УДК 351.865(477)
DOI: 10.34132/pard2019.05.02

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Ємельянов В.М., д-р наук з держ. упр., професор, Інститут державного управління, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна

Бондар Г.Л., канд. політ. н., доцент, Інститут державного управління, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна

Стаття присвячена аналізу особливостей кібербезпеки як важливої складової національної безпеки України, законодавчого і нормативно-правового забезпечення даної сфери, реалізації чисельних заходів державою під час боротьби з кібернападами на об'єкти критичної інфраструктури, об'єкти громадянського суспільства та діяльності спеціалізованих державних структур, які забезпечують кіберзахист країни в умовах протидії російській агресії, з використанням сучасних світових практик, зокрема країн НАТО та ЄС в означеній сфері. Розкрито особливості, стратегії та суб'єкти кібернападів на стратегічні об'єкти критичної інфраструктури України, приватні підприємства та ЗМІ. Проаналізовано закордонний досвід боротьби з кіберзлочинністю за допомогою комплексних, збалансованих стратегій управління кіберризиками. Результати дослідження досвіду України та світу у боротьбі з кіберзлочинністю доводять, що неможливо повністю позбутись ризиків у сфері кібербезпеки. Проте, на нашу думку, спільні зусилля світової спільноти щодо обміну досвідом, технологіями, здобутками фахівців у сфері кіберзахисту, взаємна фінансова підтримка, скоординована спільна системна відповідь країн на кіберзлочини, запровадження

нових світових стандартів з кібербезпеки та інформаційної безпеки, оновлення національних та міжнародних стратегій, законодавства, які б відповідали новим кібервикликам, є запорукою подолання спільними зусиллями нових сучасних викликів. Також авторами розглянуто нагальність розробки окремої комплексної державної програми для освітніх закладів, державних установ, програми співпраці з підприємцями, громадськими організаціями, з метою охопити всі категорії населення та навчити елементарним заходам кібербезпеки, інформаційної безпеки, ознайомлення їх з кіберризиками під час здійснення діяльності в кіберпросторі, інформування про спеціалізовані державні підрозділи, які можуть надати кваліфіковану допомогу у випадку нападів з боку кіберзлочинців.

Ключові слова: *кібербезпека, кіберзахист, кібернапад, критична інфраструктура України, кіберризики, фішинг.*

Постановка проблеми у загальному вигляді.

Кібербезпека є важливою складовою національної безпеки України. У 2015 році Україна затвердила Стратегію національної безпеки [1], відповідно до якої захист критичної інфраструктури є одним з пріоритетних напрямків державної політики, а у 2016 році Стратегію кібербезпеки [2]. Прийняттю цих Стратегій передували надзвичайні події, з якими Україна зіткнулася вперше. Зокрема, у 2014 році зафіксовано 1240 зовнішніх втручань у діяльність об'єктів критичної інфраструктури України, у 2015 році – 865, у 2016 – трохи більше 200 [3]. У 1 кварталі 2019 року в Україні зафіксовано 1 582 054 кіберінцидентів [4]. Критична інфраструктура є життєво важливою для будь-якої країни світу, оскільки вона включає в себе сектори оборони, промисловий, енергетичний, охорони здоров'я, виробництво критично важливих продуктів і продуктів харчування, водопостачання і транспорт. В Україні триває процес розробки і розвитку власної моделі кіберзахисту держави в умовах протидії російській агресії, з використанням сучасних світових практик, практик країн НАТО та ЄС в означеній сфері. Саме тому розробка нових сучасних заходів боротьби з кібернападами українських фахівців, досвід цієї боротьби є дуже корисним і для іноземних партнерів,

в контексті кіберзахисту своїх країн та спільної світової протидії кіберзлочинності, оскільки вона все більше використовується не лише для вимагання коштів, а й як потужна стратегія дестабілізації та геополітичного впливу з боку окремих країн.

Аналіз останніх досліджень і публікацій. Авторами статті було проаналізовано законодавчу та нормативно-правову базу у сфері національної безпеки та кібербезпеки як її складової. Зокрема, Закон України «Про інформацію» 2.10.1992 року № 2657-XII [5]; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5.07.1994 року № 80/94-ВР [6]; Закон України «Про ратифікацію Конвенції про кіберзлочинність» 7.09.2005 року № 2824-IV [7]; Закон України «Про Державну службу спеціального зв'язку та захисту інформації» 23.02.2006 року № 3475-IV [8]; Закон України «Про захист персональних даних» 1.06.2010 року № 2297-VI [9]; Закон України «Про доступ до публічної інформації» 13.01.2011 року № 2939-VI [10]; «Стратегія національної безпеки України», затверджена Указом президента України № 287/2015[1]; «Стратегія кібербезпеки України», затверджена Указом Президента України № 96/2016 [2]; Указ Президента України від 01.05.2014 № 449 «Про рішення Ради національної безпеки і оборони України від 28.04.2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»[11]; Указ Президента України від 13.02.2017 № 32 «Про рішення Ради національної безпеки і оборони України від 29.12.2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»[12]; Указ Президента України «Про Національний координаційний центр кібербезпеки» від 7.06.2016 року № 242/2016 [13]; Закон України «Про основні засади забезпечення кібербезпеки України» 5.10.2017 року № 2163─VIII [14]; «Доктрина інформаційної безпеки», затверджена Указом Президента України № 47/2017 [15]; Закон України «Про національну безпеку України» від 21.06.2018 № 2469─VIII [16]; Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [17]. Також проаналізовано дослідження вітчизняних та іноземних установ, які

опікуються системами кіберзахисту, серед них: Відділ реагування на інциденти CyS Centrum (CyS─CERT); ESET ─ міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки; Корпорація Microsoft; американська компанія ─ Fortinet, що спеціалізується на пристроях мережевої безпеки та займає 3 місце в світі за щорічним обсягом проданих пристроїв мережевої безпеки. Також використовувались дані з офіційних сайтів органів державної влади.

Формулювання цілей статті (постановка завдання). Під час дослідження автором були визначені наступні завдання:

- проаналізувати особливості кібербезпеки як важливої складової національної безпеки України, законодавчого і нормативно-правового забезпечення даної сфери, реалізації чисельних заходів державою під час боротьби з кібернападами на об'єкти критичної інфраструктури, об'єкти громадянського суспільства та діяльності спеціалізованих державних структур, які забезпечують кіберзахист країни в умовах протидії російській агресії, з використанням сучасних світових практик, зокрема країн НАТО та ЄС в означеній сфері;
- розкрити особливості, стратегії та суб'єкти кібернападів на стратегічні об'єкти критичної інфраструктури України, приватні підприємства та ЗМІ;
- проаналізувати закордонний досвід боротьби з кіберзлочинністю за допомогою комплексних, збалансованих стратегій управління кіберризиками.

Виклад основного матеріалу дослідження. Протягом першого кварталу 2019 року в державному та приватному секторі України зафіксовано понад 1,5 млн кіберінцидентів. Центр реагування на кіберзагрози Державної служби спеціального зв'язку та захисту інформації України ─ CERT-UA, який забезпечує раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах підключених до інтернету, та є механізмом координації зусиль учасників кіберзахисту державного та приватного секторів, у 1 кварталі 2019 року зафіксував 1 582 054 кіберінцидентів. Водночас, звернень щодо кіберінцидентів від власників енергетичних систем України та фінансових установ не надходило. А після

завершення виборів до парламенту спостерігається тенденція до зниження кількості кіберінцидентів. За 1 квартал 2019 року в Україні зафіксовано понад 1,5 млн кіберінцидентів [4].

Досліджуючи історичний перебіг подій, пов'язаних з кібернападами на об'єкти критичної інфраструктури України, зазначимо про їх особливості. Так, 12 травня 2014 року були надіслані електронні листи зі шкідливими програмами українським підприємствам, які займаються залізничними перевезеннями. До листа було прикріплено документ-приманку (т.зв. фішинг ─ різновид соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки, розсилка листів з проханнями повідомити свої облікові дані, пароль), який мав вигляд вікна текстового процесору Office Word. Ця кібератака була спрямована на об'єкти критичної інфраструктури України, на 6 залізних доріг, які підпорядковувались Державній адміністрації залізничного транспорту, підприємств та установ залізничного транспорту загального користування Акціонерному товариству «Українська залізниця» (державне акціонерне товариство залізничного транспорту загального користування). Це дозволяє зробити висновки про перші спроби кібератаки об'єктів критичної інфраструктури шкідливою програмою BlackEnergy2/3.

На початку березня 2015 року, було отримано інформацію про здійснення кібератаки на українські радіомовні компанії. Зловмисниками було використано шкідливу програму BlackEnergy2/3. На електронну пошту компаній надходили листи з документами (.xls і .pps), які мали шкідливий макрос та JAR-файл, який запускав PE-файл. Характерною особливістю хакерської атаки було те, що документи-приманки мали теми, присвячені революційним подіям та мобілізації в Україні [18].

Перший у світі факт вдалої атаки на об'єкти енергетичної інфраструктури було зафіксовано 23 грудня 2015 року в Україні. Внаслідок хакерської атаки були виведені з ладу автоматизовані системи управління технологічними процесами ─ енергетичними підстанціями. Внаслідок цього електромережі були знеструмлені на 3─8 годин. Про напад повідомили Київобленерго, Прикарпаттяобленерго, Чернівціобленерго [19].

 Issue DOI: 10.34132/pard

Отже, у 2014 році хакери здійснювали підготовчі заходи, а у лютому-березні 2015 року було надіслано шкідливий додаток вірус BlackEnergy на електронні пошти трьох енергопостачальних компаній України, але помітили спроби хакерів лише у червні 2015 року. Вперше вірус виявили у Хмельницькобленерго у червні 2015 року, однак державою не було вжито належних системних заходів щодо захисту об'єктів критичної інфраструктури. На думку фахівців, зараження інформаційних мереж підприємств енергетичного сектору відбулось за 6 місяців до подій 23 грудня 2015 року. Після запуску вірусу зловмисники отримали можливість збирати інформацію про структуру інформаційних мереж, програмних засобів, що використовуються, інформацію про облікові записи віддаленого доступу до інфраструктури, паролі тощо. Потім відбулось захоплення управління АСДУ з виконанням операцій вимикань на підстанціях, виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори), знищення інформації на серверах та робочих станціях (утилітою KillDisk) та атака з номерів у Російській Федерації на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Перерва в електропостачанні склала від 1 до 3,5 годин. Загальний недовідпуск – 73 МВт*год (0.015 % від добового обсягу споживання України). З метою стабілізації ситуації з неконтрольованими відключеннями та взяття її під контроль, зловмисники змусили технічний персонал обленерго вивести АСДУ з роботи та перевести управління перемиканнями в розподільчих мережах у ручний режим [20].

Разом зі шкідливою програмою «BlackEnergy» дві третини зловмисників застосували й «програму-руйнівник» для приховування слідів протиправної діяльності шляхом знищення інформації на засобах обчислювальної техніки. Ця програма відрізнялася від тієї, яку застосовували проти телевізійних ЗМІ тим, що мала функціонал «таймера» і завершувала роботу двох конкретних процесів «sec_service.exe» і «komut.exe». Фахівці так і не дійшли згоди щодо того, чи були підстанції відключені автоматично спеціальною програмою, чи це було зроблено віддалено. Але факт наявності доступу

до сегменту мережі (комп'ютера), з якого можливий доступ до інтерфейсу управління SCADA-системами, за допомогою RDP / VNC / SSH, містить в собі велику загрозу критичній інфраструктурі та національній безпеці України [18] та світовій енергетичній спільноті.

За висновками робочої комісії Міненерговугілля України, причинами несанкціонованого втручання були відсутність загальних обов'язкових вимог до енергетичних компаній щодо забезпечення ІТ-безпеки систем автоматизації виробництва, недостатня поінформованість та підготовка технічного персоналу в частині кібербезпеки, відсутність внутрішніх структур контролю з кібербезпеки, незалежних від системних адміністраторів тощо [21].

19 та 20 січня 2016 р. зловмисниками було здійснено масову вірусну розсилку на електронні адреси підприємств електроенергетики ДП «НЕК «Укренерго»». Інформація у розсилці стосувалася зміни дати громадських обговорень Плану розвитку ОЕС України, до повідомлення був доданий файл з нібито Проектом згаданого плану, який був заражений вірусом. ДП «НЕК «Укренерго»» оприлюднив офіційне звернення, у якому було застереження про те, що він не надсилає подібних листів електронною поштою [22].

6 грудня 2016 р. були здійснені кібератаки на інформаційно-телекомунікаційну роботу Державної казначейської служби України, Міністерства фінансів, Пенсійного фонду, Фондову біржу ПФТС. Під час здійснення атак зловмисники використовували легітимні канали зв'язку (Telegram, пошту). Хакерську атаку вдалось відбити, пошкоджені сервери, внутрішні мережі, бази, сайти державних установ відновили функціонування, а всю інформацію було збережено. Для того, щоб запобігти аналогічним атакам надалі Уряд виділив 40 млн грн. Мінфіну і 40 млн грн. Держказначейству для заміни старого ІТ-обладнання, для закупівлі нового активного мережевого обладнання, маршрутизаторів, комутаторів, фаєрволів, засобів резервування та копіювання, раннього виявлення та попередження проникнення. Проте цей та інші кібернапади несуть в собі нові сучасні загрози, яким важко протистояти державним чи приватним кампаніям не лише в Україні. Серед цих загроз найбільшою є можливість компрометації хакерами будь-яких робочих станцій (і

тих, що мають, і тих, що не мають доступу до Інтернету), а також будь-якої одиниці обладнання, до якої передбачений доступ ззовні (веб-серверу, поштового серверу, маршрутизатору, АТС тощо). Це повинно бути враховано установами під час розробки моделі загроз і/або проектування мереж і систем.

12 лютого 2016 р. Міненерговугілля України створила групу представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. Робоча група працювала з 18 січня 2016 року по 3 лютого 2016 року. За результатами розслідування було виявлено, що компрометація інформаційних мереж обленерго відбулась як мінімум за 6 місяців до основних подій за допомогою методів соціальної інженерії – розсилкою підробних листів з тілом завантажувача вірусу сімейства «BlackEnergy» на електронні адреси (що були у відкритому доступі у мережі Інтернет) співробітників компаній. Після запуску вірусу зловмисники отримали можливість збирати інформацію про структуру інформаційних мереж, програмних засобів, що використовуються, інформацію про облікові записи віддаленого доступу до інфраструктури, паролі тощо [21].

Наразі Міненерговугілля працює над створенням Галузевого центру кібербезпеки енергетичних об'єктів як сегменту національної системи кібербезпеки. Головним завданням центру буде моніторинг стану кібербезпеки галузі, своєчасне інформування про кіберзагрози та агрегація і обмін інформацією про кіберінциденти із національними центрами кібербезпеки Державної служби спеціального зв'язку, захисту інформації, Служби безпеки України. Також планується створення Проектного офісу з кібербезпеки, для підтримки технічно потенційних проектів у сфері кібербезпеки. Це стосується створення Галузевого центру кібербезпеки, аудиту енергетичної галузі, розробки відповідної нормативної бази [22].

На думку С. Кобба, старшого дослідника, фахівця з безпеки компанії ESET (міжнародна компанія-розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки), критична інфраструктура є дуже важливою, оскільки вона включає

в себе сектори оборони та охорони здоров'я, виробництво критично важливих продуктів і продуктів харчування, водопостачання і транспорт. У статті він згадує про події в Україні у грудні 2015 року, коли в результаті кібератак на українських енергокомпаніях було відключено електроенергію на кілька годин для сотень тисяч будинків, та зазначає, що першою статтею опублікованою дослідниками ESET в 2016 році (про цей інцидент), була стаття А. Черепанова. В ній він детально проаналізував «BlackEnergy» – шкідливий код, використаний у згаданій кібератаці, та зазначив, що це шкідливе програмне забезпечення безпосередньо не маніпулювало пристроями промислової системи управління (ICS), але дозволяло хакерам потрапляти в мережі компаній по розподілювачу електроенергії та знищувати програмне забезпечення, що використовується обладнанням ICS [23].

Проте інша кібератака, яка відбулася в Україні у кінці 2016 року була зовсім іншою. Співробітники-дослідники кампанії ESET А. Черепанов і Р. Ліповскі повідомили про це на сайті WeLiveSecurity by ESET. Їх аналіз був присвячений новій шкідливій програмі, яка здатна безпосередньо керувати комутаторами й автоматичними вимикачами підстанцій, в деяких випадках буквально відключаючи і знову включаючи їх (що здатне серйозно порушити подачу електроенергії в значних масштабах). Вони назвали цю шкідливу програму Industroyer і навели вагомі аргументи на користь того, що це найбільша загроза для промислових систем управління з часів Stuxnet. Наслідки загрози Industroyer для критичної інфраструктури стосуються всіх. Оскільки промислове обладнання на яке орієнтується Industroyer широко використовується (далеко за межами України, наприклад, у Великобританії, ЄС і США – у багатьох критичних секторах). Окрім того більша частина обладнання ICS, що все ще використовується промисловими підприємствами сьогодні, була розроблена без урахуванням можливості підключення до Інтернету (звідки надходять загрози), що ускладнює реалізацію будь-яких захисних заходів. Тобто здатність реалізовувати кібератаки в енергосистемі матиме тенденцію до зростання, якщо тільки вона не буде блокована запобіжними заходами, такими як модернізація системи,

Issue DOI: 10.34132/pard

раннє виявлення мережевого зондування і радикальні заходи у виявленні та запобіганні фішингу.

С. Кобб вважає, що організації, які займаються критично важливою інфраструктурою, повинні продовжувати підвищувати свою безпеку, знижуючи ефективність фішингових атак (найбільш поширених векторів атак), контролюючи доступ до мережі, перевіряючи і тестуючи як старе, так і нове апаратне та програмне забезпечення, а також проводячи комплексну перевірку цифрових даних постачальників. Вони також повинні відстежувати та реагувати на тип мережевого зондування та спостереження, який може передувати масштабній кібератаці [23].

18 травня 2017 року в Україні зафіксовано перший масовий кібернапад на підприємства та державні установи з використанням вірусу XData з бекдором (з англ. back door, чорний хід в комп'ютерній системі, метод обходу стандартних процедур аутентифікації, несанкціонований віддалений доступ до комп'ютера, отримання доступу до відкритого тексту, причому шкідлива програма залишається непоміченою). 27 червня 2017 року сталась друга масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80 % підприємств в Україні (кожне четверте), а також поширилась на закордонні підприємства. Бекдор тривалий час дозволяв зловмисникам викрадати інформацію з підприємств (вимагали за дані винагороду – біткоіни) та відкривав доступ до комп'ютерних мереж. NotPetya швидко поширився по всьому світу, завдавши збитків на мільярди доларів по всій Європі, Азії та Америці. В офіційній заяві Білого дому було оголошено відповідальними за кібернапади російських військових і зазначено, що «це було частиною постійних зусиль Кремля щодо дестабілізації України та дедалі чіткіше демонструє причетність Росії до поточного конфлікту» [24].

11 липня 2018 року співробітниками СБУ була відбита кібератака російських спецслужб на мережеве обладнання товариства «Аульська хлоропереливна станція», яке є об'єктом критичної інфраструктури країни. Протягом декількох хвилин системи управління технологічними процесами та системи виявлення ознак аварійних ситуацій підприємства були умисно уражені комп'ютерним вірусом

VPNFilter (багаторівневе модульне шкідливе програмне забезпечення з універсальними можливостями, які забезпечують проведення як кіберрозвідки, так і деструктивних кібероперацій). Напад мав на меті зрив технологічних процесів та аварію, блокування сталого функціонування переливної станції, яка забезпечує підприємства рідким хлором для очищення води водопровідно-каналізаційних систем України. Техногенній катастрофі вдалося запобігти завдяки злагодженій роботі працівників спецслужб та фахівців підприємства, шкідливе програмне забезпечення VPNFilter було локалізоване та знешкоджене [25].

У межах виконання завдань із контррозвідувального забезпечення інтересів держави у сфері інформаційної безпеки, співробітники СБУ попередили спроби спецслужб РФ організувати хакерські атаки на державні установи, які були задіяні в підготовці до виборчого процесу та його проведенні. Масове поширення шкідливого програмного забезпечення здійснювалось через направлення цільових електронних повідомлень на адреси держустанов, а також уразливі ділянки Інтернет-сайтів державних органів. За висновками фахівців, такі комп'ютерні віруси застосовуються для блокування діяльності інформаційних ресурсів через підключення до держреєстрів України, що могло створити загрозу для роботи серверів і персональних комп'ютерів виборчих комісій. Співробітники СБУ спільно з кіберполіцією було проведено обшуки та виявлено комп'ютерну техніку з інстальованим програмним забезпеченням для створення та модифікації комп'ютерних вірусів. Також отримано майже десять зразків шкідливого програмного забезпечення, які були підготовлені для розповсюдження серед учасників закритого хакерського форуму [26].

За офіційними повідомленнями Служби безпеки України, співробітники ситуаційного центру забезпечення кібербезпеки ДКІБ СБУ (Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ) попередили хакерську атаку на популярні ЗМІ та телекомунікаційні об'єкти України з боку російських спецслужб. Зазначається, що виконавці упродовж кількох попередніх місяців створювали розгалужену Інтернет-інфраструктуру, що нараховує кілька десятків доменів, які за своєю назвою співп-

 Issue DOI: 10.34132/pard

адають або походять на офіційні домени популярних українських електронних засобів масової інформації, операторів зв'язку та великих телекомунікаційних компаній. Новостворені доменні імена вперше зафіксовані на потужностях дата-центрів декількох російських Інтернет-провайдерів, а облікові записи, використані для їх реєстрації, раніше застосовувались для кібератак на державний сектор упродовж минулого року. Кібератака повинна була забезпечити суспільний резонанс та здійснити негативний інформаційний вплив на перебіг виборчої кампанії в Україні [27].

16 липня 2019 року на сайті СБУ оприлюднено інформацію про те, що співробітниками СБУ спільно з партнерами із США було припинено діяльність потужного хакерського угруповання. Учасники угруповання на території України організували і тривалий час (з 2007 року) надавали віртуальні послуги хакерам та іншим злочинцям, створюючи їм умови для безперешкодного здійснення протиправної діяльності в мережі Інтернет. Зловмисники використовували Dark Net – приховану від звичайних користувачів частину інтернет-мережі, де можливо анонімно придбати зброю, наркотики тощо. Співробітниками СБУ було вилучено майже півтори сотні серверів з тисячами хакерських ресурсів, серед яких були і зашифровані. Попереднє дослідження мережевого обладнання та оцінка діапазонів IP-адрес, що використовувались угрупованням, вказує на три автономні системи, зарезервовані за підприємствами Російської Федерації [28].

За даними прес-центру СБУ станом на 26 липня 2019 року, співробітники СБУ у співпраці зі співробітниками Центральної виборчої комісії, Кіберполіції та Держспецзв'язку забезпечили належний рівень кібербезпеки та мінімізували загрози надійному та безпечному функціонуванню Єдиної інформаційної автоматизованої системи «Вибори» та автоматизованій інформаційно-телекомунікаційній системі «Державний реєстр виборців»[29].

Як бачимо, забезпечення кібербезпеки у 21 столітті є нагально важливим напрямком національної безпеки України та потребує надзвичайного зосередження зусиль по її забезпеченню усіх органів державної влади, які складають основу національної системи кібербезпеки.

Корпорація Microsoft повідомила, що у 2019 році майже 10 000 її клієнтів зазнали кібернападів зі сторони держав (nation-state attack). Більшість атак у кіберпросторі зафіксовано з території – Ірану, Північної Кореї та Росії. Близько 84 % цих атак були спрямовані на підприємства, які обслуговуються компанією Microsoft, а близько 16 % – на особисті облікові записи її користувачів. На думку кампанії, ці дані свідчать про те, що кібератаки перетворились на потужний інструмент впливу на світову геополітику або сприяють досягненню інших цілей з боку певних країн. Одними з важливих об'єктів для нападу обираються політичні партії, неурядові організації, які є критично важливими для суспільства, але мають менше ресурсів для захисту від кібератак, ніж великі підприємства [30].

Ще одна американська компанія – Fortinet, що спеціалізується на пристроях мережевої безпеки та займає 3 місце в світі за щорічним обсягом проданих пристроїв мережевої безпеки, опублікувала свій звіт щодо кіберзагроз у другому кварталі 2019 року. Цей щоквартальний звіт містить в собі аналіз тенденцій загроз і поведінки кіберзлочинців та публікується з метою надання допомоги організаціям для підготовки та захисту під час хакерських атак. За даними кампанії Fortinet рівень активності загроз в Інтернеті досяг своєї найвищої позначки за всю історію. Багато сучасних шкідливих програм включають в себе функції для ухилення від виявлення вірусів або інших загроз. Наприклад, спам-кампанія демонструє, як зловмисники використовують і налаштовують ці методи проти захисту кампаній. Наприклад, це стосується використання фішингових електронних листів з додатком, який може бути документом Excel зі шкідливим макросом, або варіант банківського трояна Dridex, який змінює імена і хеші файлів під час кожного входу жертви до системи, що ускладнює виявлення шкідливого ПО на заражених хост-системах, або RobbinHood Ransomware, призначений для атаки на мережеву інфраструктуру організації та здатний відключати служби Windows, які запобігають шифруванню даних і відключатися від загальних дисків. Тому зростаюче використання хакерами чисельних тактик ухилення є нагадуванням про необхідність багаторівневого захисту і виявлення загроз на підставі поведінки зловмисників під час кібернападу. Фа-

Issue DOI: 10.34132/pard

хівці кампанії Fortinet, вважають, що кібератаки країн, міст, державних та місцевих органів влади і систем освіти є нагадуванням про те, що вимагачі не відступають, а замість цього продовжують становити серйозну загрозу для багатьох організацій в майбутньому. Атаки хакерів-вимагачів коштів, трансформуються з масових розосереджених на більш цільові напади на ті організації, які сприймаються як платоспроможні, або мають стимул платити викуп. Тому незалежно від напряму, мети нападу, кіберзлочинці уособлюють серйозну загрозу для установ, слугуючи нагадуванням про пріоритизацію освіти в області кібербезпеки та підвищення обізнаності про неї [31].

Крім того, спостерігається зростання кількості випадків використання хакерами вразливості протоколу віддаленого робочого столу (RDP – Remote Desktop Protocol), це є попередженням установам про те, що служби віддаленого доступу можуть створювати можливості проникнення в систему для кіберзлочинців, а також можуть використовуватися для вимагання коштів. Таким чином, поєднання аналізу загроз з належним плануванням й інтегрованими рішеннями щодо забезпечення безпеки сприяє розробці організаціями найкращої можливої стратегії захисту від кіберзагрози [31].

Запобіганню, протидії та кіберзахисту присвячені дослідження та сервіси багатьох світових кампаній-лідерів у сфері кібербезпеки, на які Україні обов'язково варто звернути свою увагу. Зокрема, корпорація Microsoft створила новий безпековий сервіс AccountGuard, який наразі активно впроваджується у Франції, Німеччині, Швеції, Данії, Нідерландах, Фінляндії, Естонії, Латвії, Литві, Португалії, Словаччині та Іспанії. Послуга вже працює у США, Канаді, Ірландії та Великобританії та планується її впровадження і у інших країнах Європи. Microsoft AccountGuard є частиною програми «Захист демократії». Т. Берт – віце-президент корпорації, зазначає, що це найсучасніший сервіс кібербезпеки, який доступний без додаткових витрат для всіх політичних кандидатів, партій та агітаційних бюро, що працюють на місцевому чи національному рівні. Також сервіс доступний і для аналітичних центрів, некомерційних організацій та неурядових організацій, які працюють над питаннями пов'язаними з демократією та виборчою доброчесністю. Організаціям третього сектору, що вико-

ристовують Office 365, Microsoft AccountGuard надається безкоштовно. Сервіс надає сповіщення організаціям про кіберзагрози, включаючи напади відомих хакерів з територій певних держав (nation-state attack), через системи електронної пошти, якими керують організації, та особисті рахунки керівників та співробітників цих організацій. Організації можуть отримати захист і для зовнішніх осіб, тих, хто допомагає у проведенні кампанії, членів правління некомерційних організацій або волонтерів [32]. Враховуючи вищезазначене, розроблений сервіс AccountGuard корпорації Microsoft, може знадобитись українській державі під час проведення виборчих кампаній, оскільки це може бути потужною допоміжною сучасною технологічною захисною ланкою зміцнення кібербезпеки України, забезпечення національної безпеки держави від кібернападів.

В Україні напрацьовано значну законодавчу та нормативно-правову базу щодо національної безпеки та, зокрема, кібербезпеки. Законом України від 7 вересня 2005 року № 2824-IV було ратифіковано Конвенцію про кіберзлочинність [7]. 27 січня 2016 року було прийнято Стратегію кібербезпеки України, в якій зазначено, що «метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави. Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні. Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [2].

 Issue DOI: 10.34132/pard

Національна система кібербезпеки
згідно зі Стратегією кібербезпеки України [2]

№	Назва державного органу	Завдання державного органу у сфері кібербезпеки
1.	Рада національної безпеки і оборони України (РНБОУ)	Здійснює координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.
2.	Міністерство оборони України (МОУ) та Генеральний штаб Збройних Сил України	Здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури.
3.	Державна служба спеціального зв'язку та захисту інформації України	Формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість.

Продовження табл. 1

4.	Служба безпеки України (СБУ)	Попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки
5.	Національна поліція України	Забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі.
6.	Національний банк України (НБУ)	Формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері.
7.	Розвідувальні органи	Здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Issue DOI: 10.34132/pard

Стаття 27 Закону України «Про національну безпеку України» від 21.06.2018 присвячена комплексному огляду сектору безпеки і оборони. У 1 пункті цієї статті зазначено, що «комплексний огляд сектору безпеки і оборони проводиться за рішенням Ради національної безпеки і оборони України, яке вводиться в дію указом Президента України», він включає й «проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури». Пункт 6. Статті 27 визначає, що «за результатами оглядів формується перспективна модель сектору безпеки і оборони» [16].

У статті 31, пункті 2 Закону зазначено, що «організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки після затвердження Стратегії національної безпеки України. Стратегія кібербезпеки України схвалюється рішенням Ради національної безпеки і оборони України та затверджується указом Президента України» і є «основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України» – пункт 3 статті 31 Закону України «Про національну безпеку України» [16].

Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [17] визначає загальні та базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури. Також у Постанові вказано, що «на об'єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)». Цей національний стандарт ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) ідентичний ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management». Він застосовується для всіх типів організацій (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які мають намір

управляти ризиками, що здатні пошкодити інформаційну безпеку установи та оновлюється кожні 5 років.

Згідно зі змінами до Закону «Про Державну службу спеціального зв'язку та захисту інформації України»[8], у травні 2014 року був закріплений офіційний статус команди реагування на кіберзагрози в Україні **CERT-UA (Computer Emergency Response Team of Ukraine)**. Команду було засновано у 2007 році, вона співпрацювала з органами влади на громадських засадах. Наразі вона є підрозділом державної служби спеціального зв'язку та захисту інформації України. Команда розробила та розмістила на своєму сайті «Основні правила кібергігієни» для суб'єктів громадянського суспільства та представників владних установ, вони доступні усім за посиланням: **https://cert.gov.ua/recommendations/21**. Також вони розмістили на сайті «Рекомендації щодо підвищення рівня захищеності інформаційно-телекомунікаційних систем та інформаційних ресурсів державних органів і установ від несанкціонованих дій зі сторони мережі Інтернет» [33]. Наразі команда CERT-UA разом з фахівцями Кіберполіції, СБУ, фахівцями з приватних компаній та іноземними партнерами беруть участь у протидії та ліквідації наслідків масштабних хакерських атак проти України.

Результатом протидії агресії з боку РФ, держави-члени НАТО на Уельському саміті у вересні 2014 р. ухвалили заснувати п'ять нових цільових трастових фондів для допомоги Україні в критично важливих сферах, серед яких й кібернетична безпека (Cyber Defence). Трастові фонди НАТО мають на меті надання допомоги Україні у протистоянні загрозам, забезпеченні власної безпеки, проведенні необхідних реформ у секторі безпеки та оборони. Щодо кібербезпеки – це допомога у розробці технічних сил та засобів для протидії кіберзагрозам. Вона включає надання обладнання для лабораторій з розслідування випадків кібернападів та створення Центру реагування на кіберінциденти, тривалість реалізації проекту попередньо було заплановано на 2 роки. Загальна сума відрахувань членів НАТО до Трастового фонду становила на першому етапі 1 млн євро. Альянс визначив Румунію країною-лідером Фонду від НАТО. Інтереси української сторони представляла Служба безпеки

 Issue DOI: 10.34132/pard

України [34]. Станом на 1 липня 2017 року технічне обладнання та програмне забезпечення, передбачені для постачання в Україну у рамках першого етапу програми Трастового Фонду, держава в особі СБУ вже отримала [35]. Наразі Україною ведуться переговори щодо можливості реалізації другого етапу програми Трастового Фонду НАТО щодо кібернетичної безпеки.

7 червня 2016 року Указом Президента України було створено **Національний координаційний центр кібербезпеки** – робочий орган РНБО. До складу Центру входять керівник, секретар та інші члени Центру. Керівником Центру є за посадою Секретар РНБО. Секретарем Центру є за посадою керівник структурного підрозділу Апарату РНБО, до відання якого віднесені питання кібербезпеки. Членами Центру є перший заступник або заступник Міністра оборони України, начальник Генерального штабу ЗСУ, Голова СБУ, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), а також начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної прикордонної служби України, Голова Державної служби спеціального зв'язку та захисту інформації України [13].

25 січня 2018 року було відкрито **Ситуаційний центр забезпечення кібернетичної безпеки,** створений на базі Департаменту контррозвідувального захисту інтересів держави в сфері інформаційної безпеки СБУ. Ключовими можливостями Центру визначено систему виявлення та реагування на кіберінциденти та лабораторію з комп'ютерної криміналістики. Вони дозволять попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії.

Принциповим аспектом роботи ситуаційного центру окреслено його відкритість для співпраці з усіма суб'єктами забезпечення кібербезпеки: установами, організаціями, підприємствами та профільними фахівцями. Так, на сайті СБУ розміщено інформацію для згаданої співпраці, це **misp.dis.gov.ua** – платформа обміну індикаторами компрометації між об'єктами критичної інфраструктури та органами державної влади, користувачі яких заздалегідь підключені

(за умови укладання окремого Меморандуму). Публічний Меморандум про співпрацю також розміщено на сайті СБУ у форматі Word. Предметом регулювання Меморандуму є спільна суспільно-корисна діяльність з відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж, здійснення якої не суперечить чинному законодавству України та є сприянням виконанню СБУ її завдань у сфері забезпечення кібербезпеки [36].

За прогнозами корпорації Microsoft витрати підприємств на кібербезпеку в світі у 2019 році перевищать 124 млрд дол., але заробітки кіберзлочинців у 2019 році оцінюються у 1 трлн дол. [37]. Незважаючи на поширення в світі кіберризиків, дуже мало організацій вживають необхідних заходів для створення сильної «культури» кібербезпеки з належними стандартами управління і відповідальності. Проблеми з кібербезпекою можуть з'являтися щоразу, коли нові технології впроваджуються у бізнес-інфраструктуру. Кіберризики, пов'язані з новими технологіями, повинні порівнюватись з потенційними здобутками для бізнесу. За даними глобального дослідження ставлення підприємств до кіберризиків, проведенного компанією Microsoft в 2019 (було опитано 1500 підприємств, світових бізнес-лідерів), лише 36 % організацій повідомили, що вивчали потенційні ризики від нових технологій як до, так і після впровадження, 5 % сказали, що вони оцінюють кіберризик на кожному етапі життєвого циклу технології, 11 % – не оцінюють кіберризики взагалі. Дослідники компанії Microsoft відзначили, що організації, які тестують технології на кіберризик на етапах їх впровадження, більш поінформовані щодо кібербезпек, тому що безперервна оцінка ризику дозволяє в режимі реального часу бачити нові вразливості та ризики технологій. Знаючи свої потенційні слабкості або вразливість системи безпеки, вони здатні вдосконалюватись в реальному часі та розробляти плани дій в надзвичайних ситуаціях для управління ризиками, пов'язаними з цими системами [37].

Багато організацій концентрують свою стратегію управління кіберризиками на запобіганні загрозам, інвестуючи кошти в передові технології кіберзахисту, а витрати на інші інструменти та ресурси

для управління кіберризиками, такі як кіберстрахування або навчання співробітників реагуванню на події, залишаються лише частиною технологічного бюджету. Це говорить про те, що багато організацій вважають, що зможуть усунути або керувати своїм кіберризиками в першу чергу за допомогою технологій, а не за допомогою широкого спектру заходів планування, запобігання та реагування. Дуже мало уваги, за дослідженням компанії Microsoft, підприємства приділяють таким заходам, як навчання співробітників, розробці політики у сфері кібербезпеки та планів реагування на кіберінциденти. Найбільш досвідчені організації виробляють стійкість до кіберзагроз, використовуючи комплексні, збалансовані стратегії управління кіберризиками, а не концентруються виключно на профілактиці [37].

Висновки. Отже, в результаті проведеного аналізу особливостей кібербезпеки як важливої складової національної безпеки України, законодавчого та нормативно-правового забезпечення даної сфери, реалізації чисельних заходів державою під час боротьби з кібернападами на об'єкти критичної інфраструктури, об'єкти громадянського суспільства, можемо зробити висновок, що триває процес розробки та розвитку власної моделі кіберзахисту країни в умовах протидії російській агресії, з використанням сучасних світових практик, практик країн НАТО та ЄС в означеній сфері. Однак результати дослідження досвіду України, світового досвіду доводять, що неможливо повністю запобігти ризикам у сфері кібербезпеки. Проте, на нашу думку, спільні зусилля світової спільноти щодо обміну досвідом, технологіями, здобутками фахівців у сфері кіберзахисту, взаємна фінансова підтримка, скоординована спільна системна відповідь країн на кіберзлочини, запровадження нових світових стандартів з кібербезпеки та інформаційної безпеки, оновлення національних та міжнародних стратегій, законодавства, які б відповідали новим кібервикликам, є запорукою подолання спільними зусиллями нових сучасних викликів.

Велику увагу державі варто приділити навчанню громадян, розробці окремої державної програми для освітніх закладів, державних установ, програму співпраці з підприємцями, громадськими організаціями, з метою охопити всі категорії населення та навчити

елементарним заходам кібербезпеки, інформаційної безпеки (в т.ч. проблемі захисту персональних даних, паролів, кодів доступу, правилам користування соцмережами (особливо дітей та підлітків)), ознайомлення їх з кіберризиками під час здійснення діяльності в кіберпросторі, інформування про спеціалізовані державні підрозділи, які можуть надати кваліфіковану допомогу у випадку нападів з боку кіберзлочинців. Останнє стосується зокрема діяльності таких державних структур, як: Команда реагування на комп'ютерні надзвичайні події України Державної служби спеціального зв'язку та захисту інформації України ─ CERT-UA, Кіберполіції, Служби безпеки України (Ситуаційний центр забезпечення кібернетичної безпеки). Також окрему увагу країні треба звернути на розробку політики кіберстрахування, зокрема для підприємств третього сектору, можливо у тісній співпраці держави з банківським сектором щодо цього.

Для забезпечення кіберзахисту виборчих процесів Україні доцільно розглянути можливість впровадження нового безпекового сервісу AccountGuard корпорації Microsoft, який є частиною програми «Захист демократії». Це сучасний сервіс кібербезпеки, який доступний без додаткових витрат для всіх політичних кандидатів, партій та агітаційних бюро, що працюють на місцевому чи національному рівні.

Україна доклала значних зусиль у посиленні національної безпеки, також у сфері кібербезпеки, має значний досвід у боротьбі з кіберзагрозами, який активно переймають країни-партнери, також треба опановувати закордонний досвід боротьби, використовуючи комплексні, збалансовані стратегії управління кіберризиками, інвестуючи кошти в передові технології кіберзахисту, активно використовуючи фінансову та технічну допомогу спеціальних фондів (наприклад, Трастовий Фонд НАТО). Оскільки Україна стала одним з епіцентрів для чисельних кібернападів особливо з боку РФ, під час яких використовуються в тому числі й нові шкідливі програмні забезпечення, які здатні чинити руйнівний вплив не лише на діяльність окремих державних органів та підприємств третього сектору, а й, як доведено у дослідженні, на стратегічні об'єкти критичної інфраструктури країни, аналогів протистояння останньому (шкід-

лива програма Industroyer) у сфері промисловості ще не вироблено у світі, а лише вживаються заходи щодо недопущення проникнення у систему підприємств промисловості. Саме тому розробка нових сучасних заходів боротьби з кібернападами українських фахівців, досвід цієї боротьби є дуже корисним і для іноземних партнерів, в контексті кіберзахисту своїх країн та спільної світової протидії кіберзлочинності, оскільки вона все більше використовується не лише для вимагання коштів, а й як потужна стратегія дестабілізації та геополітичного впливу з боку окремих країн.

Стаття надійшла до редакції: 12.05.19

CYBER SECURITY AS A COMPONENT OF NATIONAL SECURITY AND CYBER PROTECTION OF CRITICAL INFRASTRUCTURE OF UKRAINE

Volodymyr Yemelyanov, doctor of Sciences in Public Administration Institute of Public Administration, Black Sea National University of Petro Mohyla, Mykolaiv, Ukraine

Hanna Bondar, PhD in Political Sciences, Associate Professor at the Institute of Public Administration, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine

The article is devoted to the analysis of features of cyber security as an important component of national security of Ukraine. Also, analyzed legislative and regulatory support of this sphere; implementation of numerous measures by the state during the fight against cyber-attacks on objects of critical infrastructure, objects of civil society. Authors investigated the activities of specialized state structures that provide cyber defense to the country in the face of Russian aggression, using current world practices, in particular NATO and EU. Revealed the features, strategies and actors of cyber-attacks on strategic objects of critical infrastructure of Ukraine, private enterprises and mass media. The international experience of combating cybercrime with the help of

complex cyber risk management`s strategies is analyzed. The results of the study of the experience of Ukraine and the world in the fight against cybercrime prove that it is impossible eliminate the risks in the field of cyber security at all. However, in our opinion, the joint efforts of the world community to exchange experience, technologies, achievements of cyber security experts, mutual financial support, coordinated joint systemic response of countries to cybercrime, introduction of new world standards for cyber security and information security, national and international strategies, that responds to new cyber challenges is the key to overcoming the common challenges. The authors considered the urgency of developing a separate comprehensive state program for educational institutions, state institutions, cooperation programs with entrepreneurs, public organizations, in order to cover all categories of the population and teach basic measures of cyber security and information security. It is necessary to familiarize citizens with cyber risks during their activities in cyberspace, to inform about specialized state units that can provide qualified assistance in the event of cybercrime attacks.

Keywords: *cyber security, cyber defense, cyber attack, critical infrastructure of Ukraine, cyber risk, phishing.*

Received: 12.05.19

References

1. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 6 travnya 2015 roku Pro Stratehiyu natsional′noyi bezpeky Ukrayiny : pryiniatyi 26 trav. 2015 roku N 287/2015 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of May 6, 2015 on the National Security Strategy of Ukraine 26 2015, N 287/2015]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/287/2015 [in Ukrainian].

2. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 27 sich. 2016 roku Pro Stratehiyu kiberbezpeky Ukrayiny : pryiniatyi 15 ber. 2016 roku N 96/2016 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of March 15, 2016

on the Cybersecurity Strategy of Ukraine January 27, 2016, N 96/2016]. zakon.rada.gov.ua. Retrieved from https://zakon5.rada.gov.ua/laws/show/96/2016 [in Ukrainian].

3. Spivrobitnyky SBU vzyaly uchast′ u zasidanni RB OON shchodo zakhystu krytychnoyi infrastruktury vid teroryzmu. 24 lyst. 2016 roku [SBU staff participated in UN Security Council meeting on critical infrastructure protection against terrorism]. November 24, 2016. (n.d.). www.ssu.gov.ua. Retrieved from https://www.ssu.gov.ua/ua/news/1/category/1/view/2335#.LqnEQ3zc.dpbs [in Ukrainian].

4. Za pershyy kvartal 2019 roku v Ukrayini zafiksovano ponad 1,5 mln kiberintsydentiv. 12 serp. 2019 roku [Over the first quarter of 2019, over 1.5 million cyber incidents have been reported in Ukraine]. September 12, 2019. (n.d.). www.unn.com.ua. Retrieved from https://www.unn.com.ua/uk/exclusive/1818458-za-pershiy-kvartal-2019-roku-v-ukrayini-zafiksovano-ponad-1-5-mln-kiberintsidentiv [in Ukrainian].

5. Zakon Ukrayiny Pro informatsiyu : pryiniatyi 2 zhovt. 1992 roku N 2657-XII [Law of Ukraine on Information from October 2, 1992, N 2657-XII]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12 [in Ukrainian].

6. Zakon Ukrayiny Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : pryiniatyi 5 lyp. 1994 roku N 80/94-BP [Law of Ukraine on Information Protection in Information and Telecommunication Systems from July 5, 1994, N 80/94-BP]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 [in Ukrainian].

7. Zakon Ukrayiny Pro ratyfikatsiyu Konventsiyi pro kiberzlochynnist′ : pryiniatyi 7 ver. 2005 roku N 2824-IV [Law of Ukraine on Ratification of the Convention on Cybercrime from September 7, 2005, N 2824-IV]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2824-15 [in Ukrainian].

8. Zakon Ukrayiny Pro Derzhavnu sluzhbu spetsial′noho zv'yazku ta zakhystu informatsiyi : pryiniatyi 23 fev. 2006 roku N 3475-IV [Law of Ukraine on State Service for Special Communication and Information Protection from February 23, 2006 N 3475-IV] zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15 [in Ukrainian].

9. Zakon Ukrayiny Pro zakhyst personal′nykh danykh informatsiyi : pryiniatyi 1 cherv. 2010 roku N 2297-VI [Law of Ukraine on Protection of Personal Data from June 1, 2010, N 2297-VI]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17 [in Ukrainian].

10. Zakon Ukrayiny Pro dostup do publichnoyi informatsiyi : pryiniatyi 13 sich.2011 roku N 2939-VI [Law of Ukraine on Access to Public Information from January 13, 2011, N 2939-VI]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2939-17 [in Ukrainian].

11. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 28 kvit. 2014 roku Pro zakhody shchodo vdoskonalennya formuvannya ta realizatsiyi derzhavnoyi polityky u sferi informatsiynoyi bezpeky Ukrayiny : pryiniatyi 1 trav. 2014 roku N 449 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of April 28, 2014 on Measures to Improve the Formation and Implementation of State Policy in the Field of Information Security of Ukraine from May 1, 2014, N 449]. zakon.rada.gov.ua. Retrieved from https://zakon4.rada.gov.ua/laws/show/449/2014 [in Ukrainian].

12. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 29 grud. 2016 roku Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neytralizatsiyi : pryiniatyi 13 lyut. 2017 roku N 32 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of December 29, 2016 on Cyber Security Threats to the State and Urgent Measures to Eliminate Them from February 13, 2017, N 32]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/32/2017 [in Ukrainian].

13. Ukaz Prezydenta Ukrayiny Pro Natsional′nyy koordynatsiynyy tsentr kiberbezpeky» : pryiniatyi 7 cherv. 2016 roku N 242/2016 [Decree of the President of Ukraine on National Cybersecurity Coordination Center from June 7, 2016, N 242/2016]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016 [in Ukrainian].

14. Zakon Ukrayiny Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny : pryiniatyi 5 zhovt. 2017 roku N 2163-VIII [Law of Ukraine on Basic Principles of Ensuring Cyber Security of Ukraine from October 5, 2017, N 2163-VIII]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

15. Ukaz Prezydenta Ukrayiny Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 29 grud. 2016 roku Pro Doktrynu informatsiynoyi bezpeky Ukrayiny : pryiniatyi 25 lyut. 2017 roku N 4/2017 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of December 29, 2016 on the Doctrine of Information Security of Ukraine from February 25, 2017 N4/2017]. www.president.gov.ua. Retrieved from https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].

16. Zakon Ukrayiny Pro natsional′nu bezpeku Ukrayiny : pryiniatyi 21 cherv. 2018 roku N 2469-VIII [Law of Ukraine on National Security of Ukraine from June 21, 2018, N 2469-VIII]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19 [in Ukrainian].

17. Postanova Kabinetu Ministriv Ukrayiny Pro zatverdzhennya Zahal′nykh vymoh do kiberzakhystu ob″yektiv krytychnoyi infrastruktury : pryiniata 19 cherv. 2019 N 518 [Resolution of the Cabinet of Ministers of Ukraine on Approval of the General Requirements for Cyber Defense of Critical Infrastructure Objects from June 19, 2019 N 518]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF [in Ukrainian].

18. Kiberugroza BlackEnergy2/3. Istoriya atak na kriticheskuyu IT infrastrukturu Ukrainy. Otdel reagirovaniya na intsidenty CyS Centrum (CyS-CERT). 6 sich. 2016 roku [Cyber threat BlackEnergy2/3. History of attacks on critical IT infrastructure in Ukraine. CyS Centrum Incident Response Team (CyS-CERT) from January 6, 2016]. (n.d.). cys-centrum.com. Retrieved from https://cys-centrum.com/ru/news/black_energy_2_3 [in Ukrainian].

19. Minenerhovuhillya maye namir utvoryty hrupu za uchastyu predstavnykiv usikh enerhetychnykh kompaniy, shcho vkhodyat′ do sfery upravlinnya Ministerstva, dlya vyvchennya mozhlyvostey shchodo zapobihannya nesanktsionovanomu vtruchannyu v robotu enerhomerezh. Ministerstvo enerhetyky ta vuhil′noyi promyslovosti. 12 lyut. 2016 roky [Ministry of Energy and Coal intends to form a group with the participation of representatives of all energy companies belonging to the Ministry's management, to study the possibilities of preventing unauthorized interference in the operation of power grids. Ministry of Energy and Coal Industry. February 12, 2016]. (n.d.). mpe.kmu.gov.ua. Retrieved from

http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=3510 [in Ukrainian].

20. Na Ukrenerho zdiysnyuyut′sya novi khakers′ki ataky. Ekonomichna pravda. 20 sich. 2016 roku [New hacker attacks are being carried out at Ukrenergo. Economic truth. January 20, 2016]. (n.d.). www.epravda.com.ua. Retrieved from https://www.epravda.com.ua/news/2016/01/20/577551/ [in Ukrainian].

21. Minenerhovuhillya maye namir utvoryty hrupu za uchastyu predstavnykiv usikh enerhetychnykh kompaniy, shcho vkhodyat′ do sfery upravlinnya Ministerstva, dlya vyvchennya mozhlyvostey shchodo zapobihannya nesanktsionovanomu vtruchannyu v robotu enerhomerezh. Ministerstvo enerhetyky ta vuhil′noyi promyslovosti. 12 lyut. 2016 roku [Ministry of Energy

and Coal intends to form a group with the participation of representatives of all energy companies belonging to the Ministry's management, to study the possibilities of preventing unauthorized interference in the operation of power grids. Ministry of Energy and Coal Industry. February 12, 2016]. (n.d.). mpe.kmu.gov.ua. Retrieved from

http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109 [in Ukrainian].

22. Minenerhovuhillya pratsyuye nad stvorennyam Haluzevoho tsentru z kiberbezpeky. Ministerstvo enerhetyky ta vuhil′noyi promyslovosti. 15 serp. 2019 roku [Ministry of Energy and Coal is working on the establishment of the Cyber Security Industry Center. Ministry of Energy and Coal Industry. August 15, 2019]. (n.d.). mpe.kmu.gov.ua. Retrieved from

http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245390875 [in Ukrainian].

23. Cobb, St. Trends 2018: Critical infrastructure attacks on the rise. Welivesecurity by ESET. May 30, 2018. www.welivesecurity.com. Retrieved from https://www.welivesecurity.com/2018/05/30/trends-2018-critical-infrastructure-attacks/.

24. Statement from the Press Secretary. Issued on: February 15, 2018. www.whitehouse.gov. Retrieved from https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

25. Dnipropetrovsk region: SBU prevents cyberattack of Russian special services on critical infrastructure facility. July 11, 2018. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/1/category/301/view/5037#.gkJXke6X.dpbs.

26. SBU has prevented hacking attacks on government bodies involved in the election process. March 6, 2019. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/1/category/301/view/5808#.jxBydNLR.dpbs.

27. SBU prevents hacker attack on Ukrainian information and telecommunication facilities. March 29, 2019. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/1/category/301/view/5916#.HKVce3H5.dpbs.

28. SBU jointly with foreign colleagues blocks activity of powerful hacker group. July 16, 2019. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/1/category/21/view/6281#.ftjINoYP.dpbs.

29. SBU ensures cyber security of the information infrastructure of the Central Election Commission during elections. July 26, 2019. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/16/category/21/view/6337#.KTO9Yls9.dpbs.

30. Neutze, J. Protecting political campaigns from hacking. May 6, 2019. blogs.microsoft.com. Retrieved from https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-political-campaigns-from-hacking/.

31. Fortinet Reports Increased YoY Threat Activity for Q2 2019. Threat Research. August 06, 2019. (n.d.). www.fortinet.com. Retrieved from https://www.fortinet.com/blog/threat-research/fortinet-q2-2019-threat-landscape-report.html.

32. Burt, T. New steps to protect Europe from continued cyber threats. February 20, 2019. blogs.microsoft.com. Retrieved from https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/.

33. Rekomendatsiyi shchodo pidvyshchennya rivnya zakhyshchenosti informatsiyno-telekomunikatsiynykh system ta informatsiynykh resursiv derzhavnykh orhaniv i ustanov vid nesanktsionovanykh diy zi storony merezhi Internet. Derzhavna sluzhba spetsial′noho zv″yazku ta zakhystu informatsiyi Ukrayiny Komanda reahuvannya na komp″yuterni nadzvychayni podiyi Ukrayiny CERT-UA. 18 kvit. 2014 roku [Recommendations on increasing the level of security of information and telecommunication systems and information resources of state bodies and institutions from unauthorized actions by the Internet. State Special Communications and Information Protection Service of Ukraine CERT-UA Computer Emergency Response Team. April 18, 2014]. (n.d.). www.cert.gov.ua. Retrieved from https://www.cert.gov.ua/files/pdf/18042012.pdf [in Ukrainian].

34. Dopomoha trastovykh fondiv NATO Ukrayini [NATO Trust Fund Assistance to Ukraine November 4, 2016]. (n.d.). eesri.org. Retrieved from http://eesri.org/2016/11/nato-trust-funds-assistance-to-ukraine_ukr/ [in Ukrainian].

35. SBU Head inaugurates the Cyber-Security Situation Centre. January 25, 2018. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/news/2/category/301/view/4318#.duVfjCJM.dpbs.

36. The SSU Cyber Security Situation Centre. (n.d.). ssu.gov.ua. Retrieved from https://ssu.gov.ua/en/pages/330.

37. 2019 Global Cyber Risk Perception Survey. September 2019. (n.d.). www.microsoft.com. Retrieved from https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Відомості про авторів / Information about the Authors

Ємельянов Володимир Михайлович: Чорноморський національний університет ім. Петра Могили: вул. 68 десантників 10, Миколаїв, 54003, Україна.

Volodymyr Yemelyanov: Petro Mohyla Black Sea National University: 68 Desantnykiv str. 10, Mykolaiv, 54003, Ukraine.

ORCID.ORG/0000-0002-2995-8445

E-mail: d_idu@ukr.net

Бондар Ганна Леонідівна: Чорноморський національний університет ім. Петра Могили: вул. 68 десантників 10, Миколаїв, 54003, Україна.

Hanna Bondar: Petro Mohyla Black Sea National University: 68 Desantnykiv str. 10, Mykolaiv, 54003, Ukraine.

ORCID.ORG/0000-0003-4112-263X

E-mail: gannabondar.ua@gmail.com