УДК 351.746:007

ГУЦАЛЮК М.В., *доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.*,
провідний науковий співробітник Міжвідомчого центру з проблем
боротьби з організованою злочинністю при РНБО України

ОЦІНКА РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ЄВРОПЕЙСЬКИХ І СВІТОВИХ ПРАКТИК

Анотація. *У статті аналізується міжнародний досвід проведення оцінки Стратегії кібербезпеки. Акцентується увага на необхідності проведення такої оцінки Стратегії кібербезпеки України.*

Ключові слова: *кібербезпека, кіберзлочинність, критерії оцінки, Стратегія кібербезпеки, критична інфраструктура.*

Summary. *The article analyses the international experience of conducting an assessment of the Cybersecurity Strategy. The emphasis is placed on the need for such an assessment of the Cybersecurity Strategy of Ukraine.*

Keywords: *cyber security, cybercrime, evaluation criteria, Cybersecurity strategy, critical infrastructure.*

Аннотация*. В статье анализируется международный опыт проведения оценки Стратегии кибербезопасности. Акцентируется внимание на необходимости проведения такой оценки Стратегии кибербезопасности Украины.*

Ключевые слова: *кибербезопасность, киберпреступность, критерии оценки, Стратегия кибербезопасности, критическая инфраструктура.*

Постановка проблеми. Після потужних кібератак на об’єкти критичної інфраструктури України з 2014 року значно активізувалася діяльність урядових інституцій щодо захисту кіберпростору. Координуючу роль у цих процесах відіграла Рада національної безпеки і оборони України, рішенням якої було схвалено, а в подальшому введено в дію Указом Президента України від 15 березня 2016 року № 96/2016 Стратегію кібербезпеки України. У Стратегії визначені загрози кібербезпеці, Національна система кібербезпеки та основні суб’єкти забезпечення кібербезпеки, а також пріоритети та напрями забезпечення кібербезпеки України [1].

Водночас у зв’язку з бурхливим розвитком інформаційних технологій та широким використанням хмарних сервісів, Інтернету речей, штучного інтелекту тощо, з’явилися нові види кіберзагроз, які здатні негативно впливати на стан кібербезпеки держави. У 2017 році був прийнятий Закон України “Про основні засади забезпечення кібербезпеки України” [2], який набрав чинності 9 травня 2018 року та став важливим етапом створення правових та організаційних основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, визначення основних цілей, напрямів та принців державної політики у сфері кібербезпеки. Разом з тим багато питань у сфері кібербезпеки, у тому числі стратегічних, залишаються невирішеними.

Результати аналізу наукових публікацій. Проблемам стратегічного планування у сфері кібербезпеки були присвячені праці таких науковців і практиків, як С.Л. Гнатюк [3], Д.В. Дубов [4], Н.Ю. Литвинчук [5], Н.А. Ткачук [6] та інших, проте питання оцінки стратегій кібербезпеки потребують певних уточнень та подальших ґрунтовних розробок.

Метою статті є визначення ключових критеріїв оцінки ефективності реалізації Стратегії кібербезпеки України.

Виклад основного матеріалу. Кабінет Міністрів України щороку розробляє план заходів з реалізації Стратегії кібербезпеки України [7], а також зобов'язує Адміністрацію Державної служби спеціального зв'язку та захисту інформації інформувати кожні півроку про хід виконання цих заходів Раду національної безпеки і оборони України та Кабінет Міністрів України. Надзвичайно важливого значення в сучасних умовах набуває також визначення ефективності виконання запланованих заходів.

Процес оцінки рівня ефективності реалізації Стратегії кібербезпеки України методологічно пов'язаний із визначенням належного критерію і формуванням відповідної системи показників, адже критерій – це головна ознака визначення ефективності, за яким здійснюється її кількісна оцінка. Правильно сформульований критерій має найповніше характеризувати суть ефективності реалізації запланованих заходів.

Розвинені країни, зокрема держави ЄС, мають значну практику розробки відповідних Стратегій кібербезпеки (далі – Стратегії), їх практичної реалізації, а також визначення їх ефективності. Це пов'язано з тим, що в інформаційному суспільстві ЄС широко використовуються різноманітні інформаційні технології, водночас кіберінциденти можуть нівелювати досягнення економічних вигод від використання кіберпростору.

Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU – міжнародна організація, що визначає стандарти в галузі телекомунікацій) у 2018 році був розроблений Посібник для розробки національних стратегій кібербезпеки, який спрямований на полегшення створення та оновлення національними органами відповідних документів [8].

У рекомендаціях, наданих у цьому посібнику, розглянуто процес розробки стратегії кібербезпеки починаючи від аналізу стану кібербезпеки до публікації документа та розробки плану дій на його виконання, а також подальшого вдосконалення.

Також в посібнику зазначається про необхідність періодичного оцінювання результатів від реалізації Стратегії кібербезпеки та порівнювати їх з поставленими цілями. Це надзвичайно важливо для розуміння того, чи реалізуються цілі Стратегії. Варто також регулярно переоцінювати існуючі кіберризики, щоб зрозуміти, чи впливають зовнішні зміни на результати реалізації Стратегії кібербезпеки.

Ця оцінка разом з запропонованими рекомендаціями щодо змін до Стратегії повинна бути підготовлена у вигляді звіту для відповідного керівного органу та включати в себе План дій по оновленню документа, щоб забезпечити необхідну зміну політики та переліку кіберризиків.

Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), яке є центром експертиз для інформаційної безпеки ЄС, його держав-членів, приватного сектору та громадян Європи, розробляє рекомендації щодо ефективної практики інформаційної безпеки. Воно допомагає державам-членам ЄС у розробці законодавства ЄС у сфері кібербезпеки, підвищенні стійкості критичної інформаційної інфраструктури та комп'ютерних мереж в Європі.

Проаналізувавши 18 європейських Стратегій та 8 Стратегій поза межами ЄС, ENISA відзначило чотири важливі етапи: розробку, впровадження, оцінку та коригування і запропонувало систему їх оцінювання [9].

Відповідно до рекомендацій ENISA основними цілями оцінки стратегії кібербезпеки, заснованої на даному аналізі, є:

– розробка політики та можливостей кіберзахисту;

– досягнення кіберстійкості (здатність суб'єкта досягати бажаного результату незважаючи на кіберінциденти);

– зменшення кіберзлочинності;
– підтримка промисловості у сфері кібербезпеки;
– безпека інформаційної критичної інфраструктури.

Для оцінки ефективності реалізації Стратегії використовується також емпіричний метод, який зокрема передбачає огляд повідомлень у ЗМІ, щодо оцінки стану кібербезпеки. Це дозволяє дослідити роль, яку оцінювання Стратегії відіграє в складних заходах державної політики.

Також проводиться інтерв'ювання ключових експертів у сфері кібербезпеки. Метою цих інтерв'ю є вивчення основних показників оцінки кібербезпеки.

Практика визначення показників описується акронімом *SMART*. Вони повинні бути:

Specific: конкретні – чіткі, щоб уникнути неправильного тлумачення або двозначності;

Measurable: вимірні – можуть бути кількісно виміряні (хоча вони можуть бути також якісними);

Attainable: досяжні – цілі встановлюються досяжними, спостережуваними та виконуваними за певних умов в конкретні терміни, а також незалежно перевірені;

Relevant: повинні відповідати стратегії та цілі конкретного відомства;

Time-related: визначені конкретним терміном – існує обмеження часу для досягнення результатів.

Зацікавленість ENISA у сприянні оцінюванню та підтримці стратегічного планування Стратегій вписується в більш широку картину заохочення держав-членів та інституцій ЄС до впровадження різноманітних заходів кібербезпеки. У Європейському Союзі ці стратегії включені до "Цифрової програми Європи" (Digital Agenda for Europe – DAE [10]) для безпечного цифрового суспільства, спрямованого на сприяння економічному зростанню. Держави-члени контролюють прогрес кібербезпеки відповідно до запланованих заходів та подають щороку звіти про її моніторинг. На підставі цих звітів Європейська Комісія (ЄК) порівнює досягнення держав-членів за відповідними напрямами.

Майже всі Стратегії, розглянуті в рамках дослідження ENISA, включають положення про процес розгляду та оцінки документа. Наприклад, у Фінляндії забезпечення перегляду та оцінки Стратегії є одним із десяти стратегічних напрямів діяльності. В інших стратегіях (Великобританія, Німеччина, Франція) оцінка також слугує для того, щоб забезпечити сучасну законодавчу базу щодо останніх подій у технологічному ландшафті. У ряді стратегій частота циклу оцінювання встановлюється на щорічній (Литва, Словаччина, Нідерланди) або дворічній (Австрія) основі. Деталі процесу оцінювання включені в окремий акт або в план впровадження. Навіть там, де процеси перегляду не зазначені в самій Стратегії, делеговані акти та дії, передбачені ними, підлягають перевірці державними аудиторськими органами залежно від інституційної структури країни.

Кожна оцінка реалізації Стратегії повинна визначатися відповідним незалежним органом (наприклад, національною радою з кібербезпеки). Для цього необхідно цьому органу надати належний мандат та визначити його роль і обов'язки. Необхідно також створити схему збору даних для отримання відповідних показників для оцінки стратегії та плану дій. Процес збору даних повинен стати всеохоплюючим.

На основі аналізу даних готується аналітичний звіт про оцінку, що описує досягнуті результати та очікування щодо наступного періоду.

Для отримання об'єктивної оцінки реалізації Стратегії кожна держава повинна здійснювати моніторинг найважливіших надзвичайних ситуацій, які стосуються кіберзахисту. Успіх національної програми вимірюється кількістю кіберінцидентів, що сталися в певний період часу з мінімальними заходами безпеки. Відсутність цього типу подій концептуально означає, що всі загрози були виявлено, і їхній вплив було мінімізовано.

В країнах ЄС щорічна доповідь про діяльність у сфері захисту кіберпростору додається до щорічного звіту парламенту про стратегію та політику національної безпеки.

ENISA запропонувало перелік можливих ключових індикаторів ефективності (key performance indicators – KPI), які можуть бути обрані для вимірювання ефективності реалізації Стратегії. Ці індикатори розбиті на групи відповідно до ключових цілей оцінки стратегії кібербезпеки.

Ключова ціль 1: ***Розвиток кіберзахисту***

Ключове завдання	**Доказ** (що саме оцінюється)
Наявність стратегічного національного плану з кібербезпеки	Наявність і статус такого плану, звіти про діяльність, план дій та відповідальність
Ступінь участі в ініціативах ЄС з кіберзахисту	Індикація участі, рівень участі
Ідентифікація та структура військового CERT	Оцінка можливостей; політичні документи; внутрішні оперативні документи
Наявність навчанн персоналу	Оцінка можливостей; політичні документи; внутрішні оперативні документи
Оперативна сумісність (здатність взаємодіяти з іншими структурами)	Оцінка можливостей; політичні документи; внутрішні оперативні документи
Збільшення стійкості через співпрацю у протидії військовим кібератакам (швидке виявлення, відповідь і відновлення від складних кібератак, економічно ефективний розвиток, співпраця, надійні, доступні і зрозумілі канали зв'язку)	Оцінка можливостей, звіти про кіберінциденти

Ключова ціль 2: ***Досягнення кіберстійкості***: розвиток потенціалу та ефективного співробітництва державного та приватного секторів

Ключове завдання	**Доказ** (що саме оцінюється)
Налагодження діяльності CERT або Національних агенцій кібербезпеки	Існування та мандат інституційних суб'єктів (сфера діяльності, повноваження агентств/ органів)
Наявність державно-приватного партнерства з питань кібербезпеки	Визначення та зміст такого партнерства, його значення, звіти про діяльність
Виявлення ризиків та загроз	Аналіз ризиків, аналіз загроз (проводиться CERT або Агенцією національної безпеки)
Наявність тренувань з питань кібербезпеки	Звіти про діяльність
Розширені можливості: організовані тренінги для державного та приватного секторів, взаємна навчальна діяльність (семінари та конференції)	Звіти про діяльність, назва події, компанії/ зацікавлені сторони
Координація діяльності усіх суб'єктів національної системи кібербезпеки	Звіти про діяльність
Наявність розвинених засобів реагування (плани реагування, системи раннього попередження тощо)	Плани виявлення та відновлення, раннє попередження системи та імітаційні моделі, звіт про діяльність

Посилення безпеки громадських інформаційних систем	Виявлення вразливостей (звіт-CERT або Національної Агенції кібербезпеки), документування оновлення/виправлення програмного забезпечення та створення процедур, прийняття стандартів кібербезпеки для систем ІКТ

Ключова ціль 3: ***Зменшення кіберзлочинності***

Ключове завдання	**Доказ** (що саме оцінюється)
Національна система протидії кіберзлочинності	Структура системи
Національні інституції для протидії кіберзлочинності (правоохоронні органи, CERT тощо)	Структури та законодавча база
Зміцнення правоохоронних органів (аналіз прогалин, визначення потреб, сучасні технічні активи, використання передового досвіду)	Документація щодо виявлених проблем та заходів щодо підтримки правоохоронних органів для протидії кіберзлочинності, оцінки можливостей, реєстру кращих практик, документації щодо процедур
Наявність механізмів співпраці з ЕСЗ, CEPOL, Євроюстом та іншими міжнародними організаціями	Звіти про діяльність та спільні дії
Національні рішення по справам кіберзлочинністі	Статистичні дані МВС щодо кіберзлочинів (розслідування, кримінальні переслідування тощо)
Міжнародна співпраця: – посилення можливостей боротьби з кіберзлочинністю через кордони; – зменшення бар'єрів для розслідувань; – доступ до сучасних інструментів; – зниження витрат на боротьбу з кіберзлочинністю	Процедури транскордонного співробітництва між органами влади (CERT та ін.). Статистика розслідувань і резолюцій, бюджетні звіти
Безпечний кіберпростір для всіх користувачів	Статистика (правоохоронні органи, опитування, національні статистичні управління)

Ключова ціль 4: ***Промислові розробки та технології для забезпечення кібербезпеки***

Концепція цієї ключової цілі полягає в тому, що промисловість та технологічні досягнення (у тому числі наукові) будуть підтримувати рівень національної кібербезпеки на ринку продуктів.

Ключове завдання	**Доказ** (що саме оцінюється)
Підтримка стандартизації та розробки у галузі кібербезпеки	Відповідність стандартам безпеки, перевіркам та механізмам сертифікації, встановленими регуляторними органами, рівнем прийняття стандартів
Фінансування досліджень через програми ЄС та національні дослідницькі програми	Бази даних ЄС щодо дослідницького проекту, агентства, що фінансують науку
Розробка нових національних заходів кіберзахисту	Політичні документи, державні акти, документи щодо вимоги до ІКТ, нові політики

Підтримка інновацій в електронному бізнесі	Впровадження інноваційних рішень електронного бізнесу
Доступ споживачів до безпечних технологій	Звіти про дослідження ринку

Ключова ціль 5: ***Забезпечити захист критичної інформаційної інфраструктури.***

Відповідно до ключового завдання щодо захисту критичної інформаційної інфраструктури ми досліджуємо такі поняття, як інформування про кіберінциденти, ідентифікацію цих структур, міжнародне співробітництво та обмін інформацією.

Ключове завдання	**Доказ** (що саме оцінюється)
Ідентифікація критично важливої інформаційної інфраструктури, тобто критичних активів, уразливостей, залежностей, ризиків	Перелік об’єктів критичної інформаційної інфраструктури
Оцінка ризиків та плани управління ризиками	Розподіл обов’язків та процедури, яких необхідно дотримуватися (включаючи періодичність оновлень)
Процедури інформування про кіберінциденти	Опис процедури, ролей та обов'язків, залучених органів, співпраці між країнами
Плани відновлення бізнесу та безперервності для критичної інфраструктури	Стратегічні програмні документи; імплементації рекомендацій, розподіл обов’язків різноманітних структур
Успішний обмін інформацією та надійне співробітництво між різними гравцями	Довірені канали для спілкування, регулярні зустрічі, залучення зацікавлених сторін
Швидке та ефективне реагування на випадок інцидентів на національному рівні (менше часу простою у разі кіберінциденту)	Скорочення швидкості реагування; зменшення невизначеності реакції
Прозорість і підзвітність систем	Кількість та тип документації, доступної для громадськості, вимірює обізнаність людей

Також для оцінки ефективності національної Стратегії та плану її реалізації слід враховувати показники загального рівня кібербезпеки. Це зокрема, відсоток виконання зобов'язань, рівень прозорості витрат для цілей кібербезпеки (необхідний фінансовий аудит з конкретними сферами діяльності щодо плану дій з кібербезпеки), співробітництво з іншими державами у кіберпросторі тощо.

Наступним кроком для проведення оцінки та об’єднання різних критеріїв для кінцевого результату повинна бути розробка відповідного автоматизованого інструменту.

Деякі інші підходи щодо оцінки ефективності Стратегії розглянемо на прикладі Канади [11]. Ця оцінка була проведена з метою виконання вимог Закону про фінансове адміністрування (Financial Administration Act [12]).

Основною метою проведення оцінки ефективності Стратегії було визначити наскільки:

була ефективною структура управління для виконання Стратегії;

департаменти та відомства, що беруть участь у забезпеченні кібербезпеки, виконували затверджену Стратегію діяльність;

заплановані заходи сприяли досягненню головних цілей Стратегії.

Для проведення оцінки використовувалася така методологія:

1. Огляд спеціальної літератури – це пошук в Інтернеті документів, пов'язаних із темами з кібербезпеки в цілому, і, зокрема, Стратегії кібербезпеки Канади.

2. Перегляд документів включав перегляд звітів про ефективність, фінансової інформації та останніх аудиторських звітів.

3. Інтерв'ю – це проведення 48 інтерв'ю з урядовими посадовцями з 11 урядових організацій Канади, а також з науковцями та іншими експертами.

При аналізі ефективності Стратегії увага приділялася питанням якою мірою досягнуто прогрес у забезпеченні кібербезпеки уряду Канади та зміцненні спроможності:

запобігання кіберінцидентам;

виявленні і захисту від кіберзагроз;

реагуванні і відновленні інфраструктури після кіберінцидентів.

Проведене дослідження виявило, що існуюча структура управління сприяла співпраці, координації та обміну інформацією між суб'єктами кібербезпеки. Проте обмін інформацією проходив на вибірковій основі, і не було чіткої політики щодо того, з ким і коли він здійснюється. На цей час не існує ефективного механізму обміну секретною інформацією, особливо в режимі реального часу.

Стратегія допомогла визначити ролі та обов'язки різних організацій та уряду Канади, запровадивши систему управління для уточнення цілей, призначення ролей та обов'язків, а також створення різних комітетів і робочих груп.

В результаті дослідження було виявлено, що Стратегія сприяє збільшенню спроможності уряду Канади запобігати, виявляти, реагувати та відновлюватися після кібернападів. Зокрема, практична реалізація Стратегії допомогла підвищити здатність урядових організацій швидко аналізувати та протидіяти кіберінцидентам, які, хоча все ще відбуваються, проте стають все рідше. Ці покращення були відзначені, незважаючи на збільшення державної та неурядової кіберактивності проти інформаційних мереж уряду Канади за останні роки. Тим не менше, респонденти відзначають, що є додаткові можливості для подальшого покращення кібербезпеки. Оцінка також виявила**,** що Стратегія сприяє розвитку партнерських відносин із власниками та операторами критично важливої інфраструктури, а також іншими зацікавленими сторонами приватного сектору.

Також серед більшості опитаних існує думка, що канадці сьогодні порівняно з минулим стали більш інформовані про кіберзагрози.

Враховуючи ці висновки, в оцінці було визначено ряд шляхів для вдосконалення кібербезпеки і висунуті рекомендації для їх вирішення. Як головна організація, Міністерство громадської безпеки Канади взяло на себе зобов'язання вирішувати ці питання у співпраці з партнерськими організаціями в рамках зусиль, спрямованих на поновлення стратегії кібербезпеки Канади з метою кращої підготовки до зміцнення її національної, економічної та кібернетичної безпеки.

Хоча в Україні в останні роки забезпеченню кібербезпеки надають великого значення і, як уже зазначалося, щорічно формується План заходів з реалізації Стратегії кібербезпеки України, який затверджується розпорядженням Кабінету Міністрів України, заходи, які визначені цим Планом, не завжди виконуються вчасно, а деякі залишаються взагалі не виконаними з різних причин.

Наприклад, ***найбільш актуальним*** на сьогодні залишається питання ***формування переліку об'єктів критичної інформаційної інфраструктури, яке передбачене пунктом 2 Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України*** (далі – План). Це питання не вирішується протягом значного терміну часу (п'ятий рік). Зокрема розпорядженням Кабінету Міністрів України від 5 листопада 2014 р. № 1135-р (чинне) було затверджено План заходів щодо захисту державних інформаційних

ресурсів, яким передбачалося Адміністрації Держспецзв'язку протягом 2014 – 2015 років сформувати перелік об'єктів, що належать до критичної інформаційної інфраструктури держави, організувати та провести оцінку стану захищеності державних інформаційних ресурсів зазначених об'єктів.

Пізніше пунктом 2 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 №32/2017, було ухвалено забезпечити у місячний строк виконання завдання, передбаченого пунктом 2 постанови Кабінету Міністрів України від 23 серпня 2016 року № 563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави", та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили виконання такого завдання у визначений зазначеною постановою строк. Це рішення також не було виконано. Зазначимо, що і на даний час (написання статті) перелік об'єктів критичної інформаційної інфраструктури не сформовано**.**

Також Планом на 2018 рік, як і в 2017 р. (пункт 13) передбачалось здійснити "розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик". Але ні у 2017, ні у 2018 роках ці завдання виконані не були (відповідальний за їх виконання орган – Держспецзв'язку) [6].

Однією з можливих причин цього є те, що План був затверджений тільки у липні 2018 року, і тому терміни виконання половини (9 із 18) заходів, передбачених цим Планом, були вже закінчені на час його затвердження, а відповідні заходи об'єктивно не могли бути виконаними вчасно.

З огляду на це, слід приділити серйозну увагу формуванню Плану на 2019 рік. Адже, незважаючи на те, що відповідний проект Держспецзв'язком було розроблено у листопаді 2018 року, сам план на даний час (написання статті травень 2019) Кабінетом Міністрів України ще не затверджено.

Підкреслимо, що Законом України "Про національну безпеку" [13] запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони України, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони. А відповідно до ст. 4 цього Закону предметом цивільного контролю з боку громадянського суспільства є зміст і стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони.

Тому, на нашу думку, актуальним на сьогодні є проведення незалежного аналізу ефективності реалізації Стратегії кібербезпеки України. Такий аналіз повинен бути здійснений відповідним уповноваженим органом згідно із затвердженою Методикою на основі рекомендацій ENISA.

Зазначимо також, що відповідно до пункту 3 статті 15 Закону України "Про основні засади забезпечення кібербезпеки України" щорічно має проводитись незалежний аудит діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави згідно з міжнародними стандартами аудиту. Проведення зазначеного аудиту потребує визначення відповідного органу та затвердження методики проведення такого аудиту.

Незалежний нагляд та контроль за діяльністю суб'єктів у сфері кібербезпеки держави здійснюється і в європейських країнах. Такий контроль може виявити низку недоліків у забезпеченні кібербезпеки та надати певні рекомендації для їх усунення.

Зокрема у своїй доповіді з питань інформаційної безпеки у державній адміністрації у 2014 році, Національне бюро аудиту Швеції вказало на необхідність посилення у першу чергу нагляду на об'єктах критичної інфраструктури [14].

Подібний аудит проводиться і в Польщі. Зокрема, у 2015 році Головне контрольно-ревізійне управління (Najwyższa Izba Kontroli, NIK) підготувало спеціальний аудит для оцінки реалізації стратегічних заходів, що здійснюються суб'єктами, відповідальними за кібербезпеку в Польщі. Загальна оцінка була критичною щодо успіху впровадження Стратегії кібербезпеки – рівень реалізації ключових заходів та рівень досягнення цілей були дуже низькими [15].

Висновки.

Уряди провідних країн світу і зокрема ЄС продовжують вживати різноманітних заходів для посилення безпеки кіберпростору, як елементу глобальної міжнародної безпеки. При цьому особлива увага приділяється розробкам стратегічних документів з питань кібербезпеки, їх регулярному оновленню та контролю виконання плану заходів реалізації на основі оцінки ефективності та спроможностей.

Для своєчасного поновлення таких документів в Україні необхідно розробити критерії оцінки стану кібербезпеки в державі. А після проведення відповідної оцінки визначити ключові напрями формування нової Стратегії кібербезпеки України, розрахованої на 2020 – 2025 роки.

Враховуючи міжнародний досвід, включно з фундаментальними рекомендаціями та директивами ООН, НАТО, ЄС та ОБСЄ, основний стратегічний напрям діяльності суб'єктів національної системи кібербезпеки повинен бути спрямований на кіберзахист критичної інформаційної інфраструктури.

Тому Кабінету Міністрів України необхідно прискорити затвердження Переліку об'єктів критичної інформаційної інфраструктури, а також постанови "Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" та "Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури". Це дозволить виявити реальний стан кіберзахисту на зазначених об'єктах та вжити заходів для його посилення.

У зв'язку з тим, що відповідно до ст. 25 Закону України "Про національну безпеку України" Стратегію кібербезпеки та інші стратегічні документи, якими визначаються основні напрями і завдання державної політики у сферах національної безпеки і оборони розробляє РНБО України, яка також здійснює координацію і контроль за їх виконанням, на нашу думку, доцільно було б, щоб План заходів з реалізації Стратегії кібербезпеки України також затверджувався б Рішенням РНБО України, а його підготовку та контроль виконання здійснював Національний координаційний центр кібербезпеки, що передбачено у Положенні про Національний координаційний центр кібербезпеки [16]. Це надасть змогу більш оперативно планувати відповідні заходи та здійснювати контроль їх виконання.

Використана література

1. DR Mykhaylo Gutsalyuk. Ukraine's Cybersecurity strategy and ways to implement it. *European Cybersecurity journal*. Volume 2 (2016). The Kosciuszko Institute. Poland. P. 65-69.

2. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України": станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

3. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. URL: http://niss.gov.ua/doslidzhennya/analiti chni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya (дата звернення: 21.05.2019).

4. Дубов Д.В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети*. 2013. № 4. С. 119-127. URL: http://nbuv.gov.ua/UJRN/spa_2013_4_18 (дата звернення: 21.05.2019).

5. Литвинчук Н.Ю. Формування системи забезпечення кібернетичної безпеки: збірник тез наук. доповідей X Всеукр. наук.-практ. конф. *Актуальні проблеми управління інформаційною безпекою держави,* м. Київ, 4 квіт. 2019 р. Київ: Нац. акад. СБУ, 2019. С. 240-243.

6. Ткачук Н.А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

7. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 11.07.18 р. № 481-р. URL: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80 (дата звернення: 21.05.2019).

8. Guide to Developing A National Cybersecurity Strategy. URL: https://www.itu.int/ dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf (дата звернення: 21.05.2019).

9. An evaluation Framework for National Cyber Security Strategies. URL: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies (дата звернення: 21.05.2019).

10. Europe 2020 strategy URL: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy (дата звернення: 21.05.2019).

11. Horizontal Evaluation of Canada's Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx (дата звернення: 21.05.2019).

12. Financial Administration Act (R.S.C., 1985). URL: https://laws-lois.justice.gc.ca/eng/acts/f-11 (дата звернення: 21.05.2019).

13. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19?find=1&text=%D1%F2%F0%E0%F2%E5%E3%B3%FF+%EA%B3%E1%E5%F0%E1%E5%E7%EF%E5%EA%E8 (дата звернення: 21.05.2019).

14. A national cyber security strategy (Sweden). URL: https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213 (дата звернення: 21.05.2019).

15. NIK o bezpieczeństwie w cyberprzestrzeni. URL: https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html

16. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7.06.16 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 21.05.2019).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~