Економічна безпека суб'єктів господарської діяльності

УДК 351.865

Живило Євген Олександрович
аспірант кафедри інформаційних технологій і систем управління
Харківського регіонального інституту державного управління
Національної академії державного управління при Президентові України
Живило Евгений Александрович
аспирант кафедры информационных технологий и систем управления
Харьковского регионального института государственного управления
Национальной академии государственного управления
при Президенте Украины
Zhivilo Evgen
Postgraduate Student of the
Department of Information Technologies and Management Systems
Kharkiv Regional Institute of Public Administration of the
National Academy of Public Administration under the President of Ukraine

МЕТОДИКА РОЗРАХУНКУ ІНДИКАТОРІВ КІБЕРОБОРОНИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ (ВІДОМСТВІ, УСТАНОВІ, ПІДПРИЄМСТВІ, ОРГАНІЗАЦІЇ) В ІНТЕРЕСАХ ВОЄННОЇ СФЕРИ АБО СФЕРИ ОБОРОНИ УКРАЇНИ

МЕТОДИКА РАСЧЕТА ИНДИКАТОРОВ КИБЕРОБОРОНЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ (ВЕДОМСТВАХ, УЧРЕЖДЕНИЯХ, ПРЕДПРИЯТИЯХ, ОРГАНИЗАЦИЯХ) В

ИНТЕРЕСАХ ВОЕННОЙ СФЕРЫ ИЛИ СФЕРЫ ОБОРОНЫ УКРАИНЫ

METHOD OF CALCULATION INDICATORS CALCULATION INFORMATION AND TELECOMMUNICATION SYSTEMS IN GOVERNMENT BODIES (OFFICES, INSTITUTIONS, ENTERPRISES, ORGANIZATIONS) IN INTEREST THE MILITARY SPACE OR THE DEFENSE FIELD OF UKRAINE

Анотація. *В статті автором було здійснено аналіз загальних вимог що визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.*

Запропоновано методику розрахунку індикаторів кібероборони в інформаційно-телекомунікаційних системах органів державної влади (відомствах, установах, підприємствах та організаціях) в інтересах воєнної сфери або сфери оборони України у відповідності до існуючої нормативно-правової бази.

Імплементуючи керівні документи країн-членів НАТО, перелік індикаторів кібероборони та і сама методика розрахунку індикаторів кібероборони має комплексний підхід враховуючи результати проведення огляду громадської безпеки та цивільного захисту, огляду оборонно-промислового комплексу та огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації.

Індикатори кібероборони інформаційно-телекомунікаційних систем що призначені для використання в органах державної влади в інтересах воєнної

сфери або сфери оборони розроблено у відповідності до вимог Інструкцій Міністерства оборони Сполучених штатів Америки та оперативних стандартів НАТО (STANAG's).

Реалізація методики розрахунку індикаторів кібероборони здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової та матеріально-технічної допомоги від НАТО та країн-партнерів.

Ключові слова: *критична інфраструктура, індикатори кібероборони, кібероборона держави, інформаційно-телекомунікаційні системи.*

Аннотация. *В статье автором был осуществлен анализ общих требований определяющих организационно-методологические, технической и технологической условия киберзащиты объектов критической инфраструктуры, являются обязательными к выполнению предприятиями, учреждениями и организациями, которые согласно законодательству отнесены к объектам критической инфраструктуры.*

Предложена методика расчета индикаторов кибероборонны в информационно-телекоммуникационных системах органов государственной власти (ведомствах, учреждениях, предприятиях и организациях) в интересах военной сферы или сферы обороны Украины в соответствии с существующей нормативно-правовой базы.

Имплементируя руководящие документы стран-членов НАТО, перечень индикаторов кибероборонны да и сама методика расчета индикаторов кибероборонны имеет комплексный подход учитывая результаты проведения осмотра общественной безопасности и защиты, учитывая оборонно-

промышленного комплекса и осмотра состояния киберзащиты критической информационной инфраструктуры, государственных информационных ресурсов и информации.

Индикаторы кибероборонь информационно-телекоммуникационных систем предназначенных для использования в органах государственной власти в интересах военной сферы или сферы обороны разработана в соответствии с требованиями Инструкции Министерства обороны Соединенных Штатов Америки и оперативных стандартам НАТО (STANAG's).

Реализация методики расчета индикаторов кибероборонь осуществляется на основе государственного оборонного, безопасности, экономического, интеллектуального потенциала с использованием механизмов государственно-частного партнерства, а также с привлечением международной консультативной, финансовой и материально-технической помощи от НАТО и стран-партнеров.

Ключевые слова: *критическая инфраструктура, индикаторы кибероборонь, кибероборона государства, информационно-телекоммуникационные системы.*

Summary. *The article analyzes the general requirements that determine the organizational, methodological, technical and technological conditions of cyber defense of critical infrastructure objects, which are mandatory for the implementation of enterprises, institutions and organizations, which according to the law are assigned to critical infrastructure objects.*

The method of calculation of cyber defense indicators in information and telecommunication systems of state bodies (departments, institutions, enterprises

and organizations) in the interests of the military or defense sphere of Ukraine in accordance with the existing regulatory framework is proposed.

Implementing NATO guidance documents, the list of cyber defense indicators, and the methodology itself for calculating cyber defense indicators, takes a comprehensive approach, taking into account the results of the public security and civil defense review, defense industry review and review of cyber defense information and critical information infrastructure.

Cyber defense indicators for information and telecommunication systems designed for use by public authorities in the interests of the military or defense sector have been developed in accordance with the requirements of the United States Department of Defense's instructions and NATO's Standards of Operations (STANAG's).

The methodology for calculating cyber defense indicators is implemented on the basis of national defense, security, economic, intellectual potential, using public-private partnership mechanisms, as well as involving international advisory, financial and logistical assistance from NATO and partner countries.

Key words: *critical infrastructure, cyber defense indicators, state cyber defense, information and telecommunication systems.*

Постановка проблеми. Одним з пріоритетів національних інтересів України у сфері кібербезпеки, є наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина. Тому урахування негативних наслідків, до яких можуть призвести кібератаки на інформаційно-телекомунікаційну систему держави є вкрай важливою.

Можливими негативними наслідками є: виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону); негативний вплив на стан енергетичної безпеки

держави (регіону); негативний вплив на стан економічної безпеки держави; негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі; негативний вплив на систему управління державою; негативний вплив на суспільно-політичну ситуацію в державі; негативний вплив на імідж держави; порушення сталого функціонування фінансової системи держави; порушення сталого функціонування транспортної інфраструктури держави (регіону); порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав [1].

Враховуючи зазначене, введення показників (технічних даних), що використовуються для виявлення та реагування на кіберзагрози, в рамках функціонування діючої моделі системи кібероборони, здатної забезпечувати режим постійної готовності об’єктів критичної інформаційної інфраструктури на реальні і потенційні кіберзагрози будь-якого характеру є пріоритетним завданням.

Тому впровадження запропонованої методики розрахунку індикаторів кібероборони в інформаційно-телекомунікаційних системах органів державної влади в інтересах воєнної сфери або сфери оборони України у відповідності до сучасного міжнародного нормативно-правового поля є вкрай важливим та необхідним.

Аналіз останніх досліджень і публікацій. Загальні вимоги що визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями [2], які відповідно до законодавства віднесені до об’єктів критичної інфраструктури висвітлені в: Стратегії національної безпеки України, затвердженій Указом Президента

України від 26.05.2015 № 287/2015, Концепції розвитку сектору безпеки і оборони України, затвердженій Указом Президента України від 14.03.2016 № 92/2016, Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.2016 № 563, Рішенні Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року – Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32, Законі України "Про національну безпеку України", від 21.06.2018 № 2469-VIII.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури/об'єкта критичної інфраструктури, окреслені в затвердженому постановою Кабінету Міністрів України від 19.06.2019 № 518 Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації [3].

Проте, незважаючи на значну кількість керівних документів за даною тематикою, існує багато невирішених питань щодо визначення індикаторів кібероборони, їх методика розрахунку в інформаційно-телекомунікаційних системах органів державної влади в інтересах воєнної сфери або сфери оборони України, системах оборонного та військового призначення до кібероборони [4-5].

Формулювання цілей статті (постановка завдання). Мета статті полягає у визначенні загальних індикаторів готовності інформаційно-

телекомунікаційних систем оборонного і військового призначення до кібероборони, оцінці спроможностей (можливостей) до відбиття агресії в кіберпросторі України та розроблення методики розрахунку індикаторів кібероборони інформаційно-телекомунікаційних систем в органах державної влади (відомстві, установі, підприємстві, організації) в інтересах реалізації державної політики в сфері оборони України.

Виклад основного матеріалу. З метою імплементації керівних документів країн-членів НАТО, перелік індикаторів кібероборони розроблено у відповідності до вимог Інструкції Міністерства оборони Сполучених штатів Америки "Cybersecurity Activities Support to DoD Information Network Operations" від 07.03.2016 № 8530.01 [6], враховуючи розгалуженість існуючих інформаційно-телекомунікаційних систем органів державної влади, державних ресурсів і т.і. у сфері оборони України.

Впровадження зазначених вище стандартів НАТО забезпечить планомірне нарощування боєздатності військ (сил) та досягнення взаємосумісності з силами та засобами провідних країн світу, сприятиме підвищенню ефективності використання державних ресурсів у сфері оборони.

Індикатори кібероборони інформаційно-телекомунікаційної системи класу "2" або "3" (з підключенням або без підключення до глобальної мережі), що призначена для використання в органі державної влади (відомстві, установі, підприємстві, організації) в інтересах воєнної сфери або сфери оборони складаються з :

1. Індикатору оцінки та аналізу вразливостей (Indication Vulnerability Assessment and Analysis) [I_{vula}];

2. Індикатору керування вразливостями (Indication Vulnerability Management) [I_{vulm}];

3. Індикатору захищеності від шкідливого програмного

забезпечення (Indication Malware Protection) [I_{malp}];

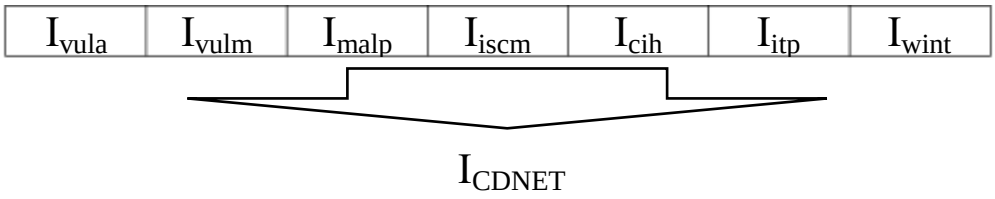
4. Індикатору моніторингу безпеки інформації (Indication Information Security Continuous Monitoring (ISCM)) [I_{iscm}];

5. Індикатору обробки кіберінцидентів (Indication Cyber Incident Handling) [I_{cih}];

6. Індикатору моніторингу інсайдерської діяльності користувачів (Indication user activity monitoring (UAM) of information network for Insider Threat Program) [I_{itp}];

7. Індикатору попередження мережевої розвідки (Indication Warning Intelligence) [I_{wint}].

Порядок розрахунку індикатору кібероборони для однієї інформаційно-телекомунікаційної системи:



$$\boldsymbol{I_{CDNET\ 1} = \frac{\sum_{i=1} I_n}{n}, \quad n = 7, \quad I_{CDNET\ 1} = [0,1]}$$

Порядок розрахунку індикатору кібероборони для сукупності інформаційно-телекомунікаційних систем, що призначені для використання в інтересах воєнної сфери або сфери оборони, одного органу державної влади (відомства, установи, підприємства, організації):

$$\boldsymbol{I_{CDNET\ DEP} = \frac{\sum_{i=1}^{n} I_{CDNET\ n}}{n}, \quad I_{CDNET\ DEP} = [0,1]}$$

Індикатори діяльності органу державної влади (відомства, установи, підприємства, організації) у сфері кібероборони складається з :

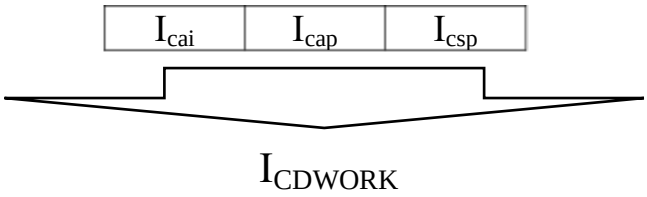
1. Індикатору інтеграції діяльності з кібербезпеки за напрямом

операцій в кіберпросторі (Indication Cybersecurity Activities Integration to support operations in cyberspace) [I_{cai}];

2. Індикатору інтеграції діяльності з кібербезпеки за напрямом кіберзахисту інформаційно-телекомунікаційних систем воєнної сфери та сфери оборони (Indication Cybersecurity Activities Integration to protect the information network) [I_{cap}];

3. Індикатору ефективності діяльності постачальника послуг з кібербезпеки (Indication Cybersecurity Service Providers) [I_{csp}].

Порядок розрахунку індикатору діяльності у сфері кібероборони для одного органу державної влади (відомства, установи, підприємства, організації):



$$\boldsymbol{I_{CDWORK\ DEP} = \frac{\sum_{i=1}^{n} I_n}{n}}, \qquad \boldsymbol{n = 3}, \qquad \boldsymbol{I_{CDWORK\ DEP} = [0, 1]}$$

Таким чином, у відповідності до розроблених методик для кожного органу державної влади (відомства, установи, підприємства, організації), що виконує завдання в інтересах воєнної сфери або сфери оборони, проводиться визначення двох індикаторів, а саме:

– індикатор кібероборони для сукупності інформаційно-телекомунікаційних систем (що призначені для використання в інтересах воєнної сфери або сфери оборони) одного органу державної влади (відомства, установи, підприємства, організації) – $\mathbf{I_{CDNET\ DEP}}$;
– індикатор діяльності органу державної влади (відомства, установи,

підприємства, організації) у сфері кібероборони – $\mathbf{I_{CDWORK\ DEP}}$.

Після визначення зазначених індикаторів для кожного органу державної влади (відомства, установи, підприємства, організації), що виконують завдання у воєнній сфері або сфері оборони, проводиться обчислення загальнодержавних індикаторів кібероборони, а саме:

– індикатор кібероборони інформаційно-телекомунікаційних систем воєнної сфери та сфери оборони:

$$\boldsymbol{I_{CDNET\ GOV} = \frac{\sum_{i=1}^{n} I_{CDNET\ DEP\ n}}{n}}, \quad \boldsymbol{I_{CDNET\ GOV} = [0, 1]}$$

– індикатор діяльності суб'єктів воєнної сфери та сфери оборони з кібероборони держави:

$$\boldsymbol{I_{CDWORK\ GOV} = \frac{\sum_{i=1}^{n} I_{CDWORK\ DEP\ n}}{n}}, \qquad \boldsymbol{I_{CDWORK\ GOV} = [0, 1]}$$

Розробку методик для проведення оцінки (тестування) інформаційно-телекомунікаційних систем та діяльності суб'єктів воєнної сфери і сфери оборони за напрямом кібероборони держави, пропонується здійснити на основі вже розроблених методик, що наведені в керівних документах Міністерства оборони та Генерального штабу Збройних Сил Сполучених штатів Америки, а також керівних документах Збройних Сил країн-членів НАТО.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Встановлення і оперативна адаптація розробленої методики, на об'єктах критичної інформаційної інфраструктури держави, у тому числі під час їх створення, введення в експлуатацію, під час експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, надасть змогу:

– визначити загальні індикатори готовності інформаційно-телекомунікаційних систем оборонного і військового призначення до кібероборони;
– оцінити спроможності (можливості) до відбиття агресії в кіберпросторі України;
– розрахувати індикатори кібероборони інформаційно-телекомунікаційних систем в органах державної влади (відомстві, установі, підприємстві, організації) в інтересах воєнної сфери або сфери оборони України;
– впровадити єдину (універсальну) систему індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;
– здійснювати постійний моніторинг національної системи кібербезпеки, у відповідності до індикаторів стану кібербезпеки.

Як перспектива подальших розвідок, слід зазначити, що для своєчасного отримування відомостей про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли, за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз, планується продовжити дослідження щодо оптимізації системи індикаторів, що запропоновані.

Література

1. Постанова Кабінету Міністрів України № 518 від 19.06.2019 року, Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п.
2. Постанова Кабінету Міністрів України № 563 від 23.08.2016 року, Про затвердження порядку формування переліку інформаційно-

телекомунікаційних систем об’єктів критичної інфраструктури держави. URL: https://zakon.rada.gov.ua/laws/show/563-2016-п.

3. Указ Президента України № 254/2017 від 30.08.2017, Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року “Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”. URL: https://www.president.gov.ua/documents/2542017-22502.
4. Закон України № 2469-VIII від 21.06.2018 року, Про національну безпеку України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
5. Закон України № 2163-VIII від 05.10.2017 року, Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
6. CJCSM 6510.01B, DISTRIBUTION: A, B, C, JEL, S 10 July 2012, Cyber incident handling program. URL: https://www.dtic.mil/cjcs_directives.

References

1. Postanova Kabinetu Ministriv Ukrajiny # 518 vid 19.06.2019 roku, Pro zatverdzhennja zaghaljnykh vymogh do kiberzakhystu ob'jektiv krytychnoji infrastruktury. URL: https://zakon.rada.gov.ua/laws/show/518-2019-p.
2. Postanova Kabinetu Ministriv Ukrajiny # 563 vid 23.08.2016 roku, Pro zatverdzhennja porjadku formuvannja pereliku informacijno-telekomunikacijnykh system ob'jektiv krytychnoji infrastruktury derzhavy. URL: https://zakon.rada.gov.ua/laws/show/563-2016-p.
3. Ukaz Prezydenta Ukrajiny # 254/2017 vid 30.08.2017, Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 10 lypnja 2017 roku “Pro stan vykonannja rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 29

ghrudnja 2016 roku “Pro zaghrozy kiberbezpeci derzhavy ta nevidkladni zakhody z jikh nejtralizaciji”. URL: https://www.president.gov.ua/documents/2542017-22502.

4. Zakon Ukrajiny # 2469-VIII vid 21.06.2018 roku, Pro nacionaljnu bezpeku Ukrajiny. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
5. Zakon Ukrajiny # 2163-VIII vid 05.10.2017 roku, Pro osnovni zasady zabezpechennja kiberbezpeky Ukrajiny. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
6. CJCSM 6510.01B, DISTRIBUTION: A, B, C, JeL, S 10 July 2012, Cyber incident handling program. URL: https://www.dtic.mil/cjcs_directives.