## ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

УДК 351.74:341.9

# ДІЯЛЬНІСТЬ КОНТРРОЗВІДУВАЛЬНИХ ОРГАНІВ В ДЕРЖАВНІЙ СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД КРАЇН НАТО ТА УКРАЇНСЬКІ РЕАЛІЇ

**Коваленко Є. В.,**
кандидат юридичних наук,
доцент спеціальної кафедри № 1
«Правові засади забезпечення державної безпеки»
Інституту підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого, м. Харків

**Плетньов О. В.,**
кандидат юридичних наук,
доцент спеціальної кафедри № 1
«Правові засади забезпечення державної безпеки»
Інституту підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого, м. Харків

**Анотація:** у статті досліджено особливості впровадження в практику українських контррозвідувальних органів в державній системі забезпечення інформаційної безпеки досвіду країн НАТО. Зокрема, проаналізовано особливості забезпечення інформаційної безпеки в НАТО. Здійснено оцінку нормативної бази України стосовно забезпечення кібербезпеки у контексті протидії гібридній війні. Окреслено перспективи реформи Служби безпеки України відповідно до стандартів НАТО.
**Ключові слова:** інформаційна безпека, держава, НАТО, кібербезпека, гібридна війна.

**Аннотация:** в статье исследованы особенности внедрения в практику украинских контрразведывательных органов в государственной системе обеспечения информационной безопасности опыта стран НАТО. В частности, проанализированы особенности обеспечения информационной безопасности в НАТО. Осуществлена оценка нормативной базы Украины по обеспечению кибербезопасности в контексте противодействия гибридной войне. Определены перспективы реформы Службы безопасности Украины в соответствии со стандартами НАТО.
**Ключевые слова:** информационная безопасность, государство, НАТО, кибербезопасность, гибридная война.

**Annotation:** the features of introduction of experience of the NATO countries into the practice of the Ukrainian secret service bodies in the state system of ensuring information security are investigated in the article. In particular, the features of ensuring information security in NATO are analyzed. An assessment of the regulatory base of Ukraine on ensuring cyber security in the context of counteraction to hybrid war is carried out. The prospects of reform of Security Service of Ukraine according to the NATO standards are defined.
**Key words:** information security, state, NATO, cyber security, hybrid war.

---

**Постановка проблеми.** Протягом останніх десятиріч спостерігається активізація злочинності у кіберпросторі. Підвищується рівень ризиків безпечного використання глобальної мережі Інтернет, корпоративних систем консолідації інформації, з'являються нові сервіси, на які вигідно спрямовувати кібератаки. Країни Північноатлантичного альянсу накопичили суттєвий досвід стосовно діяльності контррозвідувальних органів в державній системі забезпечення інформаційної безпеки. Відповідно, актуальним і необхідним є впровадження цього досвіду у вітчизняну практику.

**Аналіз останніх досліджень і публікацій.** Проблеми забезпечення інформаційної безпеки в нинішніх умовах досліджувалися численними вченими,зокрема: А. Дорожкіним [1], В. Широковим [2], В. Ярочкіним [3] та ін.

Однак недостатньо опрацьованим залишається коло проблем, що стосується впровадження досвіду країн НАТО у вітчизняну практику відносно протистояння гібридним війнам, зокрема, забезпечення кібербезпеки.

**Формулювання цілей статті.** Приймаючи до уваги актуальність означеної проблематики, метою даної статті є впровадження в практику українських контррозвідувальних органів в державній системі забезпечення інформаційної безпеки досвіду країн НАТО.

Досягнення поставленої мети обумовлює необхідність вирішення таких завдань:

- дослідити особливості забезпечення інформаційної безпеки в НАТО;

- проаналізувати нормативну базу України стосовно забезпечення кібербезпеки у контексті протидії гібридній війні;
- окреслити перспективи реформи Служби безпеки України відповідно до стандартів НАТО.

**Виклад основного матеріалу.**

Головним елементом боротьби США з кіберзлочинністю залишається «Міжнародна стратегія США для кіберпростору», прийнята у 2011 році. Це основоположний документ, який підтримує три принципи:

- свободу самовираження;
- недоторканність приватних даних;
- вільний доступ до інформації.

«Міжнародна стратегія США для кіберпростору» відповідає основній меті США: глобальній роботі з розвитку відкритої, доступної, безпечної й надійної інформаційної інфраструктури, яка б підтримувала міжнародну комерційну діяльність, забезпечувала належний рівень безпеки і заохочувала самовираження і використання новітніх технологій.

Міжнародна стратегія США для кіберпростору» повністю підтримує думку про те, що існуючі міжнародні норми мирної поведінки і вирішення конфліктів цілком можна застосувати і в кіберпросторі, визнаючи при цьому, що ці норми потрібно адаптувати для інформаційного простору. Таким чином, ці норми слід прив'язати до традиційних принципів підтримки фундаментальних свобод, поваги права приватної власності, права на збереження таємниці особистих даних, права на захист від правопорушників, а також права на застосування засобів самозахисту. Саме на цьому фундаменті стоять міжнародні норми, перераховані нижче:

- глобальна сумісність систем;
- стабільність мережі;
- надійний доступ до мережевих ресурсів;
- багатостороннє управління;
- забезпечення кібербезпеки зусиллями держав.

У «Міжнародній стратегії США для кіберпростору» описуються три ключових вектори, яких дотримуються США щодо забезпечення кібербезпеки:

- поліпшення міжнародних дипломатичних відносин;
- відображення і запобігання нападам за допомогою поліпшення систем захисту;
- сприяння загального процвітання і безпеки за допомогою інвестицій в їх розвиток.

У «Міжнародній стратегії США для кіберпростору» також детально розкриваються 7 пріоритетних напрямків розвитку безпечної, надійної та доступної мережі Інтернет:

- просування міжнародних стандартів і підтримка відкритих ринків з метою економічного зростання;
- підвищення безпеки, надійності і відмовостійкості глобальних мереж;
- розвиток співпраці у правовій сфері та забезпечення дотримання законів;
- готовність збройних сил до протистояння загрозам в кіберпросторі;
- створення ефективних структур управління мережею Інтернет;
- нарощування можливостей підвищення безпеки і процвітання;
- побудова в мережі Інтернеті системи фундаментальних свобод і прав на приватну власність.

Вищенаведений план відноситься до розробленої більше двох років тому в США комплексної дорожньої карти, яка описує розвиток політики взаємодії з електронним середовищем для кожного відомства. Ця ж дорожня карта є базою для розвитку програм кібербезпеки і демонструє, як саме США бачать майбутнє безпечної і ефективної мережі Інтернет.

За минулий час було запущено кілька програм, націлених на впровадження зазначеної стратегії з урахуванням посилення описаних загроз. Багато в чому зростання загроз стимулює підвищення кількості ініціатив щодо забезпечення безпеки. Так, у 2012 році США підтримали проекти ООН, зусилля ОБСЄ та НАТО, націлені на пошуки компромісів щодо питань безпеки.

У лютому 2013 року Білий дім США видав указ, який регулює процедури підвищення захищеності критичних об'єктів інфраструктури. Даний указ є можливістю для сторонніх осіб отримати уявлення про комплексну взаємодію численних федеральних агентств з питань кібербезпеки, починаючи з Міністерства внутрішньої безпеки, Міністерства торгівлі, Міністерства оборони, Міністерства юстиції і закінчуючи такими органами як Адміністративно-бюджетне управління і Федеральне бюро розслідувань. І це одні з небагатьох захисників державної інфраструктури. Також в лютому в Конгрес було подано законопроект під назвою Cyber Intelligence Sharing and Protection Act, який стосувався нелегального контенту в мережі Інтернет. Передбачалося, що він буде схвалений до кінця року. Ці ж служби є відповідальними за налагодження зв'язків зі своїми зарубіжними колегами і координування питань кібербезпеки (від правозастосування до стандартів сумісності).

Вищезазначене дозволяє констатувати, що забезпечення інформаційної безпеки в НАТО являє собою забезпечення кібербезпеки або протистояння гібридним війнам, одним із різновидів яких є кібератаки. Стратегії гібридних війн і рекомендації щодо протистояння гібридним загрозам протягом останніх років розробляються в США і НАТО, при цьому робиться висновок про принципові зміни в характері гібридної війни. Суть цих змін зводиться до посилення впливу на підготовку, хід і результат гібридної війни як військової, так і іррегулярної складових контингенту з одночасним залученням потенціалу цивільних компонентів.

В нинішніх умовах поняття «гібридних воєн і загроз» містяться у деяких офіційних і робочих документах США і НАТО. На думку фахівців альянсу, такі війни включають в себе проведення широкого спектру прямих бойових дій і таємних операцій, що здійснюються за єдиним планом збройними силами, партизанськими і іншими іррегулярними формуваннями за участю різних цивільних компонентів.

В інтересах вдосконалення здатності союзників протистояти новим гібридним загрозам, в документах США і НАТО містяться вимоги налагодити тісну координацію між міністерствами внутрішніх справ; залучати сили поліції і жандармерії для припинення нетрадиційних загроз, пов'язаних з пропагандистськими кампаніями, кібератаками і діями місцевих сепаратистів. Проведення навчань для відпрацювання дій в гібридної війні є одним з пріоритетів функціонування альянсу.

Фактично поняття «гібридні загрози» об'єднує широкий діапазон ворожих обставин і намірів, таких як кібервійна, сценарії асиметричних конфліктів низької інтенсивності, глобальний тероризм, піратство, незаконна міграція, корупція, етнічні та релігійні конфлікти, безпека ресурсів, демографічні виклики, транснаціональна організована злочинність, проблеми глобалізації і поширення зброї масового знищення. У концепції НАТО, яка отримала назву «NATO's Bi-Strategic Command Capstone Concept» (2010), гібридні загрози визначаються як загрози, що створюються супротивником, здатним одночасно адаптивно використовувати традиційні і нетрадиційні засоби для досягнення власних цілей.

Що стосується українського досвіду державного забезпечення кібербезпеки, то ключовим нормативним актом України у цьому контексті є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII.

Проаналізувавши зазначений закон, можна зазначити, що питання забезпечення кібербезпеки є надзвичайно актуальними для України, а заходи з протидії викликам і загрозам у зазначеній сфері перебувають на початковому етапі і не мають комплексного характеру.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Але аналіз тексту даного закону свідчить про те, що багато положень мають декларативний характер, він перевантажений положеннями, в яких мова йде про наміри, принципи, що непритаманні для закону. Більш того, закон багато в чому дублює положення Указу Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96.

Відповідно, необхідно доопрацювати понятійний апарат закону, оскільки введення в правове поле нової термінології має здійснюватися комплексно і узгоджуватися з вже існуючою. Дійсно, присутні в законі визначення термінів є занадто складними. Зокрема, у Стратегії кібербезпеки України, рівно як і у Законі України «Про основні засади забезпечення кібербезпеки України» відсутнє визначення гібридної війни.

Крім Закону України «Про основні засади забезпечення кібербезпеки України» правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

У контексті дотримання вимог сучасного законодавства України відносно державного забезпечення кібербезпеки в Україні, а також на вимогу виконання перехідних положень Закону України «Про національну безпеку України» 21 червня 2018 року № 2469-VIII, в Україні було започатковано процес реформування Служби безпеки України. Так, ще у 2016 році, коли з'явилася міжнародна дорадча група з питань реформування СБУ, було розроблено проект концепції реформи СБУ. Окрім українських представників, до групи увійшли експерти з Консультативної місії ЄС та офісу зв'язку НАТО. Вони займалися розробкою концепції, яка визначає основні напрями реформи спецслужби. Однак зазначений законопроект було повернено на доопрацювання.

Крім того, було розроблено проект закону «Про внесення змін до Закону України «Про Службу безпеки України». Даний законопроект спрямований на посилення і розширення повноважень відомства, поліпшення соціального та правового захисту особового складу.

При цьому ключовими векторами реформи Служби безпеки України, відповідно до зазначеного законопроекту, є наступні:

- ліквідація підрозділів по боротьбі з корупцією та організованою злочинністю;
- трансформація підрозділів з контррозвідувального захисту економіки до підрозділу контррозвідувального захисту критичної інфраструктури;
- скорочення підслідності (економічні злочини, в тому числі контрабанди, фінансування тероризму, а також злочини проти миру, безпеки людства, міжнародного правопорядку тощо, які пропонується передати до інших державних органів);
- створення на базі військової контррозвідки окремого державного органу (з урахуванням польського досвіду);
- передача з СБУ до РНБО антитерористичного центру;
- відновлення окремого самостійного органу з охорони державної таємниці (до 1998 року існував Державний комітет України з питань державних секретів та технічного захисту інформації);
- демілітаризація всіх підрозділів забезпечення;
- істотне збільшення грошового утримання особового складу СБУ за аналогією з законодавчо закріпленими зарплатами співробітників прокуратури, Державного бюро розслідувань, Національного антикорупційного бюро України і інших органів;
- створення кваліфікаційно-дисциплінарної комісії СБУ з залучення громадянського контролю;
- уніфікація відомчої: медицини, освіти, науки із загальнодержавною системою;

- особливий порядок і права в кримінальному провадженні.

Крім того, у ст. 22 Закону України «Про національну безпеку України» розглядаються функції Державної служби спеціального зв'язку та захисту інформації України, яка є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону.

Відповідно, проведення зазначеної реформи СБУ в Україні потребує вдосконалення процесів підготовки кадрів в сфері забезпечення інформаційної безпеки відповідно до стандартів НАТО. При цьому особлива увага повинна приділятися спеціалізованим заходам за участю представників НАТО: кілька великих навчань, освітні семінари, курси англійської мови, а також стажування в аналогічних підрозділах США.

**Висновки з даного дослідження та перспективи подальших розвідок у цьому напрямку.** За результатами проведених досліджень було отримано наступні висновки.

1. Досліджено особливості забезпечення інформаційної безпеки в НАТО. Відмічено, що забезпечення інформаційної безпеки в НАТО являє собою забезпечення кібербезпеки або протистояння гібридним війнам, одним із різновидів яких є кібератаки. Стратегії гібридних війн і рекомендації щодо протистояння гібридним загрозам протягом останніх років розробляються в США і НАТО з метою посилення впливу на підготовку, хід і результат гібридної війни як військової, так і іррегулярної складових контингенту з одночасним залученням потенціалу цивільних компонентів.

2. Проаналізовано нормативну базу України стосовно забезпечення кібербезпеки у контексті протидії гібридній війні. Зазначено, що необхідно доопрацювати понятійний апарат діючого у сфері кібербезпеки законодавства, оскільки введення в правове поле нової термінології має здійснюватися комплексно і узгоджуватися з вже існуючою.

3. Окреслено перспективи реформи Служби безпеки України відповідно до стандартів НАТО. Підкреслено, що ключовим напрямом реформи СБУ відповідно до стандартів НАТО є трансформація підрозділів з контррозвідувального захисту економіки до підрозділу контррозвідувального захисту критичної інфраструктури; створення на базі військової контррозвідки окремого державного органу та відновлення окремого самостійного органу з охорони державної таємниці.

Результати дослідження дозволять суттєво вдосконалити процеси функціонування контррозвідувальних органів в державній системі забезпечення інформаційної безпеки України з урахуванням досвіду країн НАТО.

**ЛІТЕРАТУРА**

1. Дорожкин А. В. Информационная безопасность как инструмент обеспечения экономической безопасности хозяйствующего субъекта / А. В. Дорожкин, В. Н. Ясенев // Экономика и предпринимательство. 2015. − № 5-1 (58-1). − С. 812−816.
2. Широков В. А. Компьютерные преступления: основные тенденции развития / В. А. Широков // Юрист. – 2006. − № 10. − С. 18−21.
3. Ярочкин В. Безопасность информационных систем / В. Ярочкин. − М. : Ось-89, 2012. − 320 с.