

**Бугайчук Костянтин Леонідович**  
кандидат юридичних наук, доцент, завідувач науково-дослідної лабораторії  
з проблем протидії злочинності Харківського національного університету  
внутрішніх справ, м. Харків, Україна

**Шорохова Ганна Михайлівна**  
науковий співробітник науково-дослідної лабораторії з проблем протидії  
злочинності Харківського національного університету внутрішніх справ,  
м. Харків, Україна

## **ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК УМОВА ПРОТИДІЇ ТЕРОРИСТИЧНІЙ ДІЯЛЬНОСТІ: НОРМАТИВНО-ПРАВОВІ АСПЕКТИ**

Останнім часом **терористична діяльність** належить до найбільш небезпечних і важко прогнозованих явищ, а також характеризується здатністю до адаптації й модернізації в умовах основних тенденцій сучасності – глобалізації та інформатизації. Так, одним із загрозливих проявів тероризму стає інформаційний тероризм, в основі якого – маніпуляція свідомістю мас, розповсюдження інформаційно-емоційного ефекту, на який розраховано більшість терористичних актів, залучення прихильників серед членів суспільства, вплив на владні структури, які приймають політичні рішення.

Отже, саме кібертероризм є серйозною соціально-небезпечною загрозою для людства, у порівнянні, навіть, з ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози через свою новизну, не до кінця ще усвідомлений і вивчений. Досвід, що є у світової спільноти у цій сфері, зі всією очевидністю свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [1, с. 127]. Так,

кібербезпека є однією із суттєвих складових частин національної безпеки країни та набуває відносно самостійного наднаціонального характеру.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кібертероризмом. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV, а також відповідні Закони України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про основи національної безпеки України», та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України.

Окрім того, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ — Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Ще одним кроком у цьому напрямку був Указ Президента України від 15 березня 2016 року №96/2016, яким було введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України".

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягнення сумісності з відповідними стандартами ЄС та НАТО; формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпечного поведіння в кіберпросторі; розвиток міжнародного співробітництва та підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України з ЄС та НАТО [2].

Наступним етапом у сфері забезпечення кібербезпеки стало рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введено в дію Указом Президента України від 13 лютого 2017 року №32/2017 [3]. Такий стан справ фактично означає, що Україна поступово накопляє важливий досвід у захисті власної IT-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму.

Проте в своїй більшості вітчизняне нормативно-правове поле у сфері інформаційної безпеки оперує дефініціями визначень яких фактично немає. Ряд законів не містить визначень вживаних термінів і понять, вільно використовуються не узгоджені між собою терміни. Велика кількість загроз, що

пов'язана із використанням сучасних інформаційних технологій, мають більш широкі та комплексні наслідки. Сучасне інформаційне законодавство України не має чіткої, ієрархічної побудови, єдності, комплексності, це викликає суперечливе тлумачення та застосування його норм на практиці, зокрема через те, що окремі цілісні проблеми вирішуються в різних нормативних актах фрагментарно і без узгодження між собою. Так, серед наукових та практичних працівників немає єдності у термінологічному позначенні терористичної діяльності. Такий вид тероризму називають по-різному: "інформаційний тероризм", "комп'ютерний тероризм", "кібертероризм", "технологічний тероризм", "віртуальний тероризм" тощо.

Як на європейському, так і на міжнародному рівні погодженого визначення кібербезпеки та інших визначень у цій сфері немає. У кожній країні визначення кібербезпеки та інших ключових термінів може значно розрізнятися. Як наслідок, розрізняються і підходи до складання стратегій кібербезпеки. Відсутність спільної «мови» і підходу ускладнює процес міжнародної співпраці, в той час як важливість співпраці визначається усіма країнами.

Розмаїття термінологічних тлумачень узгодив прийнятий 5 жовтня 2017 року Закон України «Про основні засади забезпечення кібербезпеки України», а 7 листопада цей Закон підписано Президентом України. Законодавчий акт було розроблено на виконання вимог Стратегії національної безпеки України, затвердженої Указом Президента України від 15.03.2016 № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". В Законі враховано низку пропозицій експертів НАТО і Євросоюзу.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

Основними суб'єктами національної системи кібербезпеки є 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.

Закон визначає Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України [4].

Нарешті у цьому законі дано визначення таких головних понять як, кібербезпека, кіберзагроза, кіберзахист, кіберпростір, кібертероризм та інші.

Маючи офіційне тлумачення даних термінів подальшою задачею для науково-дослідних установ є дослідження питань в сфері забезпечення кібербезпеки та напрацювання фундаментальних та практичних методичних рекомендацій по боротьбі з кібертероризмом.

#### **Список використаних джерел:**

1. Бондаренко В.О. Інформаційна безпека сучасної держави: концептуальні роздуми / В.О. Бондаренко, О.В. Литвиненко // Стратегічна панорама. – 1999. – № 1-2. – С. 127-133.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : указ Президента України від 15 березня 2016 року №96/2016 [Електроний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/96/2016>.

3. Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: указ Президента України № 32/2017 від 13 лютого 2017 року [Електроний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/254/2017>.

4. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII [Електроний ресурс]. – Режим доступу: [http://search.ligazakon.ua/l\\_doc2.nsf/link1/T172163.html](http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html).