

**В. В. ПЕТРОВ  
А. В. ТАРАСЕНКО**

## **ОСОБЛИВОСТІ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ**

*Розглянуто особливості логістичного забезпечення національної системи кібербезпеки України, які безпосередньо впливають на загальний стан національної безпеки. Проаналізовано наукові джерела та нормативні акти, які стосуються даної проблематики. Охарактеризовано проблеми логістичного забезпечення кібербезпеки України, що впливають на діяльність органів державної влади та об'єктів критичної інфраструктури України.*

**Ключові слова:** інформація, захист інформації, кібербезпека, національна безпека, інформаційний простір, інформаційна політика, інформаційні технології, логістичне забезпечення.

**Петров В. В., Тарасенко А. В. Особенности логистического обеспечения национальной системы кибербезопасности Украины в современных условиях**

*Рассмотрены особенности логистического обеспечения национальной системы кибербезопасности Украины, которые непосредственно влияют на общее состояние национальной безопасности. Проанализированы научные источники и нормативные акты, которые касаются данной проблематики. Охарактеризованы проблемы логистического обеспечения кибербезопасности Украины, что влияют на деятельность органов государственной власти и объекты критической инфраструктуры Украины.*

**Ключевые слова:** информация, защита информации, кибербезопасность, национальная безопасность, информационное пространство, информационная политика, информационные технологии, логистическое обеспечение.

**Petrov Valentyn, Tarasenko Antonina. Features of the logistics system of national cybersecurity Ukraine in modern conditions**

*The article discusses the features of the logistics system of national cybersecurity Ukraine, which directly affect the overall state of national security. Analysis of scientific sources and regulations relating to this subject. The characteristic*

---

© ПЕТРОВ Валентин Володимирович – кандидат політичних наук, керівник служби з питань інформаційної безпеки Апарату РНБО України

© ТАРАСЕНКО Антоніна Валеріївна – кандидат юридичних наук, співробітник СБ України

*problems of logistics to ensure cybersecurity Ukraine affecting the activity of the government and critical infrastructure Ukraine.*

**Key words:** *information, information security, cyber security, national security, information environment, information policy, information technology, logistics software.*

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Разом з тим ураження шкідливим програмним забезпеченням ряду об'єктів енергетичного сектору України у грудні 2016 року, масовані кібератаки на фінансовий сектор держави, офіційні електронні поштові скриньки посадових осіб органів державної влади з метою отримання віддаленого доступу до службової інформації, збільшення фактів несанкціонованого втручання в роботу електронних загальнодержавних баз даних (реєстрів) свідчать про недостатню увагу державних органів влади до вирішення питання щодо ефективного логістичного забезпечення кібербезпеки України.

Відповідно до Стратегії кібербезпеки України, розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, таких заходів, а саме: розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав - членів НАТО; сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події; удосконалення системи контррозвідувального та оперативно-розшукового забезпечення кібербезпеки держави; підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також

розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі тощо<sup>1</sup>.

Окремі аспекти проблематики щодо логістичного забезпечення інформаційної безпеки України розглядали як українські науковці (Д. Дубов, О. Дзьобань, О. Манжай, А. Марушак, М. Ожеван, В. Петров, В. Пилипчук, В. Панченко, М. Присяжнюк, В. Шеломенцев), так і зарубіжні вчені (Д. Аддікотт, К. Александер, С. Бейделман, Д. Браун, Л. Вентц, Т. Вінгфільд, Д. Куел, Дж. Ліндсей, Дж. Льюїс, Р. Олдріч, Е. Тоффлер, Д. Шелдон). Разом з тим, у працях цих та інших авторів не приділено належної уваги характеристиці логістичного забезпечення кібербезпеки України у сучасних умовах.

Ефективне забезпечення захисту національних інтересів держави прямо пов'язане із рівнем забезпечення кібербезпеки України.

Питання системи національної безпеки постійно привертають увагу науковців, оскільки її вдосконалення підвищує можливості України адекватно та своєчасно реагувати на широкий спектр сучасних викликів і загроз, створює сприятливі умови для досягнення своїх національних інтересів, налагодження дієвої співпраці з іншими державами.

За сучасних умов логістичне забезпечення має бути основним у ефективному функціонуванні захисту інформації в державному секторі та критично важливих об'єктів інфраструктури, а також кібербезпеки України у цілому.

Як слушно зазначає Д. Шелдон, що основною стратегічною ознакою кіберсили, яка і робить її настільки унікальною у сучасному світі, є її можливість за воєнних і мирних часів маніпулювати стратегічною обстановкою, не даючи водночас противнику зорієнтуватися в цій обстановці. Стратегічна обстановка – це те, що вже сьогодні сприймається крізь призму кібертехнологій і, відповідно, залежить від них. Отже, здатність кіберсили впливати на сприйняття противником стратегічної обстановки з часом лише зростатиме, так само як і маніпулятивні можливості кіберпростору. Відповідно, метою кіберстратегіа є максимізація зусиль, спрямованих на використання відповідних інструментів (кіберзброї), яка дозволить вирішувати диверсійні завдання проти кіберзалежного противника, знешкоджувати його системи зв'язку, моніторингу та шпигунства в

кіберпросторі та, що найголовніше, впливати на прийняття ним тих чи інших рішень на користь того, хто маніпулює ресурсом<sup>2</sup>. Тому, ефективне логістичне забезпечення, надає можливість адекватно реагувати на виклики в сфері кібербезпеки України.

Актуальність зазначеної проблеми полягає і в тому, що 12 травня 2017 р. відбулася масштабна хакерська атака, яка вивела з ладу тисячі комп'ютерів у всьому світі. При даній кібератаці використовуються шкідливі програми – «вимогач» (Ransomware), яка вимагає 300 \$ в біткоїнах для розблокування даних. Повідомлення про кібератаку надійшли з 74 країни, зокрема Великобританії, США, Китаю, Росії, Іспанії, Італії й Тайваню. Відповідно до даних Malware Tech, на сьогодні в світі, більш 1 200 заражених комп'ютерів, крім цього 107 тис. заражених комп'ютерів знаходилися в режимі онлайн. Даний вірус являє собою оновлену версію WannaCry (WNCRY) – Wana DecryptOr2.0.<sup>3</sup>

У ході розслідування спецслужбами України вказаних інцидентів встановлено, що несанкціоноване втручання в роботу інформаційних систем Державної казначейської служби України та Міністерства фінансів України за технологією ураження ідентичне цільовим комп'ютерним атакам, що здійснювались спецслужбами Російської Федерації у відношенні об'єктів критичної інфраструктури України з використанням шкідливого програмного забезпечення «Black Energy». Водночас, зловмисниками було вжито заходів із знищення (приховування) практично усіх слідів протиправної діяльності, шляхом видалення системних файлів мережевого обладнання та журналів подій операційних систем. Національною поліцією України розпочато розслідування в рамках кримінального провадження<sup>4</sup>.

У цьому контексті надзвичайно важливо провести детальний аналіз кібератак, встановити причетних до них груп чи осіб, а також встановити наявність зв'язку кіберінцидентів із юридичними чи фізичними особами, які контролюються державою-агресором.

Наведені факти втручання в інформаційно-телекомунікаційні системи державних органів загрожують цілісності інформації в реєстрах та базах даних, які належать державі та відображають конституційно гарантовані життєво важливі інтереси громадян, що підживляє довіру суспільства до безпечного функціонування державних

електронних інформаційних ресурсів як складової процесу розвитку інформатизації в Україні.

Фахівці з Центру стратегічних і міжнародних досліджень зазначають, що «головні загрози критичній інфраструктурі походять передусім від військових і розвідувальних служб інших держав, оскільки саме вони підготовлені необхідним чином, мають необхідні ресурси та ставлять перед собою чіткі цілі»<sup>5</sup>.

В умовах масштабного зростання кіберзагроз критично важливим для України є створення ефективної системи реагування на кібератаки та кіберінциденти, вчинені по відношенню до інформаційно-телекомунікаційних систем державних інформаційних ресурсів та об'єктів критичної інфраструктури загалом, а це відповідно потребує логістичного забезпечення.

Важливість кібербезпеки демонструє динаміка витрат на неї. Глобальний ринок кібербезпеки виріс з \$3,5 млрд у 2004 році до \$75 млрд у 2015. За прогнозами компанії Gartner, він досягне \$170 млрд до 2020 року<sup>6</sup>.

На забезпечення функціонування державної системи спеціального зв'язку та захисту інформації із загального фонду бюджету України на 2017 рік додатково заплановано 7 млн грн. У свою чергу, на розвиток і модернізацію державної системи спеціального зв'язку та захисту інформації буде виділено додатково 143 млн грн.<sup>7</sup>

Крім того, НАТО сприятиме розвитку військово-технічних можливостей з протидії кіберзагрозам. Куратором трастового фонду визначена Румунія, яка внесла в нього 500 тис. євро. У рамках реалізації Трастового фонду Україна – НАТО з питань кібербезпеки почалася закупівля спеціального обладнання. Процедура закупівлі були завершені в першому кварталі 2017 року, головним партнером з реалізації даного фонду є Служба безпеки України<sup>8</sup>. Наразі відбувається процедура передачі українській стороні відповідного обладнання та технологій.

Для вирішення завдання щодо удосконалення механізму взаємодії та реагування на кіберінциденти, на наш погляд, доцільно в рамках реалізації Трастового фонду НАТО утворити центральну складову національної системи кібербезпеки, організаційно-технологічним фундаментом для якої стануть ресурси Ситуаційного центру забезпечення кібербезпеки СБ України та Державного

центру кіберзахисту та протидії кіберзагрозам Адміністрації Держспецзв'язку України (CERT-UA) під егідою Національного координаційного центру кібербезпеки РНБО України.

Важливим вбачається, що США фінансуватиме створення Центру кібербезпеки для потреб Міністерства оборони України. Проект реалізується у зв'язку з занепокоєнням попередніми діями хакерських груп із Російської Федерації, що інспіровані Кремлем, як в Україні, так і в інших державах.

Це перший проект, що презентує зусилля США та НАТО по створенню для потреб Міністерства оборони України комплексної інформаційної системи, яка б поєднувала в собі можливості забезпечення кібербезпеки, управління військами та організації їх логістичного забезпечення. Зокрема, контракт міністерства оборони США на здійснення робіт отримав відомий в США провайдер технологічних рішень корпорація Black Box. Вартість контракту становить 22,7 млн доларів. В рамках зазначеного контракту Black Box здійснить розробку, постачання комплектуючих та обладнання, інсталяцію, налагодження та тестування необхідних для повноцінної роботи Центру систем – комплексної системи управління, контролю, зв'язку, комп'ютеризації та розвідки (C4I), а також системи логістичного забезпечення тощо. Втім, це лише частина більш масштабного проекту під назвою Ukraine Security Assistance Initiative – Information Technology (USAI-IT). Реалізація проекту здійснюється в рамках підтримки Урядом США зусиль України на шляху до того, щоб стати повноцінним партнером НАТО<sup>9</sup>.

Незважаючи на наявність в системі державної влади і управління суб'єктів, які опікуються питаннями захисту державних електронних інформаційних ресурсів, розроблення законодавчої та нормативно-правової бази, неналежний механізм здійснення аналізу інформації про кібератаки, кіберінциденти та реагування на ці події для усунення можливих наслідків.

Україна володіє ресурсною базою для проведення інформаційного обміну у режимі реального часу під час виявлення кібератак та кіберінцидентів, однак відсутність протоколів спільних дій суб'єктів забезпечення кібербезпеки під час вказаних подій у кіберпросторі не дозволяє оперативно вживати адекватні заходи протидії.

В умовах гібридної війни чинники негативного впливу на загальний стан національної безпеки формують високий рівень російської присутності в інформаційній сфері України, а також обґрунтована причетність окремих суб'єктів вітчизняного ринку інформаційно-телекомунікаційних послуг до діяльності російських спецслужб.

Український ринок стільникового зв'язку фактично перебуває під контролем суб'єктів господарювання Російської Федерації. Це потенційно дозволяє використовувати технічні можливості українських операторів для зняття інформації з їх телекомунікаційних мереж в інтересах спецслужб Російської Федерації, зокрема із каналів зв'язку, які використовуються у державному управлінні та в інтересах національної безпеки і оборони, що з огляду на військову агресію з боку Російської Федерації та триваючу антитерористичну операцію негативно впливає на стан обороноздатності держави.

Аналіз представлених у державному сегменті обсягів програмних продуктів, призначених для організації управління підприємством або установою та ведення їх бухгалтерського обліку, засвідчив, що практично 100 % впроваджених систем мають російське походження, а це суперечить п. 4.12 Стратегії національної безпеки України (рішення РНБО України від 06.05.2015 р., уведене в дію Указом Президента України від 26.05.2015 р. № 287) у частині відмови від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації (наприклад, програмного продукту компаній «Лабораторія Касперського» та «Доктор Веб»).

З метою ослаблення російського впливу на інформаційну сферу країни на державному рівні було вжито низку системних заходів. Рішеннями Ради національної безпеки і оборони України від 2 вересня 2015 року та від 16 вересня 2016 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», уведених в дію Указами Президента України від 16.09.2015 № 549 та від 17.10.2016 № 467, такі санкції були застосовані, зокрема до російських антивірусних програмних продуктів «Kaspersky» та «Dr.Web». Стосовно ТОВ «Доктор Веб», ЗАТ «Лабораторія Касперського», ТОВ «Лабораторія Касперського Україна» накладена заборона здійснення в Україні державних закупівель та



використання органами державної влади вказаних антивірусних програмних продуктів.

Стратегією кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 № 96, одним із пріоритетних напрямів забезпечення кібербезпеки країни визначено обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора.

Крім цього, на сьогодні ініційовано розширення переліку російських компаній, до яких застосовані спеціальні економічні та інші обмежувальні заходи, передбачені Законом. Однак, через недосконалість та застарілість нормативно-правової бази, що регулює діяльність у сфері телекомунікацій застосування обмежувальних заходів суб'єктами забезпечення кібербезпеки суттєво ускладнюється.

Визначена статтею 16 Закону України «Про телекомунікації», вимога щодо досягнення мети державного регулювання у цій сфері з урахуванням інтересів національної безпеки не отримала свого розвитку як відповідний механізм реалізації. Зокрема, рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі – НКРЗІ) від 26.01.2006 № 179, яким затверджені ліцензійні умови здійснення діяльності у сфері телекомунікацій, не враховують цієї вимоги, що вимагає внесення відповідних змін до рішення регуляторного органу.

Зокрема, зазначені зміни дозволили б координувати діяльність СБ України, НКРЗІ та, у разі виявлення ознак протиправної діяльності на шкоду національній безпеці держави з боку операторів мобільного зв'язку, що контролюються суб'єктами господарювання Російської Федерації, ініціювати проведення НКРЗІ перевірок з метою розгляду питання щодо позбавлення зазначених операторів відповідних ліцензій.

Актуальним вбачається і той факт, що у квітні 2017 р. СБ України виявила 8 компаній (у тому числі, інвестиційну компанію Dragon Capital), які застосовували заборонене шпигунське програмне забезпечення виробництва Російської Федерації. Співробітники СБ України здійснили обшуки і вилучили комп'ютерну техніку в зазначених компаніях, які використовували і реалізовували «ро-



сійське шпигунське програмне забезпечення з прихованими функціями негласного доступу, зокрема до даних з обмеженим доступом»<sup>10</sup>.

Використання послуг представництв російських ІТ-компаній в органах державної влади та на об'єктах критичної інфраструктури посилює загрозу уразливості інформаційно-телекомунікаційних систем України.

На наш погляд, це дає змогу російським спецслужбам фактично легально отримувати інформацію, до того з обмеженим доступом, щодо фінансово-господарської діяльності, документообігу, економічного стану, організаційних та структурних особливостей, обсягів оборонного замовлення, стану його виконання тощо, що може бути використано на шкоду національним інтересам України.

Накопиченню зазначених проблем у сфері кібербезпеки сприяло неналежне фінансове забезпечення щодо формування національної телекомунікаційної мережі, модернізації телекомунікаційних систем, їх захисту, створення центру оперативного управління інформаційно-телекомунікаційними системами в особливий період.

Враховуючи постійне недофінансування системи спеціального зв'язку та захисту інформації у цьому році завдяки координаційним заходам РНБО України вдалося збільшити видатки на дану сферу на 40 %, однак досягнутий обсяг асигнувань враховує потреби належного функціонування зазначеної системи лише на 48 % від потреби. Недостатньо фінансується бюджетна програма призначена для реалізації заходів щодо підвищення обороноздатності і безпеки держави, фінансування якої передбачено спеціальним фондом в обсязі 500 млн грн. Критичним залишається стан грошового забезпечення військовослужбовців.

Погоджуємося з думкою Д.В.Дубова, який стверджує, що незважаючи на зусилля спеціально уповноважених відомств, Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово уразливою до кіберзагроз і не останньою чергою через надмірне широке використання іноземних програмних продуктів (переважно – піратських) і використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможлиблюється через за-

лежність Української держави від зазначених продуктів, що вийшла на дійсно загрозливий для національної безпеки рівень на всіх рівнях і в усіх сферах. Досі актуальною є така критично важлива проблематика: відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем органів сектору безпеки і оборони України); стимулювання з боку держави створення національного антивірусу тощо<sup>11</sup>.

На думку М.М. Присяжнюка, необхідно розвивати національну систему кібербезпеки, враховуючи правові, технологічні, матеріально-фінансові та інші аспекти. На сьогодні, інформаційна безпека може бути реалізована за умови створення відповідної ієрархічної організаційної структури і орієнтування на вітчизняну наукову і виробничу інфраструктуру<sup>12</sup>.

Функціонування системи кібербезпеки України неможливе без тісної співпраці з приватним сектором – операторами та провайдерми телекомунікації, власниками та розпорядниками критичних об'єктів інформаційної інфраструктури держави, компаній, діяльність яких пов'язана зі сферою інформаційної безпеки<sup>13</sup>. Тобто, ще однією особливістю логістичного забезпечення системи кібербезпеки України є налагодження ефективної співпраці з приватним сектором, стимулювати процвітання українських ноу-хау, інновацій для забезпечення прогресу в кіберпросторі України, а також для установа фронтальної лінії оборони проти існуючих загроз.

З метою удосконалення механізму логістичного забезпечення кібербезпеки України, варто вивчити досвід Республіки Сінгапур, Уряд якої планує прийняти закон, який зобов'яже власників і операторів ІТ-інфраструктури проходити перевірку кібербезпеки і доповідати про випадки взломів. Зазначений закон є наступним кроком у реалізації програми «Розумна нація». Зокрема, планується збільшити витрати на кібербезпеку до 8 %, на сьогодні витрати становлять 2,4 % держбюджету. Крім того, Уряд Сінгапура є головним спонсором кібербезпеки держави – у 2015 р. воно фінансувало четверту частину національного ІБ-ринку. Хоча, на думку Міністра комунікацій та інформації Республіки Сінгапур Якоба Ібрагіма «зазначених витрат недостатньо, особливо за умов атак на DNS-провайдера StarHub, яка одразу відбулася за аналогічним нападом на

американського провайдера Дун». Важливий і той факт, що Республіка Сінгапур у 2015 р. займає перше місце в індексі у мережевої готовності (NRI). Високий NRI – це заслуга Уряду даної держави, яка з 2005 р. реалізує послідовний план розвитку IT-інфраструктури, який спрямований на перетворення населення в «розумну націю». В результаті чого, на сьогодні, 95 % населення зазначеної країни користуються широкосмуговим інтернетом, а в будь-якій точці острова діє безкоштовний Wi-Fi. Також під час дії даної урядової програми 5 тис. компаній отримали допомогу щодо розвитку IT-інфраструктури, зокрема 3 тис. компаній скористалися підтримкою держави для впровадження хмарних технологій SaaS («ПО як послуга»). Також Сінгапур займає перше місце по рівню розвитку електронного уряду в рейтингу університету Васеда<sup>14</sup>.

Заслугує на увагу і досвід США, зокрема американська компанія *Booz Allen Hamilton*, яка є підрядником АНБ США (*Агенство національної безпеки США*) з багатьох кібербезпекових питань, запропонувала власну методику визначення та обчислення показників кібермогутності. На думку її фахівців, до таких показників відносяться: нормативно-правове регулювання кіберпростору; економічний та соціальний контекст; технологічна інфраструктура; промислове застосування інформаційно-телекомунікаційної інфраструктури в різних сферах<sup>15</sup>.

Варто зазначити, що у Конгресі США представлено проект «Закона 2017 про співпрацю з Україною з питань кібербезпеки». Законопроект визначає, що політикою США є надання допомоги Урядові України у вдосконаленні власної стратегії кібербезпеки, зокрема, на таких напрямках, як: встановлення найбільш сучасних безпекових оновлень на комп'ютерах органів державної влади, у тому числі систем програмного захисту, спрямованих на захист об'єктів критичної інфраструктури України; зменшення залежності України від російських технологій; сприяння розширенню участі України у програмах обміну інформацією, що пов'язана з проблематикою кібербезпеки тощо<sup>16</sup>.

Погоджуємося з думкою фахівців, які наголошують, що спецслужби інших країн не мають такого досвіду, який отримала Україна в умовах гібридної війни з боку Російської Федерації. Наприклад, США мають досвід ведення воєнних дій на чужих територіях, але

досвіду протистояти російській армії і російським спецслужбам в умовах гібридної війни, на сьогодні, крім України, немає в жодній країні світу<sup>17</sup>.

У аспекті питання, що розглядається важливим вбачається створення власного антивірусу, програмного забезпечення, виділення фінансових ресурсів на кібернавчання та посилення технологічної кіберспроможності системи СБ України, інших суб'єктів забезпечення національної кібербезпеки. Також потребує удосконалення й нормативно-правова база, що регулює діяльність у сфері телекомунікацій та визначає розвиток телекомунікацій в Україні.

Варто зазначити, що щорічно кількість злочинів, які вчиняються з використанням інформаційних технологій, зростає в середньому на 8 %, водночас, необхідно враховувати високу латентність таких кримінальних правопорушень. Для прикладу, у 2016 році Національна поліція України отримала близько 10 тис. заяв про кіберзлочини<sup>18</sup>.

Виникнення якісно нового рівня загроз, пов'язаних із комп'ютерною злочинністю, глобалізований характер їх здійснення та поширення (віртуалізація, криптографія, відсутність кордонів у мережах, транснаціональні соцмережі) вимагає від держави відповідного ефективного логістичного забезпечення кібербезпеки України та побудови системи невідворотної відповідальності за їх вчинення.

Таким чином, організація роботи з підвищення логістичного забезпечення кібербезпеки України, постійне її удосконалення є одним із основних чинників, що сприяє надійному забезпеченню кібербезпеки України, кіберзахисту державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури тощо.

З метою ефективного логістичного забезпечення кібербезпеки України доцільно: збільшити обсяги фінансування на придбання сучасної техніки, на науково-технічну діяльність; укомплектувати відповідні підрозділи кваліфікованими кадрами із високим рівнем соціального захисту.

Водночас, на нашу думку, при розгортанні та розвитку національної системи кібербезпеки України, її логістичному забезпеченні має обов'язково враховуватись високий рівень присутності у національній інформаційній інфраструктурі як структур пов'язаних з дер-

жавою-агресором, так і програмних та апаратних рішень, розроблених чи виготовлених в Російській Федерації. Зазначене вимагатиме насамперед, додаткового нормативно-правового врегулювання, застосування у встановленому порядку запобіжних механізмів, передбачених Законом України «Про санкції».

Ці та інші заходи можуть створити сприятливе підґрунтя для підвищення логістичного забезпечення суб'єктів кібербезпеки України та ефективної її діяльності в умовах протидії гібридній війні.

1. *Про рішення* Ради національної безпеки і оборони України: Указ Президента України № 96/2016 від 27 січня 2016 р. «Про Стратегію кібербезпеки України» // Офіційний вісник України. 2016. № 23. 2. *Sheldon J.B.* Deciphering cyberpower strategic purpose in peace and war // *Strategic Studies Quarterly*. 2011. № 5(2). P.95–112. 3. *Зараження* вирусом-вымогателем: как обезопасить свой компьютер. URL: <https://bykvu.com/bukvy/65943>. 4. *СБУ* виявила вируси, которыми были атакованы Госказначейство и Минфин. URL: <http://itc.ua/news/sbu-vyiy>. 5. *Securing Cyberspace for the 44th Presidency* / ed.by A.J. Lewis. URL: <http://csis.org/files/media/isis/pubs/08120>. 6. *Горобець В.* Віртуальний ворог: як захистити бізнес від кібератак. URL: <http://biz.censor.net.ua/m3>. 7. *Парламент* додатково виділив 150 мільйонів гривень на кіберзахист. URL: <https://ua.censor.net.ua/news/420381>. 8. *Трастовий фонд НАТО* з питань кібербезпеки почав закупівлю обладнання для СБУ. URL: <http://dt.ua/UKRAINE/trastoviy>. 9. *В Україні* створять центр кібербезпеки, роботи фінансуватимуть США. URL: <https://defenceua.com/index.php>. 10. *СБУ* викрила 8 компаній, зокрема Dragon Capital, у використанні шпигунського ПЗ із РФ. URL: <https://asn.in.ua/ua/news/news/98679>. 11. *Дубов Д.В.* Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: дис. доктор. юрид. наук: 21.01.01. Київ, 2016. 434 с. 12. *Присяжнюк М.М., Бєлошєвич Я.С.* Інформаційна безпека України в сучасних умовах // Вісник Київського національного університету імені Тараса Шевченка. 2013. № 30. С. 42–46. 13. *Петров В.В.* Щодо формування національної системи кібербезпеки України // Стратегічні пріоритети. 2013. № 4 (29). С. 127–130. 14. *Сингапур* примет закон о кибербезопасности. URL: <http://safe.cnews.ru/news/top/2016-11-09>. 15. *Формирование* организационно-правовой системы защиты национальной инфраструктуры от киберугроз / В.В. Бик, А.А. Климчук, В.Н.Панченко, В.В. Петров. Київ: Академпресс, 2013. 200 с. 16. *У Конгресі США* представлено проект «Закону 2017 про співпрацю з Україною з питань кібербезпеки». URL: [detector.media/infospace/article/124911](http://detector.media/infospace/article/124911). 17. *Глава контррозвідки СБУ:* Россия делает ставку на криминалитет. URL: [news.liga.net/interview/politics/1468205](http://news.liga.net/interview/politics/1468205). 18. *Департамент* кіберполіції НПУ залучив до співпраці 40 хакерів. URL: <http://ua.censor.net.ua/n407633>.

**Petrov Valentyn, Tarasenko Antonina. Features of the logistics system of national cybersecurity Ukraine in modern conditions**

The rapid development of information technology is gradually transforming the world. Open and free cyberspace expands the freedom and opportunities of people, enriching society and creating a new global online marketplace of ideas, research and innovation, stimulate responsible and effective operation of government and the active involvement of citizens in governance and issues of local importance, providing publicity and transparency of government, promotes preventing corruption.

However, the defeat of malware series of the energy sector in Ukraine in December 2016, a massive cyberattack on the financial sector of the state, official electronic mailboxes officials of state power for remote access to proprietary information, increasing unauthorized interference in the national electronic databases (registers) indicate a lack of attention of public authorities to resolve the issue of providing efficient logistics CIB erbezpeky Ukraine.

In terms of large-scale growth of cyber threats crucial for Ukraine an effective system for responding to cyber attacks and kiberintsydeny committed in relation to the information and telecommunication systems of state information resources and critical infrastructure in general, and that accordingly requires logistic support.

One of the features of the logistics system to ensure cybersecurity Ukraine is to establish effective cooperation with the private sector to stimulate prosperity Ukrainian know-how, innovation to ensure progress in cyberspace Ukraine, and to set the front line of defense against existing threats.

In terms of hybrid warfare negative factors affecting the overall national security form the high level of Russian presence in the information field of Ukraine and justified the involvement of individual actors domestic market information and telecommunications services to the activities of Russian intelligence services.

Thus, the organization works to improve the logistics to ensure cybersecurity Ukraine, its continuous improvement is one of the main factors contributing to reliable supply Ukraine cyber security, cyber public electronic information resources and critical information infrastructure and so on.

In order to ensure efficient logistics Ukraine cybersecurity appropriate: increase funding for the acquisition of modern technology, the scientific and technical activities; relevant departments staffed with qualified personnel with a high level of social protection.

However, we believe that the deployment and development of national cyber security systems Ukraine, its logistics software has always taken into account the high level of presence in the national information infrastructure as structures associated with the state-aggressor, and software and hardware solutions developed or produced in.

The above will require above all further legal regulation, the application in the prescribed manner safeguards under the Law of Ukraine "On sanctions". These and other measures can create fertile ground for improving logistics software business effective cybersecurity Ukraine and its activities in terms of combating hybrid warfare.

**Key words:** information, information security, cyber security, national security, information environment, information policy, information technology, logistics software.