УДК 343.98

Галина Костянтинівна Авдєєва,
кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (м. Харків)

Проблеми застосування інноваційних продуктів у протидії кіберзагрозам

За допомогою інформаційно-комунікаційних технологій та програмно-апаратних засобів в усьому світі щороку вчиняються десятки тисяч злочинів. Генеральний секретар ООН Антониу Гуттереш зазначає, що щорічні збитки від кіберзлочинності у світі складають 1,5 трлн доларів. Не зважаючи на те, що у статистичних звітах Генеральної прокуратури рівень злочинності щороку знижується, у 2018 р. в Україні кіберзлочинів зафіксовано у 10 разів більше, ніж у 2017 р. Правопорушники використовують новітні науково-технічні засоби та інноваційні продукти не лише як предмет злочину, а й як засіб його підготовки та вчинення.

Останніми роками великі державні і приватні установи України і інших країн неодноразово потерпали від кібератак. Яскравим прикладом слугує розповсюдження вірусу Petya влітку 2017 року, через який було тимчасово заблоковано роботу аеропорту «Бориспіль», «Ощадбанку», «Укртелекому», «Укрпошти», «Укрзалізниці» та низки інших державних і приватних установ. Частково пошкоджена інформація в інформаційних системах Кабінету Міністрів, окремих міністерств і навіть кіберполіції. Це обумовлює необхідність використання адекватних засобів протидії кіберзлочинності – інноваційних продуктів у вигляді стандартного і спеціального програмного забезпечення, сучасних програмно-апаратних приладів і систем, а також методів їх застосування.

Вчені-криміналісти та експерти з кібербезпеки вважають, що в майбутньому кіберзагрози посиляться, а кількість злочинів та збитків від кібератак зростатиме тому, що правопорушники спочатку використовують певні інноваційні продукти для вчинення злочину, а лише після цього розробляються і застосовуються відповідні механізми щодо їх запобігання і розкриття. Тобто, кіберзлочинці завжди випереджають осіб, які їм протидіють.

Правова основа кібернетичної безпеки в Україні складається з відповідних норм Конституції України, Кримінального кодексу України, законів України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та ін., Доктрини інформаційної безпеки України, Конвенції Ради Європи про кіберзлочинність та інших міжнародних нормативно-правових актів, ратифікованих Верховною Радою України.

Реалізацію державної політики у сфері боротьби з кіберзлочинністю здійснює низка державних органів, а саме: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених державних органів створено відповідні підрозділи, співробітники яких постійно підвищують свою кваліфікацію. Зокрема, у 2016–2017 рр. співробітники Департаменту кіберполіції пройшли курси з підвищення кваліфікації на базі Харківського національного університету внутрішніх справ та взяли участь у тренінгах за участі експертів Великої Британії.

Протягом 2018 року працівники Департаменту кіберполіції України викрили більше 800 осіб, які були причетні до вчинення злочинів, що вчинялися з використанням інформаційних технологій. Найбільше виявлено правопорушників, які вчиняли злочини за допомогою вірусних програм, придбаних через анонімну «мережу» DarkNet. Однак, виходячи з показників роботи кіберполіції України у 2018 р., відсоток розкритих злочинів, що вчиняються з використанням інформаційних технологій, є не досить високим. Однією з причин такого становища є проблеми впровадження інноваційних продуктів у роботу органів правопорядку.

На шляху впровадження інновацій у практику боротьби з кіберзлочинністю існує низка перешкод, а саме: недостатність знань співробітників слідчих органів в даній галузі і відсутність можливості їх отримати, професійна деформація або неправильне відношення до всього нового, передового та ін. Гальмують впровадження інновацій у діяльність органів правопорядку також втрата професійного ядра співробітників слідчого апарату і оперативних підрозділів органів внутрішніх справ, недостатність наявних тактичних засобів здійснення слідчої діяльності, недостатнє бюджетне фінансування процесів розроблення і впрова-

дження інновацій; наявність складнощів у залученні кваліфікованих ІТ-спеціалістів до участі у слідчих діях; проблеми взаємодії слідчого з обізнаними особами; недостатність інформації про розслідувану подію; недостатність надійних джерел отримання інформації; наявність протидії розслідуванню з боку зацікавлених осіб та ін. Більше того, в усіх країнах світу існують проблеми визнання «цифрових» доказів судом через їх неналежну фіксацію.

Подолання існуючих проблем застосування інноваційних продуктів у протидії кіберзагрозам є можливим за умови системної державної підтримки, яка передбачатиме тісну співпрацю розробників і користувачів інноваційних продуктів та державне фінансування процесів розроблення і впровадження інновацій в практику боротьби з кіберзлочинністю.

Одержано 19.10.2019