УДК 351:007:004
DOI 10.36030/2310-2837-4(99)-2020-99-104

МЕХАНІЗМИ ЗАЛУЧЕННЯ СПРОМОЖНОСТЕЙ ПРИВАТНОГО СЕКТОРУ У СФЕРУ ПРОВАДЖЕННЯ ДЕРЖАВНОЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

В. Б. Гавриляк,
Національна академія державного управління при Президентові України

У статті здійснено огляд основних типів кібератак, а також принципи і механізми їх реалізації. Проведено аналіз досвіду Сполученого Королівства Великобританії щодо залучення спроможностей приватного сектору для впровадження кібербезпеки як державного сервісу. Зроблено висновок, що у приватному секторі наявний значний потенціал, який можна розглядати як важливий ресурс системи провадження державної кібербезпеки України.
Ключові слова: державно-приватне партнерство; кібератака; державна кібербезпека; кіберзахист; сервіс.

MECHANISMS FOR ATTRACTING THE CAPACITIES OF THE PRIVATE SECTOR IN THE SPHERE OF STATE CYBERSECURITY OF UKRAINE

V. B. Havryliak,
National Academy for Public Administration under the President of Ukraine

The article reviews the main types of cyberattacks and the principles and mechanisms of their realization. The experience of the United Kingdom in attracting the capacity of the private sector to implement cybersecurity as a state service is analyzed. It is concluded that there is significant potential in the private sector, which can be considered as an important resource of the system of providing state cybersecurity of Ukraine.
Keywords: cyberattack; cyber protection; state cybersecurity; service; state-private partnerships.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями. Дедалі більша активність злочинних угруповань у кіберпросторі, поширення кібертероризму, залежність усіх сфер життєдіяльності держави від інформації зумовлюють необхідність своєчасного впровадження державою кращих зарубіжних практик провадження кібербезпеки критичної інформаційної інфраструктури.

Як правило, існує два способи задоволення потреб певної організації в кібербезпеці. Одним з них є управління всіма процесами, де відповідний ІТ-підрозділ упроваджує рішення з кібербезпеки, що забезпечуватимуть захист обладнання, комунікацій та даних. Якщо все правильно зробити, цей тип захисту є потужним і така організація матиме повний контроль над усіма його аспектами. Однак указаний спосіб вимагає значних фінансових витрат на закупівлю дороговартісного обладнання, а також наявності висококваліфікованих кіберграмотних фахівців для його обслуговування.

Інший варіант – використання аутсорсингової моделі управління ризиками кібербезпеки, за якої низка сервісів кібербезпеки забезпечується довіреними сторонніми постачальниками шляхом надання послуг з кібербезпеки. При обмеженому державному фінансуванні заходів з кібербезпеки одним із дієвих механізмів провадження кібербезпеки може бути створення умов для залучення спроможностей приватного сектору в частині надання кібербезпекових послуг для захисту критичної інформаційної інфраструктури, оскільки значні потужності та передові технології переважно перебувають саме у власності приватних компаній.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Наукові дослідження, присвячені проблемним питанням та особливостям взаємодії державних органів і приватних суб'єктів у сфері кібербезпеки, здійснювали С. Петров (2019), О. Криворучко та А. Десятко (2020), М. Карр (Carr, 2016), В. Круглов (2018) та інші науковці. Водночас такі дослідження є поодинокими та здебільшого стосуються проблемних аспектів та правових основ державно-приватної взаємодії у сфері кібербезпеки, особливостей співпраці публічних органів і приватних суб'єктів у сфері кібербезпеки, кібербезпеки бізнесу, а отже, проблематика використання спроможностей приватного сектору в частині надання кібербезпекових послуг для забезпечення державної кібербезпеки є малодослідженою, що

© Гавриляк В. Б., 2020

підвищує актуальність теми обраного наукового дослідження.

Мета статті – обґрунтування механізмів залучення спроможностей приватного сектору у сферу провадження державної кібербезпеки України.

Виклад основного матеріалу. Новітні цифрові технології можуть бути одночасно і «засобами виробництва», і кіберзброєю. Нині терміни «Шпигунська програма», «Вірус», «Троян», «DDoS-атака» увійшли до лексикону багатьох людей, але в Україні усвідомлення масштабів та наслідків сучасних кіберзагроз, необхідності забезпечення максимально захищеного кіберпростору лише розпочинає формуватися.

У вітчизняному законодавстві «кібербезпека» визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (Про основні засади, 2017).

Кібератакою вважаються спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні і технологічні засоби та обладнання) і спрямовані на досягнення однієї або сукупності таких цілей:

– порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів;

– порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

– використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

У Конвенції Ради Європи про кіберзлочинність (Конвенція, 2001) йдеться про такі групи загроз конфіденційності, цілісності й доступності комп'ютерних даних та систем, що реалізуються через:

– несанкціонований доступ до інформаційного середовища (протиправний навмисний доступ до комп'ютерної системи або її частини, здійснений в обхід систем безпеки);

– нелегальне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних);

– втручання у дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);

– втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного програмного забезпечення, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на обробку та передавання інформації, на системи захисту IP, систем і мереж, програмно-математичне забезпечення, протоколи передавання даних, алгоритми адресації та маршрутизації);

– незаконне використання комп'ютерного й телекомунікаційного обладнання.

Знання принципів і механізмів реалізації кібератак дає можливість здійснити підбір та впровадження дієвих інструментів кіберзахисту, що даватимуть змогу запобігати виникненню кіберінцидентів, виявляти кібератаки, захищати від них електронні інформаційні ресурси, ліквідовувати наслідки кібератак на електронні інформаційні ресурси, відновлювати сталість і надійність функціонування комунікаційних та/або технологічних систем тощо. Тому далі розглянемо основні типи кібератак, а також принципи і механізми їх реалізації.

За способом розповсюдження кібератаки поділяють на масові та цілеспрямовані.

Масові кібератаки спрямовані на глобальне поширення шкідливого програмного забезпечення (англ. malware – скорочення від malicious – зловмисний і software – програмне забезпечення), здатного порушити працездатність системи, видалити важливі файли або пошкодити їх.

Прикладами найбільш поширених шкідливих програм є:

– традиційні (файлові) віруси – віруси, що заражають програми, порушуючи функціонування заражених програм або створюючи перешкоди в їх функціонуванні, або видаляють певні файли з комп'ютера;

– «троянські коні» (англ. Trojan Horses, Trojans) – віруси, що маскуються під корисні програми. Можливості таких програм різні – від простого стеження за інфікованим комп'ютером до знищення певних файлів за командою з відстані або за таймером;

– «черв'яки» (англ. worms) – використовуються для розсилки спаму та створення ботнетів (ці-

лих мереж з інфікованих комп'ютерів). Можуть проникати на комп'ютер як з вини користувача (через натискання певних посилань в електронних листах), так і без його участі – використовуючи «слабкі місця» в програмах захисту;

– сніфери (англ. to sniff – нюхати) – «шпигунські» програми, призначені для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів;

– руткіти (англ. root kit – набір суперкористувача, який має право на виконання всіх без винятку операцій) – «шпигунська» програма чи набір таких програм для приховування слідів присутності зловмисника або шкідливої програми в системі;

– віруси-майнери – програми або скрипти, що використовуються для видобування криптовалюти без відома власника системи, знижуючи при цьому її обчислювальні потужності;

– програми-вимагачі – шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв;

– макровіруси – віруси, написані мовою макросів, що використовуються для автоматизації деяких процесів у програмах типу Microsoft Word. Макровіруси заражають саму програму через відкритий документ із «сюрпризом», після цього заражена програма інфікує всі документи, які потім відкриваються;

– дропери – менш шкідливі віруси (або порівняно нешкідливі програми), призначені для «відволікання уваги» системи антивірусного захисту в момент зараження системи більш шкідливим вірусом.

На відміну від масових кібератак, *цілеспрямовані (цільові) кібератаки* – це заздалегідь продумані дії для ураження інформаційних систем певної організації.

Традиційно цільова кібератака здійснюється в кілька етапів:

– дослідження, під час якого проводиться аналіз стану проникнення в інформаційну систему;

– експлуатація вразливостей зі встановленням на пристрої жертви дистанційного керування;

– закріплення в системі з придушенням засобів захисту, блокуванням контрольних систем і знищенням слідів проникнення;

– установлення цільового програмного забезпечення та його експлуатація.

Серед цільових атак яскраво виділяються так звані кібератаки APT (англ. Advanced Persistent Threat – розвинена стала загроза або постійна загроза підвищеної складності) – різновид складних кібератак з метою отримання несанкціонованого доступу до інформаційних систем «жертви» та встановлення прихованого доступу до неї для використання або контролю в майбутньому.

Найбільш уразливими в будь-якій інфраструктурі є ресурси, відкриті для доступу ззовні – вебсайти, сервери додатків, баз даних та ін. Щоб атакувати внутрішні ресурси певної організації, зловмисникові необхідно знайти уразливості в інфраструктурі і подолати мережевий захист, а атака на зовнішні ресурси вимагає набагато менше зусиль. Один з найбільш популярних видів атак на публічні сервіси – розподілена атака, спрямована на відмову в обслуговуванні (Distributed Denial of Service, DDoS), суть якої зводиться до генерації великої кількості паразитного трафіку, що направляється на цільові сервери. У разі, якщо генерований трафік перевищує пропускну здатність каналів, що забезпечують зв'язок серверів з мережею «Інтернет», або якщо обробка трафіку забирає всі ресурси сервера, нормальне функціонування припиняється. Інфраструктура перестає обробляти і відповідати на запити звичайних користувачів, що призводить до відмови в їх обслуговуванні.

Мотиви проведення DDoS-атак бувають різними, починаючи від простого хуліганства і закінчуючи політичними протестами, чи навіть цілеспрямованими кібератаками на конкретний інформаційний ресурс. Технічно атаки проводяться з безлічі різних пристроїв, найчастіше заражених шкідливим програмним забезпеченням (бот-мережі). Останнім часом також збільшилася кількість атак зі зламаних домашніх роутерів і «розумної» побутової електроніки (Internet of Things, IoT – інтернету речей), що істотно ускладнює відбиття DDoS-атаки, оскільки унеможливлює точкові блокування атакуючих комп'ютерів. Найчастіше спроби відбити атаку силами організації зводяться до відключення інформаційних сегментів від мережі та очікування закінчення атаки.

Аналізуючи розглянуті вище типи кіберзагроз та кібератак, виділимо такі з них, що однозначно криють у собі загрози кібербезпеці:

– шкідливе програмне забезпечення (зокрема віруси, черв'яки, трояни, програми-вимагачі);

– шпигунське програмне забезпечення (зокрема сніфери та руткіти);

– атаки на відмову в обслуговуванні (DoS- та DDoS-атаки);

– кібератаки APT (Advanced Persistent Threat).

При обмеженому обсязі коштів, що виділяються на утримання органів публічної влади, та за умови недостатнього усвідомлення багатьма керівниками цих органів значення кібербезпеки

та кіберзахисту для національної безпеки, фінансування заходів із кіберзахисту здійснюється, як правило, за залишковим принципом. Та й заходи з кіберзахисту не є «разовою акцією», а повинні вживатися на постійній основі.

У таких умовах одним із дієвих способів провадження кібербезпеки в Україні може стати залучення спроможностей приватного сектору в частині надання ним кібербезпекових послуг для захисту критичної інформаційної інфраструктури, оскільки значні потужності та передові технології переважно перебувають саме у власності приватних компаній. Особливо це актуалізується з огляду на те, що одним із важливих принципів, на якому має ґрунтуватися кібербезпека в Україні, є принцип державно-приватної взаємодії у сфері кібербезпеки (Про рішення, 2016).

Розглянемо далі так звану аутсорсингову модель управління ризиками кібербезпеки, за якої низка сервісів кібербезпеки забезпечується довіреними сторонніми постачальниками шляхом надання послуг з кібербезпеки.

Кібербезпека як сервіс (англ. Cyber Security as a Service – CSaaS) – це модель, за якої провайдер інтегрує сервіси кібербезпеки у власну інфраструктуру та постачає такі сервіси кібербезпеки за додаткову плату у вигляді послуги чи підписки. Підприємства, замовляючи CSaaS, отримують можливість зменшити кількість необхідного обладнання кіберзахисту і, відповідно, потребу у висококваліфікованому персоналі для його обслуговування, завдяки чому зменшаться витрати на кібербезпеку.

Найбільш поширеними опціями CSaaS є захист від DDoS-атак, керування доступом користувачів, антивірусний захист, антишпигунський захист, спам-захист, виявлення мережевих вторгнень, тестування на виявлення вразливостей, управління інцидентами, навчання персоналу тощо.

Провідні держави світу, зокрема США, Німеччина та Великобританія, вже давно оцінили переваги так званого ринкового підходу до кібербезпеки у рамках провадження державно-приватного партнерства.

Для України може бути корисним досвід Великобританії. У Сполученому Королівстві Великобританії, поряд зі схемами публічно-приватного партнерства у сфері кібербезпеки, успішно діють урядові програми закупівель у сфері кібербезпеки.

У 2013 р. Урядовою цифровою службою (Government Digital Service) та Королівською комерційною службою (Crown Commercial Service) Великобританії було започатковано ініціативу «UK Government G-Cloud», у рамках якої державні структури отримали можливість закуповувати послуги у провайдерів хмарних сервісів в онлайн-магазині «Digital Marketplace» (United Kingdom). Через такий онлайн-магазин державні органи можуть замовити низку хмарних сервісів (хостингу, програмного забезпечення, послуг підтримки), отримати послуги експертів у сфері цифрових технологій (у рамках програми «Digital Outcomes and Specialists»), фізичний обсяг місця у дата-центрі (в рамках програми «Crown Hosting Data Centres»), замовити послуги з розроблення політики безпеки даних, оцінки та управління ризиками, управління інцидентами, розроблення безпекової архітектури установи тощо (в рамках програми «Cyber Security Services»). При цьому замовити зазначені сервіси від обраних компаній державні структури можуть через згаданий вище онлайн-магазин «Digital Marketplace» без необхідності проводити повний тендер або конкурсний процес закупівель.

Як бачимо, у Великобританії акцент робиться на заходах щодо посилення взаємної довіри між державним і недержавним секторами у межах механізму державних закупівель якісних послуг у сфері цифрових технологій.

В умовах недостатнього фінансування державних органів і, як наслідок, обмежених можливостей вжиття державними органами заходів щодо забезпечення кібербезпеки такий механізм взаємодії державного та приватного сектору видається надзвичайно перспективним для України.

Висновки та перспективи подальших досліджень. На сьогодні розробити і впровадити абсолютно дієву систему кіберзахисту, що дасть змогу забезпечувати належний рівень кіберзахисту, навряд чи можливо, оскільки за наявності достатнього обсягу часу і сучасних програмно-технічних засобів можна подолати будь-який опір системи кіберзахисту. Тому взагалі йдеться про достатній рівень якості роботи системи кіберзахисту, при якому фінансові витрати на її побудову та експлуатацію, ризик успішної реалізації кібератак і розмір можливого збитку від них були б сумірними між собою та прийнятними.

За результатами аналізу існуючих кіберзагроз та кібератак виділено їх основні типи, що однозначно криють у собі загрози кібербезпеці України, а саме:

– шкідливе програмне забезпечення (зокрема віруси, черв'яки, трояни, програми-вимагачі);

– шпигунське програмне забезпечення (зокрема сніфери та руткіти);

– атаки на відмову в обслуговуванні (DoS- та DDoS-атаки);

– кібератаки APT (Advanced Persistent Threat).

Проведено аналіз досвіду Сполученого Королівства Великобританії щодо залучення спроможностей приватного сектору для провадження кібербезпеки. Встановлено, що приватний сектор відіграє важливу роль у забезпеченні державних структур Великобританії якісними послугами у сфері цифрових технологій.

Установлено, що найбільш поширеними опціями моделі провадження кібербезпеки CSaaS, за якої низка завдань з кібербезпеки може забезпечуватися довіреними сторонніми постачальниками шляхом надання послуг з кібербезпеки, є захист від DDoS-атак, керування доступом користувачів, антивірусний захист, антишпигунський захист, спам-захист, виявлення мережевих вторгнень, тестування на виявлення вразливостей, управління інцидентами, навчання персоналу тощо. Також це дає змогу побудувати глибоко ешелонований захист від атак ззовні, оскільки перевірка та фільтрація трафіку відбуваються ще до того, як він досягнув активного обладнання мережі призначення.

У вітчизняному приватному секторі наявний значний потенціал, який можна розглядати як важливий ресурс системи провадження кібербезпеки. Разом з тим під час використання моделі CSaaS приватний сектор має бути не менш відповідальним за захист даних, якими він володіє, сприяти забезпеченню стійкості систем, розв'язанню кіберінцидентів та нести юридичну відповідальність за наслідки можливих кібератак.

Список використаних джерел

Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право.* 2019. № 4 (31). URL: http://ippi.org.ua/sites/default/files/15_11.pdf (дата звернення: 01.12.2020).

Криворучко О. В., Десятко А. М. Бізнес та кібербезпека. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (Київ, 15 трав. 2020 р.). Київ : НА СБУ, 2020. С. 122–124. URL: http://academy.ssu.gov.ua/upload/file/Zbirnik2020.pdf#page=122 (дата звернення: 01.12.2020).

Carr M. Public-private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf (дата звернення: 02.12.2020).

Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/3_2018/13.pdf (дата звернення: 03.12.2020).

Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.12.2020).

Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 994 : ратифіковано Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 04.12.2020).

Про рішення Ради національної безпеки і оборони України від 27.01.2016 «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96. URL: https://zakon3.rada.gov.ua/laws/show/96/2016. (дата звернення: 04.12.2020).

United Kingdom Government Digital Service. URL: https://www.gov.uk/government/organisations/government-digital-service (дата звернення: 06.12.2020).

References

Petrov, S. H. (2019). Pravovi osnovy vzaiemodii derzhavnykh orhaniv ta pryvatnykh subiektiv iz metoiu zakhystu elektronnykh informatsiinykh resursiv Ukrainy [Legal bases of the interaction of public authorities and private entities with the aim of ensuring cybersecurity and protection of electronic information resources of Ukraine]. *Informatsiia i pravo.* Is. 4 (31). Retrieved from: http://ippi.org.ua/sites/default/files/15_11.pdf [in Ukrainian].

Kryvoruchko, O. V., Desiatko, A. M. (2020). Biznes ta kiberbezpeka [Business and cybersecurity]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy* : zb. tez nauk. dop. nauk.-prakt. konf. [*Actual problems of the management of information security of the state*, collection of abstracts of scientific reports of the XI All-Ukrainian Scientific and Practical Conference]. Kyiv : Nats. akad. SBU. P. 122–124. Retrieved from: http://academy.ssu.gov.ua/upload/file/Zbirnik2020.pdf#page=122

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. Retrieved from: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Kruhlov, V. V. (2018). Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky [Public-private partnership in the field of cybersecurity]. Retrieved from: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/3_2018/13.pdf

Verkhovna Rada of Ukraine (2017). Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [The Law of Ukraine «About the basic principles of providing of cyber security of Ukraine»]. N.p., 05.10.2017 № 2163-VIII. Retrieved from: http://zakon3.rada.gov.ua/laws/show/2163-19

Council of Europe (2001). Konventsiia pro kiberzlochynnist vid 23.11.2001 № 994 : ratyfikovano Zakonom Ukrainy vid 07.09.2005 № 2824-IV [Convention on Cybercrime]. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_575

United Kingdom Crown Commercial Service. URL: https://www.gov.uk/government/organisations/crown-commercial-service (дата звернення: 06.12.2020).

United Kingdom Digital Marketplace. URL: https://www.digitalmarketplace.service.gov.uk (дата звернення: 06.12.2020).

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 15.03.2016 № 96. Retrieved from: https://zakon3.rada.gov.ua/laws/show/96/2016

Government Digital Service. Retrieved from: https://www.gov.uk/government/organisations/government-digital-service

Crown Commercial Service. Retrieved from: https://www.gov.uk/government/organisations/crown-commercial-service

Digital Marketplace. Retrieved from: https://www.digitalmarketplace.service.gov.uk

Гавриляк Віталій Богданович,
аспірант кафедри інформаційної політики та цифрових технологій,
Національна академія державного управління при Президентові України,
03057, Україна, м. Київ, вул. Антона Цедіка, 20

Цитування: Гавриляк В. Б. Механізми залучення спроможностей приватного сектору у сферу провадження державної кібербезпеки України. *Вісн. НАДУ. Серія «Державне управління».* 2020. № 4 (99). С. 99–104.

Стаття надійшла: 30.11.2020

Схвалено до друку: 16.12.2020

Havryliak, Vitalii B.,
Ph.D student of Information Policy and Digital Technologies Department,
National Academy for Public Administration under the President of Ukraine,
20, Anton Tsedyk St., Kyiv, 03057, Ukraine
E-mail: vitgavrilyak@gmail.com
http://orcid.org/0000-0002-2058-1987

Citation: Havryliak, V. B. (2020). Mekhanizmy zaluchennia spromozhnostei pryvatnoho sektoru u sferu provadzhennia derzhavnoi kiberbezpeky Ukrainy [Mechanisms for attracting the capacities of the private sector in the sphere of state cybersecurity of Ukraine]. *Bulletin of the NAPA. Series «Public Administration».* Is. 4 (99). P. 99–104 [in Ukrainian].

Article arrived: 30.11.2020

Accepted: 16.12.2020