

# Основні проблеми побудови системи кібернетичної безпеки України



**Шеломенцев Володимир Петрович** – заступник начальника управління Департаменту МВС України, кандидат юридичних наук, Заслужений юрист України

*У статті проаналізовано основні проблеми та визначено пріоритетні напрями побудови національної системи кібернетичної безпеки.*

**Ключові слова:** кіберпростір, кібернетична безпека, система кібернетичної безпеки, суб'єкти забезпечення кібербезпеки, національна критична інформаційна інфраструктура.

**Постановка проблеми.** Питання реалізації життєво важливих інтересів особи, суспільства, держави у кібернетичному просторі тісно пов'язані із забезпеченням їх кібернетичної безпеки (кібербезпеки), під якою розуміють стан їх захищеності від зовнішніх і внутрішніх загроз, пов'язаних з використанням деструктивного кібернетичного впливу на інформаційно-телекомунікаційні системи, що забезпечують реалізацію таких інтересів.

Необхідність побудови дієвої системи кібернетичної безпеки України обумовлена наявністю протиріччя між необхідністю більш широкого впровадження інформаційно-телекомунікаційних технологій в усі сфери людської діяльності та підвищенням рівня їхньої безпеки. В сучасних умовах глобалізації значно зростають уразливості інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури.

Крім того, в кіберпросторі реалізуються загрози національним інтересам держави в усіх сферах її життєдіяльності, включаючи і сферу оборони. Останні події, пов'язані з анексією Криму та проведенням антитерористичної операції, свідчать про неефективність заходів протидії кібернетичним загрозам з боку іноземних держав.

Відсутність в Україні дієвої системи кібернетичної безпеки поряд із зростанням кількості реальних кіберзагроз негативно впливає на загальний рівень національної безпеки України.

**Стан дослідження.** Окремі аспекти розбудови системи кібернетичної безпеки України розглядали В. М. Бутузов, В. Д. Гавловський, Д. В. Дубов, М. А. Ожеван, М. А. Погорецький, К. В. Титуніна та інші науковці.

Проте, аналіз наукових джерел свідчить, що дослідниками розглянуті лише загальні питання розбудови національної системи кібернетичної безпеки. Водночас, розкриття проблем побудови національної кібернетичної системи дозволить правильно визначити пріоритети такої побудови.

**Метою статті є** розкриття проблем побудови системи кібернетичної безпеки України.

**Виклад основного матеріалу.** Аналіз розбудови систем кібернетичної безпеки у провідних державах світу вказує на такі основні тенденції у цій сфері, як: відповідна системна реорганізація сектору безпеки та створення спеціалізованих підрозділів із захисту національних інтересів у кіберпросторі.

Під системою кібернетичної безпеки України розуміється сукупність суб'єктів забезпечення кібернетичної безпеки України, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних й технічних заходів. При цьому, системі кібернетичної безпеки слід розглядати як похідну від системи забезпечення національної безпеки України (у кібернетичному середовищі). Тобто, у такому середовищі присутні всі сфери забезпечення національної безпеки (воєнна, політична, економічна, фінансова, інформаційна тощо), а значить повинні реалізовуватись й усі основні функції суб'єктів забезпечення національної безпеки.

Метою функціонування національної системи кібернетичної безпеки слід визначити забезпечення безпеки держави у кібернетичному просторі шляхом забезпечення захисту об'єктів критичної інформаційної інфраструктури, запобігання, виявлення та припинення злочинів і правопорушень у кібернетичному просторі, здійснення розвідувальних та оборонних операцій, забезпечення злагодженого функціонування суб'єктів забезпечення кібернетичної безпеки держави.

Відповідно до основних завдань кібербезпеки, у системі кібернетичної безпеки України доцільно виділити такі функціональні підсистеми: протидії кіберзлочинності; кіберзахисту

об'єктів критичної інформаційної інфраструктури; реагування на кіберзагрози державному суверенітету в кіберпросторі; забезпечення кібербезпеки у воєнній сфері та сфері оборони.

Функціональні підсистеми системи кібернетичної безпеки повинні утворюватись центральними органами виконавчої влади у відповідній сфері управління. Перелік центральних органів виконавчої влади, що створюють функціональні підсистеми, повинні визначитися відповідним Положенням про національну систему кібернетичної безпеки.

Водночас, загальні вимоги до розбудови системи кібернетичної безпеки в Україні повинні враховувати світову тенденцію щодо зміщення основних акцентів забезпечення кібербезпеки з правоохоронних аспектів (протидія проникненню криміналу до кіберпростору, боротьба з кіберзлочинністю) до воєнних і розвідувальних, а також протидії кібертероризму.

При цьому, як свідчить досвід забезпечення кібернетичної безпеки, відповідна система, залежно від особливостей і масштабів наслідків кібератак на об'єкти критичної інформаційної інфраструктури, повинна діяти у режимах: повсякденного функціонування; підвищеної готовності; надзвичайної ситуації.

Існує ціла низка проблем щодо побудови національної системи кібернетичної безпеки, з поміж яких доречно виокремити наступні.

1. Відсутність як для державного, так і для приватного сектору стандартів кібернетичної безпеки на основі визнаних міжнародних стандартів.

При цьому, суттєвого доопрацювання потребує понятійний апарат сфери забезпечення кібернетичної безпеки. Зокрема, досі залишаються новими для національного законодавства поняття “кібернетична безпека (кібербезпека)” та “кібернетичний простір (кіберпростір)”, а також низка інших пов'язаних з ними термінів таких, як: “кіберзлочинність”, “кібертероризм”, “кіберінцидент”, “кібератака”, “національна критична інформаційна інфраструктура” тощо.

Неузгодженість зазначених термінів із чинним термінологічним апаратом, а також не визначеність співвідношення між цими поняттями ускладнює розуміння та застосування нових правових норм, що стосуються сфери забезпечення кібербезпеки. При цьому, термін “кіберзлочинність” досить широко використовується у міжнародних документах (Конвенція про кіберзлочинність 2001 року та додаткові протоколи до неї).

2. Недостатність правового регулювання процесу розбудови системи кібернетичної безпеки України. Необхідність прийняття законопроекту про кібернетичну безпеку України (основи кібернетичної системи) обумовлена неврегульованістю на законодавчому рівні відносин, пов'язаних із забезпеченням національних інтересів у кіберпросторі. Такий законопроект повинен стати основою для розроблення єдиної державної політики з питань забезпечення кібернетичної безпеки України.

При цьому, слід зважати на те, що інформаційні відносини, у тому числі відносини, пов'язані із забезпеченням кібернетичної безпеки, певним чином уже врегульовані національним законодавством України. Так, ключова роль у забезпеченні кібернетичної безпеки належить законам України “Про захист інформації в інформаційно-телекомунікаційних системах” (який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах), “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” (щодо відповідальності за комп'ютерні злочини), а також Конвенції Ради Європи про кіберзлочинність і Додатковим протоколам до неї. Також на врегулювання відносин у даній сфері спрямовані закони України “Про інформацію”, “Про науково-технічну інформацію”, “Про телекомунікації”, “Про доступ до публічної інформації”, “Про боротьбу з тероризмом” та ін.

Кабінет Міністрів України 5 листопада поточного року, на виконання рішень РНБО України, в черговий раз ухвалив рішення про необхідність розробки та схвалення закону щодо кібербезпеки України. На даний час мова йде про розроблений адміністрацією Державної служби спецзв'язку і захисту інформації проект Закону України “Про основні засади забезпечення кібербезпеки України”, розроблений на виконання рішення РНБО України від 28 квітня 2014 року “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”, уведеного в дію Указом Президента України від 1 травня 2014 року № 449.

Даний законопроект визначає правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України. Національна система кібербезпеки, на думку авторів законопроекту, повинна розглядатися як сукупність політичних, соціальних, економічних та інформаційних відносин разом з адміністративними і технологічними заходами, реалізація яких представляється можливою у тісній взаємодії державного і приватного секторів та громадянського суспільства. У Держспецзв'язку вважають, що реалізація цього документа дозволить впровадити комплексний підхід у визначенні основних заходів формування державної політики у сфері кібербезпеки, а також створити умови для забезпечення захисту інформаційної інфраструктури держави.

Також Уряд схвалив План заходів програми захисту державних інформаційних ресурсів. Як заявив Міністр Кабінету Міністрів Остап Семерак: “Мова йде про формування захищеної інформаційної структури всіх державних органів. Маємо також на меті виключити можливість втручання у роботу інформаційно-телекомунікаційних систем, у тому числі, спецслужбами іно-

земних держав” [1]. Зазначені події можна розглядати як продовження процесу формування національної системи кібербезпеки. Попереднім кроком було схвалення Кабінетом Міністрів України 17 липня 2014 року проекту Указу Президента “Про Стратегію забезпечення кібернетичної безпеки України” (також розробленого Адміністрацією Держспецзв’язку України) і подання його на розгляд Президентіві України [2].

Доцільним вбачається й удосконалення національного законодавства щодо спрощення процедур міжнародного співробітництва при реагуванні на кібернетичні інциденти кримінального характеру, забезпечення імплементації необхідної термінології у сфері кібербезпеки до чинного законодавства України.

3. Відсутність затвердженого переліку об’єктів критичної національної інфраструктури, що потребують першочергового захисту від кібернетичних атак. Так, кожній інформаційно-телекомунікаційній системі, що використовується на окремому об’єкті критичної національної інфраструктури, властиві конкретні уразливості, а значить і відповідні кіберзагрози.

Тобто, лише визначивши об’єкти критичної національної інфраструктури та встановивши основні зовнішні та внутрішні загрози кібернетичного характеру, можна приступити до формування системи безпеки, ефективність якої буде обумовлена підбором: найбільш ефективних заходів захисту від різних видів кібернетичних загроз; суб’єктів, здатних забезпечити необхідний рівень кіберзахисту.

4. Відсутність чіткого розподілу функцій між суб’єктами забезпечення кібернетичної безпеки, їх повноважень. При цьому, реалізація конкретних функцій суб’єктами забезпечення кібернетичної безпеки України обумовлюється їх компетенцією та можливістю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз життєво важливим інтересам особи, суспільства і держави.

Важливе значення має створення структури оперативного реагування на кіберінциденти. Хоча запобігти кібернетичним атакам технічно не уявляється можливим, незалежно від складності систем захисту – своєчасне виявлення та швидке адекватне реагування на кібернетичні атаки дозволяє значно мінімізувати наслідки від таких атак.

Так, Указом Президента України від 24 вересня 2014 року № 744/2014 “Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року “Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності” передбачено створення національного центру кіберзахисту та протидії кіберзагрозам [3]. Держспецзв’язку України вже створено оперативну групу (координаційний центр) з питань реагування на комп’ютерні інциденти. Одними із завдань оперативної групи є: якнайшвидше відпрацювання комп’ютерних інцидентів, інформація про які надійшла до команди реагування на комп’ютерні надзвичайні ситуації

CERT-UA; координація сил і засобів, спрямованих на запобігання вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах; обговорення і напрацювання дієвих механізмів забезпечення кібербезпеки шляхом консультацій експертів компаній та організацій, що беруть участь у роботі оперативної групи [4].

Передбачається, що до складу такої групи входитимуть представники Державної служби спеціального зв’язку та захисту інформації України, зокрема Адміністрації Держспецзв’язку та Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв’язку, Служби безпеки України, Міністерства внутрішніх справ України, Служби зовнішньої розвідки України, Міністерства оборони України та Генерального штабу Збройних Сил України, Генеральної прокуратури України, Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації, представники двох десятків провідних операторів і провайдерів телекомунікацій, а також громадських організацій ІнАУ, “Телас” та Київського відділення ISACA.

Також важливе значення має запровадження дієвих стимулів для залучення до спеціалізованих підрозділів по боротьбі з кіберзлочинністю фахівців відповідного рівня кваліфікації. Так, Адміністрація Державної служби спеціального зв’язку та захисту інформації України та київське відділення міжнародної неприбуткової професійної асоціації ISACA уклали меморандум про співробітництво у сфері кібербезпеки та інформаційних технологій [5]. У планах сторін – створення робочих груп з актуальних питань кібербезпеки, підготовка спільних авторизованих публікацій, повідомлень, методичних рекомендацій і настанов.

**Висновки.** На підставі аналізу основних проблем побудови системи кібернетичної безпеки України можна визначити пріоритетні напрями побудови такої системи.

Розвиток сфери забезпечення кібернетичної безпеки неможливий без чіткого законодавчого визначення основних категорій та стандартів кібербезпеки, узгодження єдиної термінології у сфері забезпечення кібернетичної безпеки. При цьому, слід брати до уваги міжнародні стандарти, а також кращий міжнародний досвід у сфері кібербезпеки.

Вбачається, що законодавча активність у сфері забезпечення кібернетичної безпеки повинна враховувати цілісність уже існуючої системи нормативно-правового регулювання інформаційної безпеки, боротьби з кіберзлочинністю, уникати колізій з іншими законодавчими актами.

Побудова національної системи кібернетичної безпеки повинна передбачати впровадження принципово нової системи організації та проведення заходів інформаційної боротьби, яка включатиме відповідні органи управління, сили та засоби, що створюються в Міністерстві оборони України, Збройних Силах України, інших складових сектору безпеки і оборони України. При цьому, слід чітко розподілити функції та завдання

між усіма суб'єктами забезпечення кібернетичної безпеки, а також визначити (створити новий) координуючий орган. Варто впроваджувати в Україні найкращі здобутки провідних країн світу в сфері забезпечення кібернетичної безпеки.

Ефективність національної системи кібернетичної безпеки України залежить від належного рівня співробітництва між суб'єктами її забезпечення та компетентними органами інших країн. З урахуванням міжнародного досвіду для підвищення рівня міжнародного співробітництва у сфері протидії кіберзлочинності необхідно: активізувати роботу в форматі комісій, експертних груп, інших дорадчих і координуючих органів ООН з питань кібербезпеки; здійснювати формування системи кібербезпеки з урахуванням тенденцій глобальної кібербезпеки; налагодити дієву співпрацю з відповідними підрозділами інших країн з метою обміну досвідом і проведення спільних заходів.

#### **Список використаних джерел**

1. Офіційний сайт Кабінету Міністрів України / [Електронний ресурс]. – Режим доступу : [http://www.kmu.gov.ua/control/uk/publish/article?art\\_id=247729333](http://www.kmu.gov.ua/control/uk/publish/article?art_id=247729333).
2. Уряд погодив проект національної Стратегії забезпечення кібернетичної безпеки / [Електронний ресурс]. – Режим доступу : <http://newsme.com.ua/ua/tech/technologies/2561163/>.
3. Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року “Про не-

відкладні заходи щодо захисту України та зміцнення її обороноздатності” : Указ Президента України від 24 верес. 2014 р. № 744/2014 / [Електронний ресурс]. – Режим доступу :

<http://www.president.gov.ua/documents/18125.html>.

4. Офіційний сайт ДССЗІ / [Електронний ресурс]. – Режим доступу :

[http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art\\_id=116283&cat\\_id=112509&mustWords](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=116283&cat_id=112509&mustWords).

5. Київське відділення ISACA та Держспецзв'язку уклали меморандум про співробітництво у сфері кібербезпеки та інформаційних технологій / [Електронний ресурс]. – Режим доступу :

<http://www.isaca.org.ua/index.php/press-center/news/165-isaca-kyiv-chapter-and-state-service-for-special-communication-and-information-protection-of-ukraine-memorandum-of-cooperation>.

*В статтє проанализированы основные проблемы и определены приоритетные направления построения национальной системы кибернетической безопасности.*

*The article deals with the problems and the priority directions of construction of the national system of cybernetic safety.*

*Стаття надійшла до редакції журналу 28 листопада 2014 року.*