ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ / ORGANIZATIONAL & LAW INFORMATION SECURITY

DOI: 10.18372/2225-5036.28.17366

АНАЛІЗ СИСТЕМНИХ І ПЕРСОНІФІКОВАНИХ ФАКТОРІВ ОРГАНІЗАЦІЙНО-РЕСУРСНИХ УМОВ ДІЯЛЬНОСТІ ІЗ ЗАБЕЗПЕЧЕНОСТІ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ І КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Олександр Потій[1], Олександр Бакалинський[2], Данило Мялковський[3], Денис Верба[4]

[1,2,3] Державна служба спеціального зв'язку та захисту інформації України

[4] Київський національний економічний університет імені Вадима Гетьмана

ПОТІЙ Олександр Володимирович, д. т. н., професор
Рік та місце народження: 1971 р., м. Кривий Ріг, Україна.
Освіта: Харківське вище військове командно-інженерне училище ракетних військ.
Посада: заступник Голови Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: комп'ютерна безпека, криптографія, кібербезпека критичної інфраструктури, вища освіта, бізнес-інформатика.
Публікації: більше 150 наукових публікацій у галузі інформаційної, кібербезпеки, криптографії, серед яких наукові статті, монографії, підручники та навчально-методичні посібники, патенти на корисні моделі.
E-mail: potav1971@gmail.com.
ORCID ID: 0000-0002-2366-0541.

БАКАЛИНСЬКИЙ Олександр Олегович, к. т. н.
Рік та місце народження: 1970 р., м. Київ, Україна.
Освіта: Київський військовий інститут управління та зв'язку, Національна академія Служби безпеки України.
Посада: заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: системи управління інформаційною безпекою, управління ризиками, кібербезпека критичної інфраструктури, вища освіта.
Публікації: більше 60 наукових публікацій у галузі інформаційної, кібербезпеки, серед яких наукові статті, монографії, підручники та навчально-методичні посібники, патенти на корисні моделі.
E-mail: baov@meta.ua.
ORCID ID: 0000-0001-9712-2036.

МЯЛКОВСЬКИЙ Данило Владиславович, к. д. у.
Рік та місце народження: 1971 р., м. Київ, Україна.
Освіта: Київський військовий інститут управління та зв'язку, Національна академія державного управління при Президентові України.
Посада: директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: державне управління у сфері кібербезпеки, захисту інформації, безпеки електронних послуг.
Публікації: більше 20 наукових публікацій, серед яких 12 наукових статей, в тому числі 4, виданих в іноземних наукових виданнях.
E-mail: daniilvm71@gmail.com.
ORCID ID: 0000-0002-8246-8437.

ВЕРБА Денис Володимирович, к.е.н., доцент
Рік та місце народження: 1974 р., м. Київ, Україна.
Освіта: Київський національний економічний університет імені Вадима Гетьмана.
Посада: доцент ДВНЗ «КНЕУ імені Вадима Гетьмана».
Наукові інтереси: економіка соціальної сфери, оцінювання державних програм та політики.
Публікації: більше 60-ти наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: denys.verba@kneu.ua.
ORCID ID: 0000-0002-8712-4027.

Анотація. *Стаття присвячена підходам до забезпечення адекватності ресурсного забезпечення діяльності з кіберзахисту органів державної влади та об'єктів критичної інфраструктури об'єктивним вимогам досягнення нормативного (визначеного Стратегією кібербезпеки України та ЗУ «Про основи забезпечення кібербезпеки в Україні») рівня дієвості та ефективності національної системи кіберзахисту. В статті використовується факторний аналіз організаційно-ресурсних факторів потенційно досяжного і фактично реалізованого рівня кіберзахисту державних установ і об'єктів критичної інфраструктури. Фактори структуровані на дві групи: системні і персоніфіковані. Перші виражають міру відповідності передбачених чинними нормативно-правовими актами регламентів взаємодії учасників та норм ресурсного забезпечення діяльності з кіберзахисту органів державної влади та об'єктів критичної інфраструктури актуальним завданням та об'єктивним потребам досягнення бажаного рівня кібербезпеки. Другі – міру реалізації того потенціалу, що створюється наявними регламентами й нормами. Обґрунтовано, що посилення впливу вертикалі реалізації централізованої національної політики кібербезпеки для компенсації надмірної диференціації організаційно-ресурсних умов діяльності з кіберзахисту, зумовленої специфікою ресурсних можливостей та організаційних рішень певного ОДВ, є вагомим джерелом резервів наближення до нормативного рівня кібербезпеки ОДВ та критичної інфраструктури в Україні. Зокрема, відсутність безперервного ланцюжка передавання управлінських сигналів та забезпечення обігу інформації між об'єктами і суб'єктами управління від центру формування політики кібербезпеки в органах державної влади до центрів їх реалізації та врахування специфіки відповідної галузі, унеможливлює досягнення нормативного рівня кібербезпеки в органах державної влади України.*

Ключові слова*: кібербезпека, організаційно-ресурсні умови, органи державної влади, служби інформаційної безпеки.*

Постановка проблеми

Забезпечення кібербезпеки органів державної влади та об'єктів критичної інфраструктури вимагає залучення відповідних людських і технічних ресурсів, а реалізація потенціалу таких ресурсів – адекватних регламентів, норм і правил взаємодії всіх груп учасників експлуатації інформаційних технологій (ІТ). Відповідно, оцінювання достатності ресурсного забезпечення діяльності з кіберзахисту органів державної влади та об'єктів критичної інфраструктури виступає необхідною умовою наближення системи кіберзахисту до нормативного (визначеного Стратегією кібербезпеки України та ЗУ «Про основи забезпечення кібербезпеки в Україні [1, 2]) рівня дієвості та ефективності національної системи кіберзахисту.

Відповідно метою цього дослідження є визначення впливу організаційно-ресурсних умов діяльності з кіберзахисту в органах державної влади на потенційно досяжний і фактично реалізований

рівень кіберзахисту державних установ і об'єктів критичної інфраструктури.

Аналіз літератури

Це стаття містить результати розвитку концепції організаційно-технічної моделі кіберзахисту [3]. Власне апробацію інструментарію оцінювання організаційно-технічних умов діяльності з кіберзахисту органів державної влади та об'єктів критичної інфраструктури. Центральна теза цієї роботи: рівень захищеності інформаційно-комунікаційних систем (ІКС), здатність служб захисту інформації (інформаційної безпеки) адекватно реагувати на загрози визначається наявністю фахівців необхідної кваліфікації (перша – абсолютно необхідна умова) та досконалістю організаційно-технічного забезпечення їх діяльності (відповідність регламентів, форм організації їх роботи – як зафіксованих в нормативних та методичних документах [4-6], так і втілених в усталених практиках та процедурах діяльності служб експлуатації ІТ державних установ). Ця концепція виходить з критичної важливості забезпеченості будь якої функції державних установ персоналом необхідної кваліфікації [7-10] та тлумачення організаційно-технічних умов діяльності персоналу – як системи факторів, що визначає міру реалізації того потенціалу, що заданий фактичною забезпеченістю служб захисту інформації персоналом [11-14]. Таким чином, ця стаття доповнює наведену вище літературу, бо містить апробацію інструментарію оцінки того, наскільки наявний рівень забезпеченості служб захисту інформації персоналом відповідає зафіксованим в чинних нормативно-правових та програмно-методичних документах вимогам та наскільки поширені серед державних структур явні (ті, що визначаються навіть на рівні первинного аналізу базових показників) відхилення від доцільних організаційно-технічних умов використання людського потенціалу служб захисту інформації.

Виклад основного матеріалу дослідження

Досліджені органи державної влади (ОДВ) суттєво диференціюються за масштабами інформаційно-телекомунікаційних мереж та кількістю користувачів ІТС. Переважну більшість з 41-єї установи становлять порівняно невеликі за чисельністю працівників і кількістю робочих станцій та їх користувачів: 23 установи з чисельністю працівників до 300 осіб (на зайнятих у цих 23-ьох ОДВ працівників припадає 5,1% загальної чисельності працівників досліджених ОДВ). Ще 13 ОДВ мають чисельність працівників від 300 до 1000 осіб (на їх персонал припадає 9,7% загальної чисельності працівників ОДВ). Нарешті п'ять установ з чисельністю працівників більше 1000 осіб сумарно забезпечують зайнятість 85,2% з усіх працівників досліджених ОДВ. Внески малих за розмірами мережі (але переважаючих за кількістю серед досліджених ДВ), середніх і великих організацій наведені на рис. 1.

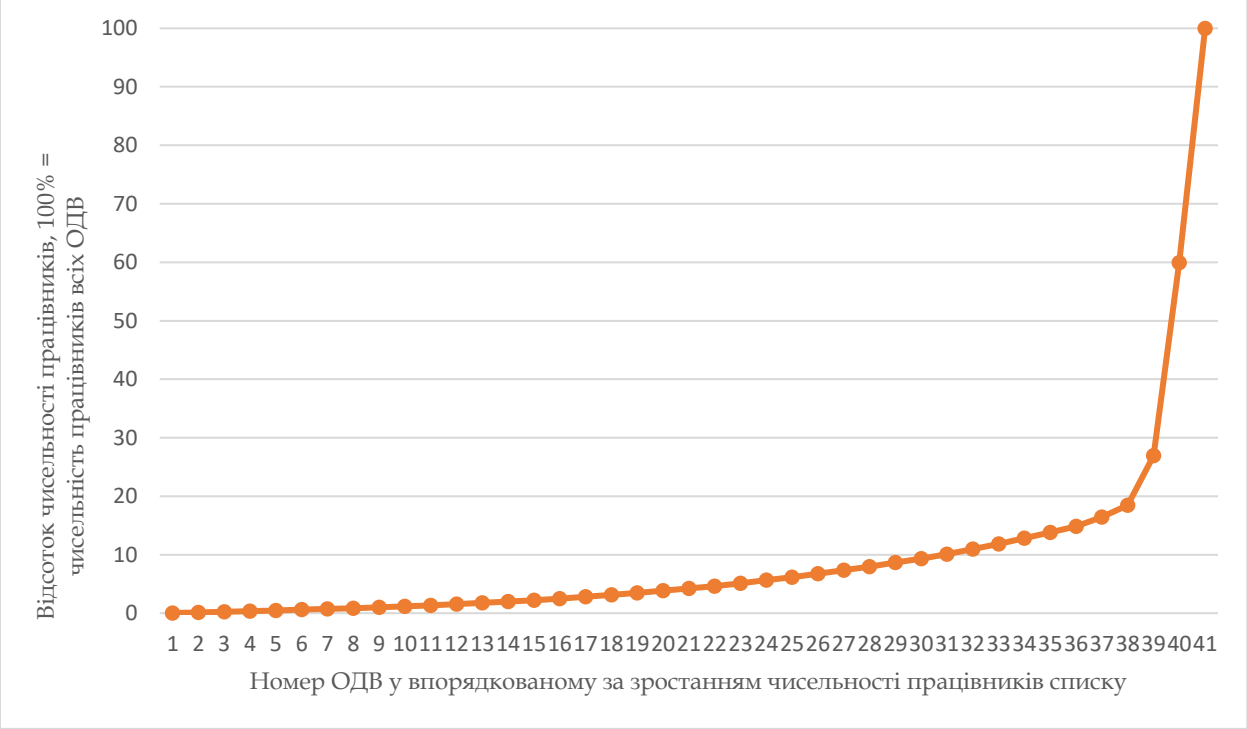

Рис. 1 Чисельність працівників органів державної влади (ОДВ), охоплених дослідженням організаційно-ресурсного забезпечення IT та IS діяльності накопичувальним підсумком

Надалі характеристики організаційно-ресурсних умов діяльності з експлуатації ІТС та забезпечення кібербезпеки будуть трактуватись виходячи з таких вихідних положень. Міра розкиду, диференціації індивідуальних характеристик організаційно-ресурсних умов по окремих ОДВ навколо середніх показників відображає силу впливу (вагомість) організаційних факторів, пов'язаних зі специфічними умовами певного ОДВ. Відповідно, чим більш однорідні (близькі) індивідуальні показники ОДВ – тим вищий вплив централізації та стандартизації умов діяльності з експлуатації ІТ та забезпечення кібербезпеки. Чим більший розкид індивідуальних показників – тим сильніші фактори специфічних, індивідуальних умов певного ОДВ, що можуть знижувати суспільну ефективність використання кращих, доступних за наявних норм ресурсного забезпечення, технічних рішень. Відповідно, висока диференціація індивідуальних характеристик організаційно-ресурсних умов діяльності з експлуатації ІТ та забезпечення кібербезпеки свідчить, що посилення централізованого мережевого керування має усунути негативні фактори, які виникають в окремих ОДВ, завдяки зростанню стандартизації організаційних умов, та посиленню централізації формування інституціональних умов діяльності з експлуатації ІТ та забезпечення кібербезпеки.

Щоб характеристики розкиду були змістовними та відображали саме вплив інституціональних факторів: тих, що виражають вплив централізованих інститутів (виражаються через зростання стандартизації і зменшення розкиду індивідуальних показників) і тих, що формуються специфікою окремих ОДВ (виражаються через зростання розкиду індивідуальних показників) середні показники розраховано як по всіх досліджених ОДВ, так і по групах найменших (з чисельністю працівників до 300 осіб), середніх (чисельність працівників від 300 до тисячі осіб) і найбільших (чисельність понад тисячу осіб) ОДВ.

Основні показники навантаження на ресурсний потенціал служб ІТ та IS ОДВ зведені до таблиці 1 (таблиця 1 не публікується з міркувань безпеки, показники можуть бути надані авторами за запитом зацікавлених осіб).

Показники таблиці свідчать, що навантаження на ресурси служб ІТ та IS ОДВ високо диференційовано. По невеликих ОДВ (з чисельністю працівників до 300 осіб) кількість користувачів на одного працівника служби ІТ в середньому дорівнює 47.7 особи (табл. 2). По середніх (з чисельністю працівників більше 300, але менше 1000 осіб) на одного працівника служби ІТ припадає 155,8 користувачів ІТС. По найбільш за чисельністю працівників ОДВ аналогічний показник дорівнює 49,6 осіб. При цьому, в середині усіх виділених груп показники також високо диференційовані: по найменших за чисельністю працівників ОДВ – від 5 до 192 користувачів на одного працівника ІТ, по середніх (більше 300 менше тисячі працівників) – від 5-ти до 248-ми, по найбільших – від 1,1 до 126,1.

Аналогічний за змістом показник – кількість робочих станцій на одного працівника служби ІТ, також демонструє високу диференціацію, яка не може бути пояснена логікою забезпечення ресурсами потреб малих і великих фірм. По найменших ОДВ на одного працівника служби ІТ припадає від 4,6 до 203,0 робочих станцій, по середніх – від 20,9 до 550,0, по найбільших – від 5-ти до 298,7 штук робочих станцій на одного працівника служби ІТ.

Аналогічна зависока диференціація показників навантаження на чисельність працівників спеціалізованої служби властива й для служби кібербезпеки: і чисельність користувачів, і кількість робочих станцій, що припадає на одного працівника служби кібербезпеки по окремих ОДВ суттєво відрізняється і від середнього по всіх досліджених ОДВ, і від середнього по групі ОДВ з близькими показниками чисельності працівників.

Так, якщо в середньому по усіх досліджених ОДВ на одного працівника служби кібербезпеки припадає 129,2 користувача ІТС та 129,2 робочих станції, то по невеликих ОДВ (з чисельністю працюючих менше 300 осіб) ці показники коливаються від 7,6 до 146,5 по чисельності користувачів на працівника служби кібербезпеки і від 8,1 до 102,0 – по кількості робочих станцій. По середніх ОДВ кількість робочих станцій на одного працівника служби кібербезпеки коливається від 83,8 до 1830,1, а чисельність користувачів на одного працівника служби – від 44,4 до 297.

Відповідно, проведене дослідження виявило, що стандартизації навантаження на ресурсне забезпечення служби експлуатації ІТ та кібербезпеки із масштабами завдань по різних ОДВ явно не спостерігається. Служби ІТ та кібербезпеки скоріше відображають високо специфічні, індивідуальні підходи відповідних ОДВ до проблем забезпечення ІТ та кібербезпеки, ніж функціонують як елементи централізованої і стандартизованої системи. Вертикальна складова формування моделі експлуатації ІТ та забезпечення кібербезпеки виражена явно слабше, ніж проявляє себе їх горизонтальна диференціація.

Наведена теза проявляється в усіх характеристиках організації служб експлуатації ІТ та забезпечення кібербезпеки в ОДВ. Зокрема, не спостерігається однорідності у характеристиках організаційних параметрів діяльності в сфері ІТ та кібербезпеки (табл. 3). Так рольова модель управління ІТ реалізована лише в 70,7% загальної кількості обстежених ОДВ. Служба кіберзахисту виділена у самостійний структурний підрозділ лише у 63,4% обстежених ОДВ.

Принципи раціональної спеціалізації стосовно служби експлуатації ІТ дотримуються лише у 51,2% ОДВ (майже в половині з їхньої загальної кількості служби ІТ виконують і не специфічні функції, пов'язані з документообігом, мобілізаційною роботою, завданнями господарчої діяльності тощо). Аналогічний показник стосовно служби кіберзахисту становить 58,5% (майже 42% ОДВ завантажують служби кіберзахисту виконанням не специфічних функцій). Особа, або структурний підрозділ відповідальний за ідентифікацію об'єктів критичної інформаційної інфраструктури в секторі/підсекторі економіки, визначені лише у 87,8% ОДВ. Значущою ми вважаємо відсутність переваг за характеристиками організаційного рівня діяльності з експлуатації ІТ та кіберзахисту у великих за чисельністю працюючих ОДВ. Їхні служби експлуатації ІТ та кіберзахисту більше, ніж по середніх та малих ОДВ завантажені невластивими для них функціями (у 60% випадків). Також у 20% випадків немає особи, чи підрозділу, який відповідав за визначення об'єктів критичної інфраструктури.

Все це ознаки невідповідності саме інституціональних умов діяльності з експлуатації ІТ та забезпечення кібербезпеки, що формуються за нестачі централізованого впливу, що забезпечить стандартизацію ресурсного забезпечення цих напрямів діяльності на основі врахування масштабів виконуваних завдань, ризиків та загроз, протидія яким забезпечується в межах такої діяльності та оцінки можливих втрат від неспроможності дати адекватну відповідь на актуальні виклики.

Таблиця 1

Середні по групах ОДВ показники навантаження на ресурсне забезпечення діяльності з експлуатації ІТ та забезпечення кібербезпеки

Кількість за чисельністю працівників ОДВ	Масштаб ІТС ОДВ (чисельність працівників = внутрішніх користувачів)	характеристики навантаження на ресурси служби експлуатації ІТ			характеристики навантаження на ресурси служби кіберзахисту	
		чисельність користувачів на одного працівника служби ІТ	кількість інформаційно-телекомунікаційних систем (ІТС) на одного працівника ІТ	кількість робочих станцій на працівника ІТ	кількість робочих станцій на працівника служби	чисельність користувачів на одного працівника служби
Середній по 5-ти найбільших за чисельністю працівників ОДВ	10562,0	49,6	0,4	59,7	244,3	204,6
Середній по 13-ти середніх за чисельністю працівників ОДВ	463,9	155,8	1,2	156,2	314,3	149,2
Середній по 23-ох найменших за чисельністю працівників ОДВ	137,4	47,7	0,8	53,2	50,9	52,2

Таблиця 2

Показники організаційних параметрів діяльності з експлуатації ІТ та забезпечення кібербезпеки по групах ОДВ

Визначення за чисельністю працівників ОДВ	Рольова модель управління ІТ реалізована	Наявна та функціонує виокремлена спеціалізована служба кіберзахисту	Служба експлуатації ІТ не виконує невластиві для неї функції	Служба кіберзахисту не виконує невластиві для неї функції	Наявна особа чи підрозділ відповідальний за визначення об'єктів критичної інфраструктури
По 5-ти найбільших за чисельністю працівників ОДВ, %	100,00	100,00	40,00	40,00	80,00
По 13-ти середніх за чисельністю працівників ОДВ, %	76,92	69,23	46,15	61,54	84,62
По 23-ох найменших за чисельністю працівників ОДВ, %	60,87	52,17	56,52	60,87	91,30

Таблиця 3

Оцінки відповідності наявних організаційно-ресурсних умов діяльності з кіберзахисту органів державної влади об'єктивним потребам досягнення нормативного рівня кібербезпеки

Установи	**Узагальнююча оцінка**	**Оцінка по системних факторах**	**Оцінка по персоніфікованих факторах**
Установа 1	0,267	0,333	0,167
Установа 2	0,607	0,604	0,611
Установа 3	0,604	0,450	0,833
Установа 4	0,547	0,467	0,667
Установа 5	0,480	0,467	0,500
Установа 6	0,538	0,563	0,500
Установа 7	0,625	0,598	0,667
Установа 8	0,437	0,506	0,333
Установа 9	0,412	0,353	0,500
Установа 10	0,273	0,010	0,667
Установа 11	0,537	0,339	0,833
Установа 12	0,361	0,380	0,333
Установа 13	0,339	0,232	0,500
Установа 14	0,348	0,468	0,167
Установа 15	0,845	0,889	0,780
Установа 16	0,775	0,699	0,889
Установа 17	0,200	0,222	0,167
Установа 18	0,531	0,395	0,733
Установа 19	0,545	0,687	0,333
Установа 20	0,133	0,111	0,167
Установа 21	0,487	0,478	0,500
Установа 22	0,554	0,571	0,528
Установа 22	0,298	0,385	0,167
Установа 23	0,544	0,462	0,667
Установа 24	0,174	0,124	0,250
Установа 25	0,267	0,333	0,167
Установа 26	0,604	0,562	0,667
Установа 27	0,428	0,380	0,500
Установа 28	0.872	0.787	1.000
Установа 29	0.645	0.574	0.750
Установа 30	0.884	0.850	0.936
Установа 31	0.440	0.456	0.417
Установа 32	0.560	0.462	0.708
Установа 33	0.530	0.578	0.458
Установа 34	0.387	0.533	0.167
Установа 35	0,267	0,444	0,000

Установа 36	0,614	0,566	0,686
Установа 37	0,357	0,151	0,667
Установа 38	0,663	0,264	1,262
Установа 39	0,726	0,805	0,607
Установа 40	0,499	0,346	0,729
Середні оцінки усій сукупності обстежених ОДВ	**0,493**	**0,461**	**0,541**

По всіх 16-ти використаних критеріях оцінки зведені до таблиці 3. Середнє по всіх 41-ій державній установі значення по всіх 16-ти оцінках – 0,493. Зокрема, по системних факторах – 0,46, а по персоніфікованих – 0,54.

Це значить, що інтегральний рівень відповідності нормативних організаційно-економічних умов об'єктивним потребам досягнення нормативного рівня кібербезпеки органів державної влади менше 50%, а рівень використання того потенціалу, що створюють чинні нормативні значення організаційно-економічних показників – близько 54%.

Наявність у органу державної влади такої ознаки як існування СЗІ виступає чинником підвищення як інтегральної оцінки умов діяльності з забезпечення кіберзахисту, так і системних, і персоніфікованих факторів. Так, по 26-ти органам державної влади з 41-го охопленого дослідженням, наявні служби захисту інформації, по 15-ти – вони відсутні.

Інтегральні оцінки факторів розраховані окремо по 26-ти органах державної влади зі створеними СЗІ, 15-ти органах державної влади, де такі служби відсутні та по всіх 41-му, охоплених дослідженням зведені в таблицю 4.

Таблиця 4

Оцінки відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту в ОДВ вимогам досягнення нормативного рівня кібербезпеки

Органи державної влади	**Узагальнююча оцінка**	**Оцінка по системних факторах**	**Оцінка по персоніфікованих факторах**
Органи державної влади (ОДВ), де існують СЗІ (інформаційної безпеки)	0,567	0,554	0,586
ОДВ, де СЗІ відсутня	0,386	0,334	0,464
Всі охопленні дослідженням ОДВ	0,493	0,461	0,541
Відношення середнього показника по ОДВ, де існують СЗІ до аналогічного показника по ОДВ, де вони відсутні	146,891	165,868	126,293

По всіх респондентах з установ, де наявна СЗІ, оцінка умов діяльності з забезпечення кібербезпеки дорівнює 0,567. Оцінка по системних факторах – 0,554, по персоніфікованих – 0,586. Водночас, по органах державної влади, де СЗІ не створена, інтегральна оцінка, узагальнена по всіх органах державної влади дорівнює 0,386, по системних факторах – 0,334, по випадкових – 0,464.

Відповідно, наявність СЗІ суттєво підвищує як відповідність нормативних параметрів діяльності з забезпечення кіберзахисту об'єктивним потребам, так і міру реалізації того потенціалу, що дають чинні норми витрачання ресурсів та організаційні регламенти. Проте сама по собі наявність спеціального структурного підрозділу не гарантує досягнення нормативного рівня кібербезпеки. Навіть інтегральна (усереднена) оцінка відповідності фактичних умов діяльності з забезпечення кібербезпеки держустанов зі створеною СЗІ становить 56,7% – тобто середній рівень відповідності фактичних умов об'єктивно потрібним для досягнення нормативного рівня кібербезпеки становить менше 60%.

При цьому, 8 охоплених дослідженням ОДВ (19,5% загальної кількості) мають інтегральну оцінку відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту менше 33% (це значить, що менше третини оцінюваних параметрів в цих установах відповідають об'єктивно необхідним для досягнення нормативного рівня кібербезпеки), 28 (68,3%) – оцінку відповідності від 33% до 66% (менше двох третин параметрів відповідають об'єктивно необхідним вимогам) і лише 5 ОДВ (12,20%) мають оцінку вище 66%. Максимальна інтегральна оцінка по всіх факторах (всіх організа-

ційно-ресурсних умовах) дорівнює 88%, мінімальна – 13%. По системних факторах аналогічний розподіл загальної кількості обстежених ОДВ виглядає так: 7 (17,1%) ОДВ мають оцінку нижче 33%, 28 (68,3%) – оцінку вище і дорівнює 33% нижче 66% і 6 ОДВ (14,6%) – оцінку вище 66%. Максимальна оцінка – 89%, мінімальна – 0,99%.

По персоніфікованих факторах – 9 ОДВ (22,0%) мають оцінку менше 33%, 14 (34,15%) оцінку вищу, чи рівну 33%, але нижчу 66% і 18 (43,9%) – вище 66%. При цьому, наявний єдиний ОДВ, що одержав оцінку «100%» – відсутні негативні відхилення від організаційно-ресурсних умов діяльності з кіберзахисту. Наявність такої оцінки свідчить, що задані параметри не є завищеними – їх досягнення реальне, а відхилення виражають недоліки індивідуальних умов в певних ОДВ від кращих можливих.

Вагомі відхилення від оптимальних організаційно-ресурсних умов діяльності з кіберзахисту по системних параметрах свідчать про відсутність єдиного стандарту реалізації політики кібербезпеки в ОДВ – специфічні фактори певної ОДВ мають більший вплив на організаційно-ресурсні умови діяльності з кіберзахисту, ніж централізовано розроблені норми і регламенти. Така відсутність стандартизації організаційно-ресурсних умов діяльності з кіберзахисту виступає ознакою відсутності єдиної дієвої вертикалі руху інформації (керуючих та регламентуючих сигналів від центрів формування політики кіберзахисту до певних ОДВ та «відклику», про перебіг адаптації такої політики до умов конкретного ОДВ й установ сфери його відповідальності – від ОДВ до центру формування політики кіберзахисту). Аналогічні показники розподілу для ОДВ, де створено СЗІ та по ОДВ, де такі служби не створені зведені до таблиць 5 – 7.

Дані таблиць 3 – 5 свідчать, що створення СЗІ виступає, в першу чергу, фактором зниження частки ОДВ, що мають вкрай низькі оцінки відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту необхідним для досягнення нормативного рівня кібербезпеки. Проте наявності такої служби є не достатньою для вирішення проблеми замалої частки ОДВ, що мають високі оцінки відповідності (вище 0,66) – навіть по групі ОДВ із створеними СЗІ частка таких установ не перевищує 19,2% по інтегральній оцінці (всі фактори), 23% – по оцінках системних факторів і 47% – по оцінках специфічних факторів.

Відповідно, обумовленість організаційно-ресурсних характеристик діяльності з кіберзахисту належністю до певного ОДВ сильніша за обумовленість належністю до єдиної системи кіберзахисту. Якщо перша зумовлює диференціацію таких характеристик (при цьому без прямого зв'язку зі складністю та масштабністю завдань забезпечення кібербезпеки в межах певного ОДВ, чи вартістю ризиків неготовності системи кіберзахисту протистояти загрозам), то друга – як раз сприяє вирівнюванню організаційно-ресурсних умов діяльності з кіберзахисту в розрахунку на «одиницю складності й масштабності завдань зі забезпечення кібербезпеки в певному ОДВ та сфері його регулювання». Отже посилення впливу вертикалі реалізації централізованої національної політики кібербезпеки для компенсації надмірної диференціації організаційно-ресурсних умов діяльності з кіберзахисту, що зумовлюється специфікою ресурсних можливостей та організаційних рішень певного ОДВ, є вагомим джерелом резервів наближення до нормативного рівня кібербезпеки ОДВ та критичної інфраструктури в Україні.

Таблиця 5

Розподіл загальної кількості ОДВ за розмірами інтегральних оцінок відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту об'єктивно необхідним для досягнення нормативного рівня кібербезпеки.

Органи державної влади	Мають оцінки відповідності менше 0,33 (до 33% параметрів відповідають вимогам)		Мають оцінки відповідності від 0,33 до 0,66		Мають оцінки відповідності більше 0,66	
	од.	**%**	**од.**	**%**	**од.**	**%**
Всі ОДВ, охоплені дослідженням	7	19,51	29	68,29	5	12,20
ОДВ, де створені СЗІ	1	3,85	20	76,92	5	19,23
ОДВ, де не створені СЗІ	6	40	9	60	0	0

Таблиця 6

Розподіл загальної кількості ОДВ за розмірами оцінок системних факторів відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту об'єктивно необхідним для досягнення нормативного рівня кібербезпеки.

Органи державної влади	Мають оцінки відповідності менше 0,33 (до 33% параметрів відповідають вимогам)		Мають оцінки відповідності від 0,33 до 0,66		Мають оцінки відповідності більше 0,66	
	од.	%	**од.**	%	**од.**	%
Всі ОДВ, охоплені дослідженням	6	17,07	28	68,29	7	14,63
ОДВ, де створені СЗІ	0	0,00	20	76,92	6	23,08
ОДВ, де не створені СЗІ	6	40,00	8	53,33	1	6,67

Таблиця 7

Розподіл загальної кількості ОДВ за розмірами оцінок персоніфікованих факторів відповідності фактичних організаційно-ресурсних умов діяльності з кіберзахисту об'єктивно необхідним для досягнення нормативного рівня кібербезпеки.

Органи державної влади	Мають оцінки відповідності менше 0,33 (до 33% параметрів відповідають вимогам)		Мають оцінки відповідності від 0,33 до 0,66		Мають оцінки відповідності більше 0,66	
	од.	%	**од.**	%	**од.**	%
Всі ОДВ, охоплені дослідженням	9	21,95	14	34,15	18	43,90
ОДВ, де створені СЗІ	2	7,69	12	46,15	12	46,15
ОДВ, де не створені СЗІ	7	46,67	2	13,33	6	40,00

Діяльність в сфері кіберзахисту нерозривно пов'язана з процесами використання інформаційних технологій і може тлумачитись як її компонент, проте в контексті оптимізації ресурсного забезпечення та регламентів взаємодії учасників такої діяльності відносини між сектором ІТ та інформаційної безпеки дещо складніші.

З одного боку, поліпшення організаційно-ресурсних параметрів діяльності в сфері ІТ прямо пов'язано з поліпшенням аналогічних параметрів сфері інформаційної безпеки (ІБ). Зокрема, коефіцієнти парної кореляції між векторами узагальнюючих оцінок організаційно-ресурсних умов діяльності в сфері ІТ і в сфері ІБ відносно високі (табл. 9).

По оцінках системних факторів – коефіцієнт кореляції векторів оцінок 41-ї державної установи в сфері ІТ і сфері ІБ дорівнює 0,627 (відносно сильна пряма кореляція), по оцінках персоніфікованих факторів – 0,641, по інтегральних (узагальнюючих обидві групи факторів оцінках) – 0,621. При цьому, стосовно тих установ, чиї оцінки організаційно-ресурсних умов в сфері ІТ та в сфері ІБ відносно вищі, спостерігається і більш висока кореляція. Так, для першої десятки з найвищими оцінками по сфері ІТ вона досягає значення 0,968, що свідчить про міцний прямий зв'язок між варіативністю показників.

Проте, по-перше, інтегральні оцінки організаційно-ресурсних умов діяльності в сфері ІТ стабільно вищі за аналогічні оцінки в сфері ІБ – наприклад для першої десятки установ з найвищими оцінками в сфері ІТ – без виключень. По-друге, відносно високі оцінки організаційно-ресурсних умов діяльності в сфері ІТ не гарантують порівняно високих оцінок в сфері ІБ. Зокрема, державна установа, що має 9-ий рейтинг з оцінкою організаційно-ресурсних умов діяльності в сфері ІТ 0,689 має аналогічну оцінку в сфері ІБ лише 0,297 і 34-ий рейтинг. Установа з оцінкою в сфері ІТ 0,675 має аналогічну оцінку в сфері ІТ 0,174. Аналогічних випадків можна навести ще як мінімум 9-ть: установи з відносно високими оцінками в сфері ІТ мають значно (в рази) нижчі оцінки в сфері ІБ.

Таблиця 9

Коефіцієнти кореляції між векторами оцінок організаційно-ресурсних умов діяльності в сфері ІТ та інформаційної безпеки (ІБ)

Органи державної влади	Узагальнююча оцінка	Оцінка по системних факторах	Оцінка по персоніфікованих факторах
Всі ОДВ, охоплені дослідженням	0,621	0,627	0,641
ОДВ, де створені СЗІ	0,829	0,750	0,766
ОДВ, де не створені СЗІ	0,405	0,729	0,470

Це свідчення специфічності потреб і вимог до організаційного і ресурсного забезпечення діяльності в сфері кіберзахисту, порівняно з діяльністю в сфері ІТ. Така специфіка вимагає і достатньої самостійності відповідного структурного підрозділу, концепція управління, що ґрунтується на інтегруванні функцій СЗІ в сферу діяльності служби ІТ не дозволяє забезпечити адекватні організаційні та ресурсні умови для діяльності з кіберзахисту. Це може виявлятись навіть не у прямій нестачі ресурсів, виділених для забезпечення кіберзахисту, а у відсутності цілісної, узгодженої як по вертикалі, так і між підрозділами одного рівня системи управління кібербезпекою, що суттєво знижує ефективність і результативність використання таких ресурсів.

Зокрема, відсутність безперервного ланцюжка передавання управлінських сигналів та забезпечення обігу інформації між об'єктами і суб'єктами управління в процесі формування та реалізації політики кібербезпеки, унеможливлює досягнення нормативного рівня захисту ІКС органів державної влади та об'єктів критичної інфраструктури. Таким чином, без спеціальної посади (посад) в кожній ОДВ, що забезпечуватиме реалізацію централізованого вектору управління захистом інформації, стандартизацію організаційно-технічних умов діяльності з забезпечення кібербезпеки навіть якісне нарощення ресурсного забезпечення такої діяльності не даватиме очікуваного приросту захищеності ІТС органів державної влади та об'єктів критичної інфраструктури.

Показовим є значне зменшення спорідненості оцінок організаційно-ресурсних умов діяльності в сфері ІБ та сфері ІТ по групі установ, де не створені СЗІ: коефіцієнт кореляції по інтегральним оцінкам для ОДВ без СЗІ лише 0,405, проти 0,829 по ОДВ, у яких створені СЗІ. На перший погляд, інтеграція функцій кіберзахисту до сфери ІТ має сприяти вирівнюванню організаційно-ресурсних умов діяльності з забезпечення кібербезпеки і в сфері ІТ в цілому. Проте насправді, така інтеграція, послаблюючи вплив вертикалі з реалізації єдиної національної політики кібербезпеки, зумовлює два наслідки: по перше, посилення диференціації організаційно-ресурсних умов діяльності в сфері кібербезпеки і в сфері ІТ в цілому; по-друге, наростання диференціації організаційно-ресурсного забезпечення на «одиницю складності й масштабності завдань забезпечення кібербезпеки» по різних ОДВ, що зумовлює зменшення органічності та резистентності національної системи кібербезпеки.

Висновки. 1. Критична нестача кваліфікованих фахівців, властива як для сфери експлуатації ІКС ОДВ так і сфери кіберзахисту, детермінована високою диференціацією заробітків в бюджетній і комерційній сфері: рівень оплати аналогічної праці в бюджетній сфері в 3-5 разів поступається комерційним підприємствам. Держава не в змозі залучити до роботи в сфері державного управління не лише висококваліфікованого фахівця (команду фахівців) з кіберзахисту, а й навіть досвідченого фахівця з ІТ. Це вимагає або зміни принципів фінансування служб ІТ та захисту інформації, або використання додаткових, неринкових механізмів приваблення (ми свідомо використовуємо саме цей термін, а не «залучення», щоб підкреслити неприпустимість відмови від принципів вигідної, вільно обраної та ефективної зайнятості) фахівців. Саме після вирішення цієї первинної проблеми, набувають сенсу всі подальші заходи з оптимізації використання того людського потенціалу, що має бути радикально поліпшений для забезпечення актуальності й адекватності чинної системи забезпечення кібербезпеки ОДВ та об'єктів критичної інфраструктури в Україні.

2. Вагомі відхилення від оптимальних організаційно-ресурсних умов діяльності з кіберзахисту по системних параметрах свідчать про відсутність єдиного стандарту реалізації політики кібербезпеки в ОДВ – специфічні фактори певної ОДВ мають більший вплив на організаційно-ресурсні умови діяльності з кіберзахисту, ніж централізовано розроблені норми і регламенти. Така відсутність стандартизації організаційно-ресурсних умов діяльності з кіберзахисту виступає ознакою відсутності єдиної дієвої вертикалі руху інформації (керуючих та регламентуючих сигналів від центрів формування політики кіберзахисту до певних ОДВ та «відклику», про перебіг адаптації такої політики до умов конкретного ОДВ й установ сфери його відповідальності – від ОДВ до центру формування політики кіберзахисту). Таким чином, без спеціальної посади (посад) в кожній ОДВ, що забезпечуватиме реалізацію централізованого вектору управління захистом

інформації, стандартизацію організаційно-технічних умов діяльності з забезпечення кібербезпеки, навіть якісне нарощення ресурсного забезпечення такої діяльності не даватиме очікуваного приросту захищеності ІТС органів державної влади та об'єктів критичної інфраструктури.

3. Обумовленість організаційно-ресурсних характеристик діяльності з кіберзахисту належністю до певного ОДВ сильніша за обумовленість належністю до єдиної системи кіберзахисту.

Якщо перша зумовлює диференціацію таких характеристик між різними ОДВ (при цьому без прямого зв'язку зі складністю та масштабністю завдань забезпечення кібербезпеки в межах певного ОДВ, чи вартістю ризиків неготовності системи кіберзахисту протистояти загрозам), то друга – як раз сприяє вирівнюванню організаційно-ресурсних умов діяльності з кіберзахисту в розрахунку на «одиницю складності й масштабності завдань зі забезпечення кібербезпеки в певному ОДВ та сфері його регулювання».

Отже посилення впливу вертикалі реалізації централізованої національної політики кібербезпеки для компенсації надмірної диференціації організаційно-ресурсних умов діяльності з кіберзахисту, що зумовлюється специфікою ресурсних можливостей та організаційних рішень певного ОДВ, є вагомим джерелом резервів наближення до нормативного рівня кібербезпеки ОДВ та критичної інфраструктури в Україні.

4. Відмінності організаційно-ресурсних умов діяльності в сфері кібербезпеки від умов діяльності в сфері ІТ вимагає і достатньої самостійності відповідного структурного підрозділу: концепція управління, що ґрунтується на інтегруванні функцій СЗІ в сферу діяльності служби ІТ не дозволяє забезпечити адекватні організаційні та ресурсні умови для діяльності з кіберзахисту.

Це обмеження може виявлятись навіть не у прямій нестачі ресурсів, виділених для забезпечення кіберзахисту, а у відсутності цілісної системи управління кібербезпекою, що суттєво знижує ефективність і результативність використання таких ресурсів.

Зокрема, відсутність безперервного ланцюжка передавання управлінських сигналів та забезпечення обігу інформації між об'єктами і суб'єктами управління в процесі формування та реалізації політики кібербезпеки, унеможливлює досягнення нормативного рівня захисту ІКС органів державної влади та об'єктів критичної інфраструктури.

Забезпечення кібербезпеки органів виконавчої влади та об'єктів критичної інфраструктури вимагає побудови цілісної вертикалі управління кібербезпекою, що дозволить забезпечити адекватну реалізацію політики та дотримання процедур кіберзахисту по всіх рівнях державної влади.

ЛІТЕРАТУРА

[1] Про Стратегію кібербезпеки України: Указ Президента №96/2016 від 15.03.2016. URL: https:// zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.05.2021).

[2] Про основні засади забезпечення кібербезпеки України: Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.

[3] Потій, О.В., Семенченко, А.І., Дубов, Д.В., Бакалинський, О.О., Мялковський, Д.В. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту україни. Захист інформації, Північна Америка, 23, кві. 2021. Доступно за адресою: http: // jrnl. nau. edu. ua/index.php /ZI/article /view/15434.

[4] Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

[5] ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. URL: http://online.budstandart.com /ua/ catalog /doc-page. html?id_ doc=69128 (дата звернення: 02.05.2021).

[6] Доктрина інформаційної безпеки України // http://www.president.gov.ua/documents/472017-21374.

[7] Кібервійна вже триває – Україну ледь не щодня атакують російські хакери. Як ми захищаємось? Інтерв'ю голови Держспецзв'язку Юрія Щиголя https://forbes.ua/inside/kiberviyna-vzhe-trivae-ukrainu-led-ne-shchodnya-atakuyut-rosiyski-khakeri-yak-mi-zakhishchaemos-intervyu-golovi-derzhspetsz-vyazku- yuriya-shchigolya-21012022-3311.

[8] Діордіца І. В. Поняття та зміст національної системи кібербезпеки / І. В. Діордіца [Електронний ресурс]. — Режим доступу: http: / /goal-int.org/ ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/.

[9] Ліпкан В.А., Діордіца І. В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України / Підприємництво, господарство і право. Вип. 5, 2017 р. С. 174-180.

[10] Марущак А.І., Петров С.Г., Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України) / Інформація і право. № 2(33), 2020. С. 77-84.

[11] Каленюк І.С., Куклін О.В. Розвиток вищої освіти та економіка знань / І.С Каленюк, Куклін О.В. – Київ: Знання, 2012.

[12] Людський розвиток в Україні: можливості та напрями соціальних інвестицій (колективна

науково-аналітична монографія) / За ред. Е.М. Лібанової. – К.: Ін-т демографії та соціальних досліджень НАН України, Держкомстат України, 2006. – 355 с.

[13] Грішнова О. А. Освіта як чинник людського розвитку і економічного зростання України [Електронний ресурс] / О. А. Грішнова. – Режим доступу : http:/ /dspace. nbuv. gov. ua / bitstream /handle /123456789/ 11836/ 11-Grishnova. pdf? sequence=1.

[14] Бабич А. М., Егоров Е. В. Экономика и финансирование социальной сферы. — Центр Экспертизы и Маркетинга КТУ, 1996. — 512с.

УДК 378:330;591.5

Potii O., Bakalynsky O., Myalkovsky D., Verba D. Analysis of systemic and personalized factors of organizational and resource conditions cyber security enduement activities bodies of state authority and critical infrastructures of Ukraine

Abstract. *The article is devoted to approaches to ensuring the adequacy of the resource provision of cyber protection activities of state authorities and critical infrastructure objects to the objective requirements of achieving the normative (defined by the Cybersecurity Strategy of Ukraine and UL "On the basics of cyber security in Ukraine) level of effectiveness and performance of the national cyber defense system. The article uses a factor analysis of organizational and resource factors of the potentially achievable and actually implemented level of cyber protection of state authorities and critical infrastructure objects. Factors are structured into two groups: systemic and personalized. The first express the degree of compliance of the rules and the norms of resource provision for cyber protection activities of state authorities and critical infrastructure objects provided by the current legal acts with the actual tasks and objective needs of achieving the desired level of cyber security. The second reflects the degree of realization of the potential created by existing regulations and norms. It is substantiated that the strengthening of the influence of the vertical implementation of the centralized national cyber security policy to compensate for the excessive differentiation of the organizational and resource conditions of cyber protection activity, caused by the specificity of the resource capabilities and organizational solutions of a certain state institution, is a significant source of reserves for approaching the normative level of cyber security in Ukraine. In particular, the lack of a continuous chain of management signals' transmission and ensuring the circulation of information between objects and subjects of management from the center of development the cyber security policy in state authorities to the departments of their implementation and considering the specifics of the relevant industry makes it impossible to achieve the normative level of cyber security in the state authorities of Ukraine and critical infrastructure objects.*

Keywords: *cyber security, organizational and resource conditions, state authorities, information security services.*

Потій Олександр Володимирович, д.т.н., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.
Oleksandr Potii, Doctor of Technical Sciences, Professor, Deputy Head of the State Service for Special Communications and Information Protection of Ukraine.

Бакалинський Олександр Олегович, к. т. н., заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Oleksandr Bakalynsky, Candidate of Technical Sciences, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.

Мялковський Данило Владиславович, к. д. у., директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Danylo Myalkovsky, Candidate of Sciences of Public Administration, Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.

Верба Денис Володимирович, к.е.н., доцент, доцент кафедри економічної теорії ДВНЗ «КНЕУ імені Вадима Гетьмана».
Denys Verba, Ph.D., Associate Professor department of Economic Theory, KNEU named after Vadym Hetman.

Отримано *3 вересня 2022 року,* затверджено редколегією *14 листопада 2022 року*