стабільне становище громадянського суспільства і окремих громадян особисто. Авторами обґрунтовується необхідність реалізації кримінологічної політики в сучасних умовах, які характеризуються постійними кризовими ситуаціями, саме з позицій системності для досягнення синергетичного ефекту і максимальної користі для громадянського суспільства.

Література

1. Иншаков С.М. Исследование преступности. Проблемы методики и методологии: монография. Москва: ЮНИТИ-ДАНА: Закон и право, 2012. 335 с.

2. Голіна В.В. Криміногений потенціал суспільства: поняття, зміст, форми реалізації. Проблеми законності: зб. наук. пр. / відп. ред. В.Я. Тацій. Харків: Нац. ун-т «Юрид. акад. України ім. Ярослава Мудрого», 2012. Вип. 119. С. 166–176.

3. Голіна В.В., Колодяжний М.Г. Кримінологічна політика України: сутність та передумови її формування. Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В.І. Борисов та ін. Харків: Право, 2012. Вип. 23. С. 53–63.

УДК 343.9.01:004(477)(043.2)

Малій М.І., директор,
Правнича компанія АЮР-КОНСАЛТИНГ, м. Київ, Україна

ЕЛЕКТРОННА КІБЕРЗЛОЧИННІСТЬ ЯК ОБ'ЄКТ КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ

Розвиток наукових досягнень у новому тисячолітті засвідчує, що особливо небезпечним сьогодні є можливість використання кримінальними угрупуваннями електронного інтелекту в злочинних цілях. Зокрема, англійські та американські вчені справедливо стверджують, що електронний інтелект у найближчому майбутньому може стати небезпечною зброєю в руках кібершахраїв, кібертерористів та кіберзлочинців. Про ці загрози, виклики і небезпеки зазначено в опублікованому днями стосторінковому дослідженні The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Тому очевидно, що постає справедливе запитання так в чому ж саме полягає реальна загроза світові з боку електронного інтелекту і як цьому реально зарадити?

Звіт, у якому висвітлюються реальні загрози електронного інтелекту для людства, був підготовлений групою із 26 провідних дослідників електронного інтелекту – відомих вчених Кембриджського, Оксфордського і Стенфордського університетів, а також експертів Electronic Frontier Foundation та OpenAI та представників інших авторитетних дослідницьких відомств, установ і організацій.

Реальна небезпека для електронної цивілізації полягає в тому, що сучасні можливості використання електронного інтелекту в освіті, науці і практиці стають більш могутніми, широкомаштабними і потужними. У зазначеному вище дослідженні визначаються три основні напрями, для яких існує найбільше викликів, ризиків, загроз і небезпек – це цифрова (електронна) безпека, фізичні об'єкти та політична сфера.

Так у чому все ж таки полягає реальна небезпека для електронної цивілізації? Фахівці стверджують, що електронний інтелект, потрапивши в руки зловмисників, може фактично знизити, а інколи можливо і знищити реально створені захисні безпекові перешкоди, перепони для проведення руйнівних хакерських атак.

Відомо, що сучасні ноозасоби і ноотехнології електронного інтелекту вже сьогодні можуть виявити критичні помилки і недоліки програмного забезпечення та швидко вибирати потенційних жертв для скоєння різного роду фінансових та економічних злочинів. Більше того, ноозасоби електронного інтелекту можуть сприяти використанню соціальної інженерії як методу кібератаки. Це обумовлено тим, що «інформація, отримана з інтернету про персональні дані тієї чи іншої людини, може бути використана для автоматизованого створення шкідливих сайтів/посилань чи електронних листів, на які, швидше за все, відповідатиме потенційна жертва, адже вони надходитимуть вірогідно від справжніх людей та імітуватимуть їхній стиль спілкування», – стверджують фахівці, які підготували даний звіт.

Іншою реальною небезпекою в кіберпросторі, яка з'являється на горизонті, є можливість кібератаки на фізичні об'єкти. Автори звіту справедливо попереджають, що ноозасоби електронного інтелекту можуть безперешкодно проникати як у системи безпілотних автомобілів, так і безпілотних літаків, поїздів, кораблів, реально управляти ними та призводити по спеціальному коду для розкрадання майна, ресурсів, коштів, і до аварій та катастроф. Ще одним прикладом може бути використання «армій дронів», які за допомогою технології розпізнавання обличчя можуть вбивати людей, наголошується у дослідженні. Отже існує реальна загроза створення роботів-убивць.

Таким чином, швидкий розвиток індустрії електронного інтелекту засвідчує, що сьогодні це уже не просто науково-фантастична літературна історія-передбачення, а дійсно створена реальність, тобто конкретна технологічна небезпека і загроза цивілізаційного розвитку. Очевидно, що це все зобов'язує відповідні установи кібербезпеки уже сьогодні приступити до розробки стратегії, тактики і мистецтва поведінки в таких ситуаціях, а також дослідження портрета і профіля електронного зловмисника [1, с. 21].

На завершення слід зазначити, що очевидно сформулювати реальний подальший чіткий розвиток сценаріїв використання можливостей

космічного кіберпростору і електронного інтелекту в злочинних цілях сьогодні складно. Водночас, важливо уже сьогодні відповідним державним органам, освітнім та науковим установам приступити до розробки та реалізації на практиці наступних стратегічних кроків і прийняття управлінських тактичних рішень, а саме:

– створити чітку і надійну безпекову міждержавну правову базу можливостей використання космічного простору і електронного інтелекту в освітній, науковій і праксеологічній діяльності з метою запобігання і протидії можливим кіберзагрозам, викликам і небезпекам;

– розробникам новітніх електронних ноозасобів, методів і технологій штучного інтелекту технологічно запобігти можливим загрозам неправомірного використання електронного інтелекту в різних сферах життєдіяльності;

– розробити впорядковану правову, організаційну і технологічну систему запобігання і протидії шкідливому використанню космічного простору і електронного інтелекту як на національному, так і на міждержавному (світовому) рівнях [2, с. 152, с. 197].

Література

1. Біленчук П.Д., Малій М.І. Кримінолого-криміналістичний портрет електронного зловмисника. Актуальні питання криміналістики та судової експертизи: матеріали Всеукр. наук.-практ. конф. (Київ, 19 лист. 2020 р.) / [редкол.: В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ: Нац. акад. внутр. справ, 2020. С. 21-23.

2. Електронне суспільство, електронне право, кібербезпека: стратегія розвитку інноваційної ери / П.Д. Біленчук, О.Л. Кобилянський, М.І. Малій, Р.В. Перелигіна, Т.Ю. Тарасевич [та ін.]. Київ: УкрДГРІ, 2020. С. 152-153, С. 197-200.

УДК 343.2/.7; 343.24/.29(043.2)

Марчук М.П., к.ю.н.,
Конституційний Суд України, м. Київ, Україна

ПРОБЛЕМНІ АСПЕКТИ ПОЛОЖЕНЬ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ЩОДО СПЕЦІАЛЬНОЇ КОНФІСКАЦІЇ

Розділ XIV Кримінального кодексу України [1] (далі – Кодекс) має назву «Інші заходи кримінально-правового характеру». Більшість його статей (92–96) стосуються примусових заходів медичного характеру. Зокрема, стаття 96 Кодексу містить положення стосовно примусового лікування. Водночас, статті 96-1 та 96-2 Кодексу дають розуміння суті спеціальної конфіскації, визначають підстави та випадки її застосування.

Із приводу викладеного, слід зазначити, що спеціальна конфіскація за