заходи заплановані щодо забезпечення в Україні безпечного, стабільного і надійного кіберпростору реалізації протягом п’яти років почали впроваджуватися у життя суспільства лише нещодавно, на межі 2020-2021 рр., що свідчить про запізнілу реакцію окремих суб’єктів національної системи кібербезпеки та необхідність активізації вказаного процесу.

З одного боку активно створюються та модернізуються органи забезпечення кіберзахисту (на рівні різних відомств – центри забезпечення кібербезпеки або кіберзахисту). Так, 31 травня 2021 р. відбулося відкриття Кіберцентру UA30. У Кіберцентрі UA30 розміщується урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, єдина команда з України, що має акредитацію у FIRST та може оперативно взаємодіяти з 571 командою реагування з 96 країн світу, та Тренінговий кіберцентр. Платформа Тренінгового кіберцентру забезпечує моделювання реальних атак на інфраструктуру, яка складається з інструментів, що імітують компоненти комунікаційних та технологічних систем. Сама урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) працює в рамках Державної служби спеціальногозв'язку та захисту інформації України в структурі Державний центр кіберзахисту. Також з 2017 році для поєднання та координації зусиль у сфері забезпечення кібербезпеки та кіберзахисту в банківському та фінансовому секторах України розпочав роюоту Центр кіберзахисту Національного банку України (НБУ). З 2018 року у складі Центру кіберзахисту функціонує команда реагування на кіберінциденти в банківській системі (CSIRT-NBU).

З іншого статистичний та якісний аналіз кіберзлочиннтсті дає можливість висновувати про те, що насьогодні актуальними в контекст протидії кіберзлочинності залишилися питання обміну інформацією про кіберзагрози між державними органами, в тому числі в контексті узгодження дій між правоохоронними і іншими органами різних держав покликаних забезпечити стабільність кіберпростору і кібербезпеку, розробки моделі державно-приватного партнерства з метою виявлення кіберзагроз й у приватному секторі, організації і проведення оперативно-розшукової профілактики у сфері протидії кіберзлочинам. Також існують проблеми комплексного використання сил і засобів усіх органів та підрозділів поліції під час розслідування та розкриття кіберзлочинів (актуалізуючись на конкретних суб'єктах взаємодії в кожному різновиді кіберзлочину). Для забезпечення ефективного функціонування та розвитку системи виявлення і досудового розслідування кримінальних правопорушень, судового провадження у зазначеній сфері постає питання організації:

- оперативного обміну інформації між компітентними правоохоронними органами у сфері протидії кібрзлочинам;
- моніторингу кіберзагроз з метою виявлення фактів підготовки до вчинення кримінальних правопорушень;
- комплексного ефективного використання компетентними органами, задіяними у системі протидії кіберзлочинів, інформації про підозрілі інциденти у кіберпросторі, отриманої в тому числі від міжнародних партнерів;
- запобігання використанню суб'єктів господарювання, зокрема підприємств, діяльність яких має ознаки фіктивності, правових утво-

рень, некомерційних та благодійних організацій у схемах виводу коштів від кіберзлочинів;

- реалізації принципу невідворотності покарання та застосування у судовому порядку ефективних та пропорційних санкцій, конфіскації доходів, одержаних злочинним шляхом;
- тісного національного та міжнародного співробітництва у зазначеній сфері.

Ключові слова: кіберзлочинність, показник, протидія, статистичні відомості.
Key words: cybercrimination, indicator, counteraction, statistical information.

ПЧОЛКІН ВАЛЕРІЙ ДМИТРОВИЧ

Харківський національний університет внутрішніх справ,
професор кафедри кримінального процесу, криміналістики та експертології,
доктор юридичних наук, професор

ОПЕРАТИВНО-РОЗШУКОВЕ ЗАБЕЗПЕЧЕННЯ В СТРУКТУРІ МЕТОДИКИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Криміналістична методика є важливим і невід'ємним інструментом діяльності органів досудового розслідування, оскільки вона розробляє найбільш раціональні й оптимальні способи розслідування окремих видів кримінальних правопорушень. Удосконалення криміналістичної методики як системи знань і окремого розділу криміналістики має відбуватися через узагальнення та філософське осмислення накопиченого емпіричного матеріалу, пізнання наукових фактів, що належать як до злочинної діяльності, так і до сфери протидії злочинності. Для того, щоб вона повною мірою виконувала поставлене перед нею завдання, її структура має бути логічною й відповідати основним методологічним засадам. У зв'язку із цим питання удосконалення структури методики розслідування вважаємо важливим і актуальним.

Слід зазначити, що загальні положення криміналістичної методики, у тому числі питання змісту структури окремих методик розслідування злочинів, неодноразово були предметом дослідження українських науковців Л. І. Аркуші, А. Ф. Волобуєва, В. А. Журавля, В. О. Малярової, Р. Л. Степанюка, В. В. Тищенка, О. В. Федосової, С. С. Чернявського, В. М. Шевчука, В. Ю. Шепітька, Б. В. Щура та інших. У сучасній криміналістичній літературі більшість учених трактує криміналістичну методику як систему наукових положень і розроблюваних на їх основі рекомендацій щодо організації і здійснення розслідування та запобігання окремим видам кримінальних правопорушень. Слід звернути увагу на те, що незважаючи на низку важливих напрацювань в окресленій царині, у змісті структури методики неоднозначно трактуються питання