ТОЛСТОНОСОВ Димитрій Юрійович,
доцент кафедри бойового та логістичного забезпечення Київського інституту Національної гвардії України
ПАВЛУШКІН Павло Олександрович,
слухач магістратури Київського інституту Національної гвардії України

ВАЖЛИВІСТЬ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТІЙКОСТІ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ

В умовах непередбачуваності та постійної зміни технологій і стратегій кіберзагроз, ефективне логістичне забезпечення національної системи кібербезпеки стає визначальним фактором для забезпечення стійкості та надійності цієї системи.

Підвищення потенціалу сектору кібербезпеки в Україні вимагає ретельного вивчення та аналізу характеристик логістичного забезпечення, оскільки саме ці параметри визначають його ефективність у протидії сучасним кіберзагрозам. В цьому контексті важливо розглянути роль, функції та особливості логістичного забезпечення національної системи кібербезпеки України у вирішенні актуальних завдань в сучасному інформаційному просторі.

Відповідно до Стратегії кібербезпеки України, розвиток сектору безпеки і оборони у сфері кібербезпеки передбачає ряд заходів для зміцнення обороноздатності країни у цифровому просторі.

Ці заходи включають розвиток спеціалізованих відділів з кібербезпеки та кіберзахисту в різних установах, забезпечення сумісності з аналогічними структурами країн-членів НАТО, підвищення здатності протистояти кібертероризму, вдосконалення системи оперативного реагування на кібернадзвичайні ситуації, а також покращення контррозвідувального та оперативно-розшукового забезпечення кібербезпеки.

Крім того, передбачається збільшення здатності суб'єктів боротьби з кібертероризмом для протидії кібератакам на важливі інформаційні ресурси та критичну інфраструктуру, а також у запобіганні розвідувально-підривній діяльності іноземних спецслужб, організацій та осіб у кіберпросторі [1].

Логістичне забезпечення інформаційної безпеки України становить складну проблему, яка вимагає уважного аналізу та вирішення на різних рівнях.

Один з аспектів цієї проблематики полягає у виявленні та аналізі вразливостей в інформаційних системах та мережах, які можуть бути використані зловмисниками для незаконного доступу або атак.

До інших аспектів відносяться забезпечення безпеки персональних даних громадян, захист критичних інфраструктур від кіберзагроз, а також розробка ефективних методів виявлення, відновлення та реагування на кібератаки.

Крім того, важливо враховувати інтернаціональний аспект інформаційної безпеки та співпрацю з міжнародними партнерами у сфері кібербезпеки. Всі ці аспекти вимагають комплексного підходу та системної роботи всіх зацікавлених сторін для ефективного логістичного забезпечення інформаційної безпеки в Україні.

Ефективний захист національних інтересів України нерозривно пов'язаний з рівнем кібербезпеки країни.

Україна відкривається перед різноманітними сучасними викликами та загрозами, що ставлять під сумнів безпеку та стійкість національного інформаційного простору.

Важливою передумовою для досягнення національних інтересів та підтримання співпраці з іншими країнами є здатність країни адекватно та своєчасно реагувати на ці виклики та загрози.

У цьому контексті, ключове значення має логістичне забезпечення, яке відіграє важливу роль у забезпеченні ефективного захисту інформації в державному секторі та критично важливих об'єктах інфраструктури.

У сучасних умовах, логістичне забезпечення стає невід'ємною складовою в ефективному захисті інформації у державному секторі та на критично важливих об'єктах інфраструктури, а також у загальному забезпеченні кібербезпеки України.

Виникають випадки незаконної діяльності в мережі Інтернет, такі як неправомірне збирання, зберігання, використання, знищення, поширення особистих даних, фінансові маніпуляції, крадіжки та шахрайства, що можуть завдати значної шкоди інтересам індивідуумів, суспільства та держави.

Російська агресія, а також інші внутрішні та зовнішні загрози, зокрема отримання безвізового режиму, вимагають негайного створення національної системи кібербезпеки як складової частини загальної системи національної безпеки України.

Під час розслідування, якого здійснювали спецслужби України, виявлено, що незаконне втручання в інформаційні системи Державної казначейської служби України та Міністерства фінансів України виконувалося аналогічно цілеспрямованим комп'ютерним атакам, які проводилися спецслужбами Російської Федерації на об'єкти критичної інфраструктури України [3].

У ході цих атак використовувалося шкідливе програмне забезпечення з кодовою назвою «Black Energy». Крім того, зловмисники вжили заходи для знищення (приховування) майже всіх слідів незаконних дій, у тому числі шляхом видалення системних файлів мережевого обладнання та журналів подій операційних систем. Національною поліцією України розпочато кримінальне розслідування даного випадку [3].

Таким чином, організація роботи з підвищення логістичного забезпечення кібербезпеки України, потрібні координація і переорієнтація наукових

досліджень і розробок у сфері комп'ютерної безпеки, в області вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливий напад і локалізацію джерела нападу [5].

Отже, ефективна організація роботи та постійне вдосконалення логістичного забезпечення є ключовими факторами для надійного забезпечення кібербезпеки України, захисту державних електронних ресурсів та критичної інформаційної інфраструктури. Для досягнення цієї мети пропонується збільшити фінансування на придбання сучасної техніки та науково-технічну діяльність, а також забезпечити відповідні підрозділи кваліфікованими кадрами із високим рівнем соціального захисту.

Крім того, важливо враховувати високий рівень присутності у національній інформаційній інфраструктурі структур, пов'язаних з державою-агресором, а також програмних та апаратних рішень, розроблених чи виготовлених в Російській Федерації. Це вимагатиме додаткового нормативно-правового врегулювання та застосування запобіжних механізмів, передбачених законодавством, зокрема, Законом України «Про санкції».

Узагальнюючи, вжиті заходи сприятимуть підвищенню логістичного забезпечення суб'єктів кібербезпеки України та ефективній боротьбі з гібридною війною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. Петров В. В., Тарасенко А. В. Особливості логістичного забезпечення національної системи кібербезпеки України в сучасних умовах, *URL:* http://jnas.nbuv.gov.ua/j-pdf/jurnaukdir_2017_76_11.pdf

3. Писаревський С. В. Механізми управління державно-приватним партнерством у логистичному забезпеченні сил безпеи України *URL:* https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPysarevskyi.pdf

4. Стратегія кібербезпеки України від 15.03.2016 р. *URL*: http://zakon3. rada.gov.ua/laws/show/96/2016.

5. О. Трофименко, Я. Дубовой, "Щодо правового потенціалу безпечного функціонування кіберпростору", Кібербезпека в Україні: правові та організаційні питання: матер. ІІІ всеукраїнської наук.-практ. конф., 30 листопада 2018 р., Одеса: ОДУВС, С. 5–7.