УДК 324.9

**ДІОРДІЦА І.В.**

# ЧИННИКИ, ЩО НЕГАТИВНО ВПЛИВАЮТЬ НА РОЗВИТОК КІБЕРНЕТИЧНОЇ ФУНКЦІЇ ДЕРЖАВИ

У статті автором зосереджено увагу на тих чинниках, що чинять негативний вплив на формування та розвиток кібернетичної функції держави. За допомогою методу класифікації чинники, що негативно впливають на реалізацію кібернетичної функції, розбито на окремі блоки. Акцентовано на формуванні кібернетичної функції держави як однієї з основних функцій держави. Зазначено, що це є елементом наукової новизни і це питання в такій інтерпретації порушується в рамках української науки вперше.

***Ключові слова:*** *кіберпростір, кібербезпека, кібернетика, кібернетична функція, чинники формування, негативні чинники.*

В статье автором сосредоточено внимание на тех факторах, которые оказывают негативное влияние на формирование и развитие кибернетической функции государства. С помощью метода классификации, факторы, негативно влияющие на реализацию кибернетической функции, разбиты на отдельные блоки. Акцентировано внимание на формировании кибернетической функции государства как одной из основных функций государства. Отмечено, что это является элементом научной новизны и данный вопрос в такой интерпретации поднимается в рамках украинской науки впервые.

***Ключевые слова:*** *киберпространство, кибербезопасность, кибернетика, кибернетическая функция, факторы формирования, негативные факторы.*

In the article the author focuses on the factors that have a negative impact on the formation and development of the cybernetic function of the state. Using the classification method, factors that negatively affect the implementation of the cybernetic function are divided into separate blocks. The emphasis is on the formation of the cybernetic function of the state as one of the main functions of the state. It is noted that this is an element of scientific novelty and this issue in this interpretation is violated in the framework of Ukrainian science for the first time.

***Key words:*** *cyberspace, cybersecurity, cybernetics, cybernetic function, formation factors, negative factors.*

У моїх роботах подано систему аргументів щодо формування наукової гіпотези стосовно того, що на сьогоднішньому етапі **кібернетична функція держави становить собою окрему, самостійну функцію держави.**

Звичайно, що цей процес на цьому етапі, зважаючи на його швидкість, динамічність, поки не є детально описаним у наукових дослідженнях, водночас це додає наукової новизни моїй роботі. Адже наука, передусім, має реалізовувати прогностичну функцію, а не тупцювати на одному місці, здійснюючи аналіз подій, які вже відбулись. Тому доцільним, з урахуванням напрацювань інших дослідників [1−6], офіційних аналітичних доповідей [7−11], чинних нормативно-правових актів, що регулюють суспільні відносини у кібербезпековій сфері, є виділення низки чинників, що впливають на формування та подальшу реалізацію цієї функції. Причому я диференціюю ці чинники на дві загальних групи, з метою зосередження та виділення як позитивних, так і негативних чинників.

У попередній статті я розглянув позитивні чинники, тож у цій статті зосереджусь на тих чинниках, що справляють негативний вплив на формування та розвиток кібернетичної функції

© ДІОРДІЦА І.В. – кандидат юридичних наук, доцент, доцент кафедри кримінального права і процесу (Національний авіаційний університет)

держави. Їх врахування є потрібним з огляду на реалізацію не лише аналізованої функції, а й взагалі державної кібербезпекової політики.

Отже, виділю ті ***чинники, що негативно впливають на реалізацію кібернетичної функції***, які за допомогою методу класифікації з урахуванням викладеного вище підходу були мною розбиті на наведені нижче блоки.

***Світоглядний блок:***

− переваги сучасного цифрового світу не були концептуалізовані на світоглядному рівні, через що бурхливий розвиток інформаційних технологій зумовив формування можливостей не лише для реалізації законних прав та інтересів, а й виникнення нових, в тому числі гібридних загроз національній та міжнародній безпеці, до яких Україна виявилася неготовою;

− несформованість в українському суспільстві сталої ідеї щодо національної самоідентичності, в тому числі й інформаційної;

− низький рівень кіберкультури та кіберосвіти, що спричиняє кібернеосвіченість нового покоління, зокрема необізнаність про кіберзагрози;

− вузька соціальна база кіберсуспільства;

− невизначеність стратегії кіберрозвитку країни та засобів (ресурсів та факторів) її забезпечення, помилкове зосередження уваги в рамках кібербезпекової політики на кіберзахисті та кібероборони, тобто на реактивних заходах, а не проактивних, що є тиражуванням сталої для безпекового кластеру дослідників НІСД та їх послідовників позиції щодо нехтування застосування проактивного підходу і створення умов для кібердомінування України. Зважаючи на важливість цієї позиції, а також мою концептуальну та принципову незгоду з нею, детальніше активні заходи я розглядатиму під час дослідження напрямів державної кібербезпекової політики.

***Безпековий блок:***

− декларативність створення національної системи кібербезпеки: попри проголошення необхідності створення цієї системи ще у 2016 р., в Україні відбулися чисельні масовані кібератаки на центральні органи виконавчої влади, що спричинили дестабілізацію протягом певного проміжку часу діяльності усієї системи державної влади в Україні;

− неможливість кардинального посилення спроможностей суб'єктів системи національної безпеки для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю через, як показали проведені масовані кібератаки, на інформаційну інфраструктуру органів державної влади України;

− недієвість Національного координаційного центру кібербезпеки, його нездатність реально забезпечити організацію реалізації кібернетичної функції в повному обсязі всіма суб'єктами національної системи кібербезпеки;

− кардинально збільшилась кількість атак типу *APT (Advanced Persistent Threat)*, тобто цільових кібератак проти комп'ютерної мережі держави в поєднанні з негласними розвідувальними або підривними акціями, основною метою яких є отримання, порушення цілісності або блокування інформації, важливої для держави [10, с. 222];

− *використання APT*-атак (*Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 та 3, Armageddon* та інші), характерних саме для України, які були спрямовані переважно проти державних інституцій і мали яскраво виражену мету збору таємної інформації чи інформації з обмеженим доступом [10, с. 222];

− відсутність створення спеціальних підрозділів щодо протидії ведення кібервійни проти України, а також можливостей використання кіберпростору для реалізації національних інтересів у національних сегментах кіберпростору інших країн [10, с. 222];

− відсутність створення спеціальних інституціональних структур щодо протидії ведення гібридної війни проти України зі значним домінуванням кібернетичного чинника [12];

− нерозробленість механізмів синхронізації заходів, які здійснюються суб'єктами національної системи кібербезпеки і суб'єктами забезпечення національної безпеки щодо удосконалення взаємодії з міжнародними організаціями у сфері кібербезпеки та забезпеченні захисту національних інтересів України на міжнародному рівні;

− фрагментарна декларативність поглиблення міжнародного співробітництва у цій сфері, оскільки формування захищеного кіберпростору в Україні стратегічно не відповідає інтересам розвинених в інформаційному та кібернетичному плані країн та керівних угруповань;

− несформованість трьох взаємопов'язаних національних систем: захисту критичної інфраструктури, кібероборони та кіберзахисту, що передбачає вживання комплексу заходів щодо підготовки інформаційної інфраструктури сил оборони держави заради набуття необхідних

спроможностей із забезпечення здатності виконувати в кіберпросторі завдання будь-якої складності з метою реалізації національних інтересів.

***Інфраструктурний блок (див. проект концепції інфраструктури КМУ):***

− недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

− безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

− недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

− збереження критичної кіберуразливості об'єктів у районі проведення АТО.

***Організаційний блок:***

− відсутність системи кіберконтролю як за реалізацією державної кібербезпекової політики, так і за діяльністю суб'єктів національної системи кібербезпеки;

− відсутність персональної відповідальності суб'єктів кібербезпекової політики за нереалізацію окремих заходів кібербезпекової політики, а також відповідальності недержавних суб'єктів за невжиття предписаних згаданим вище суб'єктами завдань, що призвели до порушення рівня кібернетичної безпеки;

− недостатня ефективність суб'єктів забезпечення національної безпеки і суб'єктів національної системи кібербезпеки у протидії кіберзагрозам воєнного, кримінального, терористичного, розвідувального та іншого характеру;

− недостатній рівень координації, взаємодії, у тому числі інформаційної, та інформаційного обміну між суб'єктами національної системи кібербезпеки;

− нерозвиненість практики залучення недержавних суб'єктів та аналітичних організацій до реалізації окремих завдань кібербезпекової політики, зокрема відсутність розроблених правових засад інформаційного волонтерства в Україні;

− відсутність реально чинної системи е-урядування;

− відсутність концепції державної інфраструктурної політики, в якій одним із ключових аспектів мали б стати питання кібербезпекової політики в частині захисту інформаційної інфраструктури, створення умов для її сталого та безперешкодного функціонування відповідно до національних інтересів;

− невикористання достатнього позитивного досвіду неурядових організацій, у тому числі аналітичних центрів, волонтерських організацій у реалізації окремих завдань кібербезпекової політики, зокрема в транскордонному масштабі;

− відсутність конкретних кроків із реалізації проголошеного Президентом України завдання щодо інституалізації співробітництва держави та інститутів громадянського суспільства;

− відсутність розроблених навіть на модельному та імітаційному рівні дієвих механізмів кібернетичного контролю за реалізацією кібернетичної функції в рамках реалізації різнохарактерних сценаріїв кібербезпекової політики;

− відсутність єдиного підходу до застосування інструментів і механізмів організації та координації діяльності суб'єктів національної системи кібербезпеки.

***Інформаційний блок:***

− відсутність процедури погодження з адміністрацією ДССЗЗІ створення та розвитку інформаційно-телекомунікаційних систем, в яких оброблятиметься інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законодавством;

− низький рівень взаємодії замовників Національної програми інформатизації щодо погодження Генеральним державним замовником Національної програми інформатизації завдань (проектів) створення інформаційно-телекомунікаційних систем державними органами;

− відсутність національної системи параметрів (індексів та індикаторів) оцінювання стану реалізації як кібернетичної функції, так і кібербезпекової політики взагалі;

− відсутність участь методичних документів і рекомендацій щодо організації, участі та проведення міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки;

− відсутність командних навчань із реалізації заходів щодо взаємоузгодженого розгортання підрозділів кібербезпеки Збройних сил України, інших утворених за законами України

військових формувань, правоохоронних органів спеціального призначення та приведення їх у готовність до виконання завдань в умовах особливого періоду, воєнного, надзвичайного стану і під час виникнення кризових ситуацій, що загрожують національній безпеці України;

– недостатня ефективність взаємодії Національного координаційного центру з кібербезпеки з Головним ситуаційним центром РНБОУ, а також Державним центром кіберзахисту та протидії кіберзагрозам ДССЗЗІ України;

– недостатньо застосовані методики прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України в рамках усієї національної системи кібербезпеки;

– не є розробленими і впровадженими у власну діяльність суб'єктами національної системи кібербезпеки механізми обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків;

– відсутність розробленої методики визначення національних інтересів України у сфері кібербезпеки, пріоритетних напрямів, концептуальних підходів до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави;

– відсутність єдиних стандартів та регламентів функціонування системи електронного документообігу з використанням електронного цифрового підпису, а також ведення державних інформаційних ресурсів, адаптованих до міжнародних;

– використання посадовими особами державних органів спрощених паролів, що уможливлюють легкий доступ до серверів та програмного забезпечення, а також взагалі даних конкретного суб'єкта кібербезпеки;

– відсутність ідентифікаторів, які пов'язують інформаційні об'єкти в різних базах даних;

– використання електронних інформаційних систем та баз даних державних органів, взаємодія яких з ресурсами інших державних органів не була передбачена під час їх проектування і виходить за межі протоколів безпеки і захищеного контуру, що його створює ДССЗЗІ;

– відсутність системи електронної взаємодії державних електронних інформаційних ресурсів, впровадження та функціонування якої забезпечує створення, використання, обмін та збереження інформації, що належить державі, відповідно до запитів і повноважень державних органів;

– істотного вдосконалення потребує система кіберзахисту державних інформаційних ресурсів. Складно ігнорувати той факт, що Комплексна система захисту інформації (далі – КСЗІ) була побудована для значної частини тих систем, які було зламано внаслідок атаки на державні інформаційні ресурси фінансового сектору в 2016 р. Це вкотре доводить необхідність ґрунтовного перегляду чинних законодавчих документів і технічних вимог щодо побудови кіберзахисту державних установ (зокрема щодо відповідності системи КСЗІ сучасним викликам і загрозам) [11, с. 55];

– технічні складнощі, що виникають під час реалізації державної кібербезпекової політики;

– відсутність дієвих механізмів забезпечення технологічної сумісності системи електронної взаємодії державних електронних інформаційних ресурсів з електронними інформаційними системами та базами даних державних органів;

– відсутність системного інструментарію знешкодження бот мереж (наприклад, Pony та Linux/Mumblehard).

***Кримінальний блок:***

– поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет, в тому числі порушення протоколів захисту персональних даних із боку потужних соціальних мереж та месенджерів, про що детальніше йтиметься в розділі, де я аналізуватиму загрозу кібербезпеці України;

– кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави;

– зростає кількість та потужність кібератак, вмотивованих інтересами окремих транснаціональних корпорацій, держав, груп та осіб, анонімних груп хакерів, кіберальянсів, які діють почасти на замовлення спецслужб іноземних держав;

– кібертероризм перетворився з віртуальної загрози на реальну;

– кібершпигунство стає основою успішної та ефективної діяльності транснаціональних корпорацій та розвинених держав;

– збільшується кількість злочинів, пов'язаних із несанкціонованим втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку, порушенням правил їх експлуатації, несанкціонованими діями з інформацією, яка в них обробляється тощо [13]. Якщо в 2015 р. було зареєстровано 778 таких злочинів (163 справи було передано до суду) [14], то лише за 4 місяці 2017 р. вже скоєно 705 таких злочинів (185 справ передано до суду) [15].

***Правовий блок:***

− невідповідність безпекового законодавства в частині компетенції суб'єктів національної системи кібербезпеки Стратегії кібербезпеки України, зокрема необхідність чіткого визначення предметної компетенції, конкретної персональної відповідальності і механізмів контролю за реалізацією кожного завдання в рамках кібербезпекової політики згідно з: 1) Законом України «Про основи національної безпеки України»; 2) відповідних законів, що регулюють порядок організації окремих центральних органів виконавчої влади − суб'єктів забезпечення національної безпеки / суб'єктів національної системи кібербезпеки; 3) Стратегією національної безпеки України; 4) Доктриною інформаційної безпеки України; 5) Стратегією кібербезпеки України; 6) Положенням про Національний координаційний центр з кібербезпеки; 7) іншими указами Президента України, якими уводяться в дію рішення РНБОУ із зазначених питань.

− відсутність механізмів системного та ефективного державного контролю за станом реалізації кібербезпекової політики;

− практична нереалізованість і декларативність більшості правових актів, що регулюють кібернетичні відносини, зокрема, стосовно впровадження концепції е-урядування, впровадження інформаційної взаємодії, захисту кібернетичних прав у кіберпросторі тощо;

− нерозробленість правової основи для обміну електронною інформацією між електронними інформаційними системами та базами даних державних органів;

− неготовність ідентифікувати штучний інтелект як суб'єкт кібернетичних відносин з усіма правовими наслідками;

− неврегульованість суспільних відносин у сфері інтернет-телебачення;

− відсутність модельного правового регулювання відносин: людина−машина, машина−машина, машина−машина−людина через застосування консервативної правової доктрини;

− недосконалість нормативно-правової і методологічної бази, що унеможливлює в контексті інформаційної глобалізації реалізацію кібернетичних національних інтересів у кіберпросторі його суб'єктам;

− відсутність Інформаційного кодексу, в рамках якого було б здійснено систематизацію не лише інформаційного, а й кібернетичного законодавства;

− відсутність дієвого механізму правового регулювання реалізації кібернетичної функції;

− відсутність розробленої та ухваленої на рівні Указу Президента Концепції державної інформаційної політики України як керівного документа стратегічного рівня, а також відповідного законодавства у сфері лобізму як ключової правової основи успішного розвитку держави в умовах багатоальтернативних загроз у поєднанні з незначними власними можливостями щодо збереження національної інформаційної ідентичності;

− значний рівень правової небезпеки в кібернетичній сфері через порушення балансу забезпечення прав і свобод і забезпечення національної безпеки;

− відсутність правових механізмів і реальних управлінських знань стратегічного рівня лобіювання національних інтересів.

***Фінансово-економічний блок:***

− відсутність комплексної методики моніторингу (аналізу, оцінки та прогнозу) стану фінансового та організаційного забезпечення стратегій, програм та заходів із реалізації державної кібербезпекової політики;

− незбалансованість складників в інформаційній сфері через незабезпеченість цілей реалізації інформаційної функції, розвитку інформаційного суспільства та впровадження концепції е-урядування, а загалом реалізації державної інформаційної політики ресурсами;

− порівняно низький рівень розвитку вітчизняної інформаційної інфраструктури, вітчизняних кібернетичних технологій, товарів, робіт та послуг, слабка мотивація приватного сектору до формування конкурентного інформаційного ринку й недостатня політична воля керівництва держави, вираженого у сформованому інтересі до кібернетичного лідерства;

− збереження застарілих елементів регламентованої системи господарювання, що зумовлює дискретний характер державного управління у сфері кібербезпекової політики, гальмування концепції е-урядування на місцях, прояви бюрократизму, політизація процесів безпеки через

заграванння з електоратом у процесі гальмування обмежувальних заходів суб'єктів національної системи кібербезпеки у кіберпросторі;

− відсутність системної програми реалізації заходів щодо забезпечення кіберзахисту об'єктів критичної інфраструктури та захисту технологічних процесів на виробництві у реальному секторі економіки;

− системна корумпованість усіх гілок влади, відсутність національної еліти, призначенням якої стало формування гарантованих умов реалізації національних інтересів як загалом, так і в кіберпросторі зокрема.

Отже, можу зробити висновки про формування кібернетичної функції держави як однієї з основних функцій держави, враховуючи:

1) віртуалізацію та цифровізацію сучасного світу;
2) перенесення більшості державних функцій у кібернетичний простір;
3) зародження, формування та розвиток окремих національних інтересів безпосередньо в кіберпросторі;
4) залежність ефективного функціонування об'єктів критичної інфраструктури та інформаційної інфраструктури від рівня кібербезпеки;
5) необхідність формування кібербезпекової культури як засади функціонування сучасної людини кібернетичної;
6) формування інфраструктури електронних комунікацій.

Це є елементом наукової новизни, і це питання в такій інтерпретації порушується в рамках української науки вперше.

**Список використаних джерел:**

1. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні: монографія / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян / за заг. ред. В.А. Ліпкана. К., 2015. 664 с.

2. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом: монографія / В.А. Ліпкан, В.Ю. Баскаков / за заг. ред. В.А. Ліпкана. К., 2013. 344 с.

3. Ліпкан В.А. Консолідація інформаційного законодавства України: монографія / В.А. Ліпкан, М.І. Дімчогло / за заг. ред. В.А. Ліпкана. К., 2014. 416 с.

4. Ліпкан В.А. Інкорпорація інформаційного законодавства України: монографія / В.А. Ліпкан, К.П. Череповський / за заг. ред. В.А. Ліпкана. К., 2014. 408 с.

5. Стратегічні комунікації: словник / Т.В. Попова, В.А. Ліпкан ; за заг. ред. В.А. Ліпкана. К., 2016. 416 с.

6. Климентьєв О.П. Перспективи розвитку інформаційної функції держави. Підприємництво, господарство і право. 2013. № 12. С. 101−104.

7. Про внутрішнє та зовнішнє становище України в 2013 році: щорічне Послання Президента України до Верховної Ради України. К., 2013. 576 с.

8. Аналітична доповідь Національного інституту стратегічних досліджень до позачергового Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України у сфері національної безпеки». К., 2014. 148 с.

9. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2015 році». К., 2015. 684 с.

10. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». – К. : НІСД, 2016. – 688 с.

11. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». К., 2017. 928 с.

12. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К., 2017. 496 с.

13. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III (зі змінами) / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2341–14.

14. Лист Генеральної прокуратури України від 21.10.2016 р. № 19/4–1581 вих-16 URL: https://dostup.pravda.com.ua/request/kibierzlochinnist_5.

15. Лист Генеральної прокуратури України від 11.05.2017 р. № 19/4–681 вих-17. URL: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v.