## ПРОБЛЕМИ ТА СУДЖЕННЯ

УДК 342.9

***М. Василенко,***
доктор юридичних наук, доктор фізико-математичних наук, професор,
академік Академії наук вищої освіти України,
професор кафедри права міжнародного та європейського права
Національного університету «Одеська юридична академія»

# ПІДВИЩЕННЯ СТАНУ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ: ЯКІСТЬ У КОНТЕКСТІ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА

Інформатизація як явище сучасності призвела до переходу людства в інформаційне (цифрове) суспільство, в якому були створені інформаційно-комунікаційні технології (далі ІКТ) та інформаційно-комунікаційні системи (далі ІКС). Вони стали важливим ресурсом та рушійною силою культурного, соціально-економічного та технологічного розвитку сучасної цивілізації. У результаті технологічного розвитку галузі також було створено та вдосконалено ефективність систем захисту критичної інфраструктури від внутрішніх та зовнішніх загроз кібернетичного характеру, адже ризики кібербезпеки постійно зростають як у їх поширеності, так і руйнівному потенціалі. Сьогодні практично всі національні стратегії щодо забезпечення кібербезпеки пов'язані з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет). Використання комп'ютерних технологій, особливо в сукупності з телекомунікаційними мережами, породило особливий (вірусний) клас загроз інформаційній безпеці. Ситуація набуває ще більшого загострення разом із поширенням використання мережі Інтернет. Однак широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів. Це пояснюється значним коефіцієнтом «корисної» дії цих загроз, тому що обсяг ресурсів, що витрачаються на реалізацію загроз, є набагато меншим, ніж результати, що отримуються. При цьому прогресуючі ризики, пов'язані з кібербезпекою (див. [1]), стали наближатися до загроз, зв'язаних із природними катаклізмами (див. [2]), а новою небезпекою для кібербезпеки стало створення в багатьох країнах кібервійськ, які здатні суттєво впливати на інфраструктуру «противника». Крім того, кіберзлочини завдають значних фінансових збитків національним економікам (див. [3]). У цьому контексті захист інформації має передбачати досягнення та збереження властивостей безпеки в ресурсах користувачів, які спрямовані на запобігання відповідним кіберзагрозам, шляхом покращення якості характеристик (модернізації) ІКТ, ІКС та постійного вдосконалення інформаційного законодавства.

Метою статті є дослідження впливу якості кібербезпеки ІКС та її залежності від стану вдосконалення законодавства.

Сьогодні існує чимало праць із питань кібербезпеки (див. роботи та-

ких авторів, як Є. Бабич, О. Баранов, І. Валюшко, С. Гнатюк, М. Гуцалюк, І. Діордіца, Д. Дубов, В. Думанська, К. Ісмайлов, Ю. Нізовцев, Ю. Олійник, І. Сопілко, О. Шаховал, В. Шеломенцев, А. Шинкаренко). Однак, не дивлячись на чималу кількість робіт із кібербезпеки, праць, що досліджують зв'язок якості кібербезпеки ІКС та законодавства, практично не існує. Із позицій права важливим для визначення обсягу юрисдикції поняття «кібербезпека» і впливу на нього якості є знання об'єкта можливих загроз, а також видів і типів можливого збитку. Ці знання мають високу практичну цінність, оскільки саме від них залежить зміст стратегій кібербезпеки, охоплення об'єктів, які підпадають під заходи щодо забезпечення кібербезпеки, рівень і перелік інституцій та органів, склад і обсяги ресурсів, які повинні бути при цьому задіяні. Кібербезпека визначається як стратегічна проблема державного рівня [4, с. 27] і охоплює різноманітні контексти її проявів. Існуючі види діяльності, де задіяна кібербезпека (за охопленням), не дозволяють розглядати її як єдину науку з професійного сприйняття, а спрогнозувати потрібне поєднання з упевненістю знань і навичок в цій галузі в теперішній час практично неможливо. Скоріше можна говорити про соціотехнічні та техніко-юридичні сторони питання, які породжують нову проблему, зумовлену саме якістю і пов'язану як із законодавством, так і з якістю технічних послуг. Очевидно, що процеси управління нерозривно пов'язані з інформаційними процесами як у процесі підготовки управлінських рішень, так і безпосередньо у процесі управління. Сучасні системи управління, особливо великими територіально-розподіленими соціотехнічними системами (системи управління енергетичною інфраструктурою, повітряним і залізничним рухом, банківськими та фінансовими системами, великими промислово-виробничими комплексами тощо), неможливо уявити без використання комп'ютерних систем і телекомунікаційних мереж. Не викликає сумнівів, що якість законодавства представляє собою внутрішню сукупність соціальних та юридичних властивостей, притаманних його формі та змісту, що зумовлюють здатність законодавства задовольняти конкретні потреби суспільства. Технічна якість і її характеристики можуть трактувати по-різному, розглядаючи її як набір властивостей виробу (послуги), що характеризують його здатність задовольнити встановлені або передбачувані потреби замовника. У нашому випадку йдеться про необхідність досягнення високої якості кібербезпеки як необхідної умови розвитку інформаційного суспільства. Мова може йти про фундаментальні системні загрози, пов'язані з порушенням власне обігу інформації на будь-якому з його етапів – створення, поширення, використання, зберігання й знищенні інформації, так і про загрози, пов'язані з недостовірністю, несвоєчасністю і неповнотою інформації. Крім того, до таких загроз слушно віднести загрози, пов'язані з несанкціонованим використанням та поширенням інформації, порушенням її цілісності та конфіденційності. Проблема кібербезпеки має відношення до обігу інформації, зокрема до забезпечення суб'єктів інформаційних відносин достовірною, своєчасною та повною інформацією, а також до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності.

Проблеми закладені в самому інформаційному суспільстві через широке використання в останні роки комп'ютерних систем і телекомунікаційних мереж для створення та розповсюдження інформації, коли була істотно підвищена ефективність інформаційного впливу. Однак поряд із позитивом комп'ютерні системи та телекомунікаційні мережі також дозволили істотно підвищити ефективність негативного інформаційного впливу. Значна частина з них пов'язана з використанням інтернет-технологій. Тому протидія

негативному інформаційному впливу здійснюється на технологічному рівні, тобто протидія може бути віднесена до заходів із кібербезпеки. Логічним для цієї ситуації буде те, що з кібербезпекою пов'язана проблема нейтралізації негативних інформаційних впливів на технологічному рівні, а це, у свою чергу, пов'язане з проблемою підвищення якості кібербезпеки.

Відзначимо, що категорія «якість» представляє собою безпосередню визначеність предмету. завдяки якій він є саме цим, а не іншим предметом [5, с. 200]. Вважають, що внутрішня визначеність предмета становить ту специфіку, що відрізняє його від усіх інших; а саме ступінь вартості, цінності, придатності чого-небудь для його використання за призначенням [6, с. 1423]. Крім того, сьогодні загальновідомо, що якість будь-якої продукції (відповідних систем) представляє собою сукупність властивостей продукції, яка зумовлює її придатність задовольнити певні потреби відповідно до призначення, а показники безпеки характеризують особливості кіберсистеми, що забезпечують безпеку людини (персоналу) під час експлуатації або її споживання, монтажу, обслуговування, ремонту і т. д. Отже, якість у контексті вдосконалення інформаційного законодавства виражає специфіку, оригінальність та неповторність не тільки ІКТ, ІКС, а й кіберсистеми в цілому. Із зазначеного випливає, що порушення функціонування комп'ютерних систем і телекомунікаційних мереж може призвести до погіршення або навіть припинення роботи соціальних і соціотехнічних систем, елементами яких вони є, а комп'ютерні системи та телекомунікаційні мережі зобов'язані належним чином проектуватися, будуватися, здаватися в експлуатацію, експлуатуватися, супроводжуватися проектантами і виробниками тощо. Недоліки в нормативно-правовому та нормативно-технічному забезпеченні цих процесів, прорахунки в їх організації та реалізації, які можуть призвести до порушення функціонування комп'ютерних систем і телекомунікаційних мереж у процесі їх експлуатації, становлять суттєву загрозу кібербезпеці. Ефективність кібербезпеки проявляється в спроможності протидіяти різного роду кібератакам. Не викликає сумнівів той факт, що сигнал, входячи в систему, може змінювати її характеристики як усередині системи, так і на її виході, він може вносити в саму ІКС вірус і виносити з неї несанкціоновану, але відому йому інформацію. Процес кібератаки на відбувається тоді, коли хакер, створивши комп'ютерний «вірус», направляє його в ІКС, де він реалізується у вигляді відповідного електричного або іншого сигналу як усередині системи, так і на її виході. У зв'язку із цим можна говорити про спосіб запобігання (профілактики) кібератак, розміщуючи на вході і на виході системи відповідні фільтри. Хто зможе це реалізувати більш технічно грамотно, той має перемогу в протистоянні ідей і технологій, стимулюючи їх упровадження у практику. Схематично, за уявленнями автора, це може виглядати так (рис. 1).

Як бачимо з ілюстрації, ідея реалізації способу проявляється у пропозиції поставити два (або більше) фільтри в ІКС: один ставиться на вході, другий – на виході. При цьому в обох фільтрах може бути кілька рівнів захисту, наприклад, як у нашому випадку, існує чотири рівні захисту. У разі кібератаки на таку технічно модернізовану ІКС комп'ютерний вірус затримується або знищується фільтром у самій ІКС. Якщо він все ж таки маскується і потрапляє всередину ІКС, модернізована всередині система має його розпізнати і відправити в карантин. У крайньому випадку фільтри на виході мають не дозволити вірусу винести несанкціоновану інформацію з ІКС, захищаючи її в цілому. При цьому кібербезпека ні в якому разі не залишається річчю в собі, замкненою тільки на комп'ютерних системах та телекомунікаційних мережах. Із системних позицій заходи щодо забезпечення кібербезпеки на-

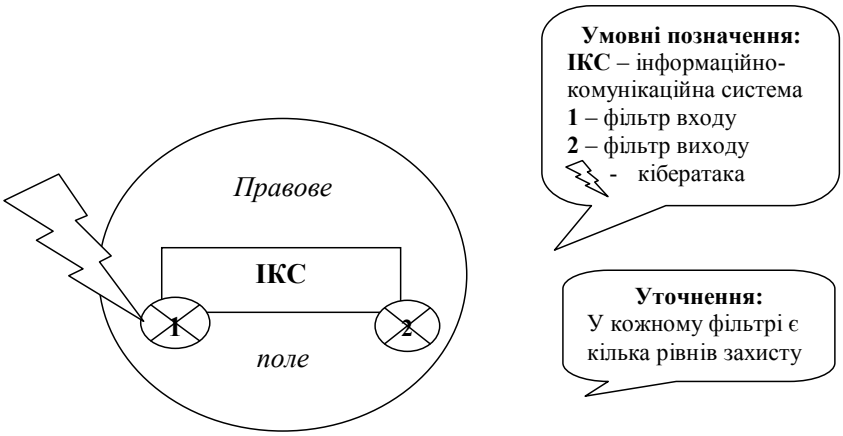


**Рис. 1. Кібератака на технічно модернізовану ІКС**

самперед спрямовані на збереження якості функціонування соціальних і соціотехнічних систем, до складу яких входять відповідні комп'ютерні системи та телекомунікаційні мережі. Таким чином, законодавство має сприяти підвищенню якості конкретних ІКС, що використовуються. У той же час серед інформаційно-комп'ютерних технологій можливо виділити певну їх частину під умовною назвою «емерджентні технології», які проявляються в багатьох галузях науки і техніки. Під «емерджентною технологією» в контексті розгляду питань правового регулювання якості відповідних суспільних відносин пропонується розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя в різноманітних сферах, які неможливо передбачити наперед. Досить значна кількість технологій, що застосовуються в інформаційній сфері, зумовлює виникнення і розвиток таких «емерджентних технологій» та їх стрибкоподібний і глобальний вплив. Для емерджентних технологій, що застосовуються в інформаційній сфері і діють у кіберпросторі, характерні тісний взаємозв'язок та взаємний вплив. При цьому загрози, що існують у кіберпросторі за весь час його існування, модифікуються та інтенсифікуються за умови використання емерджентних технологій, такі технології мають потенціал їх збільшення.

Зазначимо, що в питанні правового регулювання як реалізації функцій держави, зокрема щодо забезпечення кібербезпеки та її якості, слід виходити насамперед із загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії, зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій. Основна проблема полягає в неочевидності деструктивності та можливих помилок в оцінці суті технологій, тому пошук можливих шляхів вирішення зазначеної низки проблем є перспективним для подальших досліджень у галузі правової науки. Окрім цього, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає в забезпеченні економічної багатоманітності. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. Водночас надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати з реально існуючої необхідності.

Автор (*М.В.*) вважає, що якість інформаційного законодавства суттєво

залежить від законодавчої техніки. На жаль, протягом майже чверті століття на це мало звертали увагу, а чинне інформаційне законодавство практично не регулювало питання вдосконалення якості кібербезпеки, створивши прецеденти до виникнення в різних галузях діяльності суттєвих небезпечних ситуацій, пов'язаних із кіберзагрозами. Вважають, що для подолання таких загроз удосконалення інформаційного законодавства може вестись на двох принципово різних рівнях: або шляхом переважання підзаконних нормативних актів над законами в конкретній сфері правового регулювання громадських відносин, що є важливим, але водночас негативним щодо реалізації регулятивного потенціалу права проявом, або у процесі законодавчої нормотворчості з адаптації національного законодавства до вимог ЄС [7, с. 72]. Однак із позицій права це ті заходи, що реально можна реалізувати, але їх не можна вважати достатніми, хоча деякі заходи в даному напрямі відбулися. Так, Указом Президента України від 15 березня 2016 року № 96/2016 затверджена Стратегія кібербезпеки України [8], яка стала підґрунтям для розбудови національної системи кібербезпеки, а Указом Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [9] було затверджено Доктрину інформаційної безпеки, яка визначає напрями і пріоритети державної політики в інформаційній сфері. Наприклад, до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (05.10.2017 р.) (чинний від 09.05.2018 р.) [10] в інформаційному законодавстві було відсутнє визначення не тільки поняття «кібернетична безпека (кібербезпека)», а й таких понять, як «кібернетичний простір (кіберпростір)», «кібернетична загроза (кіберзагроза)», «кібернетична атака (кібератака)», «кібернетичний захист (кіберзахист)», «кіберзлочинність» тощо. Зазначений Закон створює засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами державного і приватного секторів та громадянського суспільства. Ним визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки. Отже, згідно із задекларованими у преамбулі положеннями законом фактично встановлюються можливість та засади регулювання за допомогою норм вітчизняного права в кіберпросторі з метою забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, а також національних інтересів України. Так, аналіз приписів, що містяться в пунктах 1 та 4 частини 1 статті 2 Закону, дозволяє зробити висновок про їх тотожність у багатьох аспектах. Узагальнюючи зазначене, можливо зробити висновок, що дія Закону не розповсюджуватиметься на внутрішні (локальні) комп'ютерні мережі, що не взаємодіють, не підключені до глобальних комп'ютерних мереж. Обмеження щодо інформації, яка становить державну таємницю, діятимуть відповідно до приписів актів спеціального законодавства в цій сфері. Водночас відносини, що складаються під час використання соціальних мереж, а також «приватних» інформаційних електронних ресурсів (однак, судячи з усього, мова йде про недержавні ресурси), не регламентуються Законом «Про основні засади забезпечення кібербезпеки в Україні» за певних умов: відсутності інформації, необхідність захисту якої встановлено законом. Проте, не дивлячись на значне покращення рівня інформаційного законодавства,

простежується значне «відставання» від світової практики законодавчого регулювання кібербезбезпеки, зокрема від ЄС, до законодавства якого Україна адаптує свою законодавству базу у відомих галузях господарства. Зауважимо, що (на кінець весни 2018 р.) на офіційному сайті європейського права (http://eur-lex.europa.eu/) із цього питання було розміщено більш ніж чотири сотні юридичних документів, із яких більше тридцяти було видано вже в 2018 році. Відставання України в цьому зрозуміле: воно пов'язане із часовим відставанням, відомими подіями та недержавним мисленням осіб, які за це відповідали. В ЄС ще у 2004 році (розуміння важливості проблеми кібербезпеки певно було) створено Європейське агентство з мережевої та інформаційної безпеки (ENISA). У подальшому це Агентство (2012 р.) оприлюднило огляд «Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання» [11], в якому було визначено термін «кібербезпека» і констатовано факт, що в національних стратегіях країн-членів не існує загальноприйнятого та однозначного визначення кібербезпеки. Однак у цьому огляді мова про якість ніяким чином не йшлася. Відомий правовий «цифровий розрив» між Україною та ЄС продовжує збільшуватися як кількісно, так, у першу чергу, і якісно. При цьому в Україні відбувається ще більша за ЄС фрагментарність у формуванні правової основи національної кібербезпеки: більша частина нормативно-правових актів регулювання у сфері безпеки та інформаційних технологій навіть і не згадують цю проблему щодо кібербезпеки, не кажучи вже про її якість (див. нещодавно схвалену урядова Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки [12]).

Отже, в Україні почалося формування національної політики кібербезпеки, яка включає сукупність національних та міжнародних актів, насамперед: Конвенцію про кіберзлочинність, ратифіковану Законом України від 07.09.2005 р. № 2824-1V; Стратегію кібербезпеки України; Закон України «Про основні засади забезпечення кібербезпеки України»; Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»; Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.2016 р. № 563 тощо. Однак сформована національна політика кібербезпеки має певні суттєві розбіжності за спрямуванням та змістом з європейською політикою, в тому числі з оновленою в 2013 р. версією Стратегії кібербезпеки ЄС [13].

Таким чином, підвищення якості кібербезпеки повинне носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки – постійно вдосконалюватися. Ефективність заходів у цій сфері повинна досягатися завдяки здійсненню оперативної оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики в кіберпросторі, а також їх завчасно ліквідовувати, і хоча ІКС існує в межах правового поля (інформаційного законодавства), проте першоосновою протидії кібератакам є технічна сторона питання. Рівні технічного захисту (фільтри) законодавчо не завжди встановлюються шляхом введення спеціальних (національних та міжнародних) стандартів, проте в цілому простежується взаємодія ІКС та інформаційного законодавства.

**Ключові слова:** кібербезпека, інформаційно-комунікаційні системи, якість, фільтри, ступені захисту, інформаційне законодавство.

*Стаття досліджує вплив якості кібербезпеки на інформаційно-комунікаційні системи та її залежність*

*від стану вдосконалення інформаційного законодавства. Доведено, що якість інформаційно-комунікаційних технологій технічно мало залежить від чинного законодавства. У цьому сенсі підвищення стану кібербезпеки інформаційно-комунікаційних систем можливе за умови наявності відповідних фільтрів із різними ступенями захисту. Рівні технічного захисту (фільтри) законодавчо не завжди встановлюються шляхом введення спеціальних (національних та міжнародних) стандартів, проте в цілому простежується прогресуюча взаємодія ІКС та інформаційного законодавства.*

*Статья исследует влияние качества кибербезопасности на информационно-коммуникационные системы и ее зависимость от состояния совершенствования информационного законодательства. Доказано, что качество информационно-коммуникационных технологий технически мало зависит от действующего законодательства. В этом смысле повышение состояния кибербезопасности информационно-коммуникационных систем возможно при наличии соответствующих фильтров с различными степенями защиты. Уровни технической защиты (фильтры) законодательно не всегда устанавливаются путем введения специальных (национальных и международных) стандартов, однако в целом прослеживается прогрессирующее взаимодействие ИКС и информационного законодательства.*

*The article investigates the impact of the quality of cyber security on information and communication systems and its dependence on the state of improving information legislation. It has been proven that the quality of information and communication technologies is technically little dependent on current legislation. In this sense, enhancing the cybersecurity status of information and communication systems is possible with the presence of appropriate filters with different degrees of protection. However, the levels of technical protection (filters) are not always legally established by the introduction of special (national and international) standards, whereas, in general, there is a progressive interaction of ICS and information legislation.*

***Література***

*1. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн. URL : https://www.radiosvoboda.org/a/news/29049044.html.*

*2. Global Risks Report 2018, 13th Edition, is published by the World Economic Forum. URL : http: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.*

*3. Збитки світової економіки від хакерів досягли $ 600 млрд. URL : https://ua.korrespondent.net/world/3943548-zbytky-svitovoi-ekonomiky-vid-khakeriv- dosiahly-600-mlrd.*

*4. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк». 2017. 107 с.*

*5. Ивакин А.А. Диалектическая философия : монография. Издание 2-е, перераб. и доп. Одесса: Фенікс ; Суми : Університетська книга; Москва : ТрансЛит, 2007. 440 с.*

*6. Великий тлумачний словник сучасної української мови / за ред. В.Т. Бусел. Київ ; Ірпінь : Перун, 2003. 1440 с.*

*7. Єсімов С. Окремі аспекти підвищення ефективності правового регулювання використання інформаційних технологій у публічному управлінні. Visegrad journal on human rights. 2017. № 1. С. 71–76. URL : http://vjhr.sk/archive/2017_1/part_2/13.pdf.*

*8. Указ Президента України про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р. URL : http://zakon.rada.gov.ua/laws/show/96/2016.*

*9. Указ Президента України про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» від 29 грудня 2016 р. URL : http://zakon.rada.gov.ua/laws/show/47/2017.*

*10. Закон України «Про основні засади забезпечення кібербезпеки України» від*

*05 жовтня 2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.*

*11. National Cyber Security Strategies. Practical Guide on Development and Execution. ENISA, 2012. URL : https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport.*

*12. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації. URL : https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-tasuspilstva-ukrayini-na-2018-2020-roki-ta-zatverdzhennyaplanu-zahodiv-shodo-yiyi-realizaciyi.*

*13. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL : https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.*