УДК 342.9
DOI https://doi.org/10.32782/klj/2024.3.27

Співак М. В.,
доктор політичних наук, професор,
доцент кафедри публічного управління та адміністрування
Національної академії внутрішніх справ

Дубіна О. М.,
доктор філософії (PhD),
начальник 9-го відділу управління протидії кіберзлочинам в м. Києві
Департаменту кіберполіції Національної поліції України

ЦИФРОВІ КОМПЕТЕНТНОСТІ ДЕРЖАВНИХ СЛУЖБОВЦІВ В УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬСТВА І ВИНИКНЕННЯ КІБЕРЗАГРОЗ

Анотація. В епоху цифрового суспільства кібербезпека стала невід'ємним аспектом у роботі органів державної влади. Зі зростанням залежності від технологій та Інтернету державні службовці стикаються з безпрецедентним рівнем кіберзагроз. Актуальність даної проблематики в Україні автори статті підтверджують статистичними даними за 2022–2023 роки.

Мета статті полягає у дослідженні та аналізі сучасних форм електронної комунікації в органах державної влади в умовах розвитку цифрового суспільства і виникнення кіберзагроз; визначення особливостей правового регулювання вказаного напрямку; виокремити низку пріоритетних напрямів підвищення кваліфікації державних службовців у контексті цифровізації.

Методичною базою дослідження є аналітичні звіти Київської міської державної адміністрації, Національного агентства України з питань державної служби, Державної служби спеціального зв'язку та захисту інформації України.

У статті наголошується на тому, що якісна комунікативна підготовка державних службовців їх обізнаність про наслідки небезпек та впровадження найсучасніших технологій, інструментів та практик в умовах постійної агресії у кіберпросторі є необхідною умовою забезпечення стабільної роботи державних інформаційних систем та надання послуг громадянам. Наводяться статистичні дані по показникам використання сучасних форм електронної комунікації у роботі державних службовців. Нині ними є: електронне звернення, електронні послуги, електронна петиція.

Розглянуті правові та організаційні основи державної політики у сферах електронних комунікацій на державній службі. Визначено перелік знань, вмінь та навичок державних службовців та посадових осіб місцевого самоврядування України щодо володіння технологіями електронного врядування. У висновках наголошується на тому, що при розробці та реалізації навчальних програм у підвищенні кваліфікації державних службовців необхідно передбачити напрями з основ державної політики у сфері інформаційної безпеки, інформаційної війни, кібербезпеки, кіберзагроз. Наступні наукові і практичні розвідки, задля оптимізації управлінських процесів, необхідно спрямувати на розроблення пропозицій з застосування алгоритмів штучного інтелекту на державній службі, а також визначення проблем конфіденційності та безпекових ризиків. Вказується на необхідності вдосконалення навичок інструментів штучного інтелекту у діяльності державної служби.

Ключові слова: *державна служба, електронна петиція, електронне звернення, електронна послуга, цифрові компетентності, кібератака, види кіберзагроз.*

Spivak M. V., Dubina O. M. Digital competences of civil servants in the context of the development of a digital society and the identification of cyber threats

Abstract. In the era of digital society, cyber security has become an integral aspect of the work of state authorities. With the growing dependence on technology and the Internet, public servants face an unprecedented level of cyber threats. The authors of the article confirm the relevance of this issue in Ukraine with statistical data for 2022–2023.

The purpose of the article is to research and analyze modern forms of electronic communication in state authorities in the context of the development of a digital society and the emergence of cyber threats;

determination of the specifics of legal regulation of the indicated direction; to single out a number of priority directions for improving the qualifications of civil servants in the context of digitalization.

The methodological basis of the research is the analytical reports of the Kyiv City State Administration, the National Agency of Ukraine for Civil Service, the State Service for Special Communication and Information Protection of Ukraine.

The article emphasizes that high-quality communication training of civil servants, their awareness of the consequences of dangers and the implementation of the most modern technologies, tools and practices in conditions of constant aggression in cyberspace is a necessary condition for ensuring the stable operation of state information systems and providing services to citizens. Statistical data on indicators of the use of modern forms of electronic communication in the work of civil servants are provided. Currently, they are: electronic appeal, electronic services, electronic petition.

The legal and organizational foundations of state policy in the spheres of electronic communications in the public service are considered. The list of knowledge, abilities and skills of civil servants and officials of local self-government of Ukraine regarding the possession of electronic government technologies has been defined. The conclusions emphasize that when developing and implementing educational programs to improve the qualifications of civil servants, it is necessary to provide directions from the basics of state policy in the field of information security, information warfare, cyber security, and cyber threats. The following scientific and practical investigations, in order to optimize management processes, should be directed to the development of proposals for the use of artificial intelligence algorithms in the public service, as well as the identification of confidentiality problems and security risks. The need to improve the skills of artificial intelligence tools in civil service activities is indicated.

Key words: *public service, electronic petition, electronic appeal, electronic service, digital competences, cyber attack, types of cyber threats.*

Актуальніть обраної теми. За даними Державної служби спеціального зв'язку та захисту інформації України кількість кібератак у 2023 році зросла, порівняно з 2022 роком, на 15,9% до 2543 інцидентів. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, 347 – кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації. Ще 92 рази було атаковано енергетичний сектор, 81 – телеком, 38 – освітні установи, 32 – транспортну галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ, 12 – медичні установи. Цілеспрямовані атаки переважно були спрямовані на міністерства та інші органи державної влади, а також на об'єкти критичної інфраструктури [1].

В умовах повномасштабної війни кібератаки російських хакерів є частиною злочинів російської армії. Статистика показує, що найчастіше вони атакують органи центральної та місцевої влади. Тому, важливо не тільки створити сприятливі умови на державній службі, в яких кожен підрозділ зможе забезпечити свій кіберзахист, а й навчити державних службовців користуватись всіма доступними інструментами ефективно.

Якісна комунікативна підготовка державних службовців їх обізнаність про наслідки небезпек та впровадження найсучасніших технологій, інструментів та практик в умовах постійної агресії у кіберпросторі – необхідна умова забезпечення стабільної роботи державних інформаційних систем та надання послуг громадянам. А також враховуючи зміст положень Розпорядження Кабінету Міністрів «Про затвердження плану заходів з розвитку системи професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад до 2027 року» розпорядження Кабінету Міністрів України від 27 грудня 2023 року та Наказу Національного агентства України з питань державної служби 23 серпня 2023 року № 133-23 «Про затвердження переліків пріоритетних напрямів (тем) підвищення кваліфікації державних службовців, голів місцевих державних (військових) адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування, депутатів місцевих рад за загальними професійними (сертифікатними) та/або короткостроковими програмами у 2024 році» обрана тематика є своєчасною та актуальною.

Аналіз досліджень і публікацій. Сучасні електронні ресурси як спосіб комунікаційної взаємодії в органах державної влади стали предметом обговорення у працях А. Барікової, Д. Войченко, Н. Ткаленко, О. Михайловської, І. Улицької, О. Леути, О. Псьоти та ін. Кібербезпека, загрози та стан захищеності держави і окремих її інститутів досліджували В. Венцель, А. Микитюк, Д. Могилевич, В. Равлюк, А. Сторчак, П. Сидоркін, З. Свердлик, С. Сальник, Р. Сбоєв, В. Фурашев та ін. Але і водночас виникають найбільші питання щодо проведення наукових досліджень оскільки цей напрям має більш високу актуальність через інтенсивне зростання науково-технічного прогресу, що викликається повсюдним впровадженням інформаційно-комунікаційних технологій у сфери суспільної діяльності та взаємовідносин.

Мета статті. Дослідити та проаналізувати сучасні форми електронної комунікації в органах державної влади в умовах розвитку цифрового суспільства і виникнення кіберзагроз; визначити особливості правового регулювання вказаного напрямку; виокремити низку пріоритетних напрямів підвищення кваліфікації державних службовців у контексті цифровізації.

Виклад основного матеріалу. Моніторинг наукових розвідок останніх років дає змогу зробити висновок про те, що нині одним із ключових ризиків, спричинених глобальною інформатизацією як на державному, так і на індивідуальному рівні, продовжує залишатися постійна поява нових кіберзагроз, цифрова нерівність, небезпеки і ризики ШІ тощо. За таких умов держава стає уразливою і змушена експерементувати з моделями взаємодії між органами влади, громадянами і іншими державами з метою отримання переваг на міжнародній арені. Високі темпи розвитку сучасних інформаційних і комунікаційних технологій, необхідність застосування їх у діяльності державних органів допомагають розкрити їх управлінський потенціал з позиції «сервісної держави».

Відповідно до Указів Президента України від 31 липня 2000 року № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» та від 17 травня 2001 року № 325 «Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади» з метою поліпшення умов для розвитку демократії, реалізації громадянами конституційних прав на участь в управлінні державними справами і на вільний доступ до інформації про діяльність органів виконавчої влади, а також забезпечення гласності та відкритості діяльності цих органів Кабінет Міністрів України урядом було затверджено Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади [2].

Секретаріату Кабінету Міністрів України, міністерствам, іншим центральним органам виконавчої влади, Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям доручено забезпечити: 1) належне інформаційне наповнення та функціонування Єдиного веб-порталу, офіційних веб-сайтів (веб-порталів) органів виконавчої влади та офіційних веб-ресурсів, що пов'язані з діяльністю органів виконавчої влади, і дотримання вимог, визначених цією постановою, під час створення (модернізації) офіційних веб-сайтів (веб-порталів) органів виконавчої влади та офіційних веб-ресурсів, що пов'язані з діяльністю органів виконавчої влади, в межах видатків, передбачених у державному бюджеті для функціонування відповідних органів, Національної програми інформатизації та інших джерел, не заборонених законодавством; 2) надсилання проектів дизайну офіційних веб-сайтів (веб-порталів) органів виконавчої влади та офіційних веб-ресурсів, що пов'язані з діяльністю органів виконавчої влади, та Єдиного веб-порталу у разі їх створення (модернізації) на погодження до Мінцифри у визначеному ним порядку [2].

Нині, формами електронної комунікації є:

– електронне звернення. Важливу роль у функціонуванні е-демократії в Україні відіграють вебсайти як центральних органів влади, так і місцевого самоврядування. Ці сайти виконують функцію інформування суспільства про діяльність органів влади, спрощують доступ громадян до відкритих даних,

державних послуг та можливостей впливати на них завдяки громадським зверненням. Тут варто згадати вебсайт Кабінету Міністрів України, де можна знайти інформацію про діяльність уряду, прийняті рішення, потрібні послуги, а також подавати е-звернення громадян. За статистикою Урядового контактного центру КМУ, за 2022 рік від громадян надійшло 1 805 339 е-звернень стосовно тих чи інших проблем, з яких було виконано 978 359. Серед найбільш активних регіонів виділяють Київ (293 441), Дніпропетровську область (155 626) та Харківську область (103 825). Здебільшого ці звернення стосуються проблем соціального захисту громадян та діяльності центральних органів влади, що вирішуються зазвичай в межах 2 тижнів [3]. У 2023 році по усих регіонах України всього надійшло 1781431 звернень, 661717 – було надіслано органам виконавчої влади, 1119714 – надано роз'яснень заявникам. У 2024 році всього надійшло 384543 звернень, 139617 – було надіслано органам виконавчої влади, 244926 – надано роз'яснень заявникам [4];

– електронні послуги. В Україні зберігається високий рівень користування державними електронними послугами. Наразі 64% респондентів (71% серед чоловіків і 58% серед жінок) відповіли, що за останній рік користувалися принаймні певними послугами. У 2022 році цей показник становив 63%, тож формально зміни – в межах похибки. Проте порівняно з показниками 2020 року (53%) відбулося зростання майже на 11%. Водночас за три роки спостережень рівень некористування знизився з 47% до 33% [5, с. 20];

– електронна петиція. Нині електронні петиції є головним інструментом електронної демократії в Україні. Для їхнього запровадження було внесено зміни до Закону України «Про звернення громадян» у 2015 році, що стосувалися електронного звернення та електронних петицій. Згідно з цим законом, е-петиція – це особлива форма колективного звернення громадян до Президента України, ВРУ, КМУ та до органів місцевого самоврядування через офіційний вебсайт органу, якому вона адресована. Наприклад, у продовж 2019–2023 років до президента України зареєстровано 50996 петицій: 2019 – 13214, 2020 – 10473, 2021 – 2021, 2022 – 13053, 2023 – 6115 [6]. На сайті Київської міської державної адміністрації показана статистика від 1 жовтня 2015 року по 8 серпня 2024 року. Відповідно до показників 8411 – петицій опубліковано, 195 – петицій що набрали достатньо підписів, 1535060 – нових користувачів, 5692711 – віддано підписів, 124 – петицій підтримано владою [7].

З метою гарантування безпеки держави, безпеки та сталості електронних комунікаційних мереж Указом Президента України № 802/2022 введено в дію рішення Ради національної безпеки і оборони України від 26 листопада 2022 року «Про забезпечення електронними комунікаційними послугами в умовах воєнного стану». Це рішення передбачає надання електронних комунікаційних послуг з дотриманням встановлених показників якості для визначеного переліку об'єктів. У тому числі з урахуванням можливої відсутності електроживлення на них щонайменше протягом трьох діб. Також передбачається проведення позапланових заходів контролю та пріоритетне електроживлення об'єктів, технічних засобів інфраструктури та споруд електронних комунікаційних мереж [8].

Також важливим у цьому напрямі є Закон України «Про електронні комунікації». Закон визначає правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами [9].

У 2023 році у Верховній Раді було зареєстровано проєкт Закону про внесення змін до Закону України «Про державну службу» (щодо обов'язковості навчання державних службовців основ кібербезпеки). У проєкті наголошувалося на тому, що цифрові компетентності, зокрема, впевнена та відповідальна взаємодія з сучасними цифровими технологіями, ефективно та безпечно працювати з програмами, можливість виявити ознаки та забезпечити належну організацію протидії впливу кіберзагроз, повинні бути одними з пріоритетів працівників державної служби. В умовах

постійної активності, зокрема, з боку Російської Федерації, у створенні реальних загроз вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури, рівень обізнаності та протидії цим загрозам з боку України, наших працівників, в першу чергу, державної служби, має бути надвисоким [10].

Зокрема ініціаторами законопроєкту пропонувалося частину третю статті 13 доповнити пунктом 6^1 такого змісту: «6^1) організовує із залученням навчальних закладів навчання державних службовців основам кібербезпеки, затверджує форму державного сертифіката з питань кібербезпеки та порядок його видачі особам, які бажають взяти участь у конкурсі на вакантні посади державної служби та державним службовцям, видає державні сертифікати з питань кібербезпеки; пункт 7 частини другої статті 17 доповнити знаком та словами: «., а також планування навчання основам кібербезпеки»; частину першу статті 25 доповнити пунктом 5^1 такого змісту: «5^1) копію державного сертифіката з питань кібербезпеки, що підтверджує рівень знань з комп'ютерної грамотності, методів захисту інформації та основ кібербезпеки, отриманого у порядку, визначеному центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері державної служби» [10].

Комітет з питань інтеграції України до Європейського Союзу, розглянувши на своєму засіданні 07.06.2023 року проект Закону про внесення змін до Закону України «Про державну службу» (щодо обов'язковості навчання державних службовців основ кібербезпеки) (р.№ 9268), визнав його положення такими, що регулюються національним законодавством країн членів Європейського Союзу та не підпадають під дію міжнародно-правових зобов'язань України у сфері європейської інтеграції [11]. У 2024 році законопрєкт був знятий з розгляду. На нашу думку пропозиція запровадження державного сертифіката з питань кібербезпеки є недоцільною. Адже, з розвитком науки і техніки, змінюються ланцюги комунікації та взаємодія в цифровому суспільстві, удосконалення потребує безпека в цифровому середовищі, виникають нові види кіберзагроз. Цей процес не є сталим. Тому, цифрові компетентності як складова підготовки державного службовця мають відповідати новим вимогам до схем навчання цифровим навичкам у реалізації професійної діяльності. Залежно від типу навичок, які потребують удосконалення та з урахуванням професійних груп, державні службовці можуть формувати навчання без відриву від роботи упродовж перебування на державній службі.

Узагальнюючи відкриті інтернет джерела, офіційні вебресурси та закони України вдається можливим визначити перелік знань, вмінь та навичок державних службовців та посадових осіб місцевого самоврядування України щодо володіння технологіями електронного врядування. Тож державний службовець повинен: знати поняття, призначення, мету, основні завдання, принципи створення і функціонування, складові інформаційної системи «Електронний уряд»; знати можливості використання технологій і методів електронного урядування у професійній діяльності; знати складові електронного уряду та його архітектурні моделі; знати технології електронного урядування; володіти навичками із розробки заходів із запровадження технологій електронного урядування на різних рівнях державного управління; вміти застосовувати у професійній діяльності технології електронного урядування, орієнтуватися в моделях впровадження електронного уряду; аналізувати і вирішувати проблеми формування і розвитку електронного урядування в Україні, розробляти вимоги, технічні завдання для впровадження технологій електронного урядування в органах державного управління; розробляти інформаційно-технологічного забезпечення Інтернет-порталу органу державного управління; володіти технологіями роботи з системами електронного документообігу, володіти технологіями використання цифрового підпису, знати технологію використання системи електронних державних закупівель, вміти проектувати алгоритми надання елементарних та композитних електронних послуг громадянам і бізнесовим структурам, іншим органам державної влади [12].

Якщо звернутися до навчально-професійних програм державних службовців, які

займають посади категорії «Б», «В»; посадові особи органів місцевого самоврядування IV-VII категорій посад ставляться такі вимоги: знати: сучасних інформаційних технологій та тенденцій їх розвитку; основних функції програмного забезпечення сучасного комп'ютера; принципів побудови і функціонування комп'ютерних мереж; основ безпеки у мережі Інтернет; уміти: оцінювати роль новітніх інформаційно-комунікаційних технологій у професійній діяльності; використовувати текстові редактори та табличні процесори в професійній діяльності; застосовувати служби та послуги мережі Інтернет; мати навички: використання сучасних комп'ютерних програм загального призначення у професійній діяльності; створення, публікації й підтримки веб-ресурсів; організації спільної роботи з документами [13]. Для підвищення спроможності з розбудови кіберзахисту державних установ Держспецзв'язку разом із проєктом ЄС «Підтримка комплексної реформи державного управління в Україні» (EU4PAR) та Національним агентством України з питань державної служби (НАДС) вже проводяться навчання для держслужбовців категорії «А» з побудови кіберзахисту в державних установах [14].

Висновки. З огляду на те, що інформаційне суспільство характеризується визнанням інформації одним з найважливіших суспільних ресурсів цей ресурс нині став ключовою складовою розвитку всіх галузей діяльності у тому числі інституту державної служби. Статистичні дані показують, що за останні роки Україна перебуває у стані постійних кібератак. Ці інциденти підкреслюють необхідність знань про кіберзагрози для корпоративної безпеки та захисту персональних даних в органах державної влади. У діючих нормативно правових актах уряд намагається закріпити вимоги і процедуру підвищення цифрової компетентності державного службовця. Вважаємо, що при розробці та реалізації навчальних програм у підвищенні кваліфікації державних службовців необхідно передбачити такі напрями: види кіберзагроз; принципи державної політики у сфері інформаційної безпеки; навички у сфері забезпечення кібербезпеки; ознаки інформаційної війни, її проявів та основних складових, актуальних дезінформаційних наративів; першочергові заходи реагування з технічної сторони на кібератаки; належне користування юридичними інструментами фіксації незаконного втручання в діяльність органів державної влади. Наступні наукові і практичні розвідки, задля оптимізації управлінських процесів, необхідно спрямувати на розроблення пропозицій з застосування алгоритмів штучного інтелекту на державній службі, а також визначення проблем конфіденційності та безпекових ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. 31 січня 2024. Анастасія Жарикова. URL: https://www.epravda.com.ua/news/2024/01/31/709355/ (дата звернення: 01.08.24)

2. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3. URL: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text (дата звернення: 01.08.24)

3. Куценко О. Що таке електронна демократія? 13 вересня 2023 року. Центр політико-правових реформ. URL: https://uplan.org.ua/elektronna-demokratiia-v-ukraini-cuchasnyi-stan-ta-perspektyvy-rozvytku/ (дата звернення: 02.08.24)

4. Інтерактивна мапа звернень. «Урядовий контактний центр». URL: https://ukc.gov.ua/a-statystyka-a/stats/(дата звернення: 02.08.24)

5. Думки і погляди населення України щодо державних електронних послуг. Аналітичний звіт. 2024 року. URL: https://www.undp.org/sites/g/files/zskgke326/files/2024-01/infographic-e-services-use-in-ukraine-2023.pdf (дата звернення: 02.08.24)

6. Почути не всіх. Чому президент Зеленський не реагує на інструмент петицій? Вікторія Олійник. 23 січня 2024 року. URL: https://www.chesno.org/post/5850/(дата звернення: 03.08.24)

7. Статистика від 1 жовтня 2015 року по 8 серпня 2024 року Київська міська державна адміністрація. URL: https://petition.kyivcity.gov.ua/statistic (дата звернення: 08.08.24)

8. Про рішення Ради національної безпеки і оборони України від 26 листопада 2022 року «Про забезпечення електронними комунікаційними послугами в умовах воєнного стану»: Указ Президента України від 26 листопада 2022 року № 802/2022. URL: https://www.president.gov.ua/documents/8022022-45001 (дата звернення: 04.08.24)

9. Про електронні комунікації: Закон України від 16 грудня 2020 року № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text(дата звернення: 04.08.24)

10. Закон України «Про внесення змін до Закону України «Про державну службу» (щодо обов'язковості навчання державних службовців основ кібербезпеки)». Верховна Рада України. URL: blob:https://itd.rada.gov.ua/1a15ac1d-131b-49a4-a01a-9eb6cdde4c5e (дата звернення: 05.08.24)

11. Висновок (експертиза щодо європейської інтеграції) Закону України «Про внесення змін до Закону України «Про державну службу» (щодо обов'язковості навчання державних службовців основ кібербезпеки)». Верховна Рада України. URL:blob:https://itd.rada.gov.ua/35bd2734-312e-4156-8c77-de7830437451(дата звернення: 05.08.24)

12. Вимоги до знань, вмінь та навичок державних службовців та посадових осіб місцевого самоврядування щодо їх інформаційно-технологічних компетенцій. URL: https://pidru4niki.com/89282/menedzhment/vimogi_znan_vmin_navichok_derzhavnih_sluzhbovtsiv_posadovih_osib_mistsevogo_samovryaduvannya_informatsiyno-tehnologichnih (дата звернення: 05.08.24)

13. Комп'ютерна грамотність та застосування сучасних інформаційних технологій у діяльності державного органу. Погоджено з НАДС – наказ НАДС від 14 лютого 2022 року № 11-22. URL: https://pdp.nacs.gov.ua/courses/kompiuterna-hramotnist-ta-zastosuvannia-suchasnykh-informatsiinykh-tekhnolohii-u-diialnosti-derzhavnoho-orhanu?course_enrollment_id=1375 (дата звернення: 05.08.24)

14. Підвищуємо кіберстійкість державних інформаційних ресурсів: Держспецзв'язку провела перший освітній курс із кіберзахисту для держслужбовців категорії «А». Державний центр кіберзахисту Держспецзв'язку. 01.12.2022. URL:https://scpc.gov.ua/uk/articles/225 (дата звернення: 08.08.24)