DOI: <https://doi.org/10.15407/emodel.43.01.067>
УДК 004.07: 352/354

О.О. Бакалинський, канд. техн. наук,

Ю.І. Циплинський, І.В. Нечаєва, В.О. Дубок

Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Україна, 03110, Київ, вул. Солом'янська 13,
e-mail: baov@meta.ua; cyber@dszsi.gov.ua

Статистичне дослідження стану кіберзахисту критичної інформаційної інфраструктури України

Наведено результати виконання доручення прем'єр-міністра України щодо опитування про стан кіберзахисту, яке було проведено в рамках виконання підготовчих заходів до «Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом». Актуальність цього дослідження зумовлена тенденціями розвитку фреймворку нормативно-правових актів з питань кіберзахисту критичної інфраструктури і сфери національної безпеки та оборони, а також невідповідністю реального стану справ із кіберзахисту об'єктів критичної інфраструктури (ОКІ) вимогам державної політики щодо захисту таких об'єктів від кіберзагроз і кібератак. Розглянуто практичний досвід проведення статистичного опитування організацій, які потенційно можуть бути віднесені до ОКІ, на відповідність до вимог нормативно-правових актів із кіберзахисту об'єктів критичної інформаційної інфраструктури.

К л ю ч о в і с л о в а: кібербезпека, кіберзахист, критична інформаційна інфраструктура, огляд, кіберстійкість.

Постановка проблеми. Відповідаючи на виклики часу, Україна розбудовує свій потенціал із кіберзахисту об'єктів критичної інфраструктури (ОКІ) та інших важливих елементів забезпечення кібербезпеки. З метою проведення аналізу стану справ в цій сфері та планування на рівні держави подальших кроків у розбудові системи кібербезпеки України Указом Президента України «Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року «Про організацію планування в секторі безпеки і оборони України» № 225/2019 було визначено необхідність провести ряд оглядів, одним із яких є «Огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».

© Бакалинський О.О., Циплинський Ю.І., Нечаєва І.В., Дубок В.О., 2021

Необхідно зазначити, що нормативно-правовий акт, який визначав би порядок проведення такого огляду, на 30.10 2020 р. не з'явився. Його проект був розроблений ще у 2018 р. Адміністрацією Держспецзв'язку, але, враховуючи особливості вимог Регламенту Кабінету Міністрів України, досі не прийнятий [1]. У проекті акту визначено, що Огляд формується за наступними чинниками:

- аналіз стану та результатів реалізації вимог законодавства у сфері кіберзахисту об'єктів огляду;
- результати самооцінки та державного контролю у сферах криптографічного та технічного захисту інформації, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів огляду;
- результати аудиту інформаційної безпеки об'єктів критичної інформаційної інфраструктури (ОКІІ);
- аналіз інформації щодо стану кіберзахисту об'єктів огляду, отриманої за результатами опитувань суб'єктів критичної інформаційної інфраструктури [2].

Таким чином, існує протиріччя між необхідністю проведення Огляду стану кіберзахисту та відсутністю інструментів для проведення самооцінки організацій — потенційних ОКІ, нормативно визначеного порядку проведення аудиту інформаційної безпеки на ОКІ, що суттєво звужує кількість джерел для отримання об'єктивних свідочств щодо реального стану кіберзахисту держави.

Опис проведених заходів опитування. Одним із джерел Огляду стану кіберзахисту є результати самооцінки у сферах криптографічного та технічного захисту інформації, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Враховуючи необхідність підготовчих заходів до проведення кіберзахисту об'єктів Огляду, Прем'єр-міністром України видано доручення № 10512/1/1-20 від 16.04.2020 «Про проведення опитування щодо стану кіберзахисту». На виконання цього доручення розроблено перелік питань (опитувальник) щодо стану виконання вимог з кіберзахисту міністерствами, іншими державними органами, підприємствами, установами та організаціями, які входять до сфери управління таких державних органів та потенційно можуть бути віднесені до ОКІ.

Метою є збір даних для проведення первинного аналізу стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, як джерела відомостей для проведення огляду стану кіберзахисту ОКІ відповідно до вимог пункту 4 частини третьої статті 27 Закону України «Про національну безпеку України» [3].

У зазначеному опитувальнику враховано вимоги щодо класифікації ОКІ, викладені у проекті Постанови КМУ «Деякі питання об'єктів критичної інфраструктури» [4], розглянутої на засіданні уряду 9.10.2020. Постанова отримала позитивне рішення щодо необхідності врахувати особливості завдань створеного Міністерства з питань стратегічних галузей промисловості України та розділ Міністерства енергетики та захисту довкілля України на Міністерство енергетики та Міністерство захисту довкілля та природних ресурсів України [5], а також вимоги Постанови Кабінету Міністрів України № 943 від 9 жовтня 2020 року «Деякі питання об'єктів критичної інформаційної інфраструктури» [6]. Отже, опитувальник став певним інструментом, завдяки якому власник (розпорядник) ОКІ може провести самоконтроль щодо стану кіберзахисту свого ОКІ.

В опитувальнику міститься близько 140 питань [7]. Відповідаючи на ці питання, потенційний ОКІ держави, уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури, може визначити:

сектор (підсектор), до якого належить потенційний ОКІ (в опитувальнику 10 секторів і 17 підсекторів);

основні послуги, які він надає (із запропонованих 74 видів основних послуг);

рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування організації.

Це дозволяє центральним органам виконавчої влади, іншим державним органам, які забезпечують формування та (або) реалізацію державної політики в одній чи декількох сферах, здійснювати наступне:

ідентифікувати ОКІ своїх секторів (підсекторів) критичної інфраструктури;

спільно з операторами основних послуг виконати віднесення об'єктів до певної категорії критичності;

отримати дані щодо ОКІІ;

отримати попередні дані щодо стану кіберзахисту ОКІІ.

Опитувальник було надіслано до державних органів та органів місцевого самоврядування, а також до 94 підприємств, установ та організацій, які наразі віднесено до об'єктів, що мають стратегічне значення та потенційно можуть вважатися ОКІ, що впливає із визначення ОКІ, наведеного у Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року [8], тобто до таких, що:

- здійснюють діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

- надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

- є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

- включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

- є об'єктами потенційно небезпечних технологій і виробництв.

З цих 94-х підприємств 21 — державне підприємство, 7 — комунальної форми власності, інші — приватної форми власності.

Основною метою опитування було отримання попередніх даних щодо стану кіберзахисту ОКІІ. Крім того, інформація, яка міститься в опитувальнику, дозволила власнику ОКІІ оцінити повноту впроваджених заходів з кіберзахисту в інформаційно-телекомунікаційних, інформаційних або телекомунікаційних системах (ІТС), що входять до складу ОКІ та забезпечують надання ним основних послуг, тобто оцінити повноту або ступінь виконання вимог Постанови КМУ № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [9].

Частина опитувальника, яка стосується кіберзахисту ОКІ, має 90 питань, розподілених за наступними розділами:

1. Загальна політика безпеки в ІТС.
2. Управління доступом користувачів та адміністраторів в ІТС.
3. Ідентифікація і автентифікація користувачів та адміністраторів ОКІІ.
4. Реєстрація подій компонентами ОКІІ та їх періодичний аудит.
5. Забезпечення мережевого захисту компонентів та інформаційних ресурсів ОКІІ.
6. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ.
7. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ.
8. Визначення умов використання програмного та апаратного забезпечення ОКІІ.
9. Визначення умов розміщення компонентів ОКІІ.

Адміністрація Держспецзв'язку отримала 1267 відповідей на опитувальник (рис. 1). Результати аналізу заповнених опитувальників є підґрунтям (базовою інформацією) для проведення оцінки стану кіберзахисту ОКІІ, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у рамках майбутнього огляду стану кіберзахисту об'єктів критичної інфраструктури.

Рис. 1. Розподіл опитувальників за ступенем заповненості

Відповідно до наведених в опитувальнику критеріїв:

250 організацій віднесли себе до ОКІ і заповнили опитувальник повністю;

272 організації не ідентифікували себе як ОКІ, однак заповнили опитувальник в частині реалізованих заходів з кіберзахисту у своїх інформаційно-телекомунікаційних системах;

745 організацій надіслали опитувальник не заповнений з різних причин, в тому числі, посилаючись на відсутність такого роду законодавчо встановлених зобов'язань. Необхідно зазначити, що певна частина організацій, які не надали відомості про себе, є відомими лідерами своїх галузей з питань забезпечення кіберзахисту власної інфраструктури, мають сертифіковані системи управління інформаційної безпеки, побудовані комплексні системи захисту інформації, тощо.

Якісні відповіді дали організації, підпорядковані державним органам (міністерствам). Якість заповнення опитувальників, розісланих від органів місцевого самоврядування, зазвичай була не на належному рівні.

Подальший аналіз проведено на основі даних, отриманих із заповнених опитувальників. Кількість незаповнених опитувальників у статистичній обробці даних не враховано.

У табл. 1 і на рис. 2, а, наведено кількість організацій, які заповнили опитувальник повністю або частково (за секторами критичної інфраструктури). Як бачимо у табл. 1, існує певний перекид в сторону організацій охорони здоров'я, активність яких була пов'язана із введенням в Україні надзвичайної ситуації через поширення коронавірусу COVID-19. На рис. 2, б, наведено розподіл організацій, які заповнили опитувальник повністю або частково, за територіальною ознакою, а в табл. 2 — кількість організацій (за секторами), які повністю заповнили опитувальник та зачислили себе до ОКІ різних категорій критичності.

До об'єктів першої категорії критичності, визначених як особливо важливі, себе зачислили дев'ять організацій, тобто 3,6 % від 250 організацій, зачислених до ОКІ. До об'єктів другої категорії критичності (життєво важливих) себе зачислили 16 організацій, тобто 6,4 %, до об'єктів третьої категорії критичності (важливих) — 86 організацій, тобто 34,4 %, до об'єктів четвертої категорії критичності (необхідних) — 139 організацій, тобто 55,6 %.

Рис. 2. Розподіл організацій, які надали заповнені опитувальники, за галузевою ознакою (а) та територіальною ознакою (б)

Таблиця 1. Розподіл організацій, надіславших заповнені опитувальники, за секторами критичної інфраструктури

Сектор критичної інфраструктури	Кількість організацій, які заповнили опитувальники
Паливно-енергетичний	35
Інформаційний	20
Мережі життєзабезпечення	91
Харчова промисловість та агропромисловий комплекс	15
Охорона здоров'я	290
Транспорт і пошта	19
Промисловість	4
Цивільний захист населення та територій	25
Екологічна безпека	4
Поза визначених секторів	19
В с ь о г о	522

Примітка: сектори критичної інфраструктури в опитувальнику наведено у попередній редакції проекту Постанови КМУ «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури»; у редакції, яку буде розглянуто на засіданні уряду, змінено назву проекту постанови і перелік секторів.

У табл. 3 наведено усереднені результати виконання вимог з кіберзахисту (постанова Кабінету Міністрів України № 518 від 19.06.2019) за секторами та підсекторами. Дані отримано за самооцінкою організацій, які заповнили опитувальник повністю або частково. Зачислення організацій, які не заповнили опитувальник повністю, до сектору або підсектору критичної інфраструктури здійснено умовно, відповідно до їх приналежності до галузі економіки. Відомості щодо ОКІ, які не належать до жодного з визначених секторів, не обраховувалися.

Таблиця 2. Організації, які зачислили себе до певної категорії критичності

Сектор критичної інфраструктури ¹	Кількість організацій, які повернули опитувальники	Кількість організацій, які зачислили себе до ОКІ	Категорія			
			I	II	III	IV
Паливно-енергетичний	35	21	3	8	9	1
Інформаційний	20	5		1	1	3
Мережі життєзабезпечення	91	49		1	13	35
Харчова промисловість та агропромисловий комплекс	15	8			1	7
Охорона здоров'я	290	129	6	6	35	82
Транспорт і пошта	19	7	–	–	3	4
Промисловість	4	0	–	–	–	–
Цивільний захист населення та територій	25	11			5	6
Екологічна безпека	4	1				1
Поза визначених секторів ²	19	19			19	
В с ь о г о	522	250	9	16	86	139

¹ Пенсійний фонд України та його територіальні підрозділи зачислили себе до ОКІ III категорії, але не зачислили себе до жодного сектору критичної інфраструктури.

² В таблицях відсутні дані щодо фінансового сектору через те, що Адміністрацією Держспецзв'язку опитування не проводилось, тому що відповідальним органом за цей сектор є Національний банк України, якому і надано повноваження на проведення Огляду стану кіберзахисту фінансового сектору.

Таблиця 3. Усереднені показники виконання вимог щодо кіберзахисту за секторами та підсекторами

Сектор	Кількість організацій, які надали дані	Впровадження вимог за сектор, %	Підсектор	Кількість організацій, які надали дані	Впровадження вимог за підсектор, %
Паливно-енергетичний	35	68,25	Електроенергетика	26	73
			Нафтова промисловість	2	93
			Газова промисловість	4	85
			Ядерна енергетика	3	22
Інформаційний	20	65	Інформаційні технології	13	65
Мережі життєзабезпечення	91	52	Телекомунікації	7	65
			Водопостачання	34	51
			Стічні води	35	49
			Теплопостачання	22	56
Харчова промисловість та агропромисловий комплекс	15				56
Охорона здоров'я	290				49
Транспорт і пошта	19	40	Транспорт		
			авіаційний	8	67
			автомобільний	4	10
			міський залізничний		
			морський та річковий	5	42
			Поштовий зв'язок	2	73
Промисловість	4	76	Хімічна промисловість		–
			Оборонна промисловість	1	81
			Ракетно-космічна та авіаційна промисловість	3	71
Цивільний захист населення та територій	25				48
Екологічна безпека	4				47

Відсутність законодавчої бази та нормативно-правового забезпечення у сфері захисту критичної інфраструктури суттєво ускладнює впровадження заходів з кіберзахисту ІТС, які забезпечують функціонування ОКІ, а відсутність затверджених механізмів формування переліку ОКІ та як наслідок — переліку таких об'єктів унеможлиблює запуск процесів моніторингу і самооцінки стану кіберзахисту ОКІ у повному обсязі для отримання об'єктивної оцінки стану їх кіберстійкості. З тих же причин ускладнюються процеси організації та проведення Огляду стану кіберзахисту, передусім, у контексті відповідального ставлення власників (керівників) ОКІ до проведення заходів з кіберзахисту та оцінювання стану їх повноти і достатності.

Відсутність об'єктивної інформації за результатами самооцінювання стану виконання вимог з кіберзахисту на кожному ОКІ унеможлиблює отримання об'єктивної оцінки стану кіберзахисту критичної інфраструктури в цілому та як наслідок — ускладнює прийняття виважених управлінських рішень на державному і місцевому рівнях з питань підвищення ефективності заходів з кіберзахисту, зокрема розробки цільових галузевих, державних або регіональних програм розвитку системи матеріально-технічного та ресурсного забезпечення сфери кіберзахисту критичної інфраструктури.

На рис. 3 наведено результати самооцінки організацій, які заповнили опитувальник повністю або частково щодо виконання базових вимог із забезпечення кіберзахисту ОКІ, наведених у додатку до постанови Кабінету Міністрів України від № 518 19.06.2019. Найвищий відсоток впроваджених вимог з кіберзахисту в організаціях паливно-енергетичного та інформаційного секторів, а найнижчий — у секторі транспорту і пошти. Слід зазначити, що деякі результати не є репрезентативними, тому що кількість підприємств, які надали інформацію, не відображає реальні дані за галузями.

За результатами аналізу отриманої інформації визначено, що розроблений опитувальник дозволяє провести первинну оцінку стану кіберзахисту ОКІ та може бути використаний при проведенні Огляду стану кіберзахисту ОКІ, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Спираючись на отриманий досвід спілкування із представниками організацій щодо порядку заповнення опитувальника, по ньому перепрацьовують методичні рекомендації щодо його заповнення. Після прийняття Кабінетом Міністрів України постанови «Деякі питання об'єктів критичної інфраструктури» до розділів опитувальника буде внесено відповідні зміни. В рамках розбудови та розвитку системи кіберзахисту Міністерства енергетики опитувальник буде використано при проведенні первинного аудиту стану кіберзахисту, як міністерства і підприємств галузі.

Рис. 3. Розподіл кількості (шт.) підприємств за виконанням вимог з кіберзахисту (%): а — паливно-енергетичний сектор; б — мережа життєзабезпечення; в — інформаційний сектор; г — сектор охорони здоров'я; д — сектор харчової промисловості та агропромисловий комплекс; е — сектор транспорту і пошта; ж — промисловість; з — сектор цивільного захисту населення та територій; і — сектор екологічної безпеки

Подальший розвиток нормативно-правової бази в сфері кіберзахисту дозволить розширити спектр джерел отримання інформації щодо реального стану кіберзахисту ОКІ, в тому числі через нормативне закріплення основних понять аудиту інформаційної безпеки та впровадження порядку його проведення. Це дозволить приймати адекватні рішення щодо фінансування заходів із забезпечення кібербезпеки на рівні держави і на рівні галузей та окремих організацій.

Формування взаємодовіри між державою та приватним сектором є невід'ємною частиною забезпечення кібербезпеки України. Організація процесу своєчасного обміну інформацією щодо кіберінцидентів та кібератак є запорукою зміцнення національної системи кіберстійкості та підґрунтям для подальшого розвитку організаційно-технічної моделі кіберзахисту. Безсумнівно, необхідним є залучення потенціалу наукових та навчальних установ для наукового супроводу проєктів із забезпечення кібербезпеки, розробки нормативно-правових актів, дослідження перспективних напрямів подальшого розвитку кібербезпеки держави в цілому і окремих галузей національної економіки. Обґрунтування основних напрямків розвитку національної системи кібербезпеки, розробка методів обчислення основних параметрів систем інформаційної безпеки, які необхідно будувати на об'єктах критичної інфраструктури, розробка системи індикаторів стану кіберзахисту є наразі актуальними проблемами.

Висновки

Проведене статистичне дослідження дозволяє проаналізувати стан кіберзахисту критичної інформаційної інфраструктури України та зробити наступні висновки.

Очевидним є те, що після нормативно-правового врегулювання порядку зачислення об'єктів до ОКІ та ОКІІ статистичні дані зазнають істотних змін, в першу чергу збільшиться кількість об'єктів I та II категорії, керівники яких, враховуючи специфіку об'єктів, не надали відповідь на опитувальник через відсутність законодавчого підґрунтя.

Після внесення в опитувальник змін з врахуванням отриманого в ході експерименту досвіду та корекції згідно з проєктом постанови «Деякі питання об'єктів критичної інфраструктури» він стане дієвим інструментом для категоризації ОКІ та проведення на таких об'єктах самоконтролю щодо їх кіберзахисту.

Відповідальне ставлення до кіберзахисту власних ОКІ є у 20 % підприємств, 21 % ставиться з розумінням, проте при заповненні опитувальника у них виникали проблеми із зачисленням себе до певного сектору критичної інфраструктури, та 59 % підприємств займає очікувальну позицію.

Отримання попередніх даних щодо стану кіберзахисту ОКІ та результати їх аналізу забезпечують можливість підготовки до проведення Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, як елементу стратегічного планування в державі.

Отримані дані щодо розподілу ОКІ за категоріями критичності та за відсотком виконання вимог щодо їх кіберзахисту надає можливість уряду спрямувати кошти державного бюджету в залежності від значущості ОКІ та реального стану його кіберзахисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Постанова Кабінету Міністрів України № 950 від 18 липня 2007 року «Про затвердження Регламенту Кабінету Міністрів України» [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу: <https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF/>. Загол. з екрану.
2. Проект Постанови КМУ «Огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом». [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу : <https://cip.gov.ua/ua/filter?tagId=10351>. Загол. з екрану.
3. Закон України «Про національну безпеку України», [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020, Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>. Загол. з екрану.
4. Проект Постанови КМУ «Деякі питання об'єктів критичної інфраструктури», [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу: <https://cip.gov.ua/ua>. Загол. з екрану.
5. Постанова Кабінету Міністрів України від 27 травня 2020 року № 425 «Деякі питання оптимізації системи центральних органів виконавчої влади», [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу : <https://www.kmu.gov.ua/npras/deyaki-pitannya-optimizaciyi-sistemi-centralnih-organiv-vikonavchoyi-t270520>. Загол. з екрану.
6. Постанова Кабінету Міністрів України № 943 від 9 жовтня 2020 року «Деякі питання об'єктів критичної інформаційної інфраструктури», [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020, Режим доступу: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text>. Загол. з екрану.
7. Опитувальник [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу: <https://cert.gov.ua/>. Загол. з екрану.
8. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. Загол. з екрану.
9. Постанова КМУ №518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», [Електронний ресурс] Вебсайт. Дата доступу 5.11.2020, Режим доступу: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>. Загол. з екрану.

Отримано 05.11.2020

REFERENCES

1. Resolution of the Cabinet of Ministers of Ukraine № 950 dated July 18, 2007, "On approval of the Regulations of the Cabinet of Ministers of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF/>, (accessed November 5, 2020).
2. Draft Resolution of the Cabinet of Ministers of Ukraine "Review of the state of cyber protection of critical information infrastructure, state information resources and information required to be protected by law", available at: <https://cip.gov.ua/ua/filter?tagId=10351>, (accessed November 5, 2020).
3. Law of Ukraine "On National Security of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>, (accessed November 5, 2020).
4. Draft Resolution of the Cabinet of Ministers of Ukraine "Some issues of critical infrastructure facilities", available at: <https://cip.gov.ua/ua/>, (accessed November 5, 2020).
5. Resolution of the Cabinet of Ministers of Ukraine № 425 dated May 27, 2020, "Some issues of optimization of the system of central executive bodies", available at: <https://www.kmu.gov.ua/npas/deyaki-pitannya-optimizaciyi-sistemi-centralnih-organiv-vikonavchoyi-t270520>, (accessed November 5, 2020).
6. Resolution of the Cabinet of Ministers of Ukraine № 943 dated October 9, 2020, "Some issues of critical information infrastructure", available at: <https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text>, (accessed November 5, 2020).
7. Questionnaire, available at: <https://cert.gov.ua/>, (accessed November 5, 2020).
8. Law of Ukraine "On the basic principles of cybersecurity of Ukraine" dated October 5, 2017, available at: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>, (accessed November 5, 2020).
9. Resolution of the Cabinet of Ministers №518 dated June 19, 2019, "On approval of the General requirements for cyber protection of critical infrastructure", available at: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>, (accessed November 5, 2020).

Received 05.11.2020

O. Bakalynskiy, Yu. Tsyplinskyi, I. Nechayeva, V. Dubok

THE RESULTS OF A STATISTICAL STUDY OF THE STATE OF CYBER PROTECTION OF THE CRITICAL INFORMATION INFRASTRUCTURE OF UKRAINE

The article examines the results of the Prime Minister of Ukraine's order to conduct a survey on the state of cyber defense, which was conducted as part of the preparatory activities for the Review of the state of cyber protection of critical information infrastructure, state information resources and information required by law. The relevance of this study is due to trends in the framework of regulations on cyber protection of critical infrastructure, and trends in the development of national security and defense, the inconsistency of the real state of affairs on cyber protection of critical infrastructure to state policy on protection of such objects from cyber threats, cyberattacks. The article considers the practical experience of conducting a statistical survey of organizations that can potentially be classified as critical infrastructure in accordance with the requirements of regulations on cyber protection of critical information infrastructure.

Keywords: cybersecurity, cyberdefense, critical information infrastructure, review, cyber resilience.

БАКАЛИНСЬКИЙ Олександр Олегович, канд. техн. наук, заст. директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України. В 1993 р. закінчив Київський військовий інститут управління та зв'язку. Область наукових досліджень — системи управління інформаційною безпекою, управління ризиками інформаційної безпеки, кіберзахист об'єктів критичної інфраструктури.

ЦИПЛИНСЬКИЙ Юрій Іванович, директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України. В 1993 р. закінчив Київський військовий інститут управління та зв'язку. Область наукових досліджень — кіберзахист об'єктів критичної інфраструктури.

НЕЧАЄВА Ірина Васильовна, заст. директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України. У 1982 р. закінчила Київський національний університет ім. Т.Г. Шевченко. Область наукових досліджень — кіберзахист об'єктів критичної інфраструктури.

ДУБОК Владислав Андрійович, спеціаліст Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України. В 2018 р. закінчив Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського». Область наукових досліджень — кіберзахист об'єктів критичної інфраструктури.