УДК 351:007:004
DOI 10.36030/2310-2837-1(100)-2021-46-52

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЄС (2021) НА ЦИФРОВЕ ДЕСЯТИЛІТТЯ: ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

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

У статті проаналізовано світові тренди в глобальному кіберсередовищі та пов'язані з ними кібербезпекові виклики та ризики. Розглянуто концептуальні положення Стратегії кібербезпеки Євросоюзу на цифрове десятиліття в контексті виявлення можливостей перейняття кращих практик європейського досвіду у сфері провадження кібербезпеки України. З урахуванням ключових кібербезпекових викликів, ризиків та загроз, стратегічних завдань та шляхів забезпечення кібербезпеки Євросоюзу розроблено пропозиції щодо подальшого розвитку національної системи кібербезпеки. Акцентовано увагу на необхідності посилення кібердіалогу з ЄС та міжнародними організаціями, а також подальшої активізації роботи з міжнародними партнерами з розвитку і просування глобального, відкритого, стабільного і безпечного кіберпростору.
Ключові слова: Євросоюз; кібербезпека; кіберстійкість; національна система кібербезпеки; стратегія кібербезпеки.

THE EU'S CYBERSECURITY STRATEGY (2021) FOR THE DIGITAL DECADE: PERSPECTIVES FOR UKRAINE

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

The article analyzes world trends in global cyberspace and related cybersecurity challenges and risks. The conceptual provisions of the EU's Cybersecurity Strategy for the Digital Decade are studied in the context of identifying opportunities for adopting the best practices of European experience in the field of ensuring cybersecurity of Ukraine. Taking into account the key cyber challenges and cyber threats, strategic objectives and ways to ensure the cyber security of the European Union, proposals have been developed for the further improvement of the national cybersecurity system. Emphasis is placed on the need to strengthen cyber dialogue with the EU and international organisations, as well as further intensifying work with international partners to developing and advancing a global, open, stable and secure cyberspace.
Keywords: cybersecurity; cyber resilience; cybersecurity strategy; European Union; national cybersecurity system.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями. Надзвичайно велика залежність усіх сфер життєдіяльності держави від інформації та всеохопне поширення цифрових технологій, зокрема у сфері публічного управління, спричинили появу викликів і загроз нового технологічного рівня. Також у міру розвитку самих цифрових технологій спостерігається підвищення технічного рівня інструментарію реалізації кіберзагроз, посилюється тенденція до зростання питомої ваги кіберзагроз у спектрі загроз національній безпеці нашої держави. З урахуванням розширення ландшафту кіберзагроз та ускладнення інструментарію їх реалізації уряди провідних країн вживають заходів щодо вдосконалення національних систем кібербезпеки та зміни стратегій протидії кіберзагрозам.

У зв'язку із цим нагальною є проблема формування збалансованої та ефективної національної системи кібербезпеки, яка б була спроможною гнучко адаптуватися до змін безпекового середовища, гарантувати громадянам нашої держави безпечне функціонування національного сегменту кіберпростору. Однією з найбільш нагальних потреб у сфері національної кібербезпеки є визначення ключових стратегічних проблем і шляхів їх вирішення з метою реалізації ефективних і дієвих механізмів провадження кібербезпеки України.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Проблемним питанням формування шляхів та застосування інструментів захисту національних інтересів у кіберпросторі з урахуванням досвіду провідних країн світу стосовно провадження кібербезпеки в розрізі загроз національній безпеці України присвячено дослідження таких вітчизняних науковців, як М. Рижкова та А. Рубан (2019), С. Кавина (2020), Є. Котуха (2020), Д. Мельника (2021) та ін. Проте в сучасних умовах глобалізації повсякчас виникають нові виклики та проблемні питання у сфері кібербезпеки, які вимагають зміни підходів щодо

визначення особливостей кіберзагроз, уточнення шляхів та механізмів захисту національних інтересів у кіберпросторі, що підвищує актуальність теми обраного наукового дослідження.

Мета статті – аналіз основних положень Стратегії кібербезпеки Євросоюзу на цифрове десятиліття в контексті виявлення можливостей перейняття кращих практик європейського досвіду у сфері провадження державної кібербезпеки та їх адаптації до українських реалій.

Виклад основного матеріалу. Кожна держава світу має право самостійно встановлювати основні елементи (складові) системи кібербезпеки, визначати перелік заходів щодо її забезпечення, суб'єктів та об'єкти кібербезпеки і кіберзахисту виходячи зі стратегічних цілей і завдань, що стоять перед державою на національному та міжнародному рівнях. У провідних країнах світу проблеми національної кібербезпеки вивчаються в контексті так званих стратегічних досліджень, а пріоритети, стратегічні цілі та завдання забезпечення кібербезпеки визначаються у відповідних стратегіях кібербезпеки.

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави указом Президента України від 15 березня 2016 р. № 96 у нашій державі було затверджено Стратегію кібербезпеки України (Про рішення, 2016).

Одним із важливих заходів щодо досягнення мети зазначеної стратегії кібербезпеки визначено, зокрема, необхідність невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Вітчизняне законодавство визначає «національну систему кібербезпеки» як сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Основу національної системи кібербезпеки становлять: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. До суб'єктів забезпечення кібербезпеки України також належать інші державні органи, що є розпорядниками інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури та інших об'єктів кібербезпеки, які провадять діяльність із надання інформаційних та/або телекомунікаційних послуг, незалежні організації та експерти.

Координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, здійснює Рада національної безпеки і оборони України відповідно до Конституції України та в установленому законом порядку. Системоутворюючим елементом усієї системи кібербезпеки та кіберзахисту України є Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України (Про Національний координаційний центр, 2016).

Ґрунтуючись на Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 р. № 287 (Про рішення, 2015), а також Стратегії кібербезпеки України, в нашій державі було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» (Про основні засади, 2017), що став основою для ухвалення інших законодавчих та підзаконних актів у царині забезпечення національної кібербезпеки.

Разом з тим у сучасних умовах глобалізації постійно з'являються нові виклики, загрози та проблемні питання у сфері кібербезпеки. Зокрема, у світі спостерігається посилення інтенсивності міждержавного протиборства і розвідувально-підривної діяльності в кіберпросторі, зростання кіберзлочинності, використання кіберпростору терористичними організаціями для вчинення актів кібертероризму тощо.

Одним з найбільш обговорюваних питань на міжнародній арені нині є пандемія COVID-19. У її контексті на глобальному рівні з початку 2020 р. спостерігається активізація незаконної діяльності у кіберпросторі. Поширення вірусу SARS-CoV-2 загострило серед іншого питання провадження кібербезпеки.

Пандемія COVID-19 ще більше демонструє повсюдну залежність від коректного функціонування цифрових систем і перевіряє ефективність і стійкість державних і приватних програм кібербезпеки. Режим віддаленої роботи додатково підвищив рівень проблем і викликів кібербезпеки, оскільки деякі з невід'ємних заходів безпеки, які сприймаються та застосовуються як належне в процесі роботи безпосередньо в захищених мережах організацій, установ та підприємств, не можуть повною мірою бути вжиті під час роботи вдома.

Основними факторами, які сприяли підвищенню деструктивної (протизаконної) кіберактивності на фоні пандемії COVID-19, є:

– наростання тривожності та глобальний страх (паніка) населення перед пандемією COVID-19;

– збільшення часу перебування людей у мережі «Інтернет» загалом, оскільки через обмеження на пересування громадяни більше часу проводять вдома;

– різке зростання кількості людей у всьому світі, які через масовий карантин перейшли на віддалену роботу;

– збільшення кількості випадків фішингових атак, у яких кіберзлочинці експлуатують тему пандемії COVID-19, застосовуючи «соціальну інженерію»;

– зростання кількості підробних сайтів, за допомогою яких зловмисники намагаються отримати зиск від пандемії;

– потенційна можливість для інформаційних та кібератак з метою дестабілізації ситуації;

– потенційна зацікавленість кіберагресивних урядів та злочинних кіберугруповань у заволодінні інформацією про розроблення вакцини проти COVID-19, технології тестування, лікування від вірусу SARS-CoV-2 та, як наслідок, перемозі в «гонитві в розробленні вакцини проти COVID-19» (Karpenko, 2021).

Пандемія COVID-19 спричинила появу так званої «нової норми» (Sagey, 2020). Зміни були загальносвітовими, швидкими та широкомасштабними, і включали: дистанційну роботу як нову норму; швидке збільшення використання інструментів для спільної роботи; пришвидшення темпів цифрових трансформацій та перехід на хмарні ресурси.

З урахуванням світових трендів у глобальному кіберсередовищі в грудні 2020 р. Європейська Комісія та Верховний представник Європейського Союзу з питань закордонних справ і політики безпеки представили Стратегію кібербезпеки Євросоюзу на цифрове десятиліття (The EU's Cybersecurity Strategy, 2020). У стратегії викладено, як ЄС захищатиме своїх людей, бізнес і установи від кіберзагроз, а також як ЄС сприятиме розвитку міжнародного співробітництва та буде лідером у забезпеченні глобального і відкритого інтернету.

Ураховуючи прогрес, досягнутий за попередніми стратегіями, Стратегія кібербезпеки Євросоюзу на цифрове десятиліття містить конкретні пропозиції щодо розгортання таких трьох основних інструментів як регуляторний, інвестиційний та політичний інструменти. Ці пропозиції та інструменти є необхідними для забезпечення трьох сфер дій ЄС:

– стійкість, технологічний суверенітет та лідерство;

– нарощування оперативного потенціалу для запобігання, стримування та реагування;

– просування глобального та відкритого кіберпростору.

ЄС прагне підтримувати цю стратегію шляхом безпрецедентного рівня інвестицій у цифровий перехід ЄС протягом наступних семи років, потенційно вчетверо збільшуючи попередні рівні інвестицій.

Стратегія кібербезпеки Євросоюзу на цифрове десятиліття спрямована на зміцнення колективної стійкості Європи проти кіберзагроз та забезпечення всім громадянам та бізнесу Європейського Союзу повної вигоди від надійних послуг та цифрових інструментів. Ця Стратегія також повинна дати змогу Євросоюзу зміцнити лідерство в галузі міжнародних норм та стандартів у кіберпросторі, а також розвивати співпрацю з партнерами по всьому світу для сприяння глобальному, відкритому, стабільному та безпечному кіберпростору.

Важливим компонентом захисту ЄС від кіберзагроз також визначено підвищення кіберкваліфікації робочої сили, розвиток, залучення та збереження найкращих талантів у галузі кібербезпеки.

Серед нових стратегічних ініціатив Євросоюзу доцільно виділити такі:

– створення Європейського кіберщита (An EU-wide Cyber Shield) через мережу Операційних центрів безпеки (Security Operations Centres, SOCs) з підтримкою штучного інтелекту, які можуть виявляти ознаки кібератаки та забезпечувати запобіжні дії до завдання збитків;

– створення Спільного кіберпідрозділу (A Joint Cyber Unit) – платформи, яка дасть змогу краще захистити Європейський Союз від найефективніших атак на кібербезпеку, особливо транскордонних, а також покращити координацію дій країн товариства з виявлення кібератак і відповіді на них;

– упровадження європейських рішень для посилення безпеки мережі «Інтернет» по усьому світу;

– розроблення положення щодо забезпечення інтернету безпечних речей (Internet of Secure Things);

– розроблення положення про високі стандарти кібер- та інформаційної безпеки в установах, органах та агентствах Європейського Союзу.

Основними напрямами забезпечення кібербезпеки Європейського Союзу є підвищення кібер-

стійкості, боротьба з кіберзлочинністю, розвиток кібердипломатії, посилення кіберзахисту, фінансування досліджень і дій, захист критично важливої інфраструктури.

Кібербезпека повинна бути інтегрована в тому числі й у такі ключові технології, як штучний інтелект, шифрування та квантові обчислення. Вживатимуться також заходи щодо кібербезпечності 5G-мереж та майбутніх поколінь мереж. Це дасть змогу стимулювати розвиток європейської галузі кібербезпеки та полегшити поступову відмову від застарілих систем.

Усі підключені до інтернету пристрої в ЄС та цілі ланцюги їх поставок повинні бути спроєктовані захищеними (secure-by-design) від кібервипадків та мати підтримку швидкого виправлення вразливостей у разі їх виявлення.

Запланована ініціатива розгортання безпечної інфраструктури квантових комунікацій (Quantum communication infrastructure, QCI) має запропонувати органам публічної влади ЄС абсолютно новий спосіб передачі конфіденційної інформації за допомогою надзахищеної форми шифрування для захисту від кібератак, створений за допомогою європейських технологій. Такий захист міститиме дві основні складові: існуючі наземні волоконно-комунікаційні мережі, що зв'язують стратегічні об'єкти на національному та транскордонному рівнях, та пов'язані космічні супутники, що охоплюють весь ЄС, у тому числі його заморські території. Ця ініціатива щодо розробки та розгортання нових та більш безпечних форм шифрування і розробки нових способів захисту критичних комунікаційних ресурсів та ресурсів даних може сприяти захисту конфіденційної інформації та, у свою чергу, критичної інфраструктури.

Європейський Союз також передбачає надання практичної допомоги партнерам щодо зміцнення кібербезпеки. Розбудова кіберпотенціалу ЄС буде зосереджуватися на Західних Балканах та в сусідніх з ЄС країнах, а також у країнах-партнерах, де відбувається швидкий цифровий розвиток. Зусиллями ЄС планується підтримувати розробку законодавства та політики країн-партнерів згідно з відповідною політикою та стандартами ЄС у галузі кібердипломатії.

Запобігання неправомірному використанню технологій, захист критично важливої інфраструктури та забезпечення цілісності ланцюгів поставок обладнання також дасть змогу ЄС дотримуватися норм, правил і принципів відповідальної поведінки держави ООН.

У березні 2021 р. Європейська Рада прийняла висновки щодо Стратегії кібербезпеки Європейського Союзу на цифрове десятиліття, в яких зазначається, що кібербезпека має важливе значення для побудови стійкої, зеленої та цифрової Європи (Cybersecurity: Council adopts, 2021). Зазначені висновки ставлять ключовою метою досягнення стратегічної автономії при збереженні відкритої економіки, включаючи підвищення здатності робити самостійний вибір у галузі кібербезпеки з метою зміцнення цифрового лідерства та стратегічного потенціалу Європейського Союзу.

Водночас Європейська Рада наголошує поряд з іншим на необхідності підтримки розвитку надійного шифрування як засобу захисту основних прав і цифрової безпеки, забезпечуючи при цьому здатність правоохоронних і судових органів здійснювати свої повноваження як у мережі, так і в автономному режимі. Євросоюзом і надалі надаватиметься підтримка правоохоронному потенціалу в галузі цифрових розслідувань та збирання цифрових доказів, включаючи справу з шифруванням у кримінальних розслідуваннях, зберігаючи при цьому свою функцію захисту основних прав та кібербезпеки.

Дедалі більший вплив на розбудову національної системи кібербезпеки справляють світові тренди в глобальному кіберсередовищі. З урахуванням світових трендів у глобальному кіберпросторі, ґрунтуючись на новій Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 р. № 392 (Про рішення, 2020), робочою групою при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України в березні 2021 р. схвалено проєкт Стратегії кібербезпеки України на 2021–2025 роки (Проєкт Стратегії, 2021). Одним з важливих напрямів реалізації пріоритетів національних інтересів України та забезпечення національної безпеки, визначених новою Стратегією національної безпеки України, є підвищення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі.

З урахуванням поглиблення євроінтеграційних процесів у нашій державі низка виявлених у Стратегії кібербезпеки Євросоюзу на цифрове десятиліття основних інструментів, спрямованих на ключові сфери дії у сфері кібербезпеки, та стратегічних ініціатив Євросоюзу доцільно врахувати при впровадженні Стратегії кібербезпеки України на 2021–2025 роки.

На нашу думку, Україні необхідно уніфікувати підходи, методи і засоби забезпечення кібербезпеки з усталеними практиками Євросоюзу, вжи-

вати інших узгоджених із ключовими іноземними партнерами заходів.

Висновки та перспективи подальших досліджень. Спроможність держави захищати національні інтереси в кіберпросторі стає важливою складовою кібербезпеки. Комплексний характер актуальних загроз національній безпеці у сфері кібербезпеки потребує визначення інноваційних підходів до формування національної системи кібербезпеки.

Світові тренди в глобальному кібербезпековому середовищі вимагають переосмислення, своєчасного оновлення та уточнення вітчизняних пріоритетів, стратегічних цілей та завдань кібербезпеки. Однією з основ для розроблення та впровадження оновленої стратегії кібербезпеки України може стати досвід у сфері кібербезпеки провідних країн, зокрема кращі практики європейського досвіду у сфері провадження кібербезпеки.

Стратегія кібербезпеки Євросоюзу на цифрове десятиліття містить конкретні пропозиції щодо впровадження трьох основних інструментів: регуляторного, інвестиційного та політичного, що спрямовані на такі три сфери дій ЄС як: 1) стійкість, технологічний суверенітет та лідерство; 2) нарощування оперативного потенціалу для запобігання, стримування та реагування; 3) просування глобального та відкритого кіберпростору.

Кібербезпеку Євросоюзу планується забезпечувати шляхом:

– підвищення безпеки основних послуг та підключених речей;

– посилення колективних можливостей реагування на великі кібератаки;

– забезпечення співпраці з партнерами по всьому світу для забезпечення міжнародної безпеки та стабільності в кіберпросторі.

За нашою оцінкою, базуючись на концептуальних положеннях Стратегії кібербезпеки Євросоюзу на цифрове десятиліття, можна окреслити таке коло рекомендованих заходів щодо підвищення спроможностей національної системи кібербезпеки:

– зміцнити систему координації суб'єктів забезпечення кібербезпеки і кібероборони України, що базується на чіткому розподілі відповідальності таких суб'єктів;

– підвищувати кіберкваліфікацію кадрового потенціалу суб'єктів кібербезпеки, розвивати, залучати найкращі таланти в галузі кібербезпеки та зберігати їх;

– розробити та впровадити індикатори стану кібербезпеки з метою фіксації досягнень та недоліків функціонування системи кібербезпеки;

– збільшити інвестиції в оновлення та розвиток критичної інфраструктури, що дасть змогу підвищити рівень кіберстійкості відповідних публічних та приватних секторів, які виконують важливі функції для економіки та суспільства;

– стимулювати наукові дослідження у сфері криптографічного захисту інформації для розробки вітчизняних постквантових алгоритмів шифрування та електронного підпису для забезпечення конфіденційності, цілісності інформації та підтвердження її авторства в разі появи квантових комп'ютерів і квантових кібератак;

– створити та впровадити дієву модель державно-приватного партнерства у сфері кібербезпеки, в тому числі розробити механізми залучення спроможностей приватного сектору у сферу провадження державної кібербезпеки України;

– посилити кібердіалог з ЄС та міжнародними організаціями, в тому числі шляхом долучення до неформальної мережі кібердипломатії ЄС, що дасть змогу Україні брати участь у наданні ефективної та всебічної спільної дипломатичної відповіді на зловмисну кібердіяльність, а також підтримувати ситуаційну обізнаність, обмінюватися інформацією та брати регулярну участь у координації подій в кіберпросторі;

– імплементувати положення оновленої NIS-директиви ЄС, а також Конвенцію Ради Європи про кіберзлочинність;

– здійснювати подальшу гармонізацію нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Євросоюзу та НАТО, що дасть змогу посилити безпеку національного сегменту мережі «Інтернет».

Запропоновані заходи поряд з іншими сприятимуть посиленню кіберстійкості України, розвитку спроможностей національної системи кібербезпеки та захисту національних інтересів у кіберпросторі, а також активізації роботи з міжнародними партнерами з розвитку і просування глобального, відкритого, стабільного і безпечного кіберпростору, в якому дотримуються міжнародне право, права людини, основні свободи і демократичні цінності.

Список використаних джерел

Рижков М. М., Рубан А. Стратегія інформаційної і кібербезпеки ЄС: сучасний вимір. *Міжнародні відносини. Серія «Політичні науки»*. 2019. № 21. URL: http://

References

Ryzhkov, M. M., Ruban, A. (2019). Stratehiia informatsiinoi i kiberbezpeky YeS : suchasnyi vymir [EU Information

journals.iir.kiev.ua/index.php/pol_n/article/view/3866 (дата звернення: 15.03.2021).

Кавин С. Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. *Актуальні проблеми держави і права.* 2020. № 87. URL: http://apdp.onua.edu.ua/index.php/apdp/article/view/2797 (дата звернення: 15.03.2021).

Котух Є. В. Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток.* 2020. № 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1596 (дата звернення: 16.03.2021).

Мельник Д. С. Щодо сучасних загроз національній безпеці України в інформаційній сфері. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (Київ, 26 бер. 2021 р.). Київ : НА СБУ, 2021. С. 68–71. URL: http://academy.ssu.gov.ua/upload/file/конференція%2026.03.2021.pdf (дата звернення: 30.03.2021).

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: 01.04.2021).

Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 01.04.2021).

Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 № 287. URL: https://zakon.rada.gov.ua/laws/show/287/2015/ed20150526#Text (дата звернення: 01.04.2021).

Про основні засади забезпечення кібербезпеки України : Закон України. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.04.2021).

Karpenko O., Kuczabski A., Havryliak V. Mechanisms for providing cybersecurity during the COVID-19 pandemic: Perspectives for Ukraine. *Security and Defence Quarterly.* Is. 33(1). URL: https://doi.org/10.35467/sdq/133158 (дата звернення: 01.04.2021).

Sagey M. Securing the «new normal» – protecting the post Covid-19 world. URL: https://blog.checkpoint.com/2020/06/09/securing-the-new-normal-protecting-the-post-covid-19-world (дата звернення: 01.04.2021).

European Commission. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (дата звернення: 02.04.2021).

European Council. Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy (дата звернення: 02.04.2021).

Про рішення Ради національної безпеки і оборони України від 14.09.2020 «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392. URL: https://zakon.rada.

and Cybersecurity Strategy : A Modern Dimension]. *Mizhnarodni vidnosyny. Seriia «Politychni nauky»*. № 21. Retrieved from: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3866

Kavin, S. Y. (2020). Pravovi zasady zabezpechennia kiberbezpeky v derzhavakh – chlenakh Yevropeiskoho Soiuzu [Legal framework for cybersecurity in European Union member states]. *Aktualni problemy derzhavy i prava*. №. 87. Retrieved from: http://apdp.onua.edu.ua/index.php/apdp/article/view/2797

Kotukh, Y. (2020). Formuvannia system kiberbezpeky v orhanakh publichnoi vlady [Formation of cyber security systems in public authorities]. *Derzhavne upravlinnya: udoskonalennya ta rozvytok*. № 3. Retrieved from: http://www.dy.nayka.com.ua/?op=1&z=1596

Melnyk, D. S. (2021). Shchodo suchasnykh zahroz natsionalnii bezpetsi Ukrainy v informatsiinii sferi [On modern threats to the national security of Ukraine in the information sphere]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy :* zb. tez nauk. dop. nauk.-prakt. konf. Kyiv : Nats. akad. SBU. P. 68–71. Retrieved from: http://academy.ssu.gov.ua/upload/file/конференція%2026.03.2021.pdf

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

Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky : Ukaz Prezydenta Ukrainy vid 07.06.2016 № 242. Retrieved from: https://zakon.rada.gov.ua/laws/show/242/2016

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 26.05.2015 № 287. Retrieved from: https://zakon.rada.gov.ua/laws/show/287/2015/ed20150526#Text

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

Karpenko, O., Kuczabski, A., Havryliak, V. (2021). Mechanisms for providing cybersecurity during the COVID-19 pandemic : Perspectives for Ukraine. *Security and Defence Quarterly.* Is. 33 (1). Retrieved from: https://doi.org/10.35467/sdq/133158

Sagey, M. (2020). Securing the «new normal» – protecting the post Covid-19 world. Retrieved from: https://blog.checkpoint.com/2020/06/09/securing-the-new-normal-protecting-the-post-covid-19-world

European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

European Council (2021). Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy

gov.ua/laws/show/392/2020#Text (дата звернення: 03.04.2021).

Проєкт Стратегії кібербезпеки України (2021–2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 03.04.2021).

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» : Ukaz Prezydenta Ukrainy vid 14.09.2020 № 392. Retrieved from: https://zakon.rada.gov.ua/laws/show/392/2020#Text

Proiekt Stratehii kiberbezpeky Ukrainy (2021–2025 roky). Retrieved from: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

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. Стратегія кібербезпеки ЄС (2021) на цифрове десятиліття: перспективи для України. *Вісн. НАДУ. Серія «Державне управління».* 2021. № 1 (100). С. 46–52.

Стаття надійшла: 25.02.2021

Схвалено до друку: 01.03.2021

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). Stratehiia kiberbezpeky YeS (2021) na tsyfrove desiatylittia: perspektyvy dlia Ukrainy [The EU's Cybersecurity Strategy (2021) for the Digital Decade: perspectives for Ukraine]. *Bulletin of the NAPA. Series «Public Administration».* Is. 1 (100). P. 46–52 [in Ukrainian].

Article arrived: 25.02.2021

Accepted: 01.03.2021