сучасності, інтеграція мотиваційного підходу в систему професійної підготовки майбутніх рятувальників має розглядатися не як побажання, а як необхідна стратегія формування людського ресурсу національної безпеки.

Список використаних джерел

1. Воловикова М. І. Психологія особистості: український погляд на формування мотиваційної структури. Київ: Видавничий дім «Слово», 2020. 220 с.
2. Занюк С. С. Психологія мотивації : навч. посіб. Київ : Либідь, 2002. 371 с.

Сергій ЗЕЛЕНСЬКИЙ,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

КІБЕРЗЛОЧИННІСТЬ ТА ПРОТИДІЯ ЇЙ НА МІЖНАРОДНОМУ РІВНІ

Кіберзлочинність визнається однією з найбільших загроз сучасного світу, оскільки охоплює широкий спектр злочинів, пов'язаних із використанням інформаційних технологій. В умовах глобалізації та цифровізації економіки злочинці отримують нові можливості для вчинення кримінальних протиправних діянь. Отже, потреба у ефективних механізмах протидії кіберзлочинності та у відповідь на виклики і загрози, що несе кіберзлочинність, міжнародна спільнота об'єднує зусилля для боротьби з цим явищем та зміцнення безпеки у інформаційнім світі.

Кіберзлочинність розглядаємо як суспільно небезпечне явище в інформаційному середовищі – сукупність злочинних дій, вчинених з використанням комп'ютерної техніки та мережевого обладнання. Здійснюючи свої дії, кіберзлочинці використовують анонімність і зручність сучасних технологій для вчинення злочинів проти окремих осіб, підприємств і навіть державних структур.

Серед злочинів в інформаційному середовищі поширені: хакерські атаки на державні та корпоративні системи; фінансові кіберзлочини (фішинг, шахрайство, крадіжка банківських даних); поширення шкідливого програмного забезпечення; кібершпигунство та несанкціонований доступ до інформації; кібертероризм та атаки на критичну інфраструктуру, кількість яких значно зросла в Україні з часу початку повномасштабної війни росії проти нашої держави.

Визнаючи глибокі зміни в сучасному світі, які принесли цифрові технології та активне використання комп'ютерних мереж, задля протидії кіберзлочинності міжнародна спільнота згуртувалась через прийняття, приєднання і ратифікації на національному рівні Будапештської конвенції про кіберзлочинність (далі – Конвенція) [1]. В Україні ратифікована та набула чинності 01.07.2006 р. за Законом України від 07.09.2005 р. № 2824-IV.

Станом на сьогодні, у зв'язку з необхідністю співпраці між державами у сфері боротьби з кіберзлочинністю та захисту національних інтересів у використанні та розвитку інформаційних технологій, визнається, що ефективність протидії кіберзлочинності прямо залежить від виявлення доказів протиправної діяльності у кіберпросторі, їх фіксації і розслідування з подальшим притягненням осіб, винних у вчиненні кримінальних правопорушень до відповідальності. Конвенція передбачає швидке реагування на кіберправопорушення та ефективну співпрацю у кримінальних провадженнях для викриття кримінально протиправних дій, що порушують конфіденційність, цілісність та доступність комп'ютерних систем, мереж й комп'ютерних даних. Встановленням кримінальної відповідальності за такі дії Конвенцією надано достатньо повноважень правоохоронним органам для ефективної боротьби з кіберправопорушеннями, зокрема у їх виявленні, розслідуванні та судовому кримінальному провадженні, як на внутрішньому, так і на міжнародному рівнях.

Слід назвати Конвенцію ООН проти транснаціональної організованої злочинності, яка включає окремі аспекти кібербезпеки [2], та Директиву Європейського парламенту і Ради Європейського Союзу від 6.07.2016 р.

№ 2016/1148 про мережеву та інформаційну безпеку [3], що регулює стандарти кібербезпеки в країнах ЄС, нормативні документи, чинні для України, які дозволяють адаптувати національні правові механізми для боротьби з кіберзлочинністю. Враховуючи міжнародні стандарти та внутрішні потреби Україна разом з країнами ЄС та іншими державами розробляють відповідні нормативні акти й разом із цим стратегії з кібербезпеки та співробітництва з Інтерполом, міжнародною організацією кримінальної поліції, та Європолом, Європейським поліцейським управлінням, установою правопорядку Європейського Союзу, що займаються розслідуванням кіберзлочинів і координацією проведення міжнародних операцій з припинення кримінальних правопорушень та затримання кіберзлочинців [4, с. 339–343].

Кіберзлочинність є серйозним викликом глобальній інформаційній безпеці, що вимагає міжнародної координації та докладання спільних зусиль у боротьбі з кіберзлочинністю. Співпраця України з державами, міжнародними організаціями для підвищення ефективності протидії кіберзлочинності сприяє постійному вдосконаленню національного законодавства, розвитку технологій кіберзахисту та підвищенню рівня кібербезпеки.

Список використаних джерел

1. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
2. Директива ЄС про мережеву та інформаційну безпеку. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text
3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text
4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. Київ, 2024. № 6 (червень). 364 с. URL: https://ippi.org.ua/sites/default/files/2024-6.pdf