УДК 351:004.056

https://doi.org/10.62664/cpa.2025.01.18

Тетяна МАЛАХОВА,
професор кафедри публічного управління та адміністрування,
доктор наук з державного управління, професор
Державний університет інформаційно-комунікаційних технологій (м. Київ)
ORCID ID https://orcid.org/0009-0001-1113-5723

КІБЕРБЕЗПЕКА ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ В КОНТЕКСТІ СУЧАСНИХ ГІБРИДНИХ ЗАГРОЗ: ІНСТИТУЦІЙНІ ТА ТЕХНОЛОГІЧНІ АСПЕКТИ

Статтю присвячено дослідженню кібербезпеки органів публічного управління України в умовах сучасних гібридних загроз, насамперед зумовлених агресією російської федерації. Визначено актуальність проблеми забезпечення стійкості державних інформаційно-комунікаційних систем перед масованими кібератаками, що є невід'ємним складником гібридної війни. Наукова новизна цієї статті полягає в комплексному розгляді інституційних та технологічних аспектів кібербезпеки державного управління саме в контексті гібридної війни 2020–2025 рр., з урахуванням досвіду реальних кібератак цього періоду і відповідної реакції держави.

Проаналізовано останні дослідження та публікації українських і зарубіжних фахівців, нормативно-правову базу України у сфері кібербезпеки, статистичні дані про кіберінциденти 2020–2025 рр. та конкретні приклади кібератак на органи державної влади. У межах дослідження охарактеризовано інституційну структуру системи

кібербезпеки України (роль Держспецзв'язку, НКЦК, СБУ, кіберпідрозділів силових відомств тощо) та сучасні технологічні засоби захисту інформаційних систем органів публічного управління.

Надано рекомендації щодо вдосконалення державної політики у сфері кібербезпеки публічного управління України, підвищення рівня кіберстійкості державних інституцій, розвитку міжвідомчої та міжнародної координації, запровадження передового досвіду та технологій захисту. Встановлено, що досвід України вже сьогодні стає в нагоді іншим країнам, і, зміцнюючи власну кібербезпеку, наша держава робить внесок у колективну безпеку демократичного світу.

Ключові слова: *кібербезпека, органи публічного управління, гібридні загрози, кіберзагрози, кібератаки, інформаційна безпека, державна політика.*

Tetiana MALAKHOVA,
Professor at Department of Public Administration and Management,
Doctor Sciences in Public Administration, Professor
State University of Information and Communication Technologies
(the city of Kyiv)
ORCID ID https://orcid.org/0009-0001-1113-5723

CYBERSECURITY OF PUBLIC ADMINISTRATION BODIES IN THE CONTEXT OF MODERN HYBRID THREATS: INSTITUTIONAL AND TECHNOLOGICAL ASPECTS

The article is devoted to the study of cybersecurity of public administration bodies in Ukraine in the context of modern hybrid threats, primarily caused by the aggression of the russian federation. The relevance of ensuring the resilience of state information and communication systems against massive cyberattacks,

which are an integral part of hybrid warfare, is determined. The scientific novelty of this article lies in its comprehensive examination of the institutional and technological aspects of cybersecurity in public administration, specifically in the context of the hybrid war of 2020–2025, taking into account the experience of real cyberattacks during this period and the state's response.

The latest research and publications by Ukrainian and foreign experts, the regulatory framework of Ukraine in the field of cybersecurity, statistical data on cyber incidents in 2020–2025, and specific examples of cyberattacks on state authorities are analyzed. The study characterizes the institutional structure of Ukraine's cybersecurity system (the role of the State Special Communications Service, the National Cyber Security Center, the Security Service of Ukraine, cyber units of law enforcement agencies, etc.) and modern technological means of protecting information systems of public administration bodies.

Recommendations are provided on improving state policy in the field of cybersecurity in Ukraine's public administration, increasing the cyber resilience of state institutions, developing interagency and international coordination, and introducing best practices and protection technologies. It has been established that Ukraine's experience is already proving useful to other countries, and by strengthening its own cyber security, our state is contributing to the collective security of the democratic world.

Key words: *cybersecurity, public administration, hybrid threats, cyber threats, cyber attacks, information security, state policy.*

Постановка проблеми. Гібридна агресія проти України, що триває останніми роками, наочно продемонструвала, що кібератаки на органи державної влади та об'єкти критичної інфраструктури стали одним із ключових інструментів сучасної війни. Нині кіберпростір є ареною протиборства не менш важливою, ніж традиційні поля бою, оскільки успішна атака на державні інформаційні системи може призвести до

дестабілізації управлінських процесів, порушення роботи економіки, комунікацій, фінансової та безпекової сфер. З початком повномасштабного вторгнення рф 2022 року інтенсивність та масштаб кібернетичних загроз різко зросли. За даними Служби безпеки України, лише впродовж одного року було попереджено понад 4500 кібератак на органи влади та критичну інфраструктуру країни [1]. Така безпрецедентна кількість інцидентів підтверджує, що кібербезпека є невід'ємним складником національної безпеки в сучасних умовах.

Органи публічного управління, відповідальні за функціонування держави та надання публічних послуг, є пріоритетною ціллю ворожих кібероперацій. Зловмисники прагнуть отримати несанкціонований доступ до урядових інформаційних ресурсів, викрасти службові дані, порушити роботу електронних реєстрів, систем зв'язку, електронного урядування тощо. Кібератаки часто поєднуються з іншими засобами гібридного впливу – дезінформацією, економічним та дипломатичним тиском, фізичним руйнуванням інфраструктури – щоб досягти максимального деструктивного ефекту. В умовах тривалої збройної агресії рф проти України (що супроводжується офіційно не оголошеною, але фактичною кібервійною), стійкість державних інформаційних систем стала критично важливою. Актуальність теми зумовлено потребою захистити органи публічного управління від сучасних кіберзагроз, забезпечити неперервність їх роботи та збереження конфіденційності, цілісності і доступності інформації.

Проблематика кібербезпеки публічного сектору є відносно новою для наукового середовища, проте за останнє десятиліття вона швидко розвивається. Постає потреба в комплексному дослідженні як інституційних аспектів (державна політика, законодавство, структура відповідальних органів), так і технологічних (засоби та методи захисту, реагування на інциденти) з урахуванням поточного досвіду протидії реальним кібератакам на державні установи.

Аналіз останніх досліджень та публікацій. Питання кібербезпеки в державному секторі перебуває в полі зору як українських, так і зарубіжних дослідників, особливо після резонансних кібератак останніх років. В Україні формування засад державної кібербезпеки було започатковано ухваленням ключових нормативних документів, зокрема Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163–VIII [2]. Цим Законом було визначено базові поняття, суб'єкти забезпечення кібербезпеки та їх повноваження, що заклало інституційний фундамент у цій сфері. У подальшому стратегічні орієнтири було закріплено в Стратегії кібербезпеки України на 2021–2025 роки, схваленій рішенням РНБО та введеній в дію Указом Президента від 26 серпня 2021 року № 447/2021 [3]. У цій Стратегії акцентовано увагу на зростанні кіберзагроз в умовах гібридної війни, потребі розбудови національної кіберстійкості, розвитку державно-приватного партнерства та міжнародної кооперації.

Науковці досліджують різні аспекти проблеми. Зокрема, українські фахівці з державного управління аналізують питання інтеграції кібербезпеки в систему національної безпеки та оборони. У працях вітчизняних авторів (наприклад, О. Власюк, В. Горбулін та ін.) наголошується, що кіберпростір перетворився на ще один театр бойових дій, а Україна стала полігоном для відпрацювання нових кіберударів з боку держави-агресора. Дослідники відзначають, що кібероперації рф спрямовано не лише на військові або енергетичні об'єкти, а й на органи державної влади, щоб підірвати їх спроможність керувати державою в кризових умовах. Серед зарубіжних джерел варто відзначити аналітичні звіти міжнародних організацій. *Європейське агентство з кібербезпеки ENISA* в своєму щорічному огляді *Threat Landscape 2022* констатує, що в світі зростає частка саме державних кібератак та складних багатоетапних загроз, які часто є частиною гібридних кампаній. НАТО та ЄС в офіційних

документах останніх років також визнають, що гібридні загрози поєднують у собі військові й невійськові засоби, у тому числі кібератаки на державні установи та об'єкти інфраструктури. Так, у *Концепції колективної безпеки* НАТО кіберпростір з 2016 р. визнано окремим оперативним доменом, а у 2018 р. створено Оперативний центр кібербезпеки для координації зусиль Альянсу у цій сфері. Держави ЄС запровадили Директиву NIS (*Network and Information Security*) щодо забезпечення стійкості мереж та інформаційних систем, яка зобов'язує органи влади запроваджувати мінімальні стандарти кіберзахисту.

У сфері практичних кейсів великий інтерес дослідників викликають конкретні приклади кібератак. У публікаціях українських експертів (Держспецзв'язку, НКЦК, а також незалежних аналітиків) детально розглянуто кібератаки на українські державні ресурси впродовж 2015–2021 рр., зокрема атаки типу *Advanced Persistent Threat* (APT), пов'язані з російськими хакерськими групами APT28 (*Fancy Bear*), Sandworm та ін. Наприклад, група Sandworm, яку пов'язують з ГРУ рф, ще до повномасштабної війни здійснювала атаки на українські державні органи. 2017 року вона запустила відомий вірус-шифрувальник *NotPetya*, що вивів з ладу ІТ-системи як державних, так і приватних структур. Цей інцидент часто згадується в літературі як один із перших випадків надзвичайно руйнівної кібератаки в Україні та світі, що мала ознаки кібертероризму.

З початком нової фази агресії (2022 р.) дослідники та оглядачі фіксують появу нових видів шкідливого програмного забезпечення та тактик. У звітах команди CERT-UA (*Government Computer Emergency Response Team of Ukraine*) за 2022–2023 рр. відзначено активізацію кількох кіберкампаній проти українських держорганів. Зокрема, групу UAC-0010 (також відома як *Armageddon* або *Gamaredon*) – кіберпідрозділ ФСБ рф – лише впродовж 2023 року було відповідально за 277 задокументованих кіберінцидентів проти України [4]. Кампанії *Gamaredon* характеризуються масовим

розсиланням фішингових листів з темами, прив’язаними до військової тематики (наприклад, вигадані накази про переміщення військ, мобілізацію тощо), що містять шкідливі вкладення або посилання. Аналіз останніх зразків атаки засвідчив, що зловмисники активно використовують легітимні на вигляд інструменти адміністрування (наприклад програми віддаленого доступу типу *Remcos*), маскуючи їх під службові документи, – така тактика ускладнює виявлення атаки антивірусними засобами [4].

Отже, огляд літератури свідчить про існування суттєвої бази досліджень, присвячених окремим аспектам кібербезпеки публічного управління. Водночас, стрімка еволюція загроз (нові віруси-«*вайпери*», шпигунські програми, цільові атаки на реєстри тощо) та динаміка розвитку української системи кіберзахисту в останні 2–3 роки потребують оновленого аналізу.

Метою статті є проаналізувати стан кібербезпеки органів публічного управління України в контексті гібридної агресії, виявити проблемні аспекти та запропонувати напрямки вдосконалення як на інституційному, так і на технологічному рівнях. Для досягнення цієї мети передбачено виконати такі завдання: узагальнити характерні кібер- та гібридні загрози, що були спрямовані проти органів публічного управління України в останні роки, й проаналізувати найбільш резонансні інциденти; дослідити інституційну структуру забезпечення кібербезпеки в Україні (суб’єкти, їх функції та взаємодію), оцінити ефективність державної політики та нормативно-правового забезпечення у цій сфері; проаналізувати сучасні технологічні підходи та рішення, що застосовуються для захисту державних інформаційних ресурсів (системи виявлення та реагування на інциденти, засоби захисту мереж, шифрування, резервування даних тощо); запропонувати рекомендації щодо підвищення рівня кібербезпеки органів публічного управління України, посилення інституційної спроможності та впровадження новітніх технологічних рішень.

Виклад основного матеріалу. Період 2020–2025 рр. ознаменувався численними кібератаками на державні інформаційні ресурси України, що відбувалися на тлі ескалації російської гібридної агресії. Показовим був інцидент 14 січня 2022 року, коли одночасно було атаковано близько 70 веб-сайтів українських міністерств та відомств, у тому числі Міненергетики, МОН, Дія тощо; на головних сторінках зловмисники розмістили погрози на адресу українців. Ця атака супроводжувалася запуском шкідливого ПЗ типу wiper (вайпер), відомого як *WhisperGate*, що намагався знищити дані на вражених системах. Хоча цю атаку вдалося локалізувати, вона стала сигналом про високий рівень кібернебезпеки напередодні військового вторгнення.

Після 24 лютого 2022 року кіберфронт фактично став складником воєнних дій. Російські хакерські групи скоординовано намагалися паралізувати роботу державних органів: уже в перші дні війни було здійснено сильні DDoS-атаки на урядові портали, телекомунікаційні компанії та банки, а також цільові проникнення в мережі об’єктів критичної інформаційної інфраструктури. 2023 року кібероперації рф набули більш витонченого характеру. Значущою тенденцією стало використання персональних даних та скомпрометованих облікових записів для проникнення в урядові системи. Наприклад, навесні 2023 року СБУ повідомила про нейтралізацію декількох внутрішніх агентів ворога, що за винагороду передавали хакерам доступ до облікових записів державних службовців. Такого роду інсайдерські загрози є частиною гібридної тактики ворога, що поєднує кібернетичну й агентурну роботу. Однією із найрезонансніших кібератак стала атака на компанію «Київстар» у грудні 2023 року, яка фактично вплинула і на державний сектор, оскільки Київстар є найбільшим телекомунікаційним провайдером України, що обслуговує також й урядові установи. Як встановило розслідування СБУ, російські хакери із групи *Sandworm* ще з травня 2023 року непомітно проникли в

внутрішню мережу Київстар, а 12 грудня здійснили скоординований удар, що знищив ключові сервери та IT-обладнання оператора [5]. Цей безпрецедентний інцидент продемонстрував, що навіть приватні компанії, критично важливі для суспільства, стають мішенню воєнних кібератак; водночас держава має враховувати їх захист у загальному контурі національної кібербезпеки. Ще один небезпечний інцидент трапився наприкінці 2024 року – масштабна кібератака російських спецслужб на державні реєстри Міністерства юстиції. 19 грудня 2024 р. було зафіксовано цілеспрямований зовнішній кіберудар по інформаційно-телекомунікаційній системі держреєстрів, що призвело до повного блокування роботи понад 60 різних державних реєстрів (у тому числі Єдиного держреєстру юросіб та ФОП, реєстру речових прав на нерухоме майно, реєстру актів цивільного стану та інших) [6]. За повідомленням Мін'юсту, це була наймасштабніша атака на державні інформаційні ресурси за останні роки. Упродовж кількох тижнів роботу електронних послуг, пов'язаних з цими реєстрами (реєстрація актів, видача витягів, е-сервіси «Дія» щодо майнових операцій тощо), було паралізовано. На відновлення систем знадобилося близько місяця: лише 20 січня 2025 року Міністерство юстиції офіційно повідомило про повне відновлення функціонування Єдиних та Державних реєстрів після цієї атаки [7].

На початку 2025 року фіксуються нові кіберкампанії проти урядових структур. CERT-UA у березні 2025 р. повідомила про виявлення шпигунського ПЗ *WRECKSTEEL*, що застосовувалося хакерським угрупованням UAC-0219 для крадіжки даних з мереж державних органів [8]. Ця кампанія, активна з осені 2024-го, базувалася на розсиланні фішингових листів від імені скомпрометованих облікових записів, що містили посилання на файли в хмарних сховищах (*DropMeFiles, Google Drive*). При переході за посиланням у жертв виконувалася PowerShell-скрипт – так на комп'ютери непомітно встановлювався стілер *WRECKSTEEL*, здатний

викрадати документи (DOCX, PDF, зображення тощо) і робити скриншоти екрану [8]. Важливо, що зловмисники використовували соціальну інженерію: одну із фішингових розсилок було замасковано під повідомлення про «скорочення зарплат» у державному органі з вкладеним «списком співробітників» – ця тема спонукала адресатів відкрити файл [9]. Вірус *WRECKSTEEL* не мав модулів постійного закріплення в системі, тобто після перезавантаження зараженої машини зникав, що ускладнювало його виявлення [10]. Проте, до моменту перезавантаження він встигав зібрати чутливу інформацію та передати на сервери нападників. CERT-UA ідентифікувала цю активність і видала рекомендації щодо негайного повідомлення про ознаки компрометації та оновлення політики безпеки. У цілому кампанія *WRECKSTEEL* підтвердила тенденцію до використання вбудованих засобів Windows (PowerShell, скрипти) замість файлів-вірусів – така «*безфайлова*» техніка є характерною для сучасних APT-операцій і суттєво ускладнює роботу антивірусів [10].

Варто пригадати й про кібератаку на інфраструктуру «Укрзалізниці» у березні 2025 року, що хоч і не безпосередньо на орган державної влади, але безпосередньо торкнулася державного управління критичним об’єктом. Цю атаку розцінена РНБО як акт кібертероризму проти критичної інфраструктури [8]. Цей випадок підтверджує, що ворог продовжує розширювати спектр цілей у кіберпросторі – від центральних органів влади до державних підприємств, чия стабільна робота критично важлива для населення.

Інституційна структура кібербезпеки України. У відповідь на зростання кіберзагроз держава поступово вибудувала багаторівневу систему суб’єктів забезпечення кібербезпеки. Відповідно до Закону України 2017 року [2], до основних суб’єктів належать: Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку), Служба безпеки України (у частині контррозвідувального захисту та боротьби з кібертероризмом),

Національна поліція (підрозділи кіберполіції для протидії кіберзлочинності), розвідувальні органи, а також підрозділи забезпечення кібербезпеки Збройних сил України. Координація між ними здійснюється через Національний координаційний центр кібербезпеки (НКЦК) при РНБО України, створений 2016 р. НКЦК, до складу якого входять представники всіх ключових відомств, відповідає за узгодження політики та обмін інформацією про кіберінциденти. Як свідчить практика, НКЦК відіграв важливу роль у швидкому реагуванні на загрозливі ситуації, особливо під час масових атак 2022 р., коли на його базі збиралися міжвідомчі групи для ліквідації наслідків.

Держспецзв'язку виконує функції технічного регулятора й оператора урядового CERT-UA. Саме фахівці Держспецзв'язку та CERT-UA займаються моніторингом державних інформаційних ресурсів, аналізом кібератак та видачею рекомендацій щодо захисту. Крім того, Держспецзв'язку відповідає за забезпечення урядового сегменту зв'язку, захист державних інформаційних реєстрів, сертифікацію засобів захисту інформації тощо.

Служба безпеки України (СБУ), зокрема Департамент кібербезпеки СБУ, зосереджується на виявленні та нейтралізації кіберзагроз, що мають ознаки підривної діяльності іноземних спецслужб або тероризму. Фактично СБУ веде боротьбу з найбільш небезпечними державними APT-групами. Як зазначалося, СБУ у співпраці з іноземними партнерами ідентифікувала групу Sandworm за атакою на Київстар, збирає докази для міжнародного притягнення російських хакерів до відповідальності (зокрема, готує матеріали до Міжнародного кримінального суду) [5]. Окремо СБУ надає уваги кіберрозвідці – завдяки власним технічним засобам та агентурі, іноді вдається попереджувати атаки, проникаючи до інфраструктури противника (як пригадував Ілля Вітюк, 2021 р. СБУ змогла відстежити діяльність

Sandworm усередині мереж росіян і завчасно зірвати нову атаку на телеком-оператора) [1].

Кіберполіція (Департамент кіберполіції Національної поліції) розслідує інциденти кіберзлочинності, що часто переплітаються з атаками на органи влади (наприклад, фішингові кампанії для шахрайства з даними громадян, що зачіпають державні системи, чи атаки з метою викупу – ransomware). Упродовж 2022–2023 рр. кіберполіція разом із СБУ брала участь у викритті кількох хакерських груп, що діяли на території України, координуючись з рф. Також кіберполіція тісно співпрацює з міжнародними правоохоронними органами (Інтерпол, Європол) для розшуку кіберзлочинців.

З 2022 року розпочалося формування нової структури – кіберсил у складі Збройних сил України. Усвідомлюючи важливість наступальних та оборонних кібероперацій у воєнний час, Міноборони України ініціювало створення окремого військового органу, відповідального за ведення кібероборони, кібервпливу на противника та захист власних військових мереж. Наразі цей процес триває: формуються підрозділи, готуються кадри (частково за підтримки НАТО).

Таким чином, інституційна модель кібербезпеки України містить у собі декілька взаємопов’язаних ланок – цивільну (Держспецзв’язку, НКЦК), правоохоронну (СБУ, кіберполіція), військову (підрозділи ЗСУ) та координувальну (РНБО). На рівні законодавства та стратегії цю систему вкомплектовано основними документами [2, 3], що встановлюють розподіл повноважень. Водночас, виклики останніх років висвітили потребу в удосконаленні координації між суб’єктами. Наприклад, після атаки на держреєстри 2024 р. стало зрозуміло, що потрібна тісніша взаємодія між технічними фахівцями Держспецзв’язку та ІТ-службами окремих міністерств, регулярне проведення кібернавчань й аудитів безпеки. Позитивним кроком у цьому напрямку стало проведення впродовж

2023–2024 рр. серії міжвідомчих навчань «*Cyber Rapid Response*», де відпрацьовувалися спільні дії на випадок масованої кібератаки.

Технологічний захист державних інформаційних систем. Сучасні технологічні рішення у сфері кібербезпеки публічного управління можна умовно розподілити на профілактичні (попереджувальні) та реактивні (для виявлення і реагування на атаки). До перших належать, зокрема, засоби автентифікації та контролю доступу (апаратні токени, двофакторна а'тентифікація для держслужбовців, розмежування доступу на основі ролей), системи керування мережевою безпекою (міжмережеві екрани, системи запобігання вторгнень – IPS/IDS), захищений зв'язок (використання VPN, урядової криптографії для конфіденційного зв'язку). Після 2022 р. впроваджено централізовану систему керування оновленнями і патчами для критичних державних систем, щоб знизити ризик експлуатації відомих вразливостей – раніше деякі мережі держорганів не встигали вчасно оновлювати ПЗ, чим і користувалися хакери.

Особливої уваги надано резервуванню та дублюванню даних. Трагедія війни змусила подбати про те, щоб ключові державні реєстри та бази даних мали резервні копії поза межами основних центрів оброблення. У цьому контексті реалізовано проєкт так званих «електронних державних резервних копій за кордоном» (зокрема, створено Data Embassy – резервний дата-центр України в хмарній інфраструктурі в одній із європейських країн, за аналогією до естонської моделі). Такий підхід гарантує, що навіть у разі фізичного знищення серверів (від ракетного удару чи диверсії) інформацію не буде втрачено. Власне, випадок з реєстрами Мін'юсту продемонстрував ефективність резервування – дані громадян збереглися та їх було відновлені з бекапів.

Для оперативного виявлення вторгнень на державних об'єктах розгорнуто систему датчиків і моніторингу. Держспецзв'язку впровадила програмно-апаратний комплекс, що відстежує аномальну активність у

мережах державних органів і передає дані до центру кіберзахисту. Ця система в реальному часі аналізує трафік на предмет відомих сигнатур атак або підозрілих поведінкових моделей (наприклад, масового шифрування файлів, що може вказувати на вірус-шифрувальник). З 2022 р. значно розширено парк засобів SIEM (*Security Information and Event Management*), які дозволяють агрегувати журнали подій з різних серверів і мережевого обладнання, щоб виявляти комплексні атаки.

Коли виявлено кіберінцидент, надзвичайно важливо швидко реагувати й ліквідовувати наслідки. Тут на перший план виходять команди реагування на інциденти – CERT-UA та внутрішні CERT у відомствах. Вони використовують набір інструментів для аналізу шкідливого коду (дизасемблери, «*пісочниці*» для запуску підозрілих файлів), відстеження IP-адрес, що атакують, установлення *Indicators of Compromise* (IoCs). Після виявлення атаки розробляються «*імунітети*»: наприклад, у разі з *WRECKSTEEL* CERT-UA оперативно підготувала індикатори компрометації – хеші файлів, адреси серверів управління – і передала їх адміністраторам мереж для блокування [10]. Такий обмін інформацією дозволяє іншим органам завчасно виявити наявність загрози.

Варто зазначити, що українські фахівці дедалі більше використовують унікальний досвід, здобутий у реальних умовах війни, для вдосконалення технологій кіберзахисту. Наприклад, після масованих російських атак на енергетику та транспорт упродовж 2022–2023 рр. Держспецзв'язку разом з вітчизняними ІТ-компаніями розробили низку власних програмних рішень для аналізу телеметрії та аномалій, адаптованих під специфіку українських мереж. Так поступово формується національна школа кібербезпеки, здатна не лише використовувати закордонні продукти, а й створювати власні.

Рекомендації щодо вдосконалення системи кібербезпеки органів публічного управління. Аналіз ситуації дозволяє окреслити кілька

пріоритетних напрямків, на яких варто зосередитися для підвищення кіберстійкості державного управління України:

1. Удосконалення нормативно-правової бази та політики. Потрібно актуалізувати чинну Стратегію кібербезпеки з урахуванням досвіду 2022–2025 рр., передбачивши в ній більш конкретні заходи щодо захисту публічного сектору. Варто розробити галузеві стандарти кібербезпеки для органів влади (наприклад, обов'язкові профілі безпеки для електронних реєстрів, вимоги до хмарних сервісів, що використовуються держорганами). Доцільним є ухвалення підзаконних актів щодо обов'язкового інцидент-менеджменту: кожен орган має затвердити внутрішній план реагування на кібератаки і регулярно проводити навчання персоналу. Паралельно варто передбачити посилення відповідальності за кіберзлочини проти державних інформаційних ресурсів.

2. Посилення кадрового потенціалу. Кібербезпека – це передусім люди. Варто продовжити програми підготовки кадрів (курси, сертифікація CISSP, CEH тощо) як в Україні, так і за кордоном. Доцільно запровадити систему обміну IT-спеціалістами між різними органами (ротації) для поширення досвіду. Крім того, критично підвищувати кіберграмотність усіх державних службовців: регулярні тренінги з виявлення фішингу, правил безпечної роботи з інформацією повинні стати нормою.

3. Технічне переоснащення й оновлення інфраструктури. Державні IT-системи мають швидко переходити на сучасні програмні платформи із закладеними механізмами безпеки. Старі легасі-системи, що не підтримуються і вразливі, потрібно поступово замінювати або ізолювати. Потрібно масштабувати використання багатофакторної автентифікації, шифрування даних «*на спокої*» (data at rest) та в транзиті, запроваджувати концепцію Zero Trust в урядових мережах (кожен запит на доступ перевіряється, користувачі мають мінімальні привілеї). Розширення системи резервного копіювання на більше число критичних систем – ще

одна запорука стійкості. Доцільно також створити резервні вузли зв'язку між основними органами на випадок, якщо звичайні канали буде виведено з ладу (наприклад, супутникові термінали як резерв для урядового зв'язку).

4. Удосконалення міжвідомчої взаємодії. Попри наявність НКЦК, варто налагодити швидший обмін технічною інформацією про інциденти на робочому рівні. Для цього можна створити єдину захищену платформу (портал) для повідомлення про інциденти, доступну всім уповноваженим адміністраторам держорганів. При виникненні атаки відповідний орган влади повинен негайно ділитися інформацією через цю платформу, щоб інші могли перевірити в себе аналогічні ознаки. Потрібно також розширити формат кібернавчань: проводити не лише навчання всередині країни, а й спільні міжнародні – залучати команди ЄС, НАТО (у межах тих же CRRT чи програм Трастового фонду). Це дасть змогу відпрацювати сценарії колективного реагування, коли українські та закордонні фахівці спільно протидіють атаці.

5. Міжнародна правова та практична підтримка. Україна має й надалі активно брати участь у формуванні міжнародних правил відповідальності за кібернапади. Належна документалізація й передача доказової бази щодо російських кібератак до міжнародних судових інстанцій (Міжнародний суд ООН, МКС) сприятиме визнанню таких дій актом агресії і тероризму на глобальному рівні. Паралельно треба поглиблювати співпрацю з союзниками: розглянути можливість двосторонніх угод про взаємодопомогу в кіберпросторі, участі українських фахівців у кіберцентрах інших країн і навпаки. Інтенсивний обмін розвідданими про кіберзагрози з партнерами допоможе вийти на випереджувальний рівень – отримувати попередження про підготовку атак.

Отже, реалізація цих рекомендацій має комплексний характер – від оновлення політики до впровадження технологій та навчання людей. Важливо розуміти, що кібербезпека – це не одноразовий проєкт, а

неперервний процес, що вимагає адаптації до нових умов. Гібридна війна продовжує еволюціонувати, а разом з нею і засоби нападу та захисту в кіберпросторі. Тільки завдяки проактивному, скоординованому підходу Україна зможе захистити свої органи публічного управління від невидимого, але дуже відчутного ворога – ворожих хакерів.

Висновки. Підсумовуючи, можна констатувати: кібербезпека органів публічного управління в умовах гібридних загроз стала одним із визначальних фронтів забезпечення національної безпеки. Україна вимушена в прискореному режимі вдосконалювати свою систему кіберзахисту – і досягла помітного прогресу, попри небувалий тиск. Проте загроза далека від зникнення. Потрібно реалізувати комплекс запропонованих заходів – від оновлення політик до технічних рішень та міжнародної адвокації – аби гарантувати, що державний апарат буде функціонувати стійко навіть під натиском найпотужніших кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Balmforth T. Russian hackers were inside Ukraine telecoms giant for months – cyber spy chief. *Reuters.* 2024. Jan 5. URL: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163–VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

3. Стратегія кібербезпеки України на 2021–2025 роки / Рада нац. безпеки і оборони України; введена в дію Указом Президента України від 26.08.2021 р. № 447/2021. Київ, 2021. 25 с.

4. Antoniuk Daryna. Latest gambit for Gamaredon : Fake Ukraine troop movement documents. *The Record (RFN).* 2025. Mar 31. URL:

https://therecord.media/gamaredon-phishing-campaign-fake-ukraine-documents-remcos.

5. Fornusek M. SBU : Ukraine gathers evidence for ICC on Russian GRU hackers behind Kyivstar cyberattack. *The Kyiv Independent*. 2024. Apr 4. URL: https://kyivindependent.com/sbu-russian-hackers-behind-kyivstar.

6. Кібератака на державні реєстри України. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_державні_реєстри_України_(2024).

7. У Мін'юсті заявили про відновлення роботи Держреєстрів після масштабної кібератаки. *УНІАН.* 2025. 20 січня. URL: https://www.unian.ua/society/kiberataka-na-min-yust-derzhavni-reyestri-vidnovili-robotu-12889875.html.

8. Antoniuk D. Hackers hit Ukrainian state agencies, critical infrastructure with new «Wrecksteel» malware. *The Record (Recorded Future News)*. 2025. April 3. URL: https://therecord.media/hackers-ukraine-critical-infrastructure-malware.

9. Stahie S. WRECKSTEEL Campaign Uses Fake HR Emails to Spy on Ukrainian Government Systems. *Bitdefender Hot for Security*. 2025. April 4. URL: https://www.bitdefender.com/en-us/blog/hotforsecurity/wrecksteel-fake-emails-spy-ukrainian.

10. CERT-UA. 2025. Recommended actions regarding WRECKSTEEL malware (Alert Report). In Security Affairs (Pierluigi Paganini, Ed.). 2025. URL: https://securityaffairs.com/176181/cyber-warfare-2/cert-ua-reports-attacks-in-march-2025-targeting-ukrainian-agencies-with-wrecksteel-malware.html.

REFERENCES

1. Balmforth T. (2024). Russian hackers were inside Ukraine telecoms giant for months – cyber spy chief. *Reuters.* Jan 5. URL:

https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04. [in English]

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy (2017) : Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163–VIII. *Vidomosti Verkhovnoi Rady Ukrainy*. № 45. St. 403. [in Ukrainian]

3. Stratehiia kiberbezpeky Ukrainy na 2021–2025 roky (2021) / Rada nats. bezpeky i oborony Ukrainy; vvedena v diiu Ukazom Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. Kyiv, 25 s. [in Ukrainian]

4. Antoniuk Daryna. (2025). Latest gambit for Gamaredon : Fake Ukraine troop movement documents. *The Record (RFN*). Mar 31. URL: https://therecord.media/gamaredon-phishing-campaign-fake-ukraine-documents-remcos. [in English]

5. Fornusek M. (2024). SBU : Ukraine gathers evidence for ICC on Russian GRU hackers behind Kyivstar cyberattack. *The Kyiv Independent*. Apr 4. URL: https://kyivindependent.com/sbu-russian-hackers-behind-kyivstar. [in English]

6. Kiberataka na derzhavni reiestry Ukrainy (2024). Wikipediia. URL: https://uk.wikipedia.org/wiki/Кібератака_на_державні_реєстри_України_(2024). [in Ukrainian]

7. U Min`iusti zaiavyly pro vidnovlennia roboty Derzhreiestriv pislia masshtabnoi kiberataky. (2025). *UNIAN*. 20 sichnia. URL: https://www.unian.ua/society/kiberataka-na-min-yust-derzhavni-reyestri-vidnovili-robotu-12889875.html. [in Ukrainian]

8. Antoniuk D. (2025). Hackers hit Ukrainian state agencies, critical infrastructure with new «Wrecksteel» malware. The Record (Recorded Future News). April 3. URL: https://therecord.media/hackers-ukraine-critical-infrastructure-malware. [in English]

9. Stahie S. (2025). WRECKSTEEL Campaign Uses Fake HR Emails to Spy on Ukrainian Government Systems. Bitdefender Hot for Security. April 4.

URL: https://www.bitdefender.com/en-us/blog/hotforsecurity/wrecksteel-fake-emails-spy-ukrainian. [in English]

10. CERT-UA. (2025). Recommended actions regarding WRECKSTEEL malware (Alert Report). In Security Affairs (Pierluigi Paganini, Ed.). URL: https://securityaffairs.com/176181/cyber-warfare-2/cert-ua-reports-attacks-in-march-2025-targeting-ukrainian-agencies-with-wrecksteel-malware.html. [in English]