УДК 35:004.056
DOI: 10.15587/2706-5448.2021.225271

РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ: СЕРТИФІКАЦІЯ КІБЕРБЕЗПЕКИ ОПЕРАЦІЙНИХ ТЕХНОЛОГІЙ

Цвілій О. О.

Об'єктом дослідження є система та схеми оцінки відповідності (сертифікації) кібербезпеки операційних технологій (ОТ), як набір правил та процедур, що описують об'єкти сертифікації, визначають зазначені вимоги та забезпечують методологію проведення сертифікації. Термінологічна база та понятійний апарат дослідження сертифікації кібербезпеки операційних технологій спираються на міжнародний стандарт ISO 17000:2020 Conformity assessment – Vocabulary and general principles. Основою систем і схем сертифікації кібербезпеки є оціночні стандарти, вибір та застосування яких не є однозначним та історично має безліч інтерпретацій та механізмів застосування. Ці стандарти складаються з інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, найкращих практик, гарантій та технологій тощо. Але вони мають в тій чи іншій мірі суттєвий недолік, – складність трансформації результатів оцінювання інформаційної безпеки за цими стандартами в гарантії безпеки зі скільки завгодно широким міжнародним визнанням. Це в умовах глобалізації суттєво погіршує якість кібербезпеки.

Основна гіпотеза дослідження полягає в припущенні, що якість кібербезпеки може бути підвищена шляхом конвергенції до загальної методології, яка спирається на узгоджені міжнародні стандарти та передову міжнародну практику з сертифікації. Розглянуто питання щодо ключової ролі кібербезпеки для операційних технологій, які стають основою для економіки 4.0 та розглядаються зараз як новий рубіж кібербезпеки. Показано потребу в створенні системи та схем сертифікації кібербезпеки ОТ на основі міжнародних та європейських принципів сертифікації. Розроблені Ієрархічна модель оціночних стандартів системи сертифікації кібербезпеки та Ієрархічна модель угод про взаємне визнання сертифікатів кібербезпеки, які дозволять системно підійти до створення системи та схем з сертифікації кібербезпеки ОТ. Завдяки цьому забезпечується можливість для розробників систем та схем сертифікації формувати системи сертифікації кібербезпеки ОТ на принципах широкого транскордонного визнання сертифікатів кібербезпеки в сфері ОТ.

Ключові слова: *система кібербезпеки, система оцінки відповідності, ієрархічна модель, схема сертифікації кібербезпеки.*

1. Вступ

Мережеві та інформаційні системи з відповідними послугами відіграють центральну роль у суспільстві. Для економічної та соціальної діяльності,

зокрема для функціонування внутрішнього ринку, важливо, щоб вони були надійними та безпечними. Масштаби, частота та наслідки інцидентів у галузі інформаційної безпеки зростають і становлять значну загрозу для безперебійної роботи мережевих та інформаційних систем. Такі випадки впливають на здійснення економічної діяльності, спричиняють значні фінансові втрати, підривають довіру користувачів та завдають великої шкоди економіці [1].

Одним з напрямків в забезпеченні кібербезпеки сучасної цифрової економіки має стати, поряд з кібербезпекою IT-технологій, кібербезпека операційних технологій (OT-технологій) – Operations Technology (OT) systems, таких як критично важлива інфраструктура та інтелектуальні системи, а також процеси, що забезпечують функціонування цих систем. Серед OT-технологій особливе місце посідає кібербезпека систем промислової автоматизації та управління (IACS), які є важливою частиною більшості критично важливих інфраструктур та критично важливих служб.

Процес трансформації суспільства до Індустрії 4.0 призведе до ще більшої залежності від таких систем. Досвід вже показав, що їх кібервразливість може бути використана та створити величезний вплив на критичну інфраструктуру та подальший вплив на економіку та життя людей. Практично, кібератаки на критичні інфраструктури насправді є кібератаками на їх IACS.

Таким чином, надзвичайно важливо застосовувати всі можливі заходи для підвищення рівня кібербезпеки IACS. Для побудови кібербезпеки IACS потрібно забезпечити та зібрати належним чином компоненти кібербезпеки IACS, будь то апаратне чи програмне забезпечення.

На даному етапі важливо зосередитись на сертифікації/оцінці відповідності окремих компонентів IACS, щоб забезпечити відповідність передбаченим вимогам щодо кібербезпеки кожним із цих компонентів, як елементів побудови всієї IACS. А наблизившись до сертифікації/оцінки відповідності на основі компонентів, можна визначити різні вимоги до безпеки та рівні забезпечення для різних елементів загальної системи IACS, залежно від конструкції системи, передбачуваного використання та робочого середовища, визначеної системи заходів безпеки. В ЄС починаючи з 2014 року працює Тематична група з сертифікації кібербезпеки компонентів – IACS TG, яка зосереджується на сертифікації кібербезпеки компонентів промислової автоматизації та систем управління. Група IACS TG вже напрацювала для ЄС загальні риси (Framework) сертифікації кібербезпеки компонентів IACS, які будуть відповідати законодавству ЄС з кібербезпеки [2, 3]. Підхід до сертифікації, що являє собою примірник методології оцінки безпеки на основі ризиків, представлених ETSI на основі ISO 31000 та стандарту в області тестування програмного забезпечення ISO 29119, розглянуто в [4]. Дослідження Директиви ЄС щодо кібербезпеки, необхідності в розробці схем сертифікації кібербезпеки, а також зобов'язань держав-членів щодо їх відповідних національних стратегій та співпраці в цих питаннях на рівні ЄС представлені в [5]. Система та схеми сертифікації взагалі можуть функціонувати на міжнародному, регіональному, національному, субнаціональному або галузевому рівні [6]. Ці обставини будуть вимагати від розробників систем та схем сертифікації кібербезпеки OT необхідності

застосування певної методологічної бази. Найбільш проблематично це для випадку міжнародного визнання сертифікатів кібербезпеки, які отримані від органів сертифікації національного рівня. На національному рівні кожна країна має для цього свої, унікальні умови. Разом з тим, національні схеми сертифікації кібербезпеки ОТ повинні забезпечити міжнародне визнання їх результатів.

В подальшому матеріал буде викладено на прикладі України, не обмежуючи можливість його застосування для будь якої іншої країни.

Тому актуальним є створення методологічного забезпечення для розробки національних систем і схем сертифікації кібербезпеки ОТ з транскордонним визнанням результатів сертифікації.

Таким чином, *об'єктом дослідження* є система та схеми оцінки відповідності (сертифікації) кібербезпеки ОТ, як набір правил та процедур, що описують об'єкти сертифікації, визначають зазначені вимоги та забезпечують методологію проведення сертифікації. А *мета роботи* полягає в розробці моделей оціночних стандартів системи сертифікації кібербезпеки та угод про взаємне визнання сертифікатів кібербезпеки, які дозволять системно підійти до створення процедур з оцінки відповідності кібербезпеки ОТ з транскордонним визнанням сертифікатів.

2. Методика проведення досліджень

Основна гіпотеза дослідження полягає в припущенні, що результативність управління кібербезпекою може бути досягнута шляхом конвергенції до загальної методології, яка спирається на узгоджені міжнародних стандартів і передової міжнародної практики з сертифікації. При цьому припускається, що такий підхід буде вимагати певного вдосконалення в нормативно-правовому забезпеченні кібербезпеки України.

Дослідження базуються на методах:

– діалектичному – при виявленні та дослідженні взаємозв'язків між учасниками процесів сертифікації кібербезпеки ОТ, визначенні факторів та умов на національному рівні, що впливатимуть на їх міжнародне визнання;

– емпіричному – при зборі інформації в процесі аналізу міжнародних стандартів, які можуть бути застосовані для сертифікації кібербезпеки ОТ, стану національного органу з акредитації України та міжнародних систем забезпечення взаємного визнання результатів сертифікації;

– системно-аналітичному – для формування організаційно-технічного механізму сертифікації кібербезпеки ОТ, розробці моделей оціночних стандартів сертифікації кібербезпеки ОТ та угод про взаємне визнання результатів сертифікації;

– узагальнюючому та порівняльному – для оцінки діючих механізмів міжнародних систем акредитації органів сертифікації та дослідженню можливостей застосуванню міжнародного досвіду для сертифікації кібербезпеки ОТ для національної системи кібербезпеки України.

3. Результати досліджень та обговорення

На сьогодні питання кібербезпеки в Україні регулюють низка нормативно-правових актів [7, 8]. Серед них найбільш актуальними є:

1. Указ Президента України від 15 березня 2016 року № 96/2016 про введення в дію «Стратегії кібербезпеки України».

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року.

В цих документах зазначається, що розвиток безпечного кіберпростору має полягати, насамперед, у гармонізації нормативних документів, у захисті інформації, інформаційної системи та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО.

В роботі перш за все проаналізовано та визначено міжнародні стандарти, які можуть бути використані для сертифікації кібербезпеки ОТ.

Серед інших, вимоги до компонентів, продуктів і устаткування, що використовуються в якості елементів ОТ-системи, можуть ґрунтуватися на міжнародних стандартах IEK та ISO, які відносяться до стандартів IACS, таких як:

1. IEK 62443-1-1 вид. 2: Термінологія, концепції та моделі.

2. IEK 62443-2-1 вид. 2: Складання програми забезпечення захищеності системи управління та промислової автоматики.

3. IEK 62443-2-3: Управління патчами в середовищі IACS.

4. IEK 62443-2-4: Вимоги до програми безпеки для постачальників послуг IACS.

5. IEK 62443-2-2: Рівні захисту IACS.

6. IEK 62443-3-2: Оцінка ризиків для безпеки та розробки системи.

7. IECEE OD-2061: Програма промислової кібербезпеки.

8. IEK 62443-4-1: Вимоги до безпеки життєвого циклу при розробці продукту.

9. IEK 62443-3-3-3: Вимоги до безпеки системи та рівні безпеки.

10. IEK 62443-4-2: Вимоги до технічної безпеки компонентів IACS.

Вимоги до особистісних компетенцій в сфері кібербезпеки можуть ґрунтуватися на наявних міжнародних стандартах ISO та IEC в цій області, таких як ISO/IEC 27021:2017: Інформаційні технології – Методи та засоби забезпечення безпеки – Вимоги до компетенції фахівців систем управління інформаційною безпекою (СУІБ).

Вимоги до процесів ОТ можуть ґрунтуватися на відповідних міжнародних стандартах IEC та ISO:

1. IEC 62443-4-1: Вимоги до безпеки життєвого циклу при розробці продукту.

2. IEC 62443-2-1: Складання програми безпеки IACS.

3. IEC 62443-2-2: Рівні захисту IACS.

4. IEC 62443-2-4: Вимоги до програми безпеки для постачальників послуг IACS.

5. IEC 62443-3-2: Оцінка ризиків для безпеки та розробки системи.

Зазначимо, що деякі з цих стандартів ще знаходяться в стадії розробки.

Разом з тим, наявність великої кількості стандартів з кібербезпеки не дає для національних регуляторів відповіді на питання вибору та порядку їх застосування в систематизованому нормативно-правовому забезпеченні кібербезпеки ОТ. Ситуація ще більше ускладняється з огляду на національний

статус цих стандартів, гарантій їх правильного впровадження на всіх етапах життєвого циклу ОТ, ризиків та довіри до ОТ, тощо.

В роботі досліджена методологія системного підходу до кібербезпеки ОТ в рамках загальної системи технічного регулювання. Вона відрізняється від інших методологій кіберзахисту тим, що на додаток до суто технічних питань кібербезпеки вона передбачає аналіз потреб в сфері оцінки відповідності (сертифікації) кібербезпеки. Потреби ж в сертифікації кібербезпеки, в свою чергу, потребують врахування стану розвитку національної системи технічного регулювання чи формулюють завдання для вдосконалення національної системи технічного регулювання з врахуванням потреб для кібербезпеки. Така конвергенція до загальної методології, яка спирається на узгоджені міжнародні стандарти та передову міжнародну практику оцінки відповідності, має низку переваг. Зокрема, в тих випадках, коли оцінка відповідності третьою стороною використовується для демонстрації відповідності компонентів і технологій, компетенцій та кваліфікації осіб, це полегшує визнання даної відповідності в міжнародній торгівлі та пересування кваліфікованих фахівців. Вона являє собою також універсальну методологію, застосовну до багатьох різних технічних систем в різних секторах економіки, які потребують регулювання. Особливо важливим є застосування цієї методології національними регуляторами, на яких покладаються питання забезпечення кібербезпеки [8].

Робота висвітлює основні елементи процесів державного регулювання, які можуть використовуватися владою та директивними органами, особливо в тих секторах, де в даний час не існує ніяких регламентів кібербезпеки. Розроблені ієрархічні моделі оціночних стандартів та міжнародних угод в сфері технічного регулювання можуть стати основою для розробки національних систем та схем сертифікації кібербезпеки. Також вони можуть стати основою для нормативних документів з кібербезпеки, маючи на увазі перш за все забезпечення транскордонності визнання результатів оцінки відповідності кібербезпеки ОТ-технологій.

3.1. Оцінка відповідності (сертифікація) кібербезпеки ОТ

Оцінка відповідності (сертифікація) – це демонстрація того, що зазначені вимоги виконуються (оцінка відповідності включає такі види діяльності, як випробування, інспектування, валідація, верифікація, сертифікація та акредитація). Зазначена вимога (specified requirement) – потреба або сподівання, яке зазначено (зазначені вимоги можуть бути викладені в нормативних документах, таких як регламенти, стандарти та технічні специфікації. Зазначені вимоги можуть бути детальними або загальними) [6].

3.2. Акредитації органів з оцінки відповідності

Як зазначено вище, конвергенція до загальної методології сертифікації кібербезпеки ОТ спирається на узгоджені міжнародні стандарти та передову міжнародну практику оцінки відповідності, яка дозволяє широко використовувати механізми взаємного визнання сертифікатів відповідності. Передова міжнародна практика оцінки відповідності перш за все спирається на

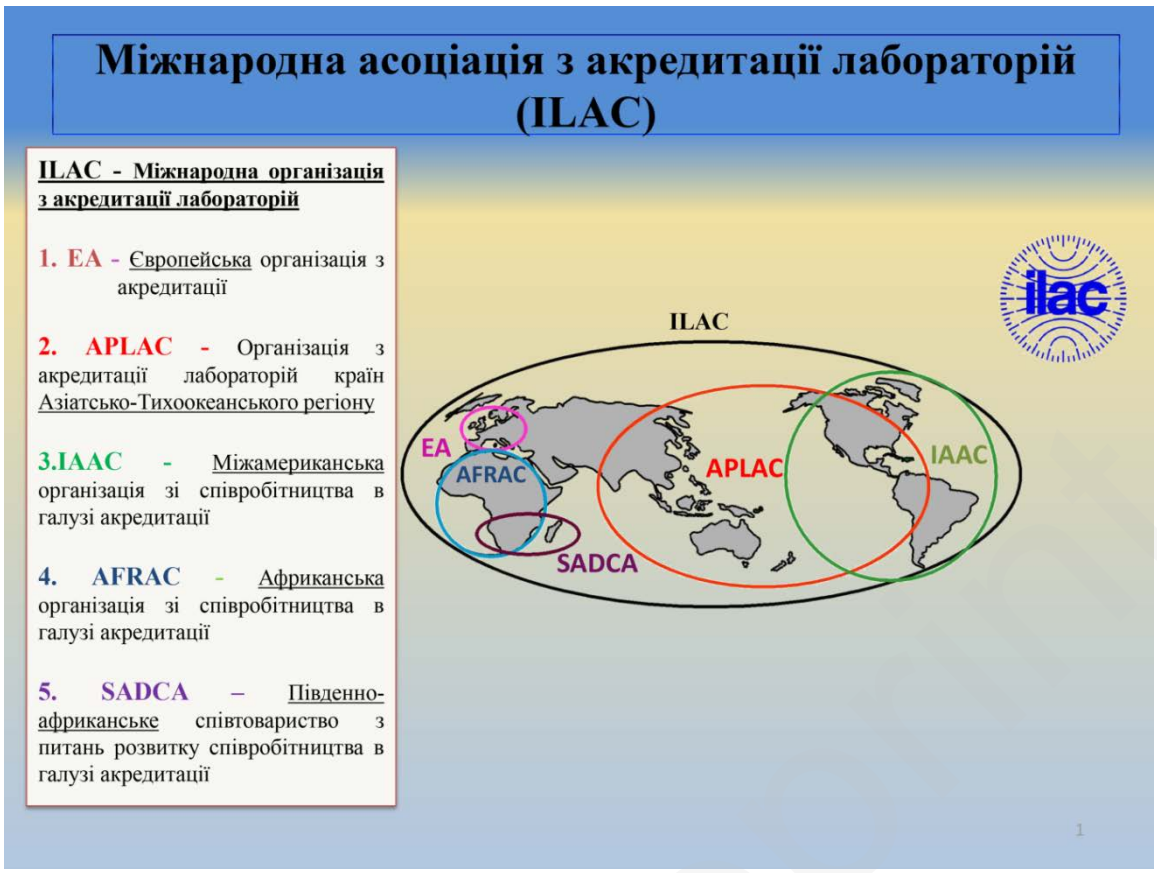
міжнародну систему акредитації органів з оцінки відповідності, що бажано застосувати і для кібербезпеки ОТ.

Акредитацією є процес, за допомогою якого авторитетний орган дає формальне визнання компетентності організації або приватної особи в виконанні конкретних завдань [9]. У структурі технічного регулювання, орган, відповідальний за акредитацію, оцінює компетенцію органів з сертифікації продукції, послуг та процесів, систем менеджменту, інспектування й персоналу, випробувальних й калібрувальних лабораторій. Офіційне визнання, іменоване «акредитацією», засвідчує клієнтам і користувачам послуг компетентність діяльності даних організацій. Акредитація часто входить в мандат державної акредитації, яка може забезпечити визнання своїх послуг з акредитації в рамках Міжнародного форуму з акредитації (IAF) та Міжнародного комітету з акредитації лабораторій (ILAC).

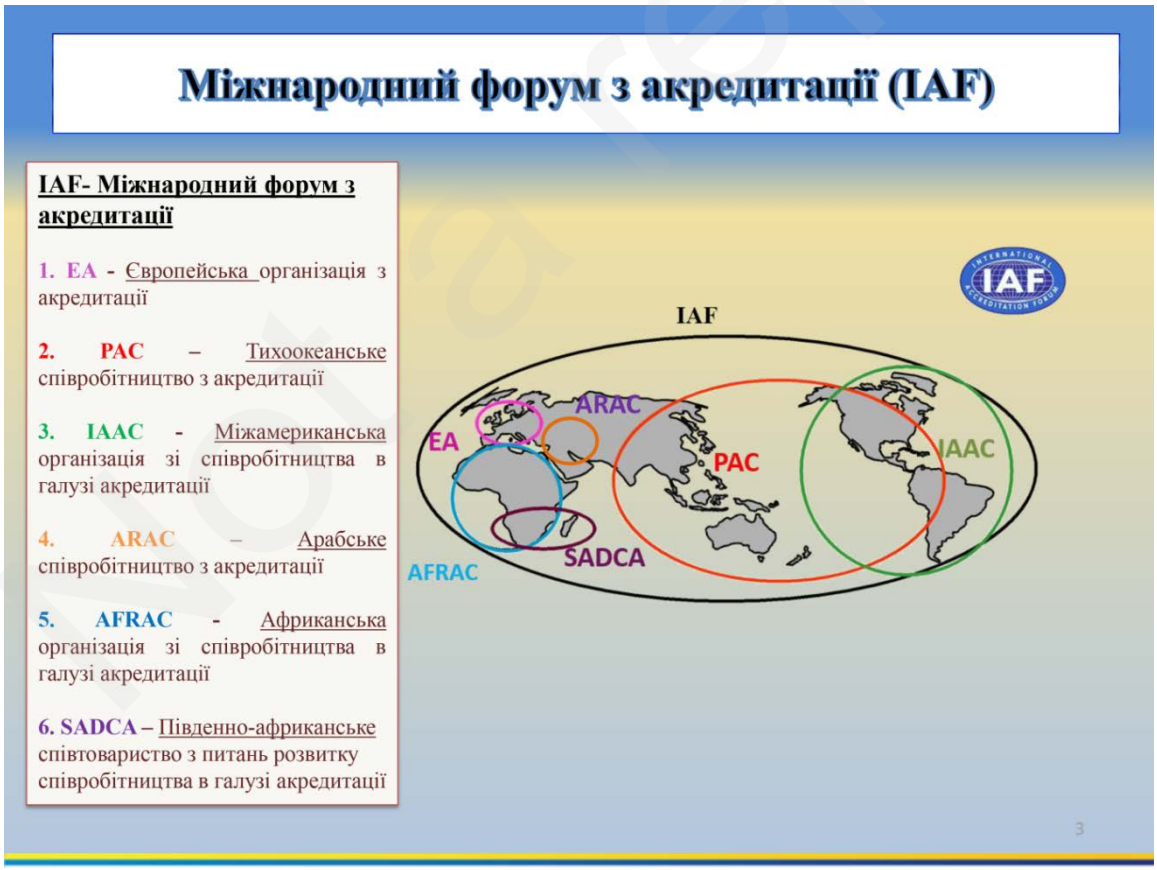
IAF та ILAC – це всесвітні організації по оцінці відповідності органів по акредитації та інших органів, зацікавлених в оцінці відповідності в області систем управління, продукції, послуг, персоналу, випробувальних лабораторій тощо. Їх основна функція – розробити єдині в усьому світі програми оцінки відповідності [10, 11].

IAF і ILAC сприяють і управляють визнанням «Двосторонніх» або «Багатосторонніх» «Угод» або «Домовленостей» (MRA/MLA), згідно з якими сторони, які беруть участь в них, погоджуються обопільно визнавати результати тестування, інспекцій, сертифікації або акредитації. Угоди MRA/MLA сьогодні стали важливим кроком на шляху оптимізації чи зменшення числа сертифікацій продуктів, послуг, систем, процесів і матеріалів, необхідних особливо в міжнародній діяльності.

Слід також зазначити, що глобальна система IAF/ILAC діє через регіональні організації з акредитації. Їх географічне розташування зображене на рис. 1.



а



б

Рис. 1. Міжнародні організації: *а* – ILAC; *б* – IAF

Для України регіональною організацією з акредитації є Європейська

організація з акредитації (ЕА). Саме ЕА в системі IAF/ILAC є первинним бар'єром, який необхідно подолати для підписання Угод MRA/MLA з метою транскордонного визнання сертифікатів кібербезпеки.

3.3. Система сертифікації кібербезпеки ОТ-технологій для України

Сертифікація кібербезпеки ОТ в національній системі кібербезпеки України перш за все потребує створення системи оцінки відповідності кібербезпеки ІКТ (далі – Система сертифікації).

Система оцінки відповідності (conformity assessment system) – набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності. Система оцінки відповідності може функціонувати на міжнародному, регіональному, національному, субнаціональному або галузевому рівні. Оцінка (підтвердження) відповідності встановленим вимогам неупередженої третьою стороною називається сертифікацією [6]. В подальшому замість узагальненого поняття «оцінка відповідності» будемо вживати термін «сертифікація». Змістом системи сертифікації є організація та управління спорідненими схемами сертифікації, загальні методи оцінювання, що лежать в основі сертифікації [6].

Спорідненими схемами оцінки відповідності для сертифікації кібербезпеки (далі – Схема сертифікації) можуть бути різноманітні застосування процедур оцінки відповідності, залежно від відношення до певних ОТ технологій (наприклад, IACS, IoT, хмарні сервіси тощо). У Схемі сертифікації слід використовувати певні правила, процедури та менеджмент, які можуть бути притаманні лише даній схемі або які можуть бути визначені в системі сертифікації продукції, яка застосовується до ряду схем. Система сертифікації повинна створюватись з врахуванням всіх важливих факторів та умов. Що стосується сертифікації кібербезпеки ОТ для України, серед них необхідно виділити три системоутворюючих фактори:

1. Необхідність дотримання вимог Угоди Україна – ЄС та статті 56 цієї Угоди.
2. Підписані Угоди про визнання в сфері акредитації органів з сертифікації.
3. Наявність в ЄС Регламенту 2019/881 щодо сертифікації кібербезпеки, основні засади якого з часом повинні будуть імплементовані в національну систему кібербезпеки України.

Врахування різнорідних суттєвих та швидкоплинних факторів для створення системи сертифікації кібербезпеки ОТ можливо шляхом введення уніфікованих моделей, які базуються на глобальних механізмах усунення технічних бар'єрів у торгівлі та сучасному стані системи технічного регулювання України:

– Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки;

– Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки.

Загальна Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки (далі – Модель Стандартів) представлена на рис. 2. Модель дозволяє упорядити визначення та застосування стандартів чи інших нормативних документів, стандартів та схем з можливими комбінаціями для розробки схем сертифікації.

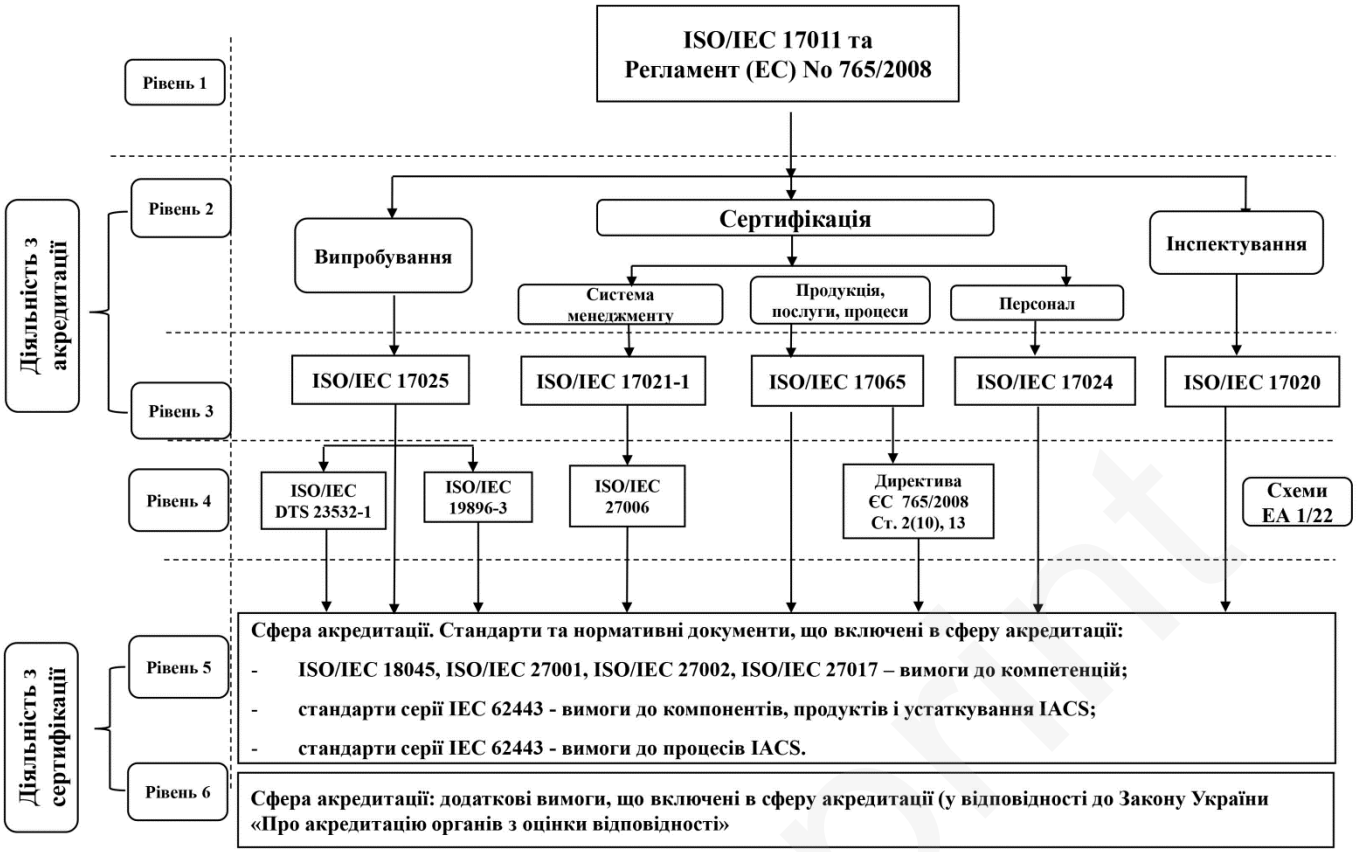


Рис. 2. Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки операційних технологій

Модель складається з 6 рівнів, системне розподілення оціночних стандартів по яким створює гнучкість для розробників схем сертифікації кібербезпеки.

1 рівень – вимоги до органів з акредитації, які акредитують органи, задіяні в сертифікації кібербезпеки. Визначені в стандарті ISO/IEC 17011, в Регламенті (ЄС) 765/2008 та, якщо необхідно, додаткові вимоги, визначені в обов'язкових документах ЕА та в документах IAF та/або ILAC (затверджених ЕА як обов'язкові для ЄС) [10, 11].

2 рівень – діяльність з оцінки відповідності ООВ (органу з оцінки відповідності), яким органи акредитації надають акредитацію відповідно до стандартів, включених до рівня 3 (далі – діяльність з оцінки відповідності). Це, як правило, визначається в схемі сертифікації. Для сертифікації кібербезпеки ОТ, залежно від схеми сертифікації, можуть бути задіяні:

– органи сертифікації продукції, послуг та процесів;

– органи з сертифікації систем менеджменту;

– органи з сертифікації персоналу;

– випробувальні лабораторії;

– органи з інспектування.

3 рівень – гармонізовані стандарти (або інші нормативні документи), що містять загальні вимоги до ООВ, що виконують діяльність з оцінки відповідності кібербезпеки, включених до рівня 2 (далі стандарти оцінки відповідності). Це наступні оціночні стандарти: ISO/IEC 17025; ISO/IEC 17020; ISO/IEC 17065; ISO/IEC 17021-1; ISO/IEC 17024.

4 рівень – документи, що містять додаткові критерії до стандартів 3 рівня. Рівень 4 застосовується лише там, де існують документи, що доповнюють стандарти 3 рівня (це означає, що рівень 5 часто безпосередньо пов'язаний зі стандартом рівня 3).

Такими документами для ЄС є: галузеві стандарти або інші нормативні документи (надалі галузеві стандарти); галузеві схеми, як зазначено у Регламенті (ЄС) 765/2008 Статті 2 (10) та 13; Схеми оцінки відповідності згідно з EA-1/22 (далі схеми).

Так, галузевим стандартом, який без сумнівів буде в Системі, є ISO/IEC 27006:2015. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

Також високоймовірним є присутність в Системі сертифікації кібербезпеки Додаткових критеріїв з Регламенту ЄС 2019/881.

5 рівень – сфера акредитації органу з сертифікації: стандарти або інші нормативні документи, що використовуються акредитованим ООВ відповідності для визначеної акредитованої сфери оцінки відповідності. Основу складають стандарти, розглянуті в пункті F. Може включати, наприклад, конкретні методи випробувань та конкретні вимоги до системи управління (наприклад: ISO/IEC 27001), ISO/IEC 27021:2017 – Вимоги до компетенції фахівців систем управління інформаційною безпекою (СУІБ).

6 рівень – сфера акредитації органу з сертифікації: додаткові вимоги до сфери акредитації, які можуть бути встановлені в державі. Визначені в законі України «Про акредитацію органів з оцінки відповідності», стаття 1 [12].

Запропонована 6-рівнева Ієрархічна Модель оціночних стандартів Системи Сертифікації кібербезпеки ОТ є інструментарієм, який надає можливість створення гнучких схем сертифікації кібербезпеки з забезпеченням транскордонного визнання результатів оцінки відповідності в сфері кібербезпеки (випробування та сертифікації).

Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки повинна відображати рівні та відповідний обсяг (сферу - scope) визнання результатів діяльності з боку міжнародних організацій з акредитації для національного органу з акредитації. Досяжність рівнів (по факту) та сфера для національного органу з акредитації визначає і обсяг визнання результатів сертифікації кібербезпеки, формуючи механізми взаємного визнання сертифікатів для системи сертифікації кібербезпеки.

На рис. 3 зображена розроблена чотирьохрівнева Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки (MRA для IAF та ILAC), де на національному рівні представлений Національний орган України з акредитації – Національне агентство з акредитації України (далі – НААУ).

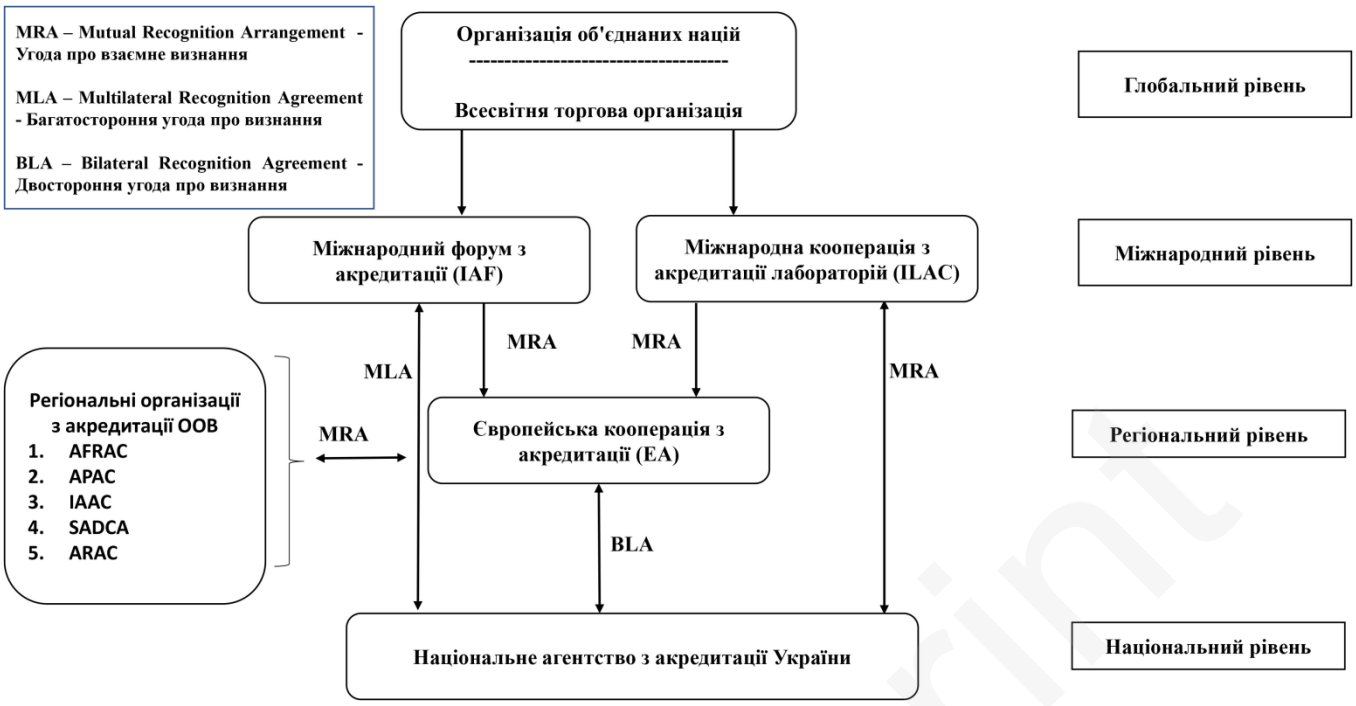


Рис. 3. Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки операційних технологій

В моделі присутні національний, регіональний, міжнародний та глобальний рівні, представлені відповідними організаціями з акредитації та типами Угод про визнання.

Для оперування моделлю при розробці системи сертифікації ОТ необхідним додатком є самі Угоди та визначені в них сфери визнання діяльності з акредитації.

Модель має методологічне значення та дозволяє при розробці системи та схем сертифікації кібербезпеки визначатись зі змістом відповідних розділів щодо оціночних стандартів, рівнів гарантій сертифікатів кібербезпеки, акредитації ООВ, взаємного визнання сертифікатів тощо [13].

Для створення ефективної Системи Оцінки Відповідності Кібербезпеки ІКТ України доцільним є аналіз угод, які є чинними для НААУ в системах ЕА та IAF/ILAC. Слід зазначити, що такий аналіз може дати наступні сценарії для створення системи сертифікації кібербезпеки ОТ в Національній системі кібербезпеки України:

– наявність Угод достатня для створення системи та схем сертифікації відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

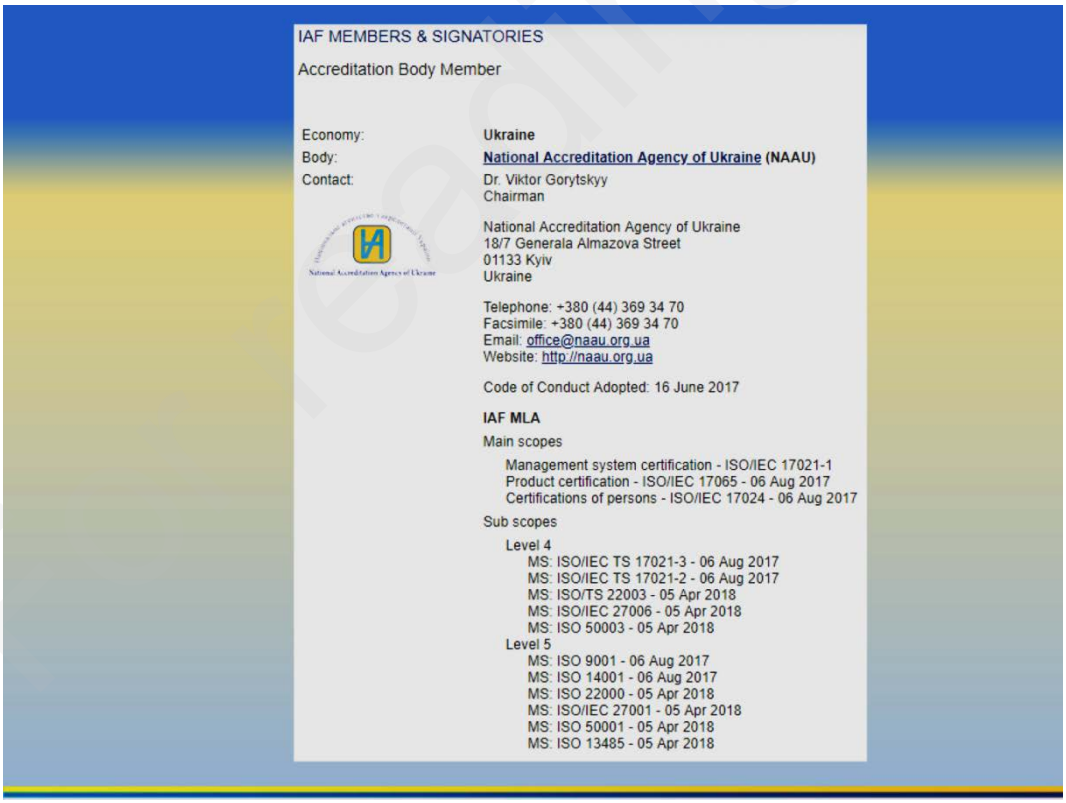
– наявність Угод недостатня та потребує додаткових зусиль з боку України та НААУ в напрямку розширення сфер визнання в системі ЕА та IAF/ILAC;

– наявність Угод недостатня та потребує створення системи на національному чи галузевому рівні без намірів на транскордонне визнання результатів сертифікації, але відповідно до міжнародних стандартів і стандартів ЄС та НАТО.

Угоди, які визначають статус Національного органу України з акредитації ООВ щодо транскордонного визнання діяльності, представлені на рис. 4. Там же представлені витяги з сайтів IAF та ILAC з зазначенням сфер акредитації,

які охоплені відповідними Угодами.

а



б

Рис. 4. Угоди та сфери визнання: *а* – MRA ILAC; *б* – MLA IAF

Аналіз діючого статусу Угод НААУ та сфер акредитації, в яких ці Угоди діють, надає можливість виділити можливі оціночні стандарти та інші

стандарти для наповнення Ієрархічної моделі стандартів та формування системи сертифікації кібербезпеки ОТ.

4. Висновки

В ході дослідження на основі стандартів та систем, які застосовуються для сертифікації продукції в системі ILAC/IAF, розроблено Ієрархічну модель оціночних стандартів Системи сертифікації кібербезпеки ОТ та Ієрархічну модель Угод в міжнародній системі ILAC/IAF/EA про взаємне визнання сертифікатів кібербезпеки.

Результати дослідження стануть у нагоді розробникам і власникам систем та схем сертифікації кібербезпеки ОТ як елементи загальної методології, яка спирається на узгоджені міжнародні стандарти та передову міжнародну практику оцінки відповідності в системі ILAC/IAF.

Також результати дослідження стануть цікаві національним регуляторним органам в сферах кібербезпеки та технічного регулювання для визначення національних потреб в оціночних стандартах, схемах сертифікації, сфери міжнародного визнання національного органу акредитації.

Література

1. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6.07.2016 concerning measures for a high common level of security of network and information systems across the Union* (2016). Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj
2. *The IACS Cybersecurity Certification Framework (ICCF)* (2018). Available at: https://erncip-project.jrc.ec.europa.eu/documents/iacs-cybersecurity-certification-framework-iccf
3. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17.04.2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* (2019). Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj
4. Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces, 62*, 64–83. doi: http://doi.org/10.1016/j.csi.2018.08.003
5. Markopoulou, D., Papakonstantinou, V., de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review, 35 (6)*, 105336. doi: http://doi.org/10.1016/j.clsr.2019.06.007
6. *Про основні засади забезпечення кібербезпеки України* (2017). Закон України № 2163-VIII. 05.10.2017. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. *Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»* (2016). Указ Президента

України; Стратегія № 96/2016. 15.03.2016. Available at: https://www.president.gov.ua/documents/2422016-20141

8. *ISO/IEC 17000:2020 Conformity assessment – Vocabulary and general principles* (2020). Committee on conformity assessment, 23. Available at: https://www.iso.org/standard/73029.html

9. *Про технічні регламенти та оцінку відповідності* (2015). Закон України № 124-VIII. 15.01.2015. Available at: https://zakon.rada.gov.ua/laws/show/3164-15#Text

10. *International Accreditation Forum.* Available at: https://www.iaf.nu/

11. *International Laboratory Accreditation Cooperation.* Available at: https://ilac.org/

12. *Про акредитацію органів з оцінки відповідності* (2001). Закон України № 2407-III. 17.05.2001. Available at: https://zakon.rada.gov.ua/laws/show/2407-14#Text

13. *ISO/IEC 17067:2013 Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes* (2013). Committee on conformity assessment, 13. Available at: https://www.iso.org/standard/55087.html