ДЕЯКІ ПРОБЛЕМИ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

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

ТАРАСЕНКО Антоніна Валеріївна - кандидат юридичних наук, співробітник Служби безпеки України

УДК 329.09.5

В статье рассмотрены проблемы логистического обеспечения кибербезопасности Украины, которые непосредственно влияют на общее состояние национальной безопасности. Раскрыты проблемы нормативного характера, которые влияют на деятельность органов государственной власти и объекты критической инфраструктуры. На основании проведенного анализа предложены пути усовершенствования правового регулирования логистического обеспечения кибербезопасности Украины.

Постановка проблеми

На сучасному етапі розбудови України як суверенної, незалежної, демократичної, соціальної, правової держави однією з найважливіших проблем є створення ефективної системи управління та діяльності державних органів, забезпечення національної безпеки України. З урахуванням соціально-економічних і політичних умов сьогодення, а також активізації спецслужб іноземних держав та терористичних організацій, першочерговими об'єктами кібернетичного впливу яких є інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури та державні електронні інформаційні ресурси, великого значення набуває подальше вдосконалення логістичного забезпечення кібербезпеки України.

Актуальність постановки та вирішення зазначеного питання зумовлена тим, що через відсутність повноцінної системи кібербезпеки держави, належної координації дій суб'єктів її забезпечення, ефективних механізмів їх взаємодії між собою, неналежне логістичне забезпечення даної сфери, стан захисту інформації в державному секторі та критично важливих об'єктів інфраструктури оцінюється як неадекватний реальним та потенційним кібернетичним загрозам.

У Стратегії кібербезпеки України визначено пріоритети та напрями в зазначеній сфері, які полягають насамперед у виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО; розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки; розвитку та вдосконаленні системи технічного і криптографічного захисту інформації; проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі; створенні умов для впровадження в Україні сучасних технологій кіберзахисту тощо [15]. Отже, на сучасному етапі застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства, що в результаті потребує відповідного логістичного забезпечення кібербезпеки України.

Аналіз останніх досліджень та публікацій

Окремі аспекти проблематики щодо логістичного забезпечення інформаційної безпеки України розглядали як українські науковці (В. Л. Бурячок, О. М. Головко, В. І. Гурковський, О. Г. Данільян, Д. В. Дубов, Б. А. Кормич, Ю. Є. Максименко, А. І. Марущак, В. М. Желіховський, В. М. Петрик, В. Б. Толубко, С. В. Толюпа, В. О. Хорошко), так і зарубіжні вчені (Р. Арон, Т. Ваден, С. Гриняєв, А. Крокер, Д. Камерон, М. Маклюен, Дж. Най, Г. Раттрей, С. Старр, Е. Тоффлер, Д. Шелдон). Проте питання щодо логістичного забезпечення інформаційної кібербезпеки України зазначені науковці спеціально не досліджували.

Мета статті полягає в дослідженні логістичного забезпечення кібербезпеки України в умовах гібридної війни, виокремленні актуальних проблем у цій сфері та формулюванні шляхів їх удосконалення.

Виклад основного матеріалу

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.

Належне та ефективне логістичне забезпечення, надає можливість адекватно реагувати на виклики у сфері кібербезпеки України.

Варто зазначити, що керівництво Північно-Атлантичного Альянсу визнало кіберпростір п'ятим виміром ведення війни паралельно з землею, морем, повітрям та космосом [2]. На наш погляд, саме кіберпростір, який немає чітко встановлених кордонів, найближчим часом буде небезпекою номер один, посунувши при цьому тероризм.

Розглянемо детальніше на практиці, які існують проблеми логістичного забезпечення кібербезпеки України.

Так, у грудні 2016 р. було несанкціоноване втручання в роботу інформаційно-телекомунікаційної системи Державної казначейської служби України та Міністерства фінансів України, які взаємодіють по виділеному каналу зв'язку, наслідком якого стало виведення з ладу мережевого комп'ютерного обладнання державної установи, яка працює під керуванням операційної системи «Windows» [10].

Оперативній групі СБ України та Держспецзв'язку України вдалося локалізувати кіберінцидент, убезпечити від несанкціонованого доступу зловмисників державні електронні інформаційні ресурси, що обробляються в інформаційних системах Державної казначейської служби України (змінено налаштування доступу до апаратного мережевого екрану Cisco ASA та мережевих маршрутизаторів інформаційно-телекомунікаційної системи, виявлення уражених складових інформаційної інфраструктури тощо). У результаті вдалося уникнути несанкціонованого доступу до центрального банку даних (зміни або знищення інформації) автоматизованої системи «Казна».

У цілому створеним у минулому році Державним центром кібербезпеки Держспецзв'язку України, тільки за І півріччя 2016 р. зафіксовано близько 15 тис. подій інформаційної безпеки, із яких 170 носили характер DDos атак [8].

За даними Держспецзв'язку України впродовж останніх двох місяців 2017 р. на об'єктах 5 відомств та 31 держресурсі виявлено 125 тис. кібератак, із них цілеспрямованих – близько 6,5 тис. За вказаний період зафіксовано: завантаження шкідливого програмного забезпечення на веб-сервер Служби зовнішньої розвідки України; ознаки зараження вірусами типу «хробак» внутрішніх вузлів Державної фіскальної служби України; віддалене керування з Російської Федерації, Чехії, Колумбії серверним обладнанням Державної фіскальної служби України та Державної міграційної служби України; ураження шкідливими макросами, що введені у файли з розширенням *.doc, *.xls, близько 30 установ, зокрема регіональних підрозділів Пенсійного фонду України; підключення до командних серверів BlakEnergy; кібердиверсії, які здійснювалися наприкінці 2015 – початку 2016 р. щодо об'єктів енергетичної галузі декількох регіонів України, мереж авіаперевезень аеропорту "Бориспіль" та залізничних перевезень [7].

Ураження шкідливим програмним забезпеченням ряду об'єктів енергетичного сектору України у грудні 2016 р.; масовані кібератаки на фінансовий сектор держави, систему соціального та правового захисту громадян, 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 та спецслужб до вирішення цього питання, в тому числі відповідного логістичного забезпечення даної сфери.

Для надання послуг захищеного Інтернет-доступу користувачам органів державної влади та недержавних установ у Держспецзв`язку України функціонує захищений вузол Інтернет-доступу (ЗВІД). Однак, до ЗВІД наразі підключено лише 8 вебсайтів державних органів та 27 веб-ресурсів Луганської ОДА.

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 [12].

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 підриває довіру суспільства до безпечного функціонування державних електронних інформаційних ресурсів як складової процесу розвитку інформатизації в Україні.

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 р. [2].

На забезпечення функціонування державної системи спеціального зв'язку та захисту інформації із загального фонду бюджету України на 2017 рік буде додатково виділено 7 млн грн. [9].

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. Планується, що процедури закупівлі будуть завершені в І кварталі 2017 р., головним партнером з реалізації даного фонду є Служба безпеки України [2].

Для вирішення завдання щодо удосконалення механізму взаємодії та реагування на кіберінциденти доцільно було 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. У 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'ютерізації та розвідки (С4І), 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 [2].

Незважаючи на наявність у 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 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»).

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

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.

Російські компанії через свої представництва, філії та дистриб'юторські компанії-

партнери поширюють продукцію програмного забезпечення на територію України з відповідним технічним супроводом.

Після внесення Україною ТОВ «Лабораторія Касперського Україна» до санкційного списку російськими власниками змінено засновників товариства на британську компанію «KaspersкyLabLimited».

Це створює умови для витоку інформації з обмеженим доступом, а також проведення диверсійної та розвідувально-підривної діяльності спецслужбами Російської Федерації, зокрема на об'єктах критичної інфраструктури України.

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

Враховуючи хронічне недофінансування системи спеціального зв'язку та захисту інформації, у цьому році завдяки координаційним заходам РНБО України вдалося збільшити видатки на цю 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 [14].

Погоджуємося з думкою О. Головка, який констатує, що запорукою ефективної протидії кіберзлочинності є високий рівень культури та професійної підготовки фахівців із забезпечення інформаційної безпеки. Прикладом міжнародної співпраці у цьому напрямку є Концепція підготовки суддів та прокурорів з питань кіберзлочинності, розроблена Радою Європи у межах Проекту «Кіберзлочинність» [3, с. 84].

В аспекті питання, що розглядається, на сьогодні актуальним є кадрова політика у сфері кібербезпеки, зокрема, для порівняння фахівець у ДССЗІ отримує 3,5 тис. грн. за місяць, кіберполіцейський – близько 11 тис. грн.. Водночас у приватних ІТ-компаніях зарплати фахівця сягають 30 тис. грн. і вище [17].

Варто зазначити, що кібербезпека – це передусім людський ресурс. Проте, на думку більшості представників відомств, задіяних у системі забезпечення кібербезпеки України, кадрове забезпечення відомств відповідними фахівцями у сфері кібернетичної безпеки все ще є незадовільним. Незважаючи на те, що низка вищих військових, цивільних і відомчих навчальних закладів здійснюють підготовку фахівців за різноманітними спеціальностями, які можна віднести до сфери інформаційної безпеки, якість їх підготовки не відповідає вимогам. Крім того, рівень матеріальних і нематеріальних стимулів унеможливлює залучення висококласних фахівців (молодих спеціалістів) до силових структур, задіяних у забезпеченні безпеки вітчизняного кіберпростору [12]. Отже, ефективне логістичне забезпечення кібербезпеки України є дієвою запорукою реагування на кіберзагрози, зокрема протистояння російським спецслужбам в умовах гібридної війни.

Як слушно зазначає Д.В.Дубов, що в Україні жодного разу не проводилися комплексні навчання з проблеми кібербезпеки (на кшталт навчань «Кіберштурм», що проводяться у США, або аналогічних навчань, що проводяться ЄС) із залученням усіх відомств, які належать до системи забезпечення кібербезпеки держави. Майже відсутні поліпрофільні науково-дослідні інститути, задіяні в комплексних дослідженнях інформаційної (кібер) безпеки. Переважно дослідження з відповідної тематики стосуються проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки; про соціально-гуманітарний компонент, а надто поєднання технологічних та гуманітарних складників, не йдеться [5, с. 335-336].

Варто зазначити, що у червні 2017 року у Києві заплановано провести перший щорічний Глобальний Саміт з Кібербезпеки 2017 (GCS17), який збере сотні експертів з кібербезпеки та технологій. Саміт буде включати виступи спеціалістів багатьох профілів,

панелі та заходи, що стосуються важливих питань в області кібербезпеки, а також використання новітніх технологій для вирішення проблем від місцевого до глобальних рівнів. Це надасть можливість представникам наукових кіл, некомерційних організацій, а також приватного сектора долучитися до передової практики, новітніх досягнень, інновацій у галузі систем захисту систем керування промисловими об'єктами, Інтернет речей (IoT) та інших сферах.

Варто зазначити, що Укроборонпром розпочав підготовку до створення в Україні нового та консолідованого центру кібербезпеки із залученням фахівців інформаційної безпеки NATO, консультантів турецької компанії HAVELSAN та спеціалістів Київського політехнічного інституту імені Ігоря Сікорського.

Ще одна проблема полягає в тому, 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 унеможливлюється через залежність Української держави від згаданих 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); стимулювання з боку держави створення національного антивірусу тощо [5, с. 336]. Тобто підтримка вітчизняного наукового потенціалу та відповідне логістичне забезпечення в зазначеній сфері є невід'ємною складовою кібермогутності України.

Крім цього, такі підприємства, як київський завод «Радіоприлад», НВО «Імпульс», НВО «Кристал», Науково-виробниче об'єднання «Електронмаш», ВО імені С. П. Корольова, завод «Арсенал», Харківський НВО «Хартрон» тощо, майже всі вони припинили своє існування, хоча працювали на національну економіку в сфері інформаційних технологій. Зокрема, саме на НВО «Кристал» вперше в СРСР розробили технологію виробництва тонкоплівкових мікросхем на основі танталу, створили перший у СРСР і Європі мікрокалькулятор на чотирьох великих інтегральних схемах МОН зі ступенем інтеграції до 500 транзисторів на кристалі й багато інших новинок [9].

Потребує фінансової підтримки нагальна необхідність посилення технологічної кіберспроможності система СБ України, інших суб'єктів забезпечення національної кібербезпеки.

В аспекті питання, що розглядається, важливим вбачається удосконалення та приведення у відповідність до національних інтересів на сучасному етапі нормативно-правову базу, що регулює діяльність у сфері телекомунікацій та визначає розвиток телекомунікацій в Україні.

В Україні загрозливих масштабів набуває використання комп'ютерними шпигунами та хакерами високих інформаційних технологій для здійснення незаконних безготівкових трансакцій, шахрайства з використанням, викраденням персональних даних. Крім того, поширюється використання інформаційних ресурсів для незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей [1]. Тобто необхідно вдосконалювати системи кібербезпеки через ефективне логістичне забезпечення даної проблематики.

Побіжною складовою проблематики кібердобровольців є не унормовані в українському законодавстві та практиці механізми взаємовідносин держави (державних органів) із середовищем ІТ-фахівців безпекового спрямування (яких часто і відносять до «хакерів»). Наприклад, якщо модель взаємовідносин із хакерами-«чорними капелюхами» (Black hat), які частіше за все є традиційними кіберзлочинцями, ситуація зрозуміла, то все ще залишається дві категорії, які напряму не завдають шкоди компаніям. Наприклад, це хакери «білі капелюхи» (White

hat) – фахівці з IT (як легально працюючі на компанії, так і одинаки), що ставлять за мету вдосконалювати системи кібербезпеки тих чи інших структур (державних чи приватних), у тому числі – через пошук недоліків коду тих інформаційних систем, які використовують ці структури. Однак пошук таких унедоліків мало чим відрізняється від дій «чорних капелюхів», крім цілі. В суто нормативно-правовому сенсі законодавство не робить різниці між ними, хоча діяльність «білих капелюхів» надзвичайно корисна. Ще більш неоднозначна ситуація із «сірими капелюхами» (Grey hat), які займають проміжну позицію між двома полюсами [5, с. 331].

На нашу думку, цінним для запозичення є досвід Федерального бюро розслідувань (далі – ФБР) США в аналізованій сфері. Зокрема, за часів керівництва ФБР Едгаром Гувером було значно піднято її престиж, головним чином завдяки співпраці із засобами масової інформації та належному фінансуванню. Необхідно зазначити, що на сьогодні захист США від кібератак і високотехнологічних злочинів належить до пріоритетних напрямів діяльності ФБР, для реалізації якого з бюджету ФБР (складає 8,3 млрд доларів США) додатково виділяються кошти [16].

Натомість в Україні фінансування як Служби безпеки України, так і інших державних органів, до повноважень яких належить боротьба із кіберзлочинністю, є недостатнім, що не дозволяє належним чином здійснювати таку діяльність, а також матеріально заохочувати їх співробітників та залучати фахівців із інших структур.

Висновки

Таким чином, необхідно використовувати власний науково-технічний потенціал для подальшого логістичного забезпечення кібербезпеки України для забезпечення захисту інформації в державному секторі та критично важливих об'єктів інфраструктури.

Отже, розвиток сучасних інформаційно-комунікаційних технологій, збільшення ролі інформації є важливим ресурсом соціально-економічного, технологічного і технічного розвитку та все більше визначають вектор нашої епохи, наближаючи її до ери інформаційного суспільства. На сьогодні інноваційні інформаційно-комунікаційні технології (є інструментарієм впливу на всі сфери сучасного суспільства) роблять величезний перетворювальний вплив на всі сфери сучасного суспільства як у межах національних кордонів, так і у світі в цілому. Можна констатувати, що в умовах гібридної війни Російської Федерації проти України головною причиною формування зазначених чинників загроз інформаційній безпеці є системні прорахунки владних структур упродовж тривалого періоду в реалізації державної інформаційної політики та неефективне використання національного потенціалу інформаційно-комунікаційних технологій, що зумовило загострення безпекових проблем у період відкритої агресії проти нашої держави.

Також необхідно звернути увагу на науковий потенціал у сфері інформаційних і технічних наук, для створення вітчизняних систем у забезпеченні кібербезпеки України, в тому числі криптографії, з метою ефективного контролю над державним телеінформаційним простором (системами). Зокрема, важливим напрямом формування законодавчо-правової системи забезпечення кібербезпеки є імплементування у вітчизняне законодавство вимог Конвенції Ради Європи «Про кіберзлочинність», що в умовах зростання кіберзлочинності як у транскордонному вимірі, так і всередині країни набуває властивостей суттєвого чинника впливу на стан національної безпеки України.

Література

1. В Україні зростає кількість кіберзлочинів. [Електронний ресурс]. –Режим доступу: https://www.epravda.com.ua/news/2016/03/28.

2. В Україні створять центр кібербезпеки, роботи фінансуватимуть США. [Електронний ресурс]. –Режим доступу: https://defenceua.com/index.php/home-page/2370.

3. Головко О. М. Проблемні питання щодо створення національної системи кібербезпеки / О. М. Головко // Матеріали постійно діючого науково-практичного семінару на тему: «Правове забезпечення оперативно-службової діяльності: актуальні

АНОТАЦІЯ

У статті розглянуто проблеми логістичного забезпечення кібербезпеки України, які безпосереднъо впливають на загальний стан національної безпеки. Розкриті проблеми нормативного характеру, які впливають на діяльність органів державної влади та об'єктів критичної інфраструктури. На основі проведеного аналізу запропоновано шляхи удосконалення правового регулювання логістичного забезпечення кібербезпеки України.

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

SUMMARY

The article deals with the problems of logistics provision of cybersecurity of Ukraine, which directly affect the general state of national security. Problems of a regulatory nature that affect the activities of public authorities and critical infrastructure facilities are disclosed. On the basis of the analysis, ways of improving the legal regulation of the logistics provision of cybersecurity of Ukraine are proposed.

проблеми та шляхи їх вирішення», 24 травня 2013 р.; м. Харків / Редкол. : С. Кучерина (голов.ред.) та ін. – Х.: Оберіг, 2013. – 272 с.

4. Горобець В. Віртуальний ворог: як захистити бізнес від кібератак /_В. Горобець. [Електронний ресурс]. Режим доступу: http://biz.censor.net.ua/m3009622.

5. Дубов Д. В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України : дис. доктор. юрид. наук : 21.01.01 / Дубов Дмитро Володимирович . – К., 2016. – 434 с.

6. З приводу працевлаштування в CERT-UA [Оновлено] [Електронний ресурс]. – Режим доступу:http://cert.gov.ua/?p=1967.

7. За 2 месяца на госструктуры совершено 6,5 тысяч кибератак, к ним причастны спецслужбы РФ – Порошенко. [Електронний ресурс]. –Режим доступу: http://nbnews.com.ua/ru/news/193789/.

8. За півроку на держоргани України було 170 DDoS-атак. [Електронний ресурс]. – Режим доступу:http://www.pravda.com.ua/news/2016/08.

9. Киевский «Кристалл»: от первого в Европе микрокалькулятора до 16-разрядных микропроцессоров. [Електронний ресурс]. – Режим доступу : http://ru.uacomputing.com/stories/crystal/.

10. Міллер К. Що знає влада про кібератаки на Мінфін, Держказначейство і Пенсійний фонд? / К. Міллер. [Електронний ресурс]. –

Режим доступу: http://www.radiosvoboda.org/a/28172354.html.

11. Парламент додатково виділив 150 мільйонів гривень на кіберзахист. [Електронний ресурс]. – Режим доступу: https://ua.censor.net.ua/news/420381.

12. СБУ выявила вирусы, которым и были атакованы Госказначейство и Минфин. [Електронний ресурс]. – Режим доступу: http://itc.ua/news/sbu-vyiyavila-virusyi-kotoryimi.

13. Трастовий фонд НАТО з питань кібербезпеки почав закупівлю обладнання для СБУ. [Електронний ресурс]. Режим доступу:http://dt.ua/UKRAINE/trastoviy.

14. Указ Президента України № 422/2016 Про рішення Ради національної безпеки і оборони України від 28 вересня 2016 р. «Про невідкладні заходи щодо фінансування потреб національної безпеки і оборони України у 2016 році» // Офіційний вісник України. – 2016. – № 78.

15. Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. «Про Стратегію кібербезпеки України» // Офіційний вісник України. – 2016. – № 23.

16. Федеральне бюро розслідувань. [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org.

17. Ще один фронт. [Електронний ресурс]. – Режим доступу : www.m.tyzhden.ua/publication/183407.

Стаття надійшла до редакції 19.01.2017 року