КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.184196
УДК 004.056.53

Гнатюк Сергій Олександрович
д.т.н., доцент, заступник декана Факультету кібербезпеки, комп'ютерної та програмної інженерії
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Поліщук Юлія Ярославівна
аспірант PhD науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0002-0686-2328
liya7954@gmail.com

Сотніченко Юлія Олексіївна
здобувач PhD
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0002-1281-9238
yu.sotnichenko@gmail.com

Жаксигулова Даурія Дарибаївна
докторант PhD
Східноказахстанський технічний університет ім. Д. Серікбаєва, Усть-Каменогорськ, Казахстан
ORCID: 0000-0003-0646-2823
dauriya.dzh@gmail.com

АНАЛІЗ КРАЩИХ СВІТОВИХ ПРАКТИК ЩОДО ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. При великій кількості кіберінцидентів та кіберзагроз, які реалізуються щодня, захист критичної інфраструктури є важливою не тільки технічною, а й науковою задачею. Проте, не всі держави світу на високому рівні можуть забезпечити якісний захист такої інфраструктури. Виходячи з того, що забезпечення захисту критичної інформаційної інфраструктури має проводитись на державному рівні, державам необхідно розробити (адаптувати, модернізувати) нормативно-правову базу для врегулювання зазначеного питання. У законодавчій базі України, як і в більшості пострадянських держав, на сьогодні відсутній чіткий підхід до захисту критичної інформаційної інфраструктури (у такому масштабі, як на приклад, в США чи ЄС). Законодавством України встановлено лише окремі об'єкти соціально-економічної сфери, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, а єдиний порядок ідентифікації та класифікації об'єктів критичної інфраструктури ще остаточно не затверджено. Нормативно невизначеною залишається низка основоположних термінів у сфері захисту критичної інфраструктури від кіберзагроз, зокрема і саме поняття «критичної інфраструктури». Потребує наукового обґрунтування механізм організації діяльності та взаємодії державних органів і приватних структур у процесі захисту критичної інфраструктури. У цій роботі проведено аналіз кращих світових практик щодо захисту критичної інформаційної інфраструктури, реалізація елементів якої на законодавчому рівні і в практичній площині, дозволить якісно покращити процес захисту критичної інформаційної інфраструктури України.

Ключові слова: критична інформаційна інфраструктура держави; інформаційна безпека; кращі світові практики, кіберзагроза, нормативно-правова база.

1. ВСТУП

Захист критичної інформаційної інфраструктури (КІІ) є складною, але важливою сферою для розвинених держав світу. Суспільство цих держав повністю залежить від послуг критичної інфраструктури (КІ), таких як енергопостачання, телекомунікації, фінансові системи, питна вода, державні послуги тощо. На сьогодні фізична шкода (або навіть руйнування) критичних елементів КІ не є єдиним чинником, що загрожує правильній роботі КІ. Послуги (сервіси), що базуються на сучасних інформаційно-комунікаційних технологіях (ІКТ), стають все більш важливими для функціонування КІ. Порушення у роботі інформаційної інфраструктури може спричинити серйозні наслідки для держави та її громадян – це призводить до розуміння КІІ, яка включає як інформаційну, так і комунікаційну інфраструктуру (наприклад, послуги мобільної телефонії та доступу до Інтернету), а також системи ІКТ та управління процесами, які є критичною частиною надання послуг КІ. Порушення у роботі КІІ можуть бути спричинені техногенними, технічними збоями та катастрофами (як це відбувається у КІ). Однак, переваги КІІ (збільшення підключеності, віддалений моніторинг, масштабованість, надійність, зниження витрат) не завжди однаково збалансовані з можливими несприятливими наслідками несправності КІІ. Сьогодні, КІІ стає все більш важливою частиною КІ. У той же час КІІ може бути одночасно і мішенню для зловмисного програмного забезпечення, хакерів, хактивістів та несприятливих державних операцій, а також засобом нападу на КІІ іншої держави. Скомпрометована або порушена КІІ може поставити під загрозу національну безпеку та стабільність, економічне зростання, процвітання громадян та повсякденне життя і може мати далекосяжний вплив на інші держави через глобальний взаємозв'язок їх КІІ. Тому, потреба в ефективних стратегіях, політиці та нормативних документах захисту КІІ стає все більш важливою у більшості держав.

Постановка проблеми. Сьогодні, низка держав світу перебуває на шляху формування процедури захисту КІ, але вони мають не вирішені проблеми, пов’язані із різними аспектами захисту КІІ (нормативні, технічні, процедурні). У цій статті авторами пропонується аналіз кращих світових практик щодо захисту КІІ, що в перспективі може допомогти державам, які розвиваються (у тому числі і для України), розробити потужний інструмент для врегулювання проблем та пошуку можливостей для ефективного забезпечення захисту КІІ.

Мета статті. Метою цієї статті є аналіз кращих світових практик в сфері захисту КІІ, що на сьогодні реалізовано на національному та міжнародному рівнях.

2. ОГЛЯД ЛІТЕРАТУРИ ТА ТЕОРЕТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ

Основне джерело регулювання питання захисту КІІ в Європейському Союзі (ЄС) – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [1] (далі – NISD). Директива не є єдиним актом, який регулює питання кібербезпеки (КБ) в ЄС. Інциденти у сфері КІІ, які охоплюються вказаною Директивою, також є предметом регулювання інших Директив та Регламентів ЄС – наприклад, GDPR [2]. Основні області та регулюючі документи NISD показні на рис.1.

Проте, Директива NISD вимагає трансформації у внутрішньому праві, тобто не діє самостійно, а має бути доповнена окремими регламентами. Це означає, що державам-членам ЄС пропонується самостійно визначити питання імплементації

положень директиви, яка визначає лише мінімальний стандарт захисту. Відповідно до ст. 25 NISD, держави-члени ЄС повинні опублікувати відповідні законодавчі положення для виконання вимог Директиви NISD. При цьому відповідні акти повинні містити посилання на цю Директиву.

Відповідно до ст. 5. Директиви NISD, держава-член має повну свободу у виборі способів імплементації відповідних положень. Держави-члени можуть встановити більш високі стандарти безпеки. Як вказано в п. 6 Преамбули Директиви NISD, не виключено застосування більш суворих мір для операторів життєво-важливих послуг та провайдерів цифрових послуг.

Рис. 1. Сфери регулювання КІІ в ЄС

Наприклад, Німеччина у 2017 р. прийняла Закон про імплементацію положень Директив [3] та внесення змін до відповідних законодавчих актів. В Німеччині це питання урегульоване в Законі BSIG [4], а також в Указі щодо визначення критичної інфраструктури відповідно до Закону BSIG. Німецьке регулювання у багато чому є схожим з російським підходом і представляє інтерес, головним чином, у частині класифікації об'єктів КІІ. Незважаючи на BREXIT, в питаннях імплементації, Великобританія прийняла відповідний Статут № 506, який вступив у силу в травні 2018 р.

У п. 2 ст. 1, ст. 7 Директиви NISD, держави-члени повинні прийняти національні стратегії щодо забезпечення безпеки мережевих та інформаційних систем, а також встановити вимоги до відповідних суб'єктів, зокрема, визначити критерії критичності можливого негативного впливу, встановити класифікацію таких суб'єктів залежно від цих критеріїв. У п. 19 Преамбули Директиви NIS відзначається: держави-члени ЄС відповідають за визначення організацій, що відповідають критеріям визначення оператора життєво-важливих послуг. Список таких операторів повинен регулярно переглядатися державами-членами ЄС та, за необхідності, оновлюватись. Аналогічне положення міститься і в п. 25 Преамбули, згідно якого в результаті ідентифікаційного процесу державою-членом ЄС повинні бути прийняті заходи щодо визначення організацій, які повинні виконувати зобов'язання щодо забезпечення безпеки мережевих та інформаційних систем. Указані цілі можуть бути досягнуті шляхом прийняття переліку всіх операторів або прийняття загальних мір, у тому числі об'єктивних кількісних критеріїв, таких як виробнича потужність оператора або

кількість користувачів, що дозволяють визначати організації, зобов'язані виконувати вимоги щодо забезпечення безпеки мережевих та інформаційних систем.

Національні стратегії КБ діють у більшості держав ЄС. У Стратегіях КБ Німеччини особливу увагу надано питанням захисту КІ [5], приділено увагу цьому питанню і в Національній стратегії цифрової безпеки Франції [6]. У Національній стратегії КБ Об'єднаного королівства на 2016-2021 роки також ідеться про захист критичної національної інфраструктури (CNI) через захист найбільш важливих організацій та компаній від кібератак. Особи, які керують такими компаніями, несуть відповідальність за забезпечення безпеки – вони повинні ідентифікувати критичні системи та регулярно оцінювати їх уразливості. Органи державної влади також беруть участь у низці зобов'язань у зазначеній сфері [7].

Важливо відзначити, що Директива NISD не застосовується:

1) до мікропідприємств (працює не більше 50 людей, дохід не перевищує 10 млн. євро в рік) та малих підприємств (працює не більше 10 людей, дохід не перевищує 2 млн. євро в рік), відповідно до п. 11 ст. 16 Директиви 2016/1148;

2) до підприємств, що надають послуги у сфері громадських мереж зв'язку та загальнодоступних електронних комунікацій, відповідно до п. 3 ст. 1 Директиви і п. 7 Преамбули;

3) до провайдерів сервісів для електронних транзакцій, відповідно до п. 3 ст. 1 Директиви і п. 7 Преамбули;

4) до інших підприємств, діяльність яких є предметом регулювання (справжніх чи майбутніх) внутрішньогалузевих актів ЄС, що містять норми про безпеку мережевих та інформаційних систем, за винятком випадків дублювання аналогічних положень (п. 9 Преамбули);

5) до платіжних і розрахункових систем (п. 14 Преамбули);

6) до підприємств, що надають онлайн-послуги, в рамках яких представляється порівняльний аналіз цін на певні товари або послуги, що надаються різними постачальниками, і здійснюється подальший напрямок користувача до обраного ним постачальника для купівлі продукту (п. 15 Преамбули).

Як один з національних інтересів в інформаційній сфері, Доктрина інформаційної безпеки РФ забезпечує стале та безперебійне функціонування інформаційної інфраструктури, в першу чергу КІІ та єдиної мережі електрозв'язку РФ, в мирний час, в період безпосередньої загрози агресії і у воєнний час. Стратегічною метою забезпечення інформаційної безпеки є захист КІІ. Одним з напрямків забезпечення інформаційної безпеки Доктрина вважає підвищення захищеності КІІ, підвищення безпеки функціонування її об'єктів [8]. Основним актом, що регулює питання КІІ в РФ, є Федеральний Закон «Про безпеку КІІ». Система захисту КІІ в РФ є розробленою не тільки на рівні Федерального Закону, а й на рівні безлічі підзаконних актів Президента, Уряду та ФСБ. Законодавство передбачає конкретні правила категоризації об'єктів КІІ, обов'язки суб'єктів КІІ, порядок їх взаємодії з ФСБ. Кримінальний кодекс встановлює покарання за неправомірний вплив на КІІ. Разом з тим, варто зазначити, що оцінити успішність застосування положень правових актів в зазначеній сфері є досить важко так як згідно ст. 5 Закону РФ «Про державну таємницю» відомості про заходи щодо забезпечення безпеки критичної інформаційної інфраструктури РФ і про стан її захищеності від комп'ютерних атак відносяться до відомостей, що становлять державну таємницю.

У липні 2015 р. Постійний комітет Загальнокитайських зборів народних представників прийняв Закон про національну безпеку (The National Security Law,

NSL) [9]. NSL вперше передбачає «захист національного суверенітету в кіберпросторі» і вказує КБ та інформаційну безпеку в якості важливих частин національної безпеки. NSL вимагає від держави створити систему перевірки національної безпеки для розгляду питань і дій, які впливають, або можуть вплинути на національну безпеку, включаючи ті, що стосуються продуктів і послуг мережевих інформаційних технологій. Закон про боротьбу з тероризмом (The Counter-Terrorism Law, CTL) був прийнятий в кінці 2015 року, набрав чинності 1 червня 2017 року і став основним законом в Китаї щодо забезпечення КБ і особистої інформації. CTL є першим законом про боротьбу з тероризмом в Китаї, який включає в себе великий масив положень, що мають на меті охопити всі аспекти контртерористичної діяльності. CTL забезпечує зобов'язання телекомунікаційних та Інтернет-підприємств співпрацювати з державними органами у розслідуванні терористичної діяльності. Наприклад, згідно з CTL, провайдери телекомунікаційних та Інтернет-послуг зобов'язані надавати державним органам технічну допомогу в розшифруванні повідомлень. Закон про кібербезпеку (The Cyber Security Law, CSL) містить різні зобов'язання щодо захисту для мережевих операторів, включаючи, але не обмежуючись наступними аспектами: 1) дотримання низки вимог до багаторівневих систем КБ; 2) перевірку достовірності особи користувача (обов'язок для певних операторів мережі); 3) розробку планів реагування на надзвичайні ситуації в області КБ; 4) надання допомоги і підтримки слідчим органам, у разі необхідності, для захисту національної безпеки і розслідування злочинів. CSL накладає ряд підвищених зобов'язань в області безпеки для операторів КІІ, серед яких можна виділити: вимоги до внутрішньої організації, навчання, створення резервної копії даних і аварійного реагування на інциденти; вимога про захищене зберіганні особистої інформації та іншої важливої інформації на території КНР; вимога про проходження перевірки безпеки щодо закупівлі мережевих продуктів і послуг, які можуть вплинути на національну безпеку; вимога про подання щорічних звітів щодо результатів оцінки безпеки та заходи щодо поліпшення до компетентних державних органів.

У травні 1998 року у світ вийшла директива Президента США № 63 «Стратегія спільних зусиль адміністрації США і приватного сектора в галузі захисту критичної інфраструктури». Вона визначала мету і завдання, які вирішуються для забезпечення захисту національної інфраструктури від навмисних атак, і супроводжувалася адміністративними указами президента № 13130 «Про Національну раду з критичної інфраструктури» та № 13231 «Про захист національних критичних інформаційних систем». У відповідності з цими документами почалося формування центрів інформаційного обміну та аналізу (Information Sharing and Analysis Centers), а також національної ради з КІ (National Infrastructure Advisory Council – NIAC). У кінці 2001 року був створений Національний центр аналізу та імітаційного моделювання інфраструктури (The National Infrastructure Simulation and Analysis Center – NISAC), а в листопаді 2002 року утворено Міністерство внутрішньої безпеки (МВБ), на яке і було покладено загальне керівництво заходами забезпечення захисту національної інфраструктури від різних загроз.

У 2018 році набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України» [10]. Закон запроваджує поняття об'єкта КІ, визначає повноваження для формування переліку об'єктів КІ, декларує спеціальний режим для операторів КІ, однак не встановлює критеріїв, згідно з якими ті чи інші об'єкти можуть бути ідентифіковані як об'єкти критичної інфраструктури. Порядок реалізації таких повноважень відповідно до Закону мав бути прийнятий ще у 2018 році. Чинний Закон визначає, що до об'єктів КІ можуть бути віднесені підприємства, установи та

організації, які здійснюють діяльність і надають послуги в галузі енергетики, хімічної промисловості, транспорту, ІКТ, електронних комунікацій, у банківському і фінансовому секторах. Мінекономрозвитку розробило і в червні 2020 року розмістило для публічного обговорення на своєму офіційному веб-сайті проект закону «Про захист КІ» [11]. У проекті закону пропонується визначення основних принципів державної політики в сфері захисту КІ; врегулювання правових і господарських відносин, що виникають при такій діяльності; повноваження державних органів у сфері захисту КІ, серед яких Адміністрація Держспецзв'язку. Також, проєкт закону передбачає повноваження Адміністрації Держспецзв`язку у формуванні та реалізації державної політики щодо захисту критичної технологічної інформації; формуванні загальних вимог до кіберзахисту об'єктів КІ. Крім того, передбачається, що Адміністрація Держспецзв`язку буде здійснювати державний контроль у цій сфері та вести перелік об'єктів КІІ, здійснювати заходи щодо його поновлення та актуалізації. Цей Закон встановлює принципи та напрями розбудови державної системи захисту КІ, визначає правові та організаційні засади забезпечення її діяльності і є складовою частиною законодавства України у сфері національної безпеки. Також, в Україні було опубліковано «Порядок формування переліку об’єктів КІІ», що визначає механізм формування національного та секторальних переліків об’єктів КІІ. Крім того, опубліковано «Порядок віднесення об’єктів до об’єктів КІ». Порядок визначає механізм внесення об’єктів КІІ до державного реєстру об’єктів КІІ, його формування та забезпечення функціонування. Опублікована Методика категоризації об’єктів КІ, яка визначає механізм та критерії віднесення об’єктів КІ до однієї з категорій критичності.

3. ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Авторами було проведено багатокритеріальний аналіз нормативних документів в сфері захисту КІІ та досліджено досвід провідних держав за такими критеріями:

- нормативний документ, який регулює захист КІ
- поняття КІІ,
- принципи регулювання в сфері КІІ;
- предмет регулювання в сфері КІІ;
- критерії віднесення до КІІ;
- сфери забезпечення захисту КІІ;
- суб'єкти в сфері КІІ;
- органи регулювання сфери забезпечення захисту КІІ;
- економічна модель регулювання, відповідальність у сфері забезпечення захисту КІІ.

1. ЄС (у тому числі Великобританія)

Назва нормативного документу: Directive (EU) 2016/1148 of the European Parliament and of the Council.

Аналіз поняття КІІ: об'єкт, установка або її частина, яка відносяться до секторів енергетики, інформаційних технологій, телекомунікацій, транспорту, дорожнього руху, охорони здоров'я, водопостачання, харчування, фінансів, страхування; має велике значення для функціонування спільноти, тому що відмова в їх роботі або погіршення їх функціонування призведе до значного дефіциту поставок або загрозу для громадської безпеки.

Принципи регулювання в сфері КІІ: пріоритет прав і свобод; суб'єктно-діяльнісний підхід підходу; облік спрямованості діяльності; ризик-орієнтовний підхід; конфіденційність і повага бізнес-інтересів; пропорційність; встановлення мінімального рівня гарантій, з можливістю їх підвищення; комплексний підхід до питань КБ; врахування інтересів всіх зацікавлених сторін.

Предмет регулювання в сфері КІІ: оператори надання життєво-важливих послуг і провайдери цифрових послуг.

Критерії віднесення до КІІ: відносяться до секторів енергетики, інформаційних технологій, телекомунікацій, транспорту, дорожнього руху, охорони здоров'я, водопостачання, харчування, фінансів, страхування. Мають велике значення для функціонування спільноти, тому що відмова в їх роботі або погіршення їх експлуатації призведе до значного дефіциту поставок або загрозу для громадської безпеки.

Сфери забезпечення захисту КІІ: енергетика; транспорт; банківська справа; фінансовий ринок; охорона здоров'я; поставки питної води; цифрова інфраструктура.

Суб'єкти в сфері КІІ: оператор життєво-важливих послуг; провайдери цифрових послуг. Основні обов'язки: прийняття необхідних організаційних і технічних заходів захисту, повідомлення про інциденти.

Органи регулювання сфери забезпечення захисту КІІ: Національний компетентний орган, відповідальний за безпеку мережевих та інформаційних систем (СА), Єдиний національний контактний пункт з питань безпеки мережевих та інформаційних систем (SPOC), Групи реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT).

Економічна модель регулювання: Обов'язок по виконанню вимог закону розподілена між компетентними органами та органами надання життєво-важливих послуг, провайдерами цифрових послуг. Більше вимог відповідні нормативно-правові акти пред'являють до органів надання життєво-важливих послуг.

Відповідальність у сфері забезпечення захисту КІІ: [відомості відсутні].

2. РФ

Назва нормативного документу: Law on the Federal Office for Information Security

Аналіз поняття КІІ: об'єкти КІІ, а також мережі електрозв'язку, що використовуються для організації взаємодії таких об'єктів.

Принципи регулювання в сфері КІІ: принцип законності; принцип безперервності і комплексності забезпечення безпеки КІІ; принцип взаємодії органів виконавчої влади і суб'єктів КІІ; пріоритет запобігання комп'ютерних атак.

Предмет регулювання в сфері КІІ: об'єкти КІІ.

Критерії віднесення до КІІ: соціальна, економічна, політична, екологічна значимість, значимість для оборони держави, безпеки та правопорядку.

Сфери забезпечення захисту КІІ: соціальна; економічна; політична; екологічна; безпека і правопорядок.

Суб'єкти в сфері КІІ: особи, яким на праві власності, оренди або на іншій законній підставі належать інформаційні системи, інформаційно-телекомунікаційні мережі, автоматизовані системи управління, що функціонують в зазначених сферах.

Органи регулювання сфери забезпечення захисту КІІ: Президент, Уряд, Федеральна Служба Безпеки РФ, Федеральна служба з технічного та експортного контролю РФ.

Економічна модель регулювання: обов'язки по виконанню вимог Закону «Про безпеку КІІ» та підзаконних актів розподілені між державними органами і суб'єктами

КІІ. Значна кількість обов'язків по фінансовим витратам покладено виключно на суб'єктів КІІ.

Відповідальність у сфері забезпечення захисту КІІ: кримінальна, адміністративна.

3. США

Назва нормативного документу: Директива Президентської політики США «Безпека і стійкість КІ».

Аналіз поняття КІІ: системи та активи, фізичні чи віртуальні, настільки життєво-важливі для США, що порушення функціонування або руйнування таких систем і активів надасть руйнівний вплив на безпеку, національну економічну безпеку, національна охорона здоров'я або охорону здоров'я або будь-яке поєднання цих питань.

Принципи регулювання в сфері КІІ: уточнення функціональних відносин між федеральним урядом для просування національної єдності, зусиль по зміцненню безпеки і стабільності критичної інфраструктури; забезпечення ефективного обміну інформацією шляхом визначення базових даних і системних вимог для федерального уряду; впровадження функції інтеграції і аналізу для інформування про планування і прийнятті операційних рішень щодо критично важливої інфраструктури.

Предмет регулювання в сфері КІІ: діяльність і послуги в певних секторах.

Критерії віднесення до КІІ: критерії не визначені. Встановлено шістнадцять критичних секторів.

Сфери забезпечення захисту КІІ: хімічний сектор; сектор комерційних об'єктів; сектор комунікацій; сектор критичного виробництва: греблі, військово-промислові бази, аварійно-рятувальні служби; енергетика; фінансовий; продовольство і сільське господарства; державні установи; охорона здоров'я та громадське здоров'я; інформаційні технології; ядерні реактори, матеріали та відходи; транспортні системи; системи водопостачання, збору та відведення стічних вод.

Суб'єкти в сфері КІІ: власники і оператори КІ.

Органи регулювання сфери забезпечення захисту КІІ: міністр внутрішньої безпеки; галузеві агентства у критичних секторах; інші органи федеральної влади в межах певної для них компетенції.

Економічна модель регулювання: [відомості відсутні].

Відповідальність у сфері забезпечення захисту КІІ: поєднання кримінальної та адміністративної відповідальності.

4. Сінгапур

Назва нормативного документу: Cybersecurity Act 2018.

Аналіз поняття КІІ: комп'ютер або комп'ютерна система, яка необхідна для безперервного надання основних послуг, пов'язаних з втратою або виснажливими впливами на національну безпеку, оборону, міжнародні відносини, економіку, громадської охорони здоров'я, громадської безпеки або громадського порядку Сінгапуру.

Принципи регулювання в сфері КІІ: [відомості відсутні].

Предмет регулювання в сфері КІІ: [відомості відсутні].

Критерії віднесення до КІІ: [відомості відсутні].

Сфери забезпечення захисту КІІ: енергетика; інформаційні комунікації; водопостачання; охорона здоров'я; банківська справа та фінанси; охоронні і аварійні служби; авіація; наземний транспорт; морський транспорт; уряд; засоби масової інформації.

Суб'єкти в сфері КІІ: [відомості відсутні].

Органи регулювання сфери забезпечення захисту КІІ: Національні галузеві контрольні або наглядові департаменти; Національний відділ КБ та інформатизації; Підрозділи Державної ради з питань громадської безпеки, державної безпеки, адміністративному управлінню захистом державної таємниці, управління державним шифруванням.

Економічна модель регулювання: [відомості відсутні].

Відповідальність у сфері забезпечення захисту КІІ: кримінальна.

5. КНР

Назва нормативного документу: The Cyber Security Law.

Аналіз поняття КІІ: КІІ відноситься до національної безпеки, національної економіки та засобів існування людей, в сферах, що включають інформаційні мережі, енергетику, фінанси, транспорт, освіту, наукову сферу, охорону водних ресурсів, промислове виробництво, медицину та охорону здоров'я, соціальне забезпечення, комунальні послуги та інші важливі інформаційні системи.

Принципи регулювання в сфері КІІ: повага до збереження суверенітету кіберпростору; мирне використання кіберпростору; управління кіберпростором відповідно до закону; координація безпеки і розвитку мережі.

Предмет регулювання в сфері КІІ: [відомості відсутні].

Критерії віднесення до КІІ: [відомості відсутні].

Сфери забезпечення захисту КІІ: Галузі: охорона здоров'я, освіта, соціальне забезпечення і захист навколишнього середовища. Інформаційні мережі: радіо і телевізійні мережі, інтернет; постачальники послуг, що надають хмарні обчислення, великі дані та інші великі загальнодоступні інформаційні та мережеві послуги. Наукові дослідження і виробництво: оборонна промисловість, велика промисловість обладнання, нафтохімічна і харчова та фармацевтична промисловість. ЗМІ і новини: радіостанції, телевізійні станції і служби новин.

Суб'єкти в сфері КІІ: оператори КІІ

Органи регулювання сфери забезпечення захисту КІІ: [відомості відсутні].

Економічна модель регулювання: [відомості відсутні].

Відповідальність у сфері забезпечення захисту КІІ: [відомості відсутні].

5. Японія

Назва нормативного документу: The Basic Act on Cybersecurity.

Аналіз поняття КІІ: [відомості відсутні].

Принципи регулювання в сфері КІІ: вільне переміщення інформації; повага до прав громадян; дотримання інтересів всіх зацікавлених сторін; співпраця суб'єктів КІІ.

Предмет регулювання в сфері КІІ: [відомості відсутні].

Критерії віднесення до КІІ: [відомості відсутні].

Сфери забезпечення захисту КІІ: ІКТ; фінансовий сектор; авіація; залізничне сполучення; електрика; газ; уряд і державні служби (включаючи місцеві органи влади); медицина; водопостачання; логістика.

Суб'єкти в сфері КІІ: [відомості відсутні].

Органи регулювання сфери забезпечення захисту КІІ: [відомості відсутні].

Економічна модель регулювання: [відомості відсутні].

Відповідальність у сфері забезпечення захисту КІІ: [відомості відсутні].

6. Україна

Назва нормативного документу: Закон України «Про захист критичної інфраструктури»

Аналіз поняття КІІ: сукупність об'єктів КІІ.

Принципи регулювання в сфері КІІ: єдність методологічних засад; координованість; державно-приватна взаємодія; конфіденційність комерційної інформації; міжнародне співробітництво.

Предмет регулювання в сфері КІІ: об'єкти КІІ

Критерії віднесення до КІІ: відповідно до рівня важливості об’єктів КІІ для забезпечення окремих життєво важливих функцій та послуг, в межах секторів КІ здійснюється категоризація об’єктів КІ.

Сфери забезпечення захисту КІІ: Урядування та надання найважливіших державних послуг; енергозабезпечення; водопостачання та водовідведення; продовольче забезпечення; охорона здоров’я; інформаційні, комунікаційні та цифрові послуги; фінансові та банківські послуги; транспортне забезпечення; оборона; правопорядок; постачання теплової енергії.

Суб'єкти в сфері КІІ: Кабінет Міністрів України; Уповноважений орган у сфері захисту критичної інфраструктури України; міністерства та інші центральні органи виконавчої влади; Служба безпеки України; правоохоронні та розвідувальні органи; Збройні Сили України, інші військові формування, утворені відповідно до законів України; місцеві державні (військові, у разі утворення) адміністрації; органи місцевого самоврядування; оператори КІ незалежно від форми власності; підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки та стійкості КІ.

Органи регулювання сфери забезпечення захисту КІІ: органи державної влади, органи місцевого самоврядування, їхні посадові і службові особи, оператори об’єктів критичної інфраструктури.

Економічна модель регулювання: джерелами фінансування робіт і заходів із забезпечення захисту КІ є кошти державного і місцевих бюджетів, власні кошти суб’єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Відповідальність у сфері забезпечення захисту КІІ: органи державної влади, органи місцевого самоврядування, їхні посадові і службові особи, оператори об’єктів критичної інфраструктури, винні у порушенні законодавства у сфері захисту КІ, несуть відповідальність згідно із законом.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті проаналізовано кращі світові практики в сфері захисту КІІ, що реалізовано і реалізуються на національному та міжнародному рівнях різних держав. Виходячи із аналізу, можна відзначити, що найбільш ефективним засобом захисту КІІ є підхід, який забезпечує комбінування оборонної, правоохоронної та консультативно-дорадчої функцій, що затверджені на загальнодержавному рівні. Ефективна система забезпечення КІІ передбачає наявність центрального державного органу, який в подальшому формує інформаційну політику, здійснює законотворчу та нормативну діяльність у цій сфері, координує діяльність інших міністерств, відомств, забезпечує

взаємодію із приватним сектором, опікується питаннями міжнародного співробітництва щодо протидії кіберзлочинності, організує систему інформування та оповіщення населення з проблем КБ.

Виділено основні етапи захисту КІІ, серед яких: 1) визначення основних понять та їх нормативне закріплення; 2) визначення критеріїв віднесення об'єктів до критично важливих; 3) складання переліку таких об'єктів; 4) оцінка ризиків безпеки; 5) планування заходів безпеки на основі результатів оцінювання ризиків із метою оптимізації витрат. Саме така послідовність розвитку систем захисту національної інфраструктури від кіберзагроз простежується у розвинених державах, серед яких, зокрема, США та ЄС.

У подальших дослідженнях планується розробити концепції захисту КІІ певних секторів КІ (наприклад, авіаційної галузі), врахувавши стан і особливості галузі, а також досвід провідних держав світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] "EUR-Lex - 32016L1148 - EN - EUR-Lex", Eur-lex.europa.eu, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Accessed: 16- Dec- 2020].

[2] "EUR-Lex - 32016R0679 - EN - EUR-Lex", Eur-lex.europa.eu, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: 16- Dec- 2020].

[3] "BSIGuaÄndG Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.", Buzer.de, 2020. [Online]. Available: https://www.buzer.de/gesetz/12607/index.htm. [Accessed: 16- Dec- 2020].

[4] "BSIG BSI-Gesetz", Buzer.de, 2020. [Online]. Available: https://www.buzer.de/gesetz/8987/index.htm. [Accessed: 16- Dec- 2020].

[5] Bmi.bund.de, 2020. [Online]. Available: http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf. [Accessed: 16- Dec- 2020].

[6] Ssi.gouv.fr, 2020. [Online]. Available: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf. [Accessed: 16- Dec- 2020].

[7] Assets.publishing.service.gov.uk, 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed: 16- Dec- 2020].

[8] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», 2020.

[9] H. Panyue, "National Security Law of the People's Republic of China (2015) [Effective] - Ministry of National Defense", Eng.mod.gov.cn, 2020. [Online]. Available: http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm. [Accessed: 16- Dec- 2020].

[10] Zakon.rada.gov.ua, 2020. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. [Accessed: 16- Dec- 2020].

[11] W1.c1.rada.gov.ua, 2020. [Online]. Available: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996. [Accessed: 16- Dec- 2020].

р.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Sergiy O. Gnatyuk
DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Yuliia Ya. Polishchuk
PhD student in NAU R&D Cybersecurity Lab
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-0686-2328
liya7954@gmail.com

Yuliia O. Sotnichenko
PhD Student
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-1281-9238
yu.sotnichenko@gmail.com

Dauriya D. Zhaksigulova
PhD Student
D. Serikbayev East Kazakhstan Technical University, Ust`-Kamenogorsk, Kazakhstan
ORCID ID: 0000-0003-0646-2823
dauriya.dzh@gmail.com

WORLD'S BEST PRACTICE ANALYSIS FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Abstract. According to the large number of cyber incidents that occur every day, the process of critical infrastructure protection is an important not only technical but also scientific task. However, not all states in the world have an opportunity to provide high-quality protection of such infrastructure at a high level. Based on the fact that the critical information infrastructure protection should be managed at the state level, states need to develop a regulatory framework to address the above issue. Considering the legal framework of Ukraine, as in most post-Soviet countries, there is no effective approach to the protection of critical information infrastructure, such as in the USA or in the EU. The legislation of Ukraine identifies only certain objects of the socio-economic sphere, emergencies where they can lead to socially dangerous consequences, while a single procedure for identification and classification of critical infrastructure is not developed. A number of basic terms in the field of critical infrastructure protection from cyber threats, including “critical infrastructure” term, remain normatively vague. The mechanism of organization of activity and interaction of state and private structures in the process of critical infrastructure protection needs scientific substantiation. In this paper, the analysis of the world’s best practices concerning critical information infrastructure protection was carried out, that allows to improve qualitatively, at the state legislative level and practice, process of critical information infrastructure protection of Ukraine.

Keywords: critical information infrastructure of the state; informational security; world’s best practices, cyber threat, normative and legal base.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] "EUR-Lex - 32016L1148 - EN - EUR-Lex", Eur-lex.europa.eu, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Accessed: 16- Dec- 2020].

[2] "EUR-Lex - 32016R0679 - EN - EUR-Lex", Eur-lex.europa.eu, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: 16- Dec- 2020].

[3] "BSIGuaÄndG Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.", Buzer.de, 2020. [Online]. Available: https://www.buzer.de/gesetz/12607/index.htm. [Accessed: 16- Dec- 2020].
[4] "BSIG BSI-Gesetz", Buzer.de, 2020. [Online]. Available: https://www.buzer.de/gesetz/8987/index.htm. [Accessed: 16- Dec- 2020].
[5] Bmi.bund.de, 2020. [Online]. Available: http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf. [Accessed: 16- Dec- 2020].
[6] Ssi.gouv.fr, 2020. [Online]. Available: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf. [Accessed: 16- Dec- 2020].
[7] Assets.publishing.service.gov.uk, 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed: 16- Dec- 2020].
[8] President Decree of the Russian Federation of 05.12.2016 N 646 "On the approval of the Doctrine of information security of the Russian Federation", 2020.
[9] H. Panyue, "National Security Law of the People's Republic of China (2015) [Effective] - Ministry of National Defense", Eng.mod.gov.cn, 2020. [Online]. Available: http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm. [Accessed: 16- Dec- 2020].
[10] Zakon.rada.gov.ua, 2020. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. [Accessed: 16- Dec- 2020].
[11] W1.c1.rada.gov.ua, 2020. [Online]. Available: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996. [Accessed: 16- Dec- 2020].