DOI https://doi.org/10.36059/978-966-397-501-6-100

КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА ПРОТИДІЇ ВИКОРИСТАННЮ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Євдокименко Денис Миколайович
аспірант, юридичний експерт,
BRDO (Офіс ефективного регулювання)
м. Київ, Україна

Актуальність теми дослідження зумовлена необхідністю реагування на нові виклики, які постали перед державою в умовах гібридної війни, зокрема в кіберпросторі. Шкідливе програмне забезпечення дедалі частіше застосовується як один із основних інструментів деструктивного впливу на інформаційні ресурси державних органів, критичну інфраструктуру, фінансову систему, оборонно-промисловий комплекс, зв'язок тощо. Значна кількість кібератак, зафіксованих протягом 2022–2025 років, має ознаки скоординованих дій іноземних спецслужб або підпорядкованих ним приватних компаній і вимагає системного кримінально-правового реагування.

З огляду на практику застосування кримінального законодавства, статті 361, 361-1, 361-2 та 362 Кримінального Кодексу України наразі є основою притягнення до відповідальності за дії, пов'язані з несанкціонованим втручанням в інформаційні системи. Водночас, відсутність визначення самого поняття «шкідливе програмне забезпечення», або «програмне забезпечення, що становить загрозу національній безпеці» в законодавстві ускладнює правозастосування та створює підґрунтя для неоднозначного тлумачення. Наприклад, термінологічна невизначеність призводить до того, що правоохоронні органи не завжди можуть ефективно кваліфікувати відповідні дії або встановити умисел у вчиненні кіберзлочину.

Варто наголосити, що використання шкідливого програмного забезпечення в умовах воєнного стану може бути частиною загального плану дестабілізації країни та впливу на широке коло осіб в національному масштабі, і тому повинно трактуватися не лише як злочин проти інформаційної безпеки, а й як елемент колабораціонізму або пособництва державі-агресору. З урахуванням цього слід розглянути можливість розробки нової статті, яка б передбачала відповідальність за кіберзлочини в умовах збройної агресії, що мають ознаки співпраці з державами, визнаними у встановленому порядку країнами-терористами або сприяння діяльності окупаційних структур.

Міжнародні практики свідчать про посилення відповідальності за кіберзлочини, вчинені в контексті загрози національній безпеці. У державах ЄС спостерігається тенденція до гармонізації кримінального законодавства у сфері кібербезпеки. Наприклад, у Франції, Німеччині, Литві та Польщі передбачено окремі склади злочинів, пов'язаних із діяльністю в інтересах ворожих держав, навіть якщо така діяльність не призводить до фізичних наслідків, а лише має потенційну шкоду в цифровому середовищі. Також передбачена відповідальність за дії, що створюють передумови для дестабілізації державних систем управління та оборони через електронні комунікаційні мережі та послуги.

Отже, пропонується внести до Кримінального Кодексу України такі зміни:

(1) законодавче визначення поняття «шкідливе програмне забезпечення», або як альтернативний термін – «програмне забезпечення, що становить загрозу національній безпеці»;

(2) введення кваліфікуючої ознаки у вигляді факту використання такого програмного забезпечення в умовах воєнного стану;

(3) встановлення підвищеної відповідальності для осіб або керівників компаній, які здійснюють дії, що координуються зі спецслужбами країн-терористів.

Узагальнюючи викладене, слід визнати, що кримінально-правова політика у сфері боротьби з кіберзагрозами потребує якісного оновлення. Україна має всі передумови для створення прогресивної та ефективної системи протидії шкідливому програмному забезпеченню, здатної адаптуватися до умов воєнного часу та забезпечити належний рівень захисту національних інтересів у цифровому просторі.

Література:

1. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III // Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.

2. Конвенція про кіберзлочинність : міжнародний документ від 23 листопада 2001 р. (Будапештська конвенція). URL: https://rm.coe.int/1680081561 (дата звернення: 30 квітня 2025 року).

3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act) // Official Journal of the European Union. 2019. L 151. P. 15–69.