ПРОБЛЕМИ ВПРОВАДЖЕННЯ СУЧАСНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СТАНОВЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Анотація

У записці розглядається поточний стан і проекти подальшого розвитку (модернізації) у сфері стандартизації та сертифікації інформаційної безпеки в Україні. Окрему увагу приділено нормопроектним та регуляторним проблемам, що можуть виникнути у процесі реалізації норм вітчизняного законодавства з кібербезпеки щодо особливих вимог до безпекових стандартів і здійснення незалежного аудиту інформаційної безпеки на об’єктах критичної інформаційної інфраструктури. Надано низку рекомендацій.

ПРОБЛЕМИ ВПРОВАДЖЕННЯ СУЧАСНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СТАНОВЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Згідно з прийнятим 5 жовтня 2017 року Законом України «Про основні засади забезпечення кібербезпеки України» (набирає чинності 9.05.2018 р.), функціонування національної системи кібербезпеки, серед іншого, забезпечується шляхом «досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО», а також з урахуванням «кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту». В аспекті дотримання інформаційної безпеки це, згідно з Законом (статті 6,8), включає в себе насамперед розроблення на цій основі відповідних нормативно-правових актів, створення єдиної (універсальної) системи індикаторів кіберзагроз і запровадження національної системи аудиту інформаційної безпеки на критично важливих об’єктах кіберзахисту. Крім того, в статті 15 Закону затверджується, що основні суб’єкти національної кібербезпеки також підлягають аудиту, який має бути (а) незалежним, (б) щорічним і (в) проводитися «згідно з міжнародними стандартами аудиту».

Чинним Законом України «Про стандартизацію» затверджується принцип «добровільного застосування національних стандартів та кодексів усталеної практики, якщо інше не передбачено нормативно-правовими актами» (частина 2 статті 4). Отже, згідно з цією правовою нормою всі об’єкти кіберзахисту на території України апріорі вільні у виборі, використанні, ба-навіть в розробці[*] стандартів інформаційної безпеки. Але згідно з другою частиною цієї ж норми, тут вступають в силу обмеження та норми закону «Про основні засади забезпечення кібербезпеки України», які є досить вагомими.

[*] Відповідно до частини 1 статті 16 Закону України «Про стандартизацію», «підприємства, установи та організації мають право у відповідних сферах діяльності та з урахуванням своїх господарських і професійних потреб організовувати та виконувати роботи із стандартизації».

Так, Законом затверджується особливий режим стандартизації, сертифікації, незалежного аудиту та відповідальності за дотримання вимог інформаційної та кібернетичної безпеки для об’єктів, що належать до національної критичної інформаційної інфраструктури (далі в тексті – НКІІ, КІІ).

Для всіх об’єктів КІІ передбачене:

- встановлення (Кабінетом Міністрів України) обов’язкових вимог інформаційної безпеки, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури (частина 3 статті 8);
- обов’язковий незалежний аудит інформаційної безпеки, порядок та вимоги до якого також централізовано затверджуються Кабінетом Міністрів України (статті 5, 6);
- відповідальність власників та/або керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури за забезпечення кіберзахисту комунікаційних і технологічних систем об’єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах (частина 4 статті 6).

Станом на квітень 2018 року через брак підзаконних актів всі ці вимоги до об’єктів КІІ практично не конкретизовані, так само як не існує поки що самої системи та переліку об’єктів НКІІ. Водночас уже триває відповідна нормопроектна робота (докладніше див. нижче), а також зберігає чинність норма Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», згідно зі статтею 7 якого «державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із

застосуванням комплексної системи захисту інформації з підтвердженою відповідністю». Очевидно, що під дію цієї норми потрапляють практично всі майбутні об’єкти критичної інформаційної інфраструктури, а це, в свою чергу, означає, що наразі вони (принаймні, за буквою закону) зобов’язані дотримуватись вимог старого вітчизняного стандарту «Критерії оцінки захищеності інформації в комп'ютерних системах» КСЗІ НД ТЗІ 2.5-004-99[1] (або ж, разі їх прийняття, оновлених його версій).

На відміну від найпоширенішої у світі серії стандартів ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5-004-99 є відповідність архітектури та параметрів програмно-апаратних засобів об’єкта чіткому регламенту – комплексній системі захисту інформації (КСЗІ). З точки зору фахівців, сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту (особливо в недержавному секторі, надто ж – в бізнесі), і той факт, що ця норма досі не вилучена з чинного законодавства, піддається гострій критиці у вітчизняних експертних та бізнесових колах.[2] Найчастіше вказують на такі фундаментальні вади цього стандарту як:

- застаріла концепція захисту/захищеності;
- статичність;
- громіздкість (значна кількість документації, підтверджень та погоджень);
- обмежені можливості масштабування.[3]

Але в будь-якому разі обов’язковість використання КСЗІ (НД ТЗІ 2.5-004-99), згідно з законом, продиктована не приналежністю об’єкта кіберзахисту до НКІІ, як твердять деякі експерти, а режимом доступу до інформації, що обробляється в системі. Таким чином, під дію цієї норми,

---

[1] https://tzi.ua/ru/nd_tz_2.5-004-99.html

[2] http://uz.ligazakon.ua/ua/magazine_article/EA010553; https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci; http://infosafe.ua/article-6; http://ko.com.ua/kiberbezopasnost_v_ukraine_diskussiya_121089;

[3] Докладніше див.: http://www.niss.gov.ua/articles/2853/

очевидно, потрапить значна частина об'єктів НКІІ, але, по-перше – не всі, а по-друге – передусім державні установи та відомства.

Тим часом в Україні тривають процеси гармонізації та введення в дію сучасних міжнародних стандартів інформаційної безпеки, насамперед – серії міжнародних стандартів ISO/IEC 27000, розробленою Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими документами. Серія являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях – фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо.

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів. Національний орган стандартизації – державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») – ще в 2015 році підготував і затвердив у якості національних стандартів України чотири випуски цієї серії (ДСТУ ISO/IEC 27000:2015 «Огляд і словник», 27001:2015 «Вимоги», 27002:2015 «Звід практик щодо заходів інформаційної безпеки», 27005:2015 «Управління ризиками інформаційної безпеки»).[4] Протягом 2017 року оновлено серію національних стандартів ДСТУ ISO/IEC 270XX:2017 щодо методів захисту в системах менеджменту інформаційної безпеки.[5] У 2018 році передбачається введення в дію стандартів цієї ж серії «Настанови щодо аудиту систем керування інформаційною безпекою», «Керування інцидентами

[4] ДП «УкрНДНЦ». Наказ від 18.12.2015р. № 193 [Електронний ресурс]. - Режим доступу : http://uas.org.ua/wp-content/uploads/2016/12/N193_2015-12-18.rtf

[5] ДП «УкрНДНЦ». Наказ від 04.08.2017р. № 207 [Електронний ресурс]. - Режим доступу : http://csm.kiev.ua/images/stories/2017/nakaz/nakazukrndnc_207_2017.doc; http://uas.org.ua/ua/messages/zvit-pro-vikonannya-programi-robit-z-natsionalnoyi-standartizatsiyi-na-2017-rik-stanom-na-sichen-2018-roku/

інформаційної безпеки» і «Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій».[6]

Таким чином, база для стандартизації інформаційної безпеки (ІБ) стає в Україні дедалі сучаснішою та диверсифікованою. Модернізуються і стандарти аудиту ІБ. За рахунок цього, а також завдяки осучасненню й демократизації систем та процедур стандартизації для пересічних об'єктів кіберзахисту ситуація в цій галузі загалом розвивається в оптимальному напрямку.

Натомість проблемним і водночас дуже актуальним залишається комплекс питань, пов'язаних з формуванням основи НКІІ, включаючи «умови членства» в ній і методи захисту її об'єктів. Саме через те, що нещодавно прийнятий рамковий закон передбачає для об'єктів КІІ значно суворіші та відповідальніші порівняно з рештою об'єктів кіберзахисту вимоги і порядок дотримання/аудиту ІБ та кібербезпеки (там, де передбачена КСЗІ), особливої чутливості набуло в Україні питання методології та критеріїв формування реєстру (переліку) об'єктів НКІІ (від чого прямо залежить, хто потрапляє під дію цих жорстких норм, а хто – ні).

Власне, процес його вирішення досі знаходиться на початковій, нормопроектній стадії. У грудні 2017 року уряд схвалив Концепцію створення державної системи захисту критичної інфраструктури України, хоча власне інформаційному її сегменту, так само, як і кібербезпековим аспектам захисту КІ у даному документі не приділено значущої уваги.[7]

Ще раніше, приблизно за рік до прийняття рамкового Закону України про кібербезпеку, Кабінет Міністрів України постановою № 563 від 23 серпня 2016 року затвердив «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави»[8]. У документі, зокрема, сформульовано два критерії, згідно з якими інформаційно-телекомунікаційна система (ІТС) об'єкта може бути віднесена

[6] http://uas.org.ua/ua/services/standartizatsiya/programa-robit/
[7] https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi
[8] http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF

до критичної інфраструктури, а саме: 1) перелік «стратегічно важливих для функціонування економіки і безпеки держави, суспільства та населення» галузей; 2) характер можливих в разі кібератаки на ІТС негативних наслідків у різних сферах. У преамбулі визначено також, що сформувати даний перелік на основі пропозицій ЦОВВ, СБУ «та інших заінтересованих державних органів» і подати його Кабінетові Міністрів України повинна Адміністрація ДССЗЗІ «у шестимісячний строк з дня набрання чинності цією постановою», тобто до 23.02.2017 р. Станом на квітень 2018 року такого переліку в Україні не створено (принаймні, судячи з моніторингу відкритих джерел).

Одним з методологічних недоліків «Порядку..» є відсутність будь-якого масштабування «негативного впливу»[9] на ІТС того чи іншого об'єкта (наприклад – тривалість, територіальне охоплення, орієнтовний розмір збитків, ступінь загрози для національної безпеки тощо) а також – відповідно до цього масштабування – шкали її належності/неналежності до критичної інфраструктури.[*]

Якщо передбачається, що таку оцінку на основі представлених галузевими ЦОВВ «та іншими зацікавленими органами» списків, але в закритому режимі і керуючись украй нечітко прописаними критеріями (що дає змогу довільного їх трактування) здійснюватиме Адміністрація ДССЗЗІ, то це видається досить спірним підходом, оскільки процедура створення першого національного реєстру об'єктів КІІ, мабуть, вимагає більш широких комунікацій та консультацій – у тому числі з недержавним сектором. Що ж до процесу підготовки згаданих пропозицій галузевих ЦОВВ, то він був би значно продуктивнішим, якби у ньому, поряд з профільними фахівцями, була також передбачена системна участь спеціалістів у сфері національної безпеки та ІКТ.

---

[9] Там само.

[*] Щоправда, у згаданому вище проекті постанови Кабінету Міністрів про організацію та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави вводиться поняття категорій критичності об'єктів КІ (від І до IV), але згідно з ними встановлюється лише частота обов'язкових аудиторських перевірок даних об'єктів.

Крім того, в тексті «Порядку…» не передбачено механізмів постійного моніторингу й оновлення переліку об'єктів КІІ, що є необхідним, враховуючи динаміку суспільно-економічних змін з одного боку і ескалації кіберзагроз – з іншого. Про це ж однозначно свідчить і міжнародний досвід. Варто підкреслити також, що українські ділові кола піддали критиці не лише зміст, але й назву документу. Зокрема, у відкритому листі Інтернет Асоціації України (ІнАУ) від 28.02.2017 р. слушно вказується, що з назви та тексту «Порядку..» незрозуміло, «що саме визначатиметься предметом кіберзахисту – суб'єкти господарювання чи інформаційно-телекомунікаційні системи та телекомунікації».[10]

Таким чином чинний «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» є обмежено ефективним правовим інструментом для створення повноцінного, адекватного потребам національної кібербезпеки переліку об'єктів НКІІ. Понад це, низка його положень несе у собі і потенційні корупційні ризики. Наприклад, запропонований у ньому порядок формування переліку, як справедливо зазначається у згаданому листі ІнАУ, потенційно створює передумови для «надмірного та необґрунтованого навантаження на малі та середні підприємства, значну частину з яких, ймовірно, немає ніяких підстав відносити до критичної інфраструктури». У зв'язку з цим фахівці Асоціації наполягають, що «при підготовці законодавчих пропозицій для запровадження відповідальності за порушення вимог щодо кіберзахисту» має бути «чітко визначене коло суб'єктів, які є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури» виходячи з їх «вагомості, зокрема, для національної безпеки і оборони держави». [11]

Крім того, динаміка сучасних процесів не дозволяє раз і назавжди «чітко визначити» таке «коло суб'єктів», відтак повинна існувати чітка і зрозуміла методологія та ретельно узгоджена система максимально

[10] http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-29122016-pro-zagrozy
[11] Там само.

конкретних (аж до затвердження діапазону точних показників всюди, де це можливо) критеріїв віднесення об'єктів кіберзахисту до КІІ. Її також доведеться періодично переглядати, але через прийнятні проміжки часу. Важливо, щоб ця система допускала якомога менше неоднозначних трактувань – це сприяло б оптимізації процесу формування кінцевого реєстру, а також дещо зменшило б ризики міжвідомчих чвар, дублювання повноважень і корупційних дій. У подальшому сам реєстр КІІ, як і методологію його формування, очевидно, доведеться коригувати безпосередньо на практиці, в «режимі реального часу».

Ідентифікація, категоризація і реєстрація об'єктів КІІ є складною проблемою не лише в Україні, але і в інших державах, причому в різних країнах вирішується вона дуже по-різному.[12] Накопичено значний міжнародний досвід, який подекуди вивчається і в Україні, хоча здебільшого побіжно, в контексті більш широкої проблематики.[13] У той же час гострота проблеми і незадовільний рівень її правового осмислення свідчать про необхідність подальших науково-аналітичних досліджень в цьому напрямі.

Відповідно до затверджених Кабінетом Міністрів планів заходів з реалізації Стратегії кібербезпеки України на 2016 та 2017 рр. у цій сфері передбачене формування переліку міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки, які потребують перекладу та гармонізації (це планувалось здійснити ще протягом 2016 року), а також імплементацію їх норм і впровадження системи аудиту інформаційної безпеки в державних органах та на об'єктах критичної інфраструктури (протягом 2017 року).[14] У рамках цих планів ДССЗЗІ була висунута низка проектів нормативних актів саме в частині впровадження системи аудиту інформаційної безпеки.[15]

---

[12] http://nauka.zinet.info/23/gnatyuk.php

[13] http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf; http://www.niss.gov.ua/content/articles/files/Sots_zahust-86178.pdf; http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Zvjazok_2014_4_3

[14] http://www.kmu.gov.ua/document/249142550/R0440-00.doc; https://www.kmu.gov.ua/ua/npas/249807504

[15] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=38837

Згідно з частиною 2 статті 8 закону «Про основні засади забезпечення кібербезпеки України», ДССЗЗІ «забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість». У серпні 2017 року ДССЗЗІ розробила і представила для ознайомлення проект постанови Кабінету Міністрів «Концепція впровадження системи аудиту інформаційної безпеки («Дорожня карта»)».[16] У документі «визначаються основні засади щодо реалізації та впровадження системи аудиту інформаційної безпеки в Україні, порядок проведення сертифікації аудиторів ІБ, їх навчання та оцінювання, відповідного контролю повноти та достатності надання послуг в цій сфері через встановлені проміжки часу після надання сертифікату, а також систематизація та узагальнення результатів аудиту ІБ» через подання звітів до центральних та профільних органів влади. Крім того, в Концепції запропоновано модель функціонування системи аудиту ІБ та визначені основні етапи її впровадження в Україні (до 2020 року включно).[17] У березні 2018 року ДССЗЗІ представила також проект постанови Кабінету Міністрів «Про затвердження Порядку організації та проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури держави», в якому розвинуто й конкретизовано окремі положення Концепції.[18]

Прогресивним в цих документах можна вважати те, що, згідно з проектом Концепції, акредитацію аудиторів/аудиторських установ для перевірки інформаційної безпеки передбачається здійснювати за сучасним міжнародним стандартом «ДСТУ EN ISO/IEC 17024:2014 Оцінка відповідності. Загальні вимоги до органів, що проводять сертифікацію

[16] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837
[17] Там само.
[18] http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=287724&cat_id=38837&ctime=1521019033338

персоналу»[19], який в Україні був підтверджений та введений в дію з 01.01.2016 року. Аудит систем управління інформаційною безпекою (СУІБ) передбачається проводити у відповідності зі стандартом ISO/IEC 27001:2013, що загалом відповідає світовим практикам, хоча в Україні ще в 2015 році набула чинності свіжіша версія цього стандарту ДСТУ ISO/IEC 27001:2015 (див. вище).

Як релевантну нинішнім європейським стандартам і практикам можна розглядати також закладену в Концепцію ідею «створення інформаційно-аналітичної системи формування національних індикаторів ІБ».[20] В Україні даному питанню, за окремими виключеннями[21], не приділено спеціальної фахової уваги, в той час як у світі активно ведуться відповідні дослідження і розробки. Наприклад, комплекс індикаторів інформаційної безпеки декілька років тому було розроблено і стандартизовано Європейським інститутом телекомунікаційних стандартів (ETSI)[22] – впливовою міжнародною неприбутковою організацією, що об'єднує представників європейської (включаючи українських) та світової телеком-індустрії і офіційно визнана Єврокомісією як провідна установа у розробці галузевих стандартів. Моніторингу, вимірюванню, аналізу та оцінці безпеки у менеджменті ІБ (тобто, власне, технологіям визначення на основі кількісних показників – індикаторів – якісних характеристик) присвячений також і міжнародний стандарт ISO/IEC 27004:2016[23], у кореляції з яким, до речі, розроблялася і згадана методика ETSI.

Враховуючи наявність такого світового досвіду і загальну зорієнтованість українського галузевого законодавства на «міжнародні стандарти, стандарти ЄС та НАТО», логічним було б провести процедуру гармонізації або підтвердження відповідних стандартів Національним агентством стандартизації України, офіційно ввести в їх дію і вже далі на цій

[19] http://document.ua/ocinka-vidpovidnosti_-zagalni-vimogi-do-organiv-sho-provodja-std30073.html
[20] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837
[21] http://ippi.org.ua/sites/default/files/13fvmibi.pdf
[22] http://www.etsi.org/technologies-clusters/technologies/information-security-indicators; https://en.wikipedia.org/wiki/Information_security_indicators
[23] https://webstore.iec.ch/publication/59700

основі розробляти національні індикатори ІБ і впроваджувати інформаційно-аналітичну систему їх формування. Саме такий шлях є типовим, приміром, для країн Євросоюзу і багатьох інших, причому практика свідчить, що саме він забезпечує мінімальну затратність при максимальному ефекті: дотримуються норми національної безпеки, зміцнюється захищеність ІБ підприємства і при цьому – завдяки уніфікованості стандартів – не гальмуються міжнародні/транскордонні обміни. Але в проекті Концепції пропонується інший підхід, а саме:

- створення «центральної частини» (а згодом – «територіальних частин») інформаційно-аналітичної системи формування національних індикаторів ІБ, яка забезпечить можливість моніторингу та інформування центральних і профільних органів влади України «про стан ІБ як в окремих установах, регіонах, так і на території держави в цілому»;
- створення комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю в інформаційно-аналітичній системі формування національних індикаторів ІБ;
- періодичне «проведення робіт щодо перегляду загроз для інформації» в даній інформаційно-аналітичній системі, оцінки щодо сталого її функціонування та «за необхідністю – збільшення потужності системи».[24]

Відтак йдеться передусім про створення спеціалізованої внутрішньовідомчої (підконтрольної ДССЗЗІ) адміністративно-бюрократичної вертикалі з всеукраїнським територіальним охопленням, наглядово-контрольними функціями і можливістю подальшого розширення («збільшення потужності») лише на підставі відповідного внутрішньовідомчого рішення.

Показово, що кібербезпеку цієї вертикалі («інформаційно-аналітичної системи формування національних індикаторів ІБ») передбачається забезпечувати на основі вітчизняного стандарту НД ТЗІ щодо створення «комплексної системи захисту інформації з підтвердженою відповідністю»

[24] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837

(КСЗІ). Це відповідає чинному законодавству, але, на думку фахівців, є дуже спірним підходом у зв'язку з фундаментальними недоліками і застарілістю КСЗІ (див. вище). До того ж, з тексту проекту важко зрозуміти, що являтиме собою означена «інформаційно-аналітична система», за допомогою якої і «формують національні індикатори ІБ», з теоретико-концептуальної і техніко-технологічної точки зору. Залишається не до кінця зрозумілим і те, як самі автори проекту трактують це останнє поняття і чи співпадає їхнє трактування з визначеннями, закріпленими у міжнародних стандартах і документах.

Варто наголосити, що ідея «системи формування національних індикаторів ІБ», особливо в такій її редакції, мало корелює з чинним законодавством і зокрема – з рамковим законом «Про основні засади забезпечення кібербезпеки України». У його тексті немає згадки про *систему національних індикаторів ІБ*, зате чітко прописана норма щодо необхідності «впровадження *єдиної (універсальної) системи індикаторів кіберзагроз* з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту», а також «періодичного проведення огляду національної системи кібербезпеки, розроблення *індикаторів стану кібербезпеки*» (Ст. 8). Всі ці задачі віднесені Законом до сфери відповідальності Кабінету Міністрів України (Ст. 6), відтак саме Держспецзв'язку могла б долучитися до розробки таких систем, тим більше, що в них існує пряма необхідність, і що цією проблематикою вже займаються інші спеціальні відомства, зокрема СБУ.[25]

Видається неоднозначним і запропонований в проекті Концепції підхід до вирішення ключового питання – організації аудиту ІБ в Україні. Як єдино вірний у документі подається такий варіант: «впровадження системи аудиту ІБ на національному рівні та використання послуг аудиту ІБ, що можуть надаватися національними (з контексту зрозуміло, що на противагу міжнародним, за принципом «або – або» - *Автор*) аудиторами

[25] https://ua.interfax.com.ua/news/general/465824.html

(компаніями)».[26] Треба констатувати, що така модель не відповідає як міжнародним стандартам, так і найбільш успішним для демократичних суспільств практикам проведення аудиту ІБ. Суперечить вона також і рекомендаціям вітчизняних експертів.[27] Відомо, що діяльність міжнародних аудиторських компаній (включаючи й чутливі сфери, на кшталт перевірок інформаційної безпеки об'єктів НКІІ) є в сучасному світі однією з підвалин і констант нормального функціонування держав та економік. Ідея відмови, банавіть, мінімізації їхньої участі в аудиті ІБ на українських об'єктах, виходячи з міркувань національної безпеки, є дещо неоднозначною, оскільки може значно звузити можливості створення сучасних, адекватних потребам національного розвитку та євроінтеграції механізмів аудиту.

У проекті послідовно проводиться ідея створення у складі ДССЗЗІ єдиної системи аудиту ІБ замкненого циклу (від центрів підготовки аудиторів до мережі сертифікованих аудиторських установ) з всеукраїнським охопленням, масштаби якої дозволили б «налагодити моніторинг стану захищеності інформаційних ресурсів на території держави, що дасть можливість отримати відомості про реальний стан ІБ як в окремих установах, регіонах так і в державі в цілому в реальному часі»[28]. Значною мірою це відповідає вимогам прийнятого Верховною Радою рамкового закону про кібербезпеку (див. вище). Водночас, треба враховувати те, що (а) згідно з тим же законом ДССЗЗІ належить проводити аудит ІБ лише на об'єктах критичної інфраструктури (у той час як наведені вище формулювання містять явно більш широку трактовку відповідних повноважень Служби) і те, що (б) чинний нині «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» дозволяє максимально широко тлумачити умови віднесення ІТС до такої інфраструктури (див. вище). Тому намагання створити системи аудиту ІБ за подібною моделлю в реальному житті призведе до надмірної концентрації

[26] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837
[27] http://www.isaca.org.ua/index.php/component/content/category/79-events; https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci; http://infosafe.ua/article-6
[28] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=281277&cat_id=38837

відповідних функцій та ресурсів в руках одного відомства, що в свою чергу потягне за собою цілий спектр ризиків – адміністративних, регуляторних, економічних, корупційних та ін..

ВИСНОВКИ

1. Національна система кібербезпеки України нині знаходиться на етапі формування, що стосується і таких її складових як стандартизація та сертифікація ІБ і пов’язане нормативно-правового забезпечення (підзаконні акти).

2. Завдяки модернізації профільного законодавства (Закон України «Про стандартизацію»), а також осучасненню й демократизації інститутів та процедур стандартизації для пересічних об’єктів кіберзахисту ситуація в цій галузі загалом розвивається в оптимальному напрямку – база стандартизації ІБ стає в Україні дедалі більш сучасною та диверсифікованою, активно гармонізуються галузеві міжнародні стандарти. Модернізуються і стандарти незалежного аудиту ІБ.

3. Потенційно проблемною залишається сфера, яку безпосередньо регулює закон «Про основні засади забезпечення кібербезпеки України» і пов’язані підзаконні акти, а саме – об’єкти кіберзахисту, що належать до НКІІ, точніше – обов’язковий аудит дотримання такими об’єктами стандартних (і теж обов’язкових для них) вимог ІБ.

4. Аналіз двох принципово важливих підзаконних актів, що регулюють ці питання – «Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» (розпорядження КМУ) і «Концепція впровадження системи аудиту інформаційної безпеки» (проект, ДССЗЗІ) – виявив, що перший з них є значною мірою абстрактним і фактично не має регуляторного ефекту, а зміст другого багато в чому спрямовує побудову систему аудиту та моніторингу ІБ

у напрямку концентрації всіх її складових в під повним контролем окремих державних структур.

5. Все це робить даний сегмент правового регулювання й державного управління на перетині двох важливих проблематик однією з чутливих зон, де проблеми формування та реалізації державної політика легко можуть спричинити виникнення суттєвих дисбалансів у розвитку країни, включаючи значне зростання корупційних ризиків.

РЕКОМЕНДАЦІЇ

Кабінету Міністрів України:

1. Оскільки передбачене Законом України «Про основні засади забезпечення кібербезпеки України» впровадження та функціонування системи аудиту інформаційної безпеки на об’єктах НКІІ потребуватиме розробки відповідного нормопроектного та регуляторного забезпечення практично «з нуля» – під час розгляду в установленому порядку проекту розпорядження Кабінету Міністрів України «Концепція впровадження системи аудиту інформаційної безпеки (“Дорожня карта”)» було б доцільним істотно доопрацювати даний проект. Зокрема доповнити його нормами та пропозиціями, які передбачали б можливість забезпечення належного рівня децентралізації процедур аудиту ІБ на (майбутніх) об’єктах КІІ.

2. Одним з шляхів вирішення проблеми є налагодження фахівцями ДССЗЗІ консультацій і співробітництва з авторитетними аудиторськими компаніями (рівня PricewaterhouseCoopers або Ernst & Young), профільними міжнародними організаціями (такими як ENISA або ISACA) та галузевими професійними асоціаціями. Метою такої взаємодії має стати пошук уточненого формату системи аудиту інформаційної безпеки, яка відповідала б міжнародним стандартам в цій сфері.

3. Зважаючи на те, що формування системи аудиту ІБ буде безпосередньо пов’язано із діяльністю значного пула (майбутніх) недержавних об’єктів НКІІ – розглянути доцільність проведення серії консультацій між суб’єктами національної системи кібербезпеки (за головування ДССЗЗІ) та відповідальними представниками тих об’єктів недержавного сектору, що є найбільш важливими для забезпечення інформаційної і загалом національної безпеки України з метою:
а) комунікування очікуваного рішення відповідних державних суб’єктів;
б) узгодження позицій щодо концептуального бачення системи аудиту ІБ;
в) опрацювання практичних питань функціонування цієї системи безпосередньо щодо недержавних об’єктів критичної інфраструктури.

4. Забезпечити системне публічне звітування (у вигляді щорічної доповіді) суб’єктів національної системи кібербезпеки України про стан реалізації положень Стратегії кібербезпеки України та положень ст.8, ч.3 Закону України «Про основні засади забезпечення кібербезпеки України».

5. Для практичної реалізації ст.15 ч.3 Закону України «Про основні засади забезпечення кібербезпеки України» розпочати консультації з міжнародними аудиторськими компаніями щодо напрацювання та затвердження в подальшому «Положення про порядок проведення аудиту діяльності основних суб’єктів національної кібербезпеки».

Кабінету Міністрів України, Службі безпеки України, Адміністрації ДССЗЗІ України, науково-дослідним та науково-аналітичним установам відповідної спеціалізації:

6. З метою належної організації захисту об’єктів критичної інфраструктури від кібератак додаткових досліджень потребує міжнародний досвід в цій царині, рекомендації профільних міжнародних організацій

(наприклад, методика ENISA[29]) і можливість їх застосування в українських умовах. В подальшому з урахуванням опрацьованого матеріалу сформувати уточнену нормативно-правову базу щодо ідентифікації, реєстрації та категоризації об’єктів критичної інфраструктури і критичної інформаційної інфраструктури.

С.Л. Гнатюк
Відділу інформаційної безпеки та
розвитку інформаційного суспільства
Національний інститут стратегічних досліджень
травень 2018 р.

[29] https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis