

Державне управління

УДК 351.865

Живи́ло Ірина Олександрівна

кандидат медичних наук, молодший науковий співробітник

Державна установа «Національний науковий центр

“Інститут кардіології імені академіка М.Д. Стражеска”

Національної академії медичних наук України»

Живи́ло Ирина Александровна

кандидат медицинских наук, младший научный сотрудник

Государственное учреждение «Национальный научный центр

“Институт кардиологии имени академика М.Д. Стразеско”

Национальной академии медицинских наук Украины»

Zhyvylo Iryna

Candidate of Medical Sciences, Junior Researcher

State Institute «National Scientific Center

“Institute of cardiology named after academician M.D. Strazhesko” of the

National Academy of Medical Sciences of Ukraine»

**ПРОБЛЕМАТИКА МЕХАНІЗМІВ ВПРОВАДЖЕННЯ ТА
КООРДИНАЦІЇ ПРОЦЕСІВ ПЛАНУВАННЯ ТА ВИКОНАННЯ
ПРОЕКТІВ ІНФОРМАТИЗАЦІЇ В СИСТЕМІ
ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ
ПРОБЛЕМАТИКА МЕХАНИЗМОВ ВНЕДРЕНИЯ И КООРДИНАЦИИ
ПРОЦЕССОВ ПЛАНИРОВАНИЯ И ВЫПОЛНЕНИЯ ПРОЕКТОВ
ИНФОРМАТИЗАЦИИ В СИСТЕМЕ ОРГАНОВ ГОСУДАРСТВЕННОЙ
ВЛАСТИ**

PROBLEM OF MECHANISMS FOR THE IMPLEMENTATION AND COORDINATION OF PROCESSES OF PLANNING AND PERFORMANCE OF INFORMATION PROJECTS IN THE SYSTEM OF STATE AUTHORITIES

***Анотація.** В статті автором було здійснено аналіз проведення єдиної державної політики з питань державного регулювання у сфері телекомунікацій, інформатизації та розвитку інформаційного суспільства, проаналізовано задекларований стан захищеності існуючих на ринку операторів, провайдерів телекомунікацій, які сьогодні надають ті чи інші послуги зв'язку для органів державної влади, побудували на вимогу Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗІ) комплексну систему захисту інформації (далі - КСЗІ) і мають атестат відповідності системи захисту захищених вузлів доступу.*

Акцентовано увагу на розбудові в Україні ефективної системи електронного урядування, впровадженню та модернізації систем електронного документообігу, створенню або модернізації офіційних веб-сайтів, впровадженню процесів автоматизації ведення загальнодержавних реєстрів, забезпеченню взаємодії між державними електронними ресурсами та інтегрованою системою електронної ідентифікації, подальшому впровадженню, розвитку та захисту інформаційно-телекомунікаційних систем.

Одними з основних проблемних питань під час реалізації окремих завдань (проектів) інформатизації органів державної влади є:

- реалізація правових та організаційних основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основних цілей,*

напрямів та принципів державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основних засад координації їхньої діяльності із забезпечення кібербезпеки;

- вплив будь-яким чином на всі інциденти та події які відбуваються в мережі Інтернет, згідно з умовами договору лише своєчасне інформування всіх бажаних, в тому числі і органи державної влади та CERT про всі інциденти, які відбуваються в тому чи іншому сегменті мережі Інтернет;*
- адекватне реагування на події в інформаційно-телекомунікаційних системах і мережах, захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, кібербезпеки та кібероборони об'єктів критичної інфраструктури держави.*

Ключові слова: кібернетичний простір, кібернетичні загрози, кібероборона держави, органи державної влади, провайдер, оператор.

Аннотація. В статье автором был осуществлен анализ проведения единой государственной политики по вопросам государственного регулирования в сфере телекоммуникаций, информатизации и развития информационного общества, проанализировано задекларированное “состояние защищенности” существующих на рынке операторов, провайдеров телекоммуникаций, которые сегодня предоставляют те или иные услуги связи для органов государственной власти, построили по требованию государственной службы специальной связи и защиты информации Украины комплексную систему защиты информации и имеют аттестат соответствия системы защиты защищенных узлов доступа..

Акцентируется внимание на развитии в Украине эффективной системы электронного управления, внедрению и модернизации систем электронного документооборота, созданию или модернизации официальных сайтов, внедрению процессов автоматизации ведения общегосударственных реестров, обеспечению взаимодействия между государственными электронными ресурсами и интегрированной системой электронной идентификации, дальнейшему внедрению, развитию и защите информационно телекоммуникационных систем.

Одними из основных проблемных вопросов при реализации отдельных заданий (проектов) информатизации органов государственной власти являются:

- реализация правовых и организационных основ обеспечения защиты жизненно важных интересов человека и гражданина, общества и государства, национальных интересов Украины в киберпространстве, основных целей, направлений и принципов государственной политики в сфере кибербезопасности, полномочия государственных органов, предприятий, учреждений, организаций, лиц и граждан в этой сфере, основных принципов координации их деятельности по обеспечению кибербезопасности;*
- влияние любым образом на все инциденты и события происходящие в сети Интернет, в соответствии с условиями договора только своевременное информирование всех желающих, в том числе и органы государственной власти и CERT обо всех инцидентах, которые происходят в том или ином сегменте сети Интернет;*
- адекватное реагирование на события в информационно-телекоммуникационных системах и сетях, защищенность жизненно важных интересов человека и гражданина, общества и государства при*

использовании киберпространства, кибербезопасности и киберобороны объектов критической инфраструктуры государства.

Ключевые слова: кибернетическое пространство, кибернетические угрозы, кибероборона государства, органы государственной власти, провайдер, оператор.

Summary. In the article, the author analyzed the implementation of a unified state policy on state regulation in the field of telecommunications, informatization and the development of the information society, analyzed the declared state of security of the existing market operators, telecommunication providers, which today provide certain communications services to public authorities, built at the request of the state service of special communication and information protection of Ukraine comprehensively information security system and have a certificate of conformity of the security system of secure access nodes.

Attention is focused on the development in Ukraine of an effective electronic management system, the introduction and modernization of electronic document management systems, the creation or modernization of official sites, the introduction of automation processes for maintaining national registries, ensuring the interaction between state electronic resources and an integrated electronic identification system, the further implementation, development and protection of information telecommunication systems.

One of the main problematic issues in the implementation of individual tasks (projects) of informatization of public authorities are:

- implementation of the legal and organizational framework for ensuring the protection of the vital interests of man and citizen, society and the state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, the authority of state

bodies, enterprises, institutions, organizations, individuals and citizens in this area, the basic principles of coordination of their activities to ensure cybersecurity;

- the impact in any way on all incidents and events occurring on the Internet, in accordance with the terms of the contract, only timely informing everyone, including government and CERT about all incidents that occur in a particular segment of the Internet;
- adequate response to events in information and telecommunication systems and networks, the protection of the vital interests of man and citizen, society and the state when using cyberspace, cybersecurity and cyber defense of critical infrastructure of the state.

Key words: cyber space, cyber threats, cyber defense of the state, public authorities, provider, operator.

Постановка проблеми. Сьогодні органи державної влади мають право отримувати доступ в Інтернет тільки в операторів / провайдерів, які мають захищений вузол Інтернет-доступу. В свою чергу кожен оператор / провайдер, який побудував захищений вузол Інтернет-доступу і пройшов відповідну перевірку і сертифікацію в ДССЗІ України, має право надавати доступ до мережі Інтернет органам державної влади. Також через виникненні протиріччя в нормативно-правовому полі з 2006 року у деяких операторів, провайдерів зв'язку з'явилась можливість надавати послуги з доступу до Інтернету на комерційній основі.

Органи державної влади для виконання покладених на них завдань і на підставі статі 19 Конституції України, Законів і нормативно-правових актів, виконують свої функції та завдання і на свій розсуд роблять захист своїх телекомунікаційних мереж, тому можуть отримувати доступ до Інтернету як

через захищений вузол Інтернет-доступу так і на комерційній основі, і для свого захисту майже всі вони мають власні ІТ-підрозділи.

Тому розроблення, оновлення та внесення змін у існуючу нормативно-правову базу, враховуючи актуальність ситуації, передбачається першочерговою стадією розвитку електронних послуг.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення захисту інформації та кібернетичної безпеки України, нормативно-правові відносини в цій галузі, актуальні напрями підвищення ефективності системи забезпечення кібернетичної безпеки державних електронних інформаційних ресурсів, її функції та завдання розглядаються у наукових працях вітчизняних дослідників, а саме: Є. Ю. Бабіч [1], Д. В. Дубов [2], Н. Є. Новікова, І. В. Діордіци, С. В. Мельника, В. І. Кашука та інших.

Проте, незважаючи на значну кількість робіт із даної тематики, існує багато невирішених питань щодо шляхів врегулювання нормативно-правової бази із захисту інформації, кібербезпеки та кібероборони України [2, с.12].

Формулювання цілей статті (постановка завдання). Мета статті полягає у визначенні цілей і завдань державної інформаційної політики у сфері цифровізації органів державної влади, цифрового розвитку суспільства, цифрової економіки держави, впровадження цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства за умов захисту державних інформаційних ресурсів та інформації.

Виконання цих заходів надасть можливість забезпечити впровадження в органах державної влади заходів із захисту інформації та кібербезпеки відповідно до існуючої сучасної міжнародної нормативно-правової бази (стандартів ISO/IEC).

Виклад основного матеріалу. Роками державні послуги асоціювалися в українців з довгими чергами, приниженнями й незрозумілістю. Відвідувачі не мали змоги вплинути на процес, а посадовці - механізмів його поліпшити. Це не сприяло ані впорядковуванню державних процесів, ані довірі людей до держави. Заручниками цієї системи були всі: і громадяни, і службовці.

12 червня 2019 року в Адміністрації президента Володимира Олександровича Зеленського відбулося перше експертне обговорення концепції “Держава в смартфоні” [3]. У ньому взяли участь представники “Коаліції електронної держави”, що об’єднує 65 різних організацій і експертів в області ІТ.

За словами Віце прем’єр-міністра – міністра цифрової трансформації Михайла Федорова, переведення державних послуг в онлайн посприє не тільки комфорту громадян, а й зменшенню корупції. До 2024 року планується перевести 90% всіх державних послуг в режим онлайн, втричі зменшивши кількість взаємодії громадян і бізнесу з владою і досягнувши нульового рівня корупції в цій сфері.

Перший крок переведення державних послуг в онлайн, це створення diia.gov.ua, онлайн-сервісу державних послуг. Одним з перших елементів нового онлайн-сервісу державних послуг запроваджено електронний кабінет громадянина. Авторизувавшись у ньому (за допомогою електронного підпису, BankID або MobileID), кожен українець зможе знайти всі дані про себе - від персональних документів до власного майна, отримати потрібну послугу, а в майбутньому проголосувати.

Слід відмітити, що представники “Коаліції” надали президенту свої рекомендації і обговорили пріоритетні проекти цифровізації до яких відносяться: e-Health, Міністерство цифрової трансформації, Комітет з питань цифрової трансформації, Запуск сервісу Дія, Електронний кабінет, Mobile

app, «Малюнок, Паспорт разом з ідентифікаційним номером, Прописка дитини онлайн, е-Пенсія, SmartID, MobileID, Цифрові посвідчення громадянина, Держава без довідок, е-Резидентство, Трембіта, Кабінет забудовника, Банківський рахунок для бізнесу онлайн, е-Вибори, е-Перепис, ID-картка з електронним підписом, Автоматизація роботи Центрів надання адміністративних послуг, Брендінг сервісу Дія та інші.

Ключові пропозиції стосувалися розвитку інструментів електронної держави і демократії, цифрових інфраструктур, цифровий ідентифікації, кібербезпеки, наведення порядку в державних реєстрах, електронного народовладдя (електронних соціологічних опитувань і навіть виборів). Також йшлося про важливість створення можливостей для українських технологічних стартапів.

Зараз формування взаємодії влади та громадськості є умовою якісної зміни публічного управління, що передбачає об'єднання певних зусиль представників органів державного управління та громадянського суспільства як безпосередніх суб'єктів управління. Тому, слід визначити, що якісна та ефективна взаємодія органів державної влади з громадянським суспільством передбачає конструктивне інституційне та організаційне забезпечення взаємодії із чітко визначеними структурними та функціональними складовими цього процесу.

На сьогодні дуже важливим кроком виступає зворотній зв'язок у правовому полі між громадянським суспільством і державою. Правова держава повинна реагувати на запити і потреби асоційованого громадянства, при цьому визнаючи автономність громадянського суспільства, також видавати законодавчі акти та відстежувати їх виконання. Держава створює правове поле щодо захищеності громадян та їх інтересів, а також в правовому полі формує ефективну роботу щодо діяльності громадських

інституцій.

Досліджуючи питання зворотнього зв'язку між громадянами і органами державної влади слід відмітити, що терміни можливого впровадження інновацій будуть зірвані або зупинені взагалі. Даний аспект впливає з того, що на виконання пункту 1.5).б) рішення Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32 [4], введеного в дію Указом Президента України від 30 серпня 2017 року № 254/2017 є неможливим врегулювати питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікації, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації.

Виходячи з цього виникає вимога щодо підключення інформаційно-телекомунікаційних систем (далі – ІТС) органів, підприємств, установ і організацій державної форми власності до мережі Інтернет з використанням захищених вузлів доступу (далі - ЗВІД).

Порядок створення системи захисту інформації визначено нормативним документом у сфері технічного та криптографічного захисту інформації НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі". Відповідно до зазначеного НД вимоги до системи захисту інформації фіксуються у Технічному завданні.

Підтвердження відповідності системи захисту інформації встановленим до неї вимогам здійснюється в рамках проведення державної експертизи в

сфері технічного захисту інформації, порядок проведення якої визначається “Положенням про державну експертизу в сфері технічного захисту інформації”, затвердженим наказом Адміністрації Держспецзв’язку від 16.05.2007 № 93 зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087 [5].

На підставі позитивного рішення щодо результатів оцінки системи захисту ЗВІД видається зареєстрований у Держспецзв’язку Атестат відповідності. Невід’ємною частиною Атеста є Експертний висновок, який додається до нього. Атестат відповідності засвідчує, що система захисту інформації об’єкта експертизи (ЗВІД) побудована відповідно до НД ТЗІ 3.7-003-05 та відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у технічному завданні на ЗВІД.

При прийнятті рішення щодо використання послуг певного провайдера телекомунікацій власник (розпорядник) ІТС (окрім багатьох інших факторів) має співставити вимоги технічного завдання на власну ІТС із технічним завданням на КСЗІ ЗВІД та проектними рішеннями, які реалізовані в ЗВІД.

З іншої сторони, впровадження обов’язкових вимог стосовно здійснення державними органами, підприємствами, установами та організаціями державної форми власності ідентифікації та автентифікації джерел отриманих оновлень до програмного забезпечення, яке використовується для обробки державних інформаційних ресурсів та інформації, вимога про захист якої встановлена законом, та встановлення цілісності таких оновлень, а також вимог щодо поступового застосування посадовими (службовими) особами зазначених суб’єктів електронного цифрового підпису під час надсилання засобами електронної пошти інформації, пов’язаної з виконанням посадових (службових) обов’язків є

вкрай важливою, не виконання якої призведе до порушення кіберзахисту державних електронних інформаційних ресурсів.

Ряд ресурсів, серед яких веб-ресурси Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, розвідувальних органів, які беруть безпосередню участь в організації та реалізації заходів протидії кіберзагрозам та Державного управління справами, Генеральної прокуратури України, Міністерства закордонних справ України і ще кількох десятків держустанов, не захищені від мережових атак, при яких зловмисники можуть перехоплювати пакети даних в мережі, змінювати трафік або повністю його зупинити (ARP-spoofing). В цілому, перелік операторів / провайдерів телекомунікацій, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності систем захисту ЗВІД складає 39 організацій. Особливої пікантності ситуації додає той факт, що всі ці держустанови підключені до провайдерів, яких Державна служба спеціального зв'язку та захисту інформації України вважає захищеним.

Нижче приведена таблиця операторів [6], провайдерів телекомунікацій, які побудували на вимогу Державної служби спеціального зв'язку та захисту інформації КСЗІ і мають Атестат відповідності системи захисту захищених вузлів доступу (Табл.1). На даний момент в Україні це є обов'язковою умовою для провайдера, який надає послуги доступу до мережі Інтернет державним органам і установам і коштує від 300 тисяч гривень, однак, КСЗІ даних провайдерів зв'язку - це "ілюзія захищеності".

Таблиця 1

**Перелік операторів (провайдерів) телекомунікацій, що надають послуги
з доступу до мережі Інтернет та мають чинні атестати відповідності
систем захист ЗВІД**

№ з/п	Назва провайдера та № ліцензії	Кількість вразливих мережевих приладів
1	ТОВ «Адамант» (атестат відповідності від 23.06.2015 №12606, дійсний до 23.06.2020)	34
2	«Інфоком» у формі ТОВ (атестат відповідності від 22.07.2015 №12713, дійсний до 22.07.2020)	35
3	ПАТ «Укртелком» (атестат відповідності від 22.03.2016 №13630, дійсний до 22.03.2021)	1092
4	ПрАТ «ДАТАГРУП» (атестат відповідності від 13.09.2017 №15595, дійсний до 13.09.2022)	573
5	ТОВ «ОРІОН СІТІ» (атестат відповідності від 06.02.2018 №16229, дійсний до 06.02.2021)	4
6	ТОВ «Нові українські мережі» (атестат відповідності від 22.02.2018 №16302, дійсний до 22.02.2023)	-
7	ТОВ «АКСОН 45» (атестат відповідності від 06.03.2018 №16371, дійсний до 06.03.2023)	208
8	ПрАТ «Фарлеп-Інвест» (атестат відповідності від 17.04.2018 №16579, дійсний до 17.04.2023)	43
9	ТОВ НВП «ТЕНЕТ» (атестат відповідності від 08.05.2018 №16681, дійсний до 08.05.2023)	281
10	ТОВ «УКРКОМ» (атестат відповідності від 01.06.2018 №16785, дійсний до 01.06.2023)	33
11	ТОВ «Гігатранс Україна» (атестат відповідності від 18.06.2018 №16884, дійсний до 18.06.2023)	10
12	ТОВ «Універсальна мережева компанія» (атестат відповідності від 10.07.2018 №17077, дійсний до 10.07.2023)	-
13	ТОВ «КОСМОНОВА» (атестат відповідності від 24.07.2018 №17136, дійсний до 24.07.2023)	256
14	ТОВ «НВП Трайфл» (атестат відповідності від 07.09.2018 №17413, дійсний до 07.09.2023)	89
15	ТОВ «ІСП ШТОРМ» (атестат відповідності від 07.09.2018 №17421, дійсний до 07.09.2023)	38
16	ТОВ «Київські оптичні мережі» (атестат відповідності від 17.10.2018 №17781, дійсний до 17.10.2023)	48
17	«Українська академічна і дослідницька мережа» Інститут фізики конденсованих систем НАН України (атестат відповідності від 04.12.2018 №18105, дійсний до 04.12.2023)	273

№ з/п	Назва провайдера та № ліцензії	Кількість вразливих мережевих приладів
18	«Український державний центр радіочастот» (атестат відповідності від 18.12.2018 №18210, дійсний до 18.12.2023)	-
19	ТОВ «ВЕБ ПРО» (атестат відповідності від 18.12.2018 №18211, дійсний до 18.12.2023)	1
20	ТОВ «ФРІНЕТ» (атестат відповідності від 22.12.2018 №18240, дійсний до 22.12.2023)	597
21	ТОВ «Скайлан Телеком» (атестат відповідності від 15.02.2018 №18631, дійсний до 15.02.2023)	10

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Досліджуючи особливості взаємодії місцевих органів виконавчої влади з громадськістю, визначаючи цілі і завдання державної інформаційної політики у сфері цифровізації органів державної влади, формуючи етапність цифрового розвитку суспільства, цифрової економіки держави, порядку впровадження цифрових інновацій, впровадження електронного урядування та електронної демократії, враховуючи розвиток інформаційного суспільства за умов захисту державних інформаційних ресурсів та інформації першочерговими кроками необхідно:

- в нормативно-правовому полі врегулювати питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації;
- опрацювати питання щодо визначення Державної служби спеціального зв'язку та захисту інформації України органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів, а також щодо встановлення порядку

передачі, збереження і доступу до цих копій;

- організувати першочергове підключення до національної телекомунікаційної мережі державних органів згідно з переліком, підготовленим Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, та забезпечити виконання цими органами основних вимог до розміщення телекомунікаційних вузлів вказаної мережі, передбачивши поетапне підключення до національної телекомунікаційної мережі всіх державних органів, підприємств, установ та організацій державної форми власності;
- забезпечити в установленому порядку фінансування видатків на модернізацію ситуаційних центрів з кібербезпеки Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України;
- запровадити в установленому порядку в рамках розвитку державно-приватного партнерства механізм залучення фізичних і юридичних осіб на умовах аутсорсингу до виконання завдань кіберзахисту державних електронних інформаційних ресурсів;
- запровадити механізм додаткового стимулювання мотивації до праці фахівців Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, розвідувальних органів, які беруть безпосередню участь в організації та реалізації заходів протидії кіберзагрозам.

В подальшому виконання цих заходів надасть можливість забезпечити впровадження в органах державної влади заходів із захисту інформації та кібербезпеки відповідно до існуючої сучасної міжнародної нормативно-правової бази (стандартів ISO/IEC), під час оцифрування існуючих баз даних

державних інформаційних ресурсів й налаштування обміну даними різних реєстрів за визначеними напрямками у відповідності до порядку обробки персональних даних (здійснюється повністю або частково із застосуванням автоматизованих засобів, а також обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів).

Насамперед це не просто й потребує докорінних змін: потрібно налагодити взаємодію між міністерствами, змінити алгоритми надання послуг, сформулювати й описати всі процеси доступною мовою, спроектувати й протестувати нові інформаційні та мережеві активи і навіть змінити деякі закони.

Література

1. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листопада 2016 р. Кропивницький : КНТУ, 2016. С. 77–78.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. К: НІСД, 2014. С. 328.
3. “Государство в смартфоне”: у Зеленского хотят к 2024 году перевести 90% госуслуг в онлайн 13.06.2019. URL: <https://capital.ua/ru/news/128796-gosudarstvo-v-smartfone-u-zelenskogo-khotyat-k-2024-godu-perevesti-90-gosuslug-v-onlayn>).
4. Указ Президента України №32/2017 від 13 лютого 2017 року, Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”. URL: <https://president.gov.ua/documents/322017-21282>.

5. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України № 93 від 16 травня 2007 року, "Положенням про державну експертизу в сфері технічного захисту інформації". URL: [https:// zakon.rada.gov.ua/laws/show/z0820-07](https://zakon.rada.gov.ua/laws/show/z0820-07)
6. Інформаційні матеріали щодо захищених вузлів доступу до мережі Інтернет. URL: https://dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=283080&cat_id=44795.

References

1. Babych Je. Ju. Zabezpechennja kiberbezpeky v Ukraini / Je. Ju. Babych // Aktualjni zadachi ta dosjaghnennja u ghaluzi kiberbezpeky : materialy Vseukr. nauk.-prakt. konf., m. Kropyvnyckyj, 23–25 lystop. 2016 r. Kropyvnyckyj : KNTU, 2016. S. 77–78.
2. Dubov D. V. Kiberprostir jak novyj vymir gheopolitychnogho supernyctva : monohrafija / D. V. Dubov. K: NISD, 2014. S. 328.
3. "Gosudarstvo v smartfone": u Zelenskogo khotyat k 2024 godu perevesti 90% gosuslug v onlayn 13.06.2019. URL: <https://capital.ua/ru/news/128796-gosudarstvo-v-smartfone-u-zelenskogo-khotyat-k-2024-godu-perevesti-90-gosuslug-v-onlayn>).
4. Ukaz Prezydenta Ukrainy #32/2017 vid 13ljutogho 2017 roku, Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrainy vid 29 ghrudnja 2016 roku "Pro zaghrozy kiberbezpeci derzhavy ta nevidkladni zakhody z jikh nejtralizaciji". URL: [https:// president.gov.ua/documents/322017-21282](https://president.gov.ua/documents/322017-21282)
5. Nakaz Administraciji derzhavnoji sluzhby specialjnogho zv'jazku ta zakhystu informaciji Ukrainy # 93 vid 16 travnja 2007 roku, "Polozhennjam pro

derzhavnu ekspertyzu v sferi tekhnichnogho zakhystu informaciji". URL:
[https:// zakon.rada.gov.ua/laws/show/z0820-07](https://zakon.rada.gov.ua/laws/show/z0820-07)

6. Informacijni materialy shhodo zakhyshhenykh vuzliv dostupu do merezhi Internet. URL:
https://dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=283080&cat_id=44795.