УДК 347.83:34:002.1

Сліпченко Т. О.
к.е.н., доцент кафедри кримінального права та процесу і правоохоронної діяльності Західноукраїнського національного університету

Канюка В. Є.
к.ю.н., доцент кафедри кримінального права та процесу і правоохоронної діяльності Західноукраїнського національного університету

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СИСТЕМИ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Збільшення кількості кіберзагроз на економічну соціальну складову нашої держави все актуальнішим робить питання оптимізації правового регулювання даної сфери. В світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Явище «безпека» нерозривно пов'язане з поняттям «національні інтереси» і, можливо, в якомусь сенсі є похідним від нього, тому що, перш за все, функція національної безпеки – це забезпечення гарантій невразливості найголовніших інтересів національного суверенітету, територіальної цілісності держави, захисту населення – власне, тих інтересів, через які держава бореться і не погоджується на поступки. Національна безпека – це стратегія, необхідна для забезпечення інтересів держави [3,37]. На сьогоднішній день поняття кібербезпеки багатогранне, тому досить важко формалізуються. Наявність правильного формулювання поняття кібербезпеки є вкрай важливим для окреслення головних цілей роботи різних структур і подальшого захисту кіберпростору від загроз.

В сучасних умовах питання кібербезпеки виходять з рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації у вузькому сенсі цього слова, а й усього кіберпростору. Кіберпростір можна визначити як «метафоричну абстракцію, яка використовується в філософії і в комп'ютерній технології, яка є віртуальною реальністю, представляє неосферу, другий світ як «всередині» комп'ютерів, так і «всередині» комп'ютерних мереж» [3, 43].

Говорячи про вирішення проблем кібербезпеки, необхідно враховувати досить важливий її аспект – взаємозв'язок між учасниками, тобто користувачами, який може привести до синергетичного ефекту. Необхідні ретельні дослідження властивостей кіберпростору, динаміки його розвитку, методів управління цією динамікою. Вкрай складно, практично неможливо побудувати дійсно ефективну систему кібербезпеки без її системного аналізу, тому доцільно включити в комплекс досліджень в галузі кібербезпеки такі напрямки, як:

- вироблення єдиної термінології кібербезпеки і кіберпростору;
- розробка системи показників функціонування кіберпростору, а також його захисту від потенційних загроз;
- розробка моделей кіберпростору і факторів, що впливають на його функціонування;
- створення спеціальних методів забезпечення стійкості кіберпростору при впливі загроз;
- створення інтелектуальних методів забезпечення кібербезпеки, таких, як метод ситуаційного аналізу стану інформаційної безпеки, нові методи криптографічного захисту, інтелектуальні методи виявлення вторгнень у системи, методи інтелектуальної ідентифікації користувачів при кібератаці [2].

Останнім часом змінюється ієрархія пріоритетів в сфері кібербезпеки, якщо на початку XXI ст. на перший план виходили проблеми боротьби з міжнародними терористичними організаціями, а також питання безпеки промислової інфраструктури, то останнім часом практично всі європейські країни стурбовані можливим втручанням хакерів в їх виборчі кампанії. Кіберстратегія ряду європейських держав допускає не тільки оборонні, а й наступальні дії в кіберпросторі.

В 2013 р. Європейський Союз ухвалив Стратегію кібербезпеки, метою якої є відкритий, надійний і безпечний кіберпростір. Для цього передбачені заходи з наступних напрямків: досягнення кіберстійкості, суттєве скорочення кіберзлочинності, розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони, розвиток виробничих і технологічних ресурсів для кібербезпеки, створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС.

Правова база кібербезпеки України складається з міжнародних зобов'язань та національного законодавства. На міжнародному рівні слід виділити Будапештську конвенцію та Директиву щодо мережевої та інформаційної безпеки (NIS) [4].

У національному законодавстві мають знайти відображення зобов'язання, взяті на себе Україною як підписантом міжнародних угод і конвенцій, а також ті, які їй доведеться взяти, якщо вона й надалі демонструватиме прагнення вступити до Європейського Союзу. На національному рівні, Закон № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України є основними документами, що регулюють дану сферу. Відсутність в українському

законодавстві необхідної термінології, невизначеність питань щодо розподілу повноважень між різними державними та приватними установами в сфері кіберзахисту, відсутність законодавчо врегульованої та фінансово забезпеченої стратегії державно-приватного партнерства, невирішеність багатьох процедурних питань щодо дій правоохоронних та контролюючих органів, а також недостатня увага, що приділяється проблемам загальної освіти з кібербезпеки, підвищення обізнаності, нарощуванню потенціалу значно підвищують вразливість України перед кіберінцидентами та кібератаками. Необхідність законодавчого врегулювання перелічених питань вимагає прозорості законодавчого процесу, плідної співпраці українських та міжнародних стейкголдерів, сприяння підвищення довіри між ними.

Закон України «Про основні засади забезпечення кібербезпеки України» заклав загальну архітектуру національної системи кібербезпеки та розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки (Національним координаційним центром кібербезпеки, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Національною поліцією, Національним банком, розвідувальними органами України) [1].

У середовищі, де постійно з'являються і еволюціонують кіберзагрози, співпраця на європейському рівні необхідна не тільки для ефективної підготовки до кібератак, але і для своєчасної реакції на них. Комплексна державна стратегія кібербезпеки – перший крок на цьому шляху.

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на сьогодні, вважаємо: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності громадян.

ЛІТЕРАТУРА:

1. *Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР). 2017. № 45. 403с.*
2. *Кібербезпека: рекомендації для ЄС. URL://http://www.lawtrend.org/information-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es (дата звернення: 22.03.2021).*
3. *Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. навч.посіб. Вид 2-ге, перероб. і допов. Київ. 2018. 400 с.*
4. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). URL://http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Last Accessed: 22.03.2021)*

5. *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber- security. URL: www.iso.org/standard/44375.html. (Last Accessed: 22.03.2021).*

УДК 351.74/.76

Фаріон-Мельник А. І.
к.е.н., доцент, доцент кафедри кримінального права та процесу і правоохоронної діяльності Західноукраїнського національного університету

ПОЛІЦЕЙСЬКИЙ ОФІЦЕР ГРОМАДИ ЯК НОВИЙ ФОРМАТ СПІВПРАЦІ ПОЛІЦІЇ З ОТГ

Міністерством внутрішніх справ України в рамках реформи органів Національної поліції України в 2019 було розпочато пілотний проєкт «Поліцейський офіцер громади» [1]. Реалізація проєкту передбачалася у два етапи: перший (2019 рік) – налагодження роботи у 802 об'єднаних громадах, другий (2020-2021 рік) – на території всієї держави.

Основною метою даного проєкту є забезпечення тісної взаємодії поліцейських з об'єднаною територіальною громадою, орієнтація діяльності поліцейських, у першу чергу, саме на потреби громади. За новим проєктом офіцер поліції буде тісно взаємодіяти з жителями своєї громади та орієнтуватися на їхні потреби. Відповідно в повідомленні на сайті МВС зазначено: «80-90% робочого часу поліцейський знаходитиметься в громаді. Він буде доступний для населення, знатиме мешканців території, яку обслуговує, їхні проблеми та надаватиме якісні поліцейські послуги» [2].

Базовими етапами реалізації проекту «Поліцейський офіцер громади» є: 1) встановлення, шляхом проведення відповідних інформаційних кампаній, співпраці з об'єднаними територіальними громадами, з метою оцінювання можливостей кожної громади з наступним підписанням меморандуму; 2) проведення відбору кандидатів на посади поліцейських офіцерів громади серед діючих працівників поліції (перевага надається дільничним офіцерам поліції); 3) навчання відібраних кандидатів на курсах підготовки за спеціально розробленою програмою тривалістю до 2,5 місяців із залученням іноземних експертів; 4) організація несення служби поліцейськими офіцерами громади, під час чого відбувається спочатку його знайомство з громадою, планування безпосередньої роботи щодо реалізації спільних проектів з об'єднаною територіальною громадою, звітування перед нею; 5) здійснення контрольних заходів (регулярне оцінювання ефективності) з боку Національної поліції та вивчення громадської думки міжнародними експертами [3,с.61].

Поліцейські, які беруть участь у проєкті, здійснюють свою службову діяльність відповідно до Конституції України, законів України «Про