ПРЯМУЄМО РАЗОМ

ВЕРХОВНА РАДА УКРАЇНИ

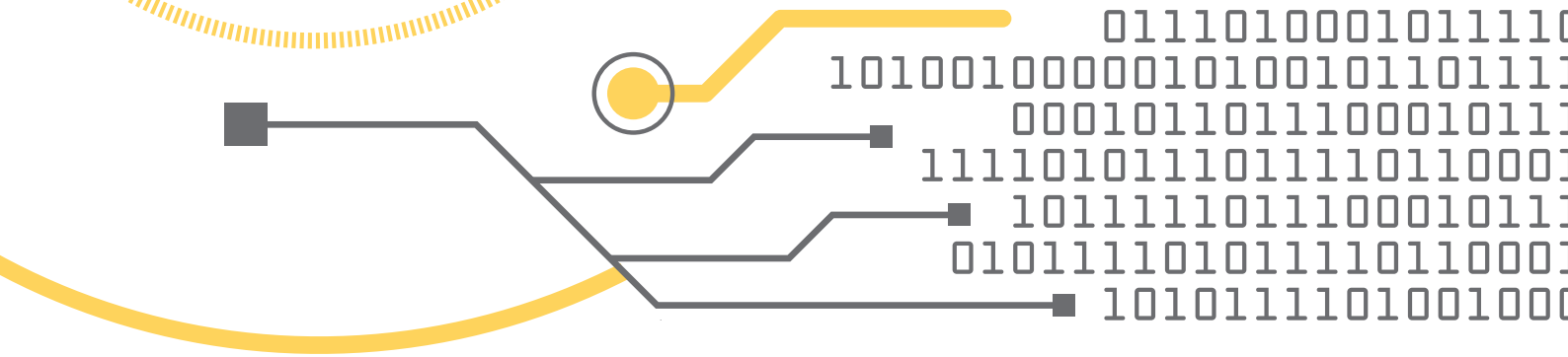
UNDP

Проєкт ЄС-ПРООН з парламентської реформи

Комітет з питань цифрової трансформації

ЗВІТ

щодо подання та подальшої оцінки щорічного звіту про результати незалежного аудиту діяльності основних суб'єктів національної кібербезпеки



Публікація підготовлена Офісом парламентської реформи в рамках проєкту ЄС-ПРООН з парламентської реформи. Зміст публікації є виключно відповідальністю автора і необов'язково відображає позицію Європейського Союзу або Програми розвитку ООН.

Авторка — **Лілія Олексюк**, кандидат наук з державного управління, юрист, позаштатний консультант Комітету Верховної Ради України з питань цифрової трансформації

ЗМІСТ

4 СКОРОЧЕННЯ

5 РЕЗЮМЕ

6 ВСТУП

8 АНАЛІЗ СИТУАЦІЇ

11 ВАРІАНТИ ВИРІШЕННЯ

22 ВИСНОВКИ

СКОРОЧЕННЯ

EUROSAI	Європейська організація вищих органів фінансового контролю
INTOSAI	Міжнародна організація вищих органів фінансового контролю
ISSAI	Міжнародні стандарти вищих органів фінансового контролю
ГШ ЗСУ	Генеральний штаб Збройних Сил України
Держспецзв'язку	Державна служба спеціального зв'язку та захисту інформації України
ЄС	Європейський Союз
Закон про кібербезпеку	Закон України «Про основні засади забезпечення кібербезпеки України»
Комітет з питань цифрової трансформації	Комітет Верховної Ради України з питань цифрової трансформації
МО	Міністерство оборони України
НАТО	Організація Північноатлантичного Договору
НБУ	Національний банк України
НПУ	Національна поліція України
РНБО	Рада національної безпеки та оборони
СБУ	Служба безпеки України

РЕЗЮМЕ

Для забезпечення проведення аудиту діяльності основних суб'єктів національної кібербезпеки, визначення критеріїв такого аудиту, а також ефективного контролю за дотриманням законодавства під час заходів із забезпечення кібербезпеки необхідно здійснити комплексний перегляд Закону України «Про основні засади забезпечення кібербезпеки України», зокрема надати основним суб'єктам національної кібербезпеки відповідні можливості щодо замовлення аудиту ефективності у Рахункової палати.

Для подання звіту щодо проведення аудиту в строки, визначені Законом про кібербезпеку, необхідно вже найближчим часом вирішити питання внесення до плану роботи Рахункової палати аудитів усіх основних суб'єктів національної кібербезпеки.

Визначені критерії проведення аудиту мають бути узгоджені аудитором та об'єктами аудиту — тоді ці критерії буде визнано об'єктивними і такими, що можуть становити основу для подальшого відстеження динаміки роботи органів.

За цих обставин необхідно розглянути також питання методології і критеріїв оглядів «стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури»[1], передбачених статтею 27 Закону України «Про національну безпеку», які можна було б використати як індикатори для оцінки ефективності заходів із кібербезпеки.

За зразок можна взяти досвід Європейського суду аудиторів[2].

Окремо варто дослідити виконання заходів Національним банком України як окремим незалежним основним суб'єктом, зокрема місце НБУ та банківської системи у системі національної безпеки України. Для НБУ жодного завдання із забезпечення національної безпеки Законом України «Про національну безпеку» не визначено.

1 https://zakon.rada.gov.ua/laws/show/2469-19

2 https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

ВСТУП

Закон України «Про основні засади забезпечення кібербезпеки України»[3] (далі — Закон, Закон про кібербезпеку) ухвалено у жовтні 2017 року.

Перехідними положеннями було встановлено час для набрання чинності — шість місяців з дня опублікування для забезпечення виконання і реалізації відповідних передбачених ним заходів.

Відповідно до статті 8 Закону про кібербезпеку основними суб'єктами національної кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Цим самим Законом (стаття 15) встановлено строки подання органам, що здійснюють контроль за діяльністю основних суб'єктів національної кібербезпеки (Президентові України, Верховній Раді України та Кабінету Міністрів України), звіту за попередній рік про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави: сорокап'ятиденний строк після закінчення календарного року, тобто до 15 лютого.

Також визначено, що незалежний аудит діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

3 https://zakon.rada.gov.ua/laws/show/2163-19

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо **ефективності системи забезпечення кібербезпеки держави**.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік **звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави**, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань Верховною Радою України.

АНАЛІЗ СИТУАЦІЇ

Комітет Верховної Ради України з питань цифрової трансформації в рамках контролю за дотриманням законодавства під час здійснення заходів із забезпечення кібербезпеки на засіданні 19 лютого 2020 року розглянув питання щодо виконання частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» — про результати **проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави**.

На цьому засіданні усім представникам основних суб'єктів національної кібербезпеки було надано можливість представити інформацію зі звітів. Заступник голови Комітету з питань цифрової трансформації Федієнко О.П. визначив регламент: дві хвилини на представлення результатів звітів — та наголосив на необхідності детально представити інформацію щодо проведення аудитів[4].

Усі представники основних суб'єктів національної кібербезпеки висловили схожі позиції з такими тезами:

1) більшість суб'єктів є силовими або військовими структурами (виняток — тільки Національний банк України), що вимагає наявності в аудитора спеціального допуску до інформації (державної таємниці);
2) у Законі не встановлено способу виконання цього завдання;
3) наявні суттєві обмеження щодо можливостей залучення міжнародних аудиторських компаній (відповідно до пункту 1 зауважень).

4 https://www.facebook.com/FediiencoAlexandr/posts/1794748600236 33?__tn__=K-R

Інформації від Національного банку України щодо заходів із організації проведення аудиту не надходило, позицію на засіданні представлено не було.На засіданні Комітету[5] було прийнято відповідні рішення:

1. Інформацію щодо виконання частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» щодо результатів проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи кібербезпеки держави взяти до відома.

2. Визнати невиконання основним суб'єктами національної кібербезпеки, а саме: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України вимог частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України».

3. Кабінету Міністрів України забезпечити виконання основними суб'єктами національної кібербезпеки (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України) вимог частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» в частині проведення незалежного аудиту діяльності основними суб'єктами національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави у відповідності до міжнародних стандартів аудиту.

4. Поінформувати Комітет Верховної Ради України з питань цифрової трансформації про стан виконання вищезазначеної норми закону до 20 травня 2020 року. Контроль за виконанням даного рішення покласти на заступника голови Комітету з питань цифрової трансформації Олександра Федієнка.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, а саме: Комітет з питань національної безпеки, оборони та розвідки, звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо **ефективності системи забезпечення кібербезпеки держави не розглядав**[6].

Висновки за результатами засідання Комітету та розгляду отриманої інформації:

- Основні суб'єкти національної кібербезпеки не приділяли належної уваги організації аудиту власної діяльності.
- Попередню оцінку можливості проведення аудиту комерційними чи державними аудиторськими органами підприємства не здійснювали.

5 http://komit.rada.gov.ua/news/main_news/povidomlen/73537.html

6 http://komnbor.rada.gov.ua/

- За весь час із набрання Законом України «Про основні засади кібербезпеки в Україні» чинності спроб вирішити питання, звернути увагу Кабінету Міністрів, законодавчого органу жоден суб'єкт національної кібербезпеки не здійснив.
- Обидва комітети Верховної Ради не надавали ВРУ рекомендацій та звітів за результатами реалізації контрольних повноважень до 2020 року, не порушували питання щодо виконання Закону і не користувалися своєю контрольною функцією.

Таким чином, для виконання законодавства про кібербезпеку необхідно вирішити такі питання:

1. Визначити індикатори (чинники, критерії тощо), за якими можна провести незалежний аудит діяльності основними суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави відповідно до міжнародних стандартів аудиту.
2. Визначити можливих аудиторів.
3. Надати рекомендації щодо організації проведення аудитів.

ОКРЕМО ВАРТО ДОСЛІДИТИ ВИКОНАННЯ ЗАХОДІВ НАЦІОНАЛЬНИМ БАНКОМ УКРАЇНИ ЯК ОКРЕМИМ НЕЗАЛЕЖНИМ ОСНОВНИМ СУБ'ЄКТОМ, ЗОКРЕМА МІСЦЕ НБУ ТА БАНКІВСЬКОЇ СИСТЕМИ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ. ДЛЯ НБУ ЖОДНОГО ЗАВДАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЗАКОНОМ УКРАЇНИ «ПРО НАЦІОНАЛЬНУ БЕЗПЕКУ» НЕ ВИЗНАЧЕНО.

Відповідно до законодавства НБУ[7]:

- визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;
- забезпечує формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об'єктів у банківській системі України до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України» є певним конфліктом інтересів.

7 https://zakon.rada.gov.ua/laws/show/679-14#n109

ВАРІАНТИ ВИРІШЕННЯ

З огляду на проблеми з реалізацією положень статті 15 Закону України «Про основні засади кібербезпеки в Україні» було проведено попередній аналіз можливого замовлення аудитів з урахуванням особливостей майбутніх замовників.

У відкритому доступі небагато інформації щодо можливого проведення аудиту великими міжнародними аудиторськими компаніями, представленими на ринку України.

Так, «PwC Україна» пропонує послугу аудиту — оцінки ефективності[8], але що саме передбачено як результат аудиту, яка застосовується методика (авторська методика як об'єкт авторського права має певну вартість, є комерційною таємницею), які критерії оцінювання і яка буде вартість такого аудиту, з'ясується в процесі індивідуальних перемовин між замовником і виконавцем.

Національний банк визначив переможця для здійснення аудиту річної фінансової звітності НБУ за міжнародними стандартами протягом наступних 5 років: це представник так званої «великої четвірки» в галузі аудиторських послуг, ТОВ «Ернст енд Янг Аудиторські послуги»[9]; але об'єктом аудиту буде тільки фінансова звітність[10]. Офіційних повідомлень про вибір аудитора для здійснення незалежного аудиту діяльності НБУ як основного суб'єкта національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави відповідно до міжнародних стандартів у відкритих джерелах немає.

Протягом попередніх п'яти років аудит річної фінансової звітності НБУ здійснювало ПрАТ «Делойт енд Туш ЮСК»[11], ще одна компанія з так званої «великої четвірки». Але відповідно до Закону України «Про Національний банк України» одна й та сама аудиторська фірма не має права проводити такий аудит більш ніж п'ять років поспіль.

8 https://www.pwc.com/ua/uk/industry/government-and-public-sector/central-gov-authorities.html

9 https://www.ey.com/en_ua/government-public-sector/services

10 https://bank.gov.ua/news/all/natsionalniy-bank-otrimav-novogo-zovnishnogo-auditora-richnoyi-finansovoyi-zvitnosti-na-nastupni-pyat-rokiv

11 https://www2.deloitte.com/ua/uk/industries/government-public-services.html?icid=top_government-public-services

Ще одна міжнародна компанія, яка може надавати такі послуги, —Civitta[12], але аудит ефективності можна проводити тільки за окремим запитом і з формулюванням власне предмета і об'єкта аудиту.

Наступний варіант — державні установи, що здійснюють аудит в Україні: Державна аудиторська служба та Рахункова палата.

Державна аудиторська служба здійснює свою діяльність як центральний орган виконавчої влади, уповноважений Кабінетом Міністрів України на реалізацію державної політики у сфері державного фінансового контролю виключно з метою здійснення державного фінансового контролю[13]. Тому проведення такого специфічного аудиту оцінки ефективності не належить до її компетенції.

Друга згадана інституція — державний колегіальний орган, що від імені Верховної Ради України здійснює контроль за надходженням коштів до Державного бюджету України та їх використанням, але має й додаткові функції.

Відповідно до статей 4 та 7 Закону України «Про Рахункову палату», до повноважень Рахункової палати належить також здійснення аудиту ефективності.

Закон визначає аудит ефективності як «встановлення фактичного стану справ та надання оцінки щодо своєчасності і повноти бюджетних надходжень, продуктивності, результативності, економності використання бюджетних коштів їх розпорядниками та одержувачами, законності, своєчасності і повноти прийняття управлінських рішень учасниками бюджетного процесу, стану внутрішнього контролю розпорядників бюджетних коштів»[14].

У статті 3 вказаного Закону визначено, що Рахункова палата застосовує у своїй діяльності основні принципи Міжнародної організації вищих органів фінансового контролю (INTOSAI), Європейської організації вищих органів фінансового контролю (EUROSAI) та **Міжнародні стандарти** вищих органів фінансового контролю (ISSAI).

Міжнародна організація вищих органів аудиту (INTOSAI)[15] — міжнародна професійна організація, яка об'єднує вищі органи аудиту країн — членів Організації Об'єднаних Націй. INTOSAI створено 1953 року, наразі до її складу входять вищі органи аудиту 194 країн світу, ще 5 є асоційованими членами та 1 — афілійованим членом організації.

Рахункова палата є повноправним членом INTOSAI з 1998 року.

12 https://civitta.com.ua/services

13 https://zakon.rada.gov.ua/laws/show/2939-12

14 https://zakon.rada.gov.ua/laws/show/576-19

15 https://www.intosai.org/ru/

Основним завданням INTOSAI є надання аудиторам усього світу можливості обміну інформацією, що становить спільний інтерес, інформацією щодо сучасних напрацювань у сфері аудиту та застосування професійних стандартів і найкращих методологій. INTOSAI сприяє покращенню державного управління, заохочуючи вищі органи аудиту до підтримки урядів у вдосконаленні їхньої діяльності, підвищення прозорості бюджетної сфери, забезпечення підзвітності, боротьби з корупцією, стимулювання кваліфікованого та ефективного використання державних ресурсів на користь суспільства.

У своїй діяльності INTOSAI керується Лімською декларацією про основні принципи здійснення аудиту (1977)[16], у якій викладено основні філософські та концептуальні підходи, визначено цінності вищих органів фінансового контролю — демократичність та незалежність, а також визначеним Мексиканською декларацією принципом незалежності вищих органів аудиту (2007)[17].

Європейську організацію вищих органів аудиту (EUROSAI)[18] створено 1990 року задля досягнення цілей INTOSAI на регіональному (європейському) рівні й надання при цьому членам можливості зосередити увагу на питаннях, актуальних для їхнього регіону.

Станом на сьогодні EUROSAI об'єднує 50 вищих органів аудиту (49 європейських і Європейський суд аудиторів).

Рахункова палата є повноправним членом EUROSAI з 1999 року.

Відповідно до статті 1 Статуту EUROSAI, основна мета організації — сприяти розвитку співпраці між національними вищими органами аудиту, які входять до неї, а також обміну інформацією і документацією, дослідженням у сфері контролю державних фінансів, створенню університетських кафедр державного аудиту та уніфікації термінології у сфері фінансового контролю. Керівними органами EUROSAI є Конгрес, Керівна рада і Секретаріат.

Функції постійного Секретаріату EUROSAI виконує Аудиторський суд Іспанії, на базі якого діє штаб-квартира організації. Секретаріат готує і проводить засідання Керівної ради, розробляє і виконує бюджет організації, а також забезпечує виконання рішень, ухвалюваних Конгресом і Керівною радою. Секретаріат видає щорічний журнал EUROSAI, а також щоквартальний бюлетень «EUROSAI Newsletter», формує і оновлює базу даних статутів і публікацій усіх вищих органів аудиту — членів організації.

Отже, Рахункова палата є достатньо незалежним органом для здійснення аудиту ефективності, при цьому застосовує міжнародні стандарти.

За інформацією INTOSAI, усі стандарти поділяються на категорії залежно від типу аудиту.

16 http://old.ac-rada.gov.ua/control/main/uk/publish/article/140217?cat_id=32836

17 http://old.ac-rada.gov.ua/control/main/uk/publish/article/1013545?cat_id=32836

18 https://www.eurosai.org/ru/about-us/about-eurosai/

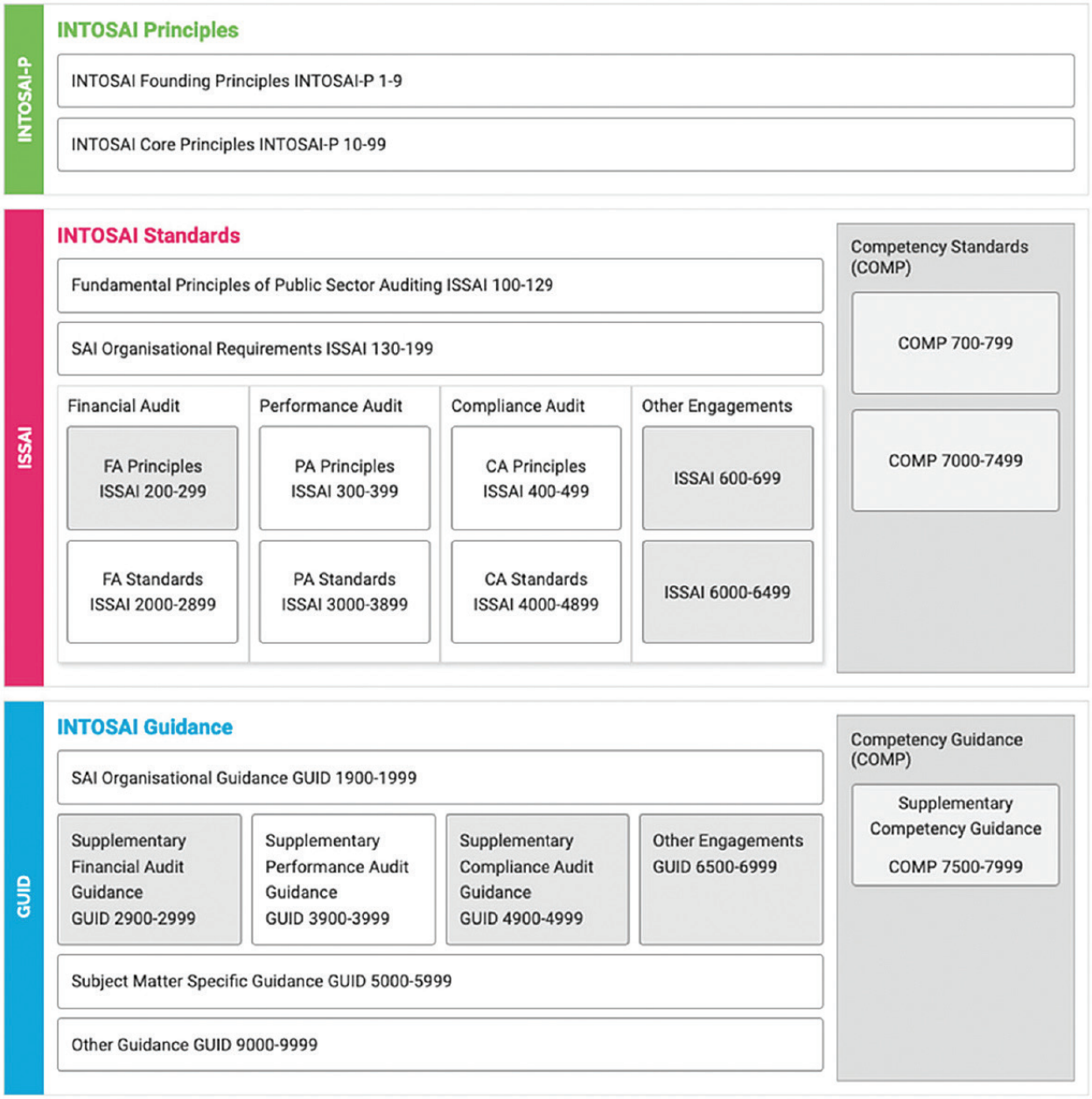


Рисунок 1. Стандарти аудитів INTOSAI

Слід зазначити, що для оцінки ефективності застосовується окремий стандарт, відмінний від фінансових: ISSAI 300 «Основоположні принципи аудиту ефективності»[19].

ISSAI 100 «Основоположні принципи аудиту в державному секторі» містить основні принципи аудиту в державному секторі в цілому і визначає сферу застосування стандартів ISSAI. ISSAI 300 «Основоположні принципи аудиту ефективності» розвиває основоположні принципи ISSAI 100 відповідно до специфічного контексту аудиту ефективності. ISSAI 300 необхідно читати і трактувати разом з ISSAI 100, який також стосується аудиту ефективності.

19 https://www.eurosai.org/handle404?exporturi=/export/sites/eurosai/.content/documents/others/ISSAI/ISSAI-300-ruso.pdf

ISSAI 300 «Основоположні принципи аудиту ефективності» містить три розділи. Перший розділ визначає систему аудиту ефективності та містить посилання на відповідні ISSAI. Другий розділ описує загальні принципи аудиту ефективності, які аудитор має враховувати перед початком і під час проведення аудиту. У третьому розділі викладено принципи основних етапів аудиту із коротким описом.

Аудитор сам визначає відповідні критерії, питання аудиту, що базуються на принципах **економічності, ефективності та результативності**.

Критерії є порівняльними зразками для оцінювання предмета перевірки. Критерії аудиту ефективності — це обґрунтовані, специфічні для аудиту стандарти діяльності, за якими можна оцінити економічність, ефективність і результативність операцій.

Критерії становлять базу для оцінки доказів, формування результатів аудиту та складання висновків відповідно до цілей аудиту. Вони також є важливим елементом обговорень усередині аудиторської групи, з керівництвом вищого органу аудиту і під час спілкування з об'єктами аудиту.

Критерії можуть бути якісними та кількісними; окремо визначаються принципи добору критеріїв, за якими безпосередньо оцінюватиметься об'єкт аудиту. Критерії можуть бути загальними чи конкретними, вказуючи, відповідно, на те, який стан має бути згідно із законами, нормативними вимогами або цілями; що очікується відповідно до основних принципів, наукових знань і найкращих практик; або яка ситуація могла би скластися (за кращих умов). Для визначення критеріїв можуть використовуватися різні джерела, зокрема системи оцінювання діяльності. Джерела мають бути публічними і прозорими, а критерії — відповідними і зрозумілими для користувачів, а також повними, надійними і об'єктивними в контексті предмета і цілей аудиту.

Критерії необхідно обговорювати з об'єктами аудиту, але остаточний вибір здійснює аудитор. Визначення і повідомлення критеріїв на етапі планування може забезпечити вищий рівень їх надійності й загальної прийнятності, але варто зазначити, що в разі аудиту комплексних питань критерії не завжди можуть бути чітко визначені вже на початку процесу. У цьому випадку вони будуть окреслені в ході проведення аудиту.

Хоча деякі види аудиту і передбачають неоднозначні законодавчі критерії, в аудиті ефективності цього, як правило, не буває. Цілі аудиту, охоплювані ним питання і підхід до його здійснення визначають відповідність і види критеріїв; впевненість користувача в надійності висновків аудиту ефективності залежить головним чином від критеріїв. Тому важливо вибирати надійні й об'єктивні критерії.

У разі аудиту ефективності, орієнтованого на проблему, відправною точкою є відоме або передбачуване відхилення від того, що має або могло би бути. Таким чином, головна мета — не просто підтвердити проблему (відхилення від критерію і наслідки такого відхилення), а й окреслити причини. Тому важливо на етапі планування вирішити, як саме перевірити й підтвердити причини. В основу висновків і рекомендацій передусім покладено аналіз і підтвердження причин, навіть попри те, що ці висновки й рекомендації випливають із нормативних умов.

На сайті робочої групи з питань IT EUROSAI можна ознайомитися з прикладами аудитів, здійснених у провідних європейських державах[20].

Серед іншого тут наведено «Аудит поточного управління та нагляду за захистом інформації та кібербезпекою у фінансовому секторі»[21]. Отже, аудит ефективності, здійснений за міжнародними стандартами достатньо незалежним органом, можливий і в Україні.

Об'єктами контролю з боку Рахункової палати під час виконання нею повноважень є державні органи, органи влади Автономної Республіки Крим, органи місцевого самоврядування, інші бюджетні установи, у тому числі закордонні дипломатичні установи України, суб'єкти господарювання, громадські чи інші організації, фонди загальнообов'язкового державного соціального і пенсійного страхування, Національний банк України та інші фінансові установи.

СТРОКИ ПРОВЕДЕННЯ АУДИТІВ ЕФЕКТИВНОСТІ ЗАЗВИЧАЙ СТАНОВЛЯТЬ ВІД 3 ДО 6 МІСЯЦІВ.

Питання аудиту ефективності неможливо розглядати без комплексного аналізу Закону України «Про основні засади забезпечення кібербезпеки України», оскільки критеріями ефективності, зокрема, будуть цілі й завдання, визначені в Законі та поставлені перед відповідними органами для «забезпечення захисту життєво важливих інтересів людини і громадянина»[22].

Як показує аналіз Закону, **цілі й завдання щодо кібербезпеки ним не визначені**, хоча дві статті цього нормативно-правового акта містять такі положення:

«Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом.

…

20 http://egov.nik.gov.pl/g/egov/sum/reports.html#UK

21 http://egov.nik.gov.pl/g/egov/KR/2014/InformationProtection/InformationProtection-RepublicOfKorea-2014.pdf

22 Стаття 1 Закону про кібербезпеку. https://zakon.rada.gov.ua/laws/show/2163-19

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону»[23].

Тому до початку аудиту під час визначення його критеріїв необхідно насамперед окреслити, якого рівня ефективності слід вимагати, якщо Законом не визначено цілі й завдання для основних суб'єктів національної кібербезпеки.

Наступне питання — визначення об'єктів кібербезпеки. Закон про кібербезпеку визначає їх так:

> «**ОБ'ЄКТАМИ КІБЕРБЕЗПЕКИ Є:**
>
> 1) КОНСТИТУЦІЙНІ ПРАВА І СВОБОДИ ЛЮДИНИ І ГРОМАДЯНИНА;
> 2) СУСПІЛЬСТВО, СТАЛИЙ РОЗВИТОК ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА ЦИФРОВОГО КОМУНІКАТИВНОГО СЕРЕДОВИЩА;
> 3) ДЕРЖАВА, ЇЇ КОНСТИТУЦІЙНИЙ ЛАД, СУВЕРЕНІТЕТ, ТЕРИТОРІАЛЬНА ЦІЛІСНІСТЬ І НЕДОТОРКАННІСТЬ;
> 4) НАЦІОНАЛЬНІ ІНТЕРЕСИ В УСІХ СФЕРАХ ЖИТТЄДІЯЛЬНОСТІ ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ;
> 5) ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»[24].

Отже, одним із критеріїв є досягнення безпеки об'єктів кібербезпеки у кіберпросторі. Розгляньмо, чи достатньо визначені об'єкти кібербезпеки для встановлення критеріїв аудиту відповідно до порядку, описаного в статті 4 Закону про кібербезпеку, та проаналізуймо перелік об'єктів кібербезпеки, визначених у Законі про кібербезпеку.

1) У Розділі II Конституції України[25] «Права, свободи та обов'язки людини і громадянина» вміщено 48 статей, положення яких гарантують права і свободи людині на території держава Україна. Відповідно до Конституції України держава гарантує:
   - свободу політичної діяльності;
   - право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості (стаття 23);
   - рівність прав жінки і чоловіка та недискримінація за будь-якою ознакою (стаття 24);
   - право на громадянство та право відмови від громадянства, рівні права для іноземців (стаття 25 та 26);

23 Стаття 2 Закону про кібербезпеку. https://zakon.rada.gov.ua/laws/show/2163-19

24 Стаття 4 Закону про кібербезпеку. https://zakon.rada.gov.ua/laws/show/2163-19

25 https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

- право на життя та право захищати своє життя і здоров'я, життя і здоров'я інших людей від протиправних посягань (стаття 27);
- право на повагу до гідності (стаття 28);
- право на свободу та особисту недоторканність, недоторканність житла (статті 29, 30);
- право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (стаття 31);
- право на невтручання в особисте і сімейне життя (стаття 32);
- право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею; на судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (стаття 32);
- свобода пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом (стаття 33);
- право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір, крім випадків, коли здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (стаття 34);
- право на свободу світогляду і віросповідання, при цьому церква і релігійні організації в Україні відокремлені від держави, а школа — від церкви. Жодна релігія не може бути визнана державою як обов'язкова (стаття 35);
- право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів, за винятком обмежень, встановлених законом в інтересах національної безпеки та громадського порядку, охорони здоров'я населення або захисту прав і свобод інших людей; право на участь у професійних спілках з метою захисту своїх трудових і соціально-економічних прав та інтересів (стаття 36);
- право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування; право доступу до державної служби, а також до служби в органах місцевого самоврядування (стаття 38);

- право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації (стаття 39);
- право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк (стаття 40);
- право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (стаття 41);
- право на підприємницьку діяльність, яка не заборонена законом; право споживати безпечні послуги та продукти (стаття 42);
- право на працю, право на належні, безпечні і здорові умови праці, на заробітну плату, не нижчу від визначеної законом, захист від незаконного звільнення та своєчасне одержання винагороди за працю (стаття 43);
- право на страйк для захисту своїх економічних і соціальних інтересів (стаття 44);
- право на відпочинок (стаття 45);
- право на соціальний захист, що включає право на забезпечення у разі повної, часткової або тимчасової втрати працездатності, втрати годувальника, безробіття з незалежних від особи обставин, а також у старості та в інших випадках, передбачених законом, при цьому право гарантується загальнообов'язковим державним соціальним страхуванням, створенням мережі державних, комунальних, приватних закладів для догляду за непрацездатними (стаття 46);
- право на житло. Держава створює умови, за яких кожний громадянин матиме змогу побудувати житло, придбати його у власність або взяти в оренду (стаття 47);
- право на достатній життєвий рівень для себе і своєї сім'ї, що включає достатнє харчування, одяг, житло (стаття 47);
- право на охорону здоров'я, медичну допомогу та медичне страхування (стаття 49);
- право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди; право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (стаття 50);
- право на сім'ю, дитинство, материнство і батьківство (стаття 51);
- право на освіту (стаття 53);
- свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності та право на результати своєї інтелектуальної, творчої діяльності (стаття 54);

- право на судовий захист; право звертатися за захистом своїх прав до Уповноваженого Верховної Ради України з прав людини; право після використання всіх національних засобів правового захисту звертатися за захистом своїх прав і свобод до відповідних міжнародних судових установ чи до відповідних органів міжнародних організацій, членом або учасником яких є Україна; право будь-якими не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань (стаття 55);
- право на відшкодування за рахунок держави чи органів місцевого самоврядування матеріальної та моральної шкоди, завданої незаконними рішеннями, діями чи бездіяльністю органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб при здійсненні ними своїх повноважень (стаття 56);
- право знати свої права і обов'язки. Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення у порядку, встановленому законом. Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними (стаття 57);
- право не відповідати за діяння, які на час їх вчинення не визнавалися законом як правопорушення (стаття 58);
- право на правову допомогу (стаття 59);
- право на індивідуальну юридичну відповідальність (стаття 61);
- презумпцію невинуватості (стаття 62);
- право на відмову давати показання або пояснення щодо себе, членів сім'ї чи близьких родичів, коло яких визначається законом (стаття 63).

2) «Суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища» як об'єкт кібербезпеки не розтлумачені нормами законодавства.

3) та 4) Усі ці об'єкти є об'єктами національної безпеки, а не тільки кібербезпеки. Законом України «Про національну безпеку» визначені як фундаментальні національні інтереси:

«1) державний суверенітет і територіальна цілісність, демократичний конституційний лад, недопущення втручання у внутрішні справи України;

2) сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення;

3) інтеграція України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами»[26].

26 https://zakon.rada.gov.ua/laws/show/2469-19

5) Критерії та порядок зарахування об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, зокрема щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки на сьогодні досі не затверджені Кабінетом Міністрів України, а в банківській системі України — Національним банком України.

Є певні неузгодженості в законах України «Про Рахункову палату» та «Про основні засади забезпечення кібербезпеки України» в частині реалізації контролю за основними суб'єктами національної кібербезпеки, що потребуватимуть вирішення на законодавчому рівні:

1. Повноваження Рахункової палати не обмежені, але оскільки Законом про кібербезпеку встановлено щорічне проведення аудиту ефективності, це потребуватиме внесення до плану діяльності Рахункової палати додаткових восьми аудитів і забезпечення необхідної кількості аудиторів, обізнаних з особливостями сфери кібербезпеки, із відповідним рівнем допуску для роботи з інформацією, що може становити державну таємницю, а також визначення порядку звернення замовників аудиту до Рахункової палати чи іншого порядку включення аудитів до плану.

2. Стаття 15 Закону про кібербезпеку не визначає для основних суб'єктів національної кібербезпеки обов'язку замовляти аудит, вимагає тільки надавати звіт про проведений аудит, таким чином, у органів є певні складнощі із замовленням бюджетних видатків на ці процедури — відсутні підстави для включення у бюджетний процес саме цих витрат.

3. Оскільки частина органів не підпорядкована Кабінету Міністрів України, здійснювати координацію процесу КМУ не зможе, тому доручення, надане йому Комітетом з питань цифрової трансформації, навряд можна реалізувати.

4. Відсутня відповідна державна програма чи національний план забезпечення кібербезпеки або реалізації заходів із забезпечення кібербезпеки.

5. Стратегія кібербезпеки27 була ухвалена 2016 року, задовго до Закону про кібербезпеку, ефективність її виконання на сьогодні також під питанням, оскільки не проведено жодного публічного обговорення виконання річних планів заходів, розроблених на її підставі (окремо слід зазначити, що з 2016 року їх було тільки 2 — ухвалений у березні 2017 р. та затверджений у липні 2018 р., що взагалі не сприяло їх ефективному виконанню).

6. Стратегія національної безпеки на 2020 р. розглянута РНБО, але Президентом досі не затверджена, тому наразі не визначено, чи з'являться інші цілі й завдання або механізми реалізації державної політики у сфері кібербезпеки, яка є похідною від національної безпеки.

27 https://zakon5.rada.gov.ua/laws/show/96/2016

ВИСНОВКИ

Забезпечення проведення аудиту діяльності основних суб'єктів національної кібербезпеки, визначення критеріїв такого аудиту, аудиторів та інших організаційних аспектів потребуватиме розробки законодавчих актів на рівні змін до законів, актів Кабінету Міністрів України та актів НБУ.

Ефективний контроль за дотриманням законодавства під час здійснення заходів із забезпечення кібербезпеки можливий після перегляду Закону України «Про основні засади забезпечення кібербезпеки України» і внесення до нього змін.

Замовлення основними суб'єктами національної кібербезпеки аудиту ефективності у Рахункової палати можливе за таких умов: визначення підстав для нього, визначення критеріїв та узгодження їх усіма учасниками процесу (аудитором та основними суб'єктами забезпечення кібербезпеки) — задля визнання цих критеріїв об'єктивними і такими, що можуть становити основу для подальшого відстеження динаміки роботи органів.

Для подачі звіту щодо проведення аудиту в строки, визначені Законом про кібербезпеку, необхідно найближчим часом вирішити питання внесення до плану роботи Рахункової палати аудитів усіх основних суб'єктів національної кібербезпеки.

Окрему увагу слід приділити методології та критеріям оглядів «стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури»[28], передбачених статтею 27 Закону України «Про національну безпеку», які можна було б використати як індикатори для оцінювання ефективності заходів із кібербезпеки. Наразі у відкритому доступі інформація про методологію відсутня.

28 https://zakon.rada.gov.ua/laws/show/2469-19

Як зразок можна використовувати європейський досвід проведення аудитів. Звіт Європейського суду аудиторів «**Challenges to effective EU cybersecurity policy**»[29] був представлений рік тому, у березні 2019 року.

Звіт не містить конкретних критеріїв, а висновки про виклики у регулюванні кібербезпеки не супроводжуються конкретними рекомендаціями щодо заходів, у них лише наголошено на необхідності спрямувати зусилля у певних напрямках.

Як зазначено у звіті, в останні роки ЄС приділяв багато уваги посиленню кібербезпеки. Однак досягнення вищого рівня кібербезпеки все ще залишається значним фундаментальним завданням. Аудитори окремо зазначають, що необхідно перейти до культури ефективності із вбудованими методами оцінювання, щоб забезпечити посутню відповідальність та оцінку. У законодавстві ЄС досі наявні певні лакуни, а держави-члени не завжди послідовно імплементують його на національному рівні. Експерти роблять акцент на збільшенні інвестицій і узгодженні їх зі стратегічними цілями.

Відповідні дослідження у ЄС дають підстави вважати, що Україні, особливо у разі її приєднання до Єдиного цифрового ринку ЄС, потрібно підсилювати управління кібербезпекою, щоб сприяти підвищенню здатності глобальної спільноти реагувати на кібератаки та інциденти у цій сфері. Сьогодні неможливо запобігти всім атакам, тож швидке виявлення проблем та реагування на інциденти й захист критичної інфраструктури, удосконалення обміну інформацією та координації між державним і приватним секторами є ключовими викликами, які потребують необхідного вирішення. Окремо варто наголосити на нагальній потребі в розвитку відповідних навичок у суспільстві та збільшенні кількості фахівців у сфері кібербезпеки й кіберзахисту.

29 https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf