УДК 004.056

СИСТЕМА СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Цвілій О.О.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
o.tsviliy@ukr.net

СИСТЕМА СЕРТИФИКАЦИИ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Цвилий Е.А.

Одесская национальна академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
o.tsviliy@ukr.net

SYSTEM OF CERTIFICATION OF CYBERSECURITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES

Olena Tsvilii

O.S. Popov Odessa National Academy of Telecommunications,
1 Kuznechna St., Odessa, 65029, Ukraine.
o.tsviliy@ukr.net

Анотація. Кібербезпека інформаційних та комунікаційних технологій (далі – ІКТ) є ключовою проблемою для збереження функціонування та безпеки цифрової економіки і державного управління в найближчому майбутньому. Важливу роль у сфері кібербезпеки відіграє оцінка відповідності (сертифікація) кібербезпеки. Це може відноситись до кібербезпеки компонентів, продуктів, обладнання, послуг та процесів ІКТ, до кібербезпеки хмарних сервісів, до кібербезпеки технологічних процесів, до особистої компетентності у сфері кібербезпеки тощо. Правила, процедури та менеджмент проведення сертифікації кібербезпеки встановлюють схему сертифікації, а набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності утворюють систему сертифікації. Створення схем сертифікації кібербезпеки на сьогодні є пріоритетним та актуальним. Зараз існує низка систем та оціночних стандартів, які можуть бути застосовані для сертифікації кібербезпеки, але вони не забезпечують взаємного визнання процедур і результатів випробувань та оцінок випробувальними лабораторіями, а також прагнення до узгоджених і порівнянних процедур оцінки та здійснення заходів щодо забезпечення кібербезпеки. Такий стан є глобальною проблемою. Відповідно, діюче законодавство України у сфері кібербезпеки встановлює завдання на застосування кращих міжнародних та європейських принципів оцінки відповідності інформаційної та кібербезпеки. Створення системи та схем сертифікації кібербезпеки на основі міжнародних та європейських принципів оцінки відповідності потребує відповідного наукового та методологічного забезпечення. У статті запропоновані Ієрархічна модель оціночних стандартів системи сертифікації кібербезпеки та Ієрархічна модель угод про взаємне визнання сертифікатів кібербезпеки. Також, в статті, на основі цих моделей, запропоновані основи Системи сертифікації кібербезпеки та Схеми сертифікації кібербезпеки продукції ІКТ і хмарних сервісів з акцентуванням на таких елементах, як: оціночні стандарти; акредитація органів з сертифікації; взаємне визнання результатів сертифікації.

Ключові слова: кібербезпека, сертифікація кібербезпеки, акредитація органів з сертифікації кібербезпеки, система сертифікації кібербезпеки, схема сертифікації кібербезпеки.

Аннотация. Кибербезопасность информационных и коммуникационных технологий (далее - ИКТ) является ключевой проблемой для сохранения функционирования и безопасности цифровой экономики и государственного управления в ближайшем будущем. Важную роль в сфере

кибербезопасности играет оценка соответствия (сертификация) кибербезопасности. Это может относиться к кибербезопасности компонентов, продуктов, оборудования, услуг и процессов ИКТ, к кибербезопасности облачных сервисов, к кибербезопасности технологических процессов, к личной компетенции в сфере кибербезопасности и тому подобное. Правила, процедуры и менеджмент проведения сертификации кибербезопасности устанавливают схему сертификации, а набор правил и процедур для управления подобными или родственными схемами оценки соответствия образуют систему сертификации. Создание схем сертификации кибербезопасности сегодня является приоритетным и актуальным. Сейчас существует ряд систем и оценочных стандартов, которые могут быть применены для сертификации кибербезопасности, но они не обеспечивают взаимного признания процедур, результатов испытаний и оценок испытательными лабораториями, а также стремление к согласованным и сопоставимым процедурам оценки и осуществления мероприятий по обеспечению кибербезопасности. Такое положение является глобальной проблемой. Соответственно, действующее законодательство Украины в сфере кибербезопасности устанавливает задачи на применение лучших международных и европейских принципов оценки соответствия информационной и кибербезопасности. Создание системы и схем сертификации кибербезопасности на основе международных и европейских принципов оценки соответствия требует соответствующего научного и методологического обеспечения. В статье предложены Иерархическая модель оценочных стандартов системы сертификации кибербезопасности и Иерархическая модель соглашений о взаимном признании сертификатов кибербезопасности. Также, в статье, на основе этих моделей, предложенные основы Системы сертификации кибербезопасности и Схемы сертификации кибербезопасности продукции ИКТ и облачных сервисов с акцентом на таких элементах, как: оценочные стандарты; аккредитация органов по сертификации; взаимное признание результатов сертификации.

Ключевые слова: кибербезопасность, сертификация кибербезопасности, аккредитация органов по сертификации кибербезопасности, система сертификации кибербезопасности, схема сертификации кибербезопасности.

Abstract. Cybersecurity of information and communication technologies (hereinafter - ICT) is a key issue for maintaining the functioning and security of the digital economy and public administration in the soon. An important role in the field of cybersecurity is played by the conformity assessment (certification) of cybersecurity. This may apply to the cybersecurity of ICT components, products, equipment, services and processes, to the cybersecurity of cloud services, to the cybersecurity of technological processes, to personal competence in the field of cybersecurity, and so on. Cybersecurity certification rules, procedures, and management establish a certification scheme, and a set of rules and procedures for managing similar or related conformity assessment schemes form a certification system. Creating cybersecurity certification schemes is a priority and relevant today. There are now a number of systems and assessment standards that can be applied to cybersecurity certification, but they do not ensure mutual recognition of test laboratory test and evaluation procedures and results, and the pursuit of harmonized and comparable cybersecurity assessment and implementation procedures. This situation is a global problem. Accordingly, the current legislation of Ukraine in the field of cybersecurity sets tasks for the application of the best international and European principles of conformity assessment of information and cybersecurity. The creation of cybersecurity certification systems and schemes based on international and European principles of conformity assessment requires appropriate scientific and methodological support. The article proposes a hierarchical model of assessment standards for the cybersecurity certification system and a hierarchical model of agreements on mutual recognition of cybersecurity certificates. Also, in the article, based on these models, the basics of the Cyber Security Certification System and Cyber Security Certification Schemes for ICT products and cloud services are proposed, with an emphasis on such elements as: assessment standards; accreditation of certification bodies; mutual recognition of certification results.

Key words: cybersecurity, cybersecurity certification, accreditation of cybersecurity certification bodies, cybersecurity certification system, cybersecurity certification scheme.

Сертифікація кібербезпеки. Цифровізація повинна супроводжуватися підвищенням рівня довіри і безпеки. Інформаційна безпека, кібербезпека, захист персональних даних, недоторканість особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками [1].

Важливу роль у підвищенні довіри та безпеки ІКТ відіграє оцінка відповідності (сертифікація) кібербезпеки ІКТ.

Оцінка відповідності – це демонстрація того, що зазначені вимоги виконуються (оцінка відповідності включає такі види діяльності, як випробування, інспектування, валідація, верифікація, сертифікація та акредитація) [2]. Дана вимога (specified requirement) – потреба або сподівання, яке зазначено (ці вимоги можуть бути викладені в нормативних документах, таких як регламенти, стандарти та технічні специфікації) [2]. Об'єкт, до якого застосовуються ці вимоги є об'єктом оцінки відповідності (наприклад продукт, процес, послуга, система, установка, проект, дані, дизайн, матеріал, особа, орган чи організація або будь-яка їх комбінація) [2]. Схема оцінки відповідності (програма оцінки відповідності) – це набір правил та процедур, що описує об’єкти оцінки відповідності, визначає ці вимоги та забезпечує методологію проведення оцінки відповідності [2]. Схемою з оцінки відповідності можна керувати в рамках системи оцінки відповідності. Система оцінки відповідності (conformity assessment system) – набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності [2]. Система оцінки відповідності може функціонувати на міжнародному, регіональному, національному, субнаціональному або галузевому рівні. Оцінка відповідності встановленим вимогам неупередженої третьою стороною називається сертифікацією [2]. В подальшому у статті замість узагальненого поняття «оцінка відповідності» для сфери кібербезпеки ІКТ будемо вживати термін «сертифікація», маючи на увазі оцінку відповідності кібербезпеки ІКТ третьою стороною, яка має назву «орган з оцінки відповідності» [2].

Питання кібербезпеки в Україні регулює низка правових актів [3-5]. В них ставиться завдання на створення Національної системи кібербезпеки України та застосування в ній міжнародних та європейських принципів оцінки відповідності інформаційної та кібербезпеки, гармонізації нормативних документів у сфері кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС і НАТО та запровадженні кращих світових практик і міжнародних стандартів. Повною мірою це стосується і сертифікації кібербезпеки ІКТ. Слід зазначити, що зараз це питання повною мірою не вирішено не тільки в Україні, а й на глобальному рівні, про що йдеться в доповіді ООН [6].

Таким чином, сертифікація у сфері кібербезпеки ІКТ повинна опиратись на Систему зі схем сертифікації кібербезпеки, кожна з яких: містить у собі набір правил та процедур, що описують об’єкти сертифікації кібербезпеки; визначає ці вимоги; забезпечує методологію проведення сертифікації. На сьогодні такої Системи сертифікації кібербезпеки в Національній системі кібербезпеки України не створено, що потребує відповідних досліджень.

У статті описується методологія системного підходу до кібербезпеки в рамках загальної системи технічного регулювання, в тому числі системи технічного регулювання України [7]. Вона відрізняється від інших методологій кіберзахисту тим, що на додаток до суто технічних питань вона передбачає аналіз потреб в області оцінки відповідності (та сертифікації) кібербезпеки. Вона являє собою універсальну методологію, застосовну до багатьох різних технічних систем в різних секторах економіки, які потребують технічного регулювання.

Викладаються основні елементи процесів регулювання, які можуть використовуватися владою і директивними органами (наприклад, Держспецзв’язку), особливо в тих секторах, на сьогодні не існує ніяких регламентів кібербезпеки. У статті визначені ієрархічні моделі та стандарти, які можуть бути корисні для використання як посилання в нормативних документах, маючи на увазі, перш за все, транскордонність визнання результатів оцінки відповідності (сертифікації) кібербезпеки.

Ця методологія буде властива для всієї Національної системи кібербезпеки України, як це визначено в Законі України «Про основні засади забезпечення кібербезпеки України» [3], де в статті 8 зазначено, що «Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення й оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури».

Метою статті э актуальна наукова задача – вдосконалення Національної системи кібербезпеки України шляхом дослідження й вирішення проблем сертифікації кібербезпеки ІКТ у цій системі.

Система сертифікації кібербезпеки ІКТ. Система сертифікації кібербезпеки ІКТ передбачає:

1. Міжнародні стандарти та системи, які застосовуються для сертифікації інформаційної та кібербезпеки. За останні десятиліття у світі була створена безліч систем та оціночних стандартів, які застосовуються для сертифікації інформаційної та кібербезпеки. Найбільш відомими серед них є: стандарти серії ISO/IEC 27000; стандарти серії IEC 62443; Framework v1.1 Національного інституту стандартів і технологій (NIST) США; стандарт COBIT-5; OWASP-Top10 – відкритий проект з безпеки веб-додатків; ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security; ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for it security evaluation; система SOG-IS (Senior Officials Group Information Systems Security); Федеральні стандарти обробки інформації (FIPS) серії 140 – США; Сертифікація IT-продукції DoD IPv6 – США; Сертифікація IT-продукції DODIN APL – США; Сертифікація Army I3MP RPL – США.

Практичне застосування – названі системи та стандарти сертифікації знаходять здебільшого в галузевих схемах сертифікації, рідше в національних схемах і деякі з них, наприклад SOG-IS, групами країн. Таке різноманіття створює потужні технічні бар'єри у визнанні відповідних оцінок (сертифікатів). Крім того, у більшості випадків існування або використання різних вимог і процедур у тих секторах, які функціонують як глобальні і комплексні сфери, може являти собою підвищений ризик.

У світі останні 20 – 25 років з метою усунення технічних бар'єрів для визнання оцінок відповідності та сертифікатів створена глобальна система, яка створює умови для взаємного визнання сертифікатів. Ця система – акредитація органів з оцінки відповідності (далі – ООВ), до яких відносяться й органи з сертифікації. Акредитація ООВ сьогодні є невід'ємною частиною процесів надання довіри до результатів сертифікації в будь-якій сфері. У сучасному технічному регулюванні акредитація є одним з основних інститутів інфраструктури, поряд зі стандартизацією та метрологією [7].

2. Акредитація органів з оцінки відповідності. Акредитацією є процес, за допомогою якого авторитетний орган дає формальне визнання компетентності організації або приватної особи у виконанні конкретних завдань [2]. 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 у мандат державної акредитації, яка може забезпечити визнання своїх послуг з акредитації в рамках Міжнародного форуму з акредитації (IAF) і Міжнародного комітету з акредитації лабораторій (ILAC).

IAF і ILAC сприяють й 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.

IAF – це Всесвітня асоціація з оцінки відповідності органів з акредитації та інших органів, зацікавлених в оцінці відповідності в області систем управління, продукції, послуг, персоналу та інших подібних програм оцінки відповідності. Основна функція IAF – розробити єдину в усьому світі програму оцінки відповідності [8].

ILAC – це міжнародна організація з питань акредитації, яка діє відповідно до стандарту ISO/IEC 17011 та бере участь в акредитації ООВ, включаючи калібрувальні лабораторії (з використанням ISO/IEC 17025), випробувальні лабораторії (з використанням ISO/IEC 17025), медичні випробувальні лабораторії (з використанням ISO 15189), контролюючих органів (з використанням ISO/IEC 17020), постачальників перевірок кваліфікації (з використанням ISO/IEC 17043) та виробників референсних матеріалів (з використанням ISO 17034) [9].

Слід також додати, що глобальна система IAF/ILAC діє через регіональні організації з акредитації. Їх географічне розташування зображене на рис. 1 та 2.

Для України регіональною організацією з акредитації є Європейська організація з акредитації (EA). Саме EA у системі IAF/ILAC є первинним технічним бар'єром, який необхідно подолати для підписання Угод MRA/MLA з метою транскордонного визнання сертифікатів кібербезпеки.

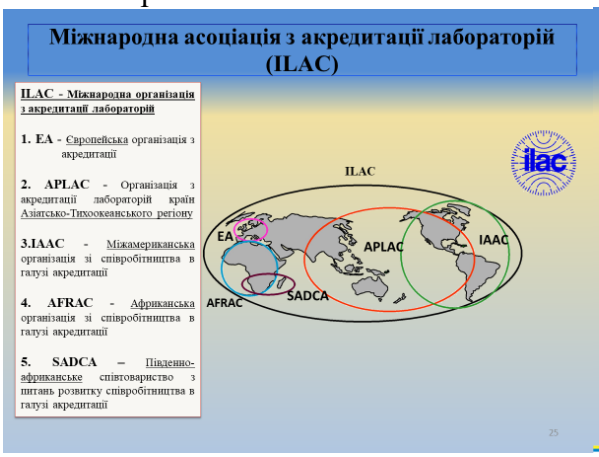

Рисунок 1 – Регіональні організації ILAC

Рисунок 2 – Регіональні організації IAF

3. Система сертифікації кібербезпеки інформаційних та комунікаційних технологій для України. Сертифікація кібербезпеки ІКТ 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 рівнях. Оцінка (підтвердження) відповідності встановленим вимогам неупередженої третьою стороною називається сертифікацією [2]. В подальшому замість узагальненого поняття «оцінка відповідності» будемо вживати термін «сертифікація». Змістом системи сертифікації є організація й

управління спорідненими схемами сертифікації, загальні методи оцінювання, що лежать в основі сертифікації [10,11].

Спорідненими схемами оцінки відповідності для сертифікації кібербезпеки ІКТ для України (далі – схеми сертифікації) можуть бути різноманітні застосування процедур оцінки відповідності, залежно від умов сертифікації в кіберпросторі, ризиків для суспільства і громадян, відношення до певних ІКТ технологій (наприклад, хмарні сервіси) тощо.

У схемах сертифікації слід використовувати певні правила, процедури та менеджмент, які можуть бути притаманні лише даній схемі або які можуть бути визначені у системі сертифікації продукції, яка застосовується до низки схем.

Система сертифікації повинна створюватись з врахуванням всіх важливих факторів та умов. Що стосується сертифікації кібербезпеки для України, серед них необхідно виділити три системоутворюючих фактори:

- необхідність дотримання вимог Угоди Україна – ЄС та статті 56 цієї Угоди;
- підписанні Угоди про визнання у сфері акредитації органів з сертифікації;
- наявність в ЄС Регламенту 2019/881 щодо сертифікації кібербезпеки, основні засади якого з часом повинні будуть імплементовані в Національну систему кібербезпеки України.

Система сертифікації кібербезпеки повинна охопити наступні елементи, які, утворюючи одне ціле, знаходяться у відносинах і зв'язках один з одним:

- вимоги для оцінювання (стандарти чи інші нормативні документи);
- акредитація ООВ;
- механізми взаємного визнання сертифікатів (Угоди про визнання);
- управління системою сертифікації кібербезпеки;
- рівні гарантій сертифікатів кібербезпеки;
- наявність регулятора (Національного органу з сертифікації кібербезпеки).
- призначення органів з сертифікації кібербезпеки.

Для створення дієвої та гнучкої Системи сертифікації кібербезпеки України, яка в майбутньому буде складатись з низки схем сертифікації кібербезпеки для ефективного реагування викликам з кібербезпеки, потрібно перш за все систематизувати два основних елементи Системи:

- вимоги для оцінювання (принципи посилань на стандарти чи інші нормативні документи);
- механізми взаємного визнання сертифікатів (Угоди про визнання).

Це 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.

Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки (далі – Модель Стандартів) показана на рис. 3. Модель дозволяє упорядити визначення та застосування стандартів чи інших нормативних документів, стандартів та схем з можливими комбінаціями для розробки схем сертифікації.

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

1 рівень – вимоги до органів з акредитації, які акредитують органи, задіяні в сертифікації кібербезпеки. Визначені у 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) [12].

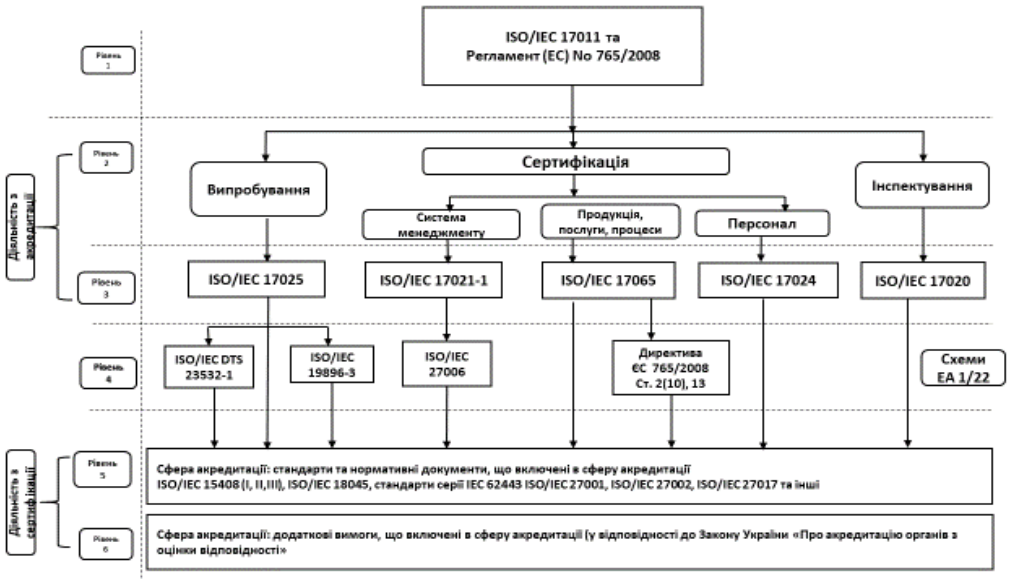

Рисунок 3 – Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки

2 рівень – діяльність з оцінки відповідності ООВ, яким органи акредитації надають акредитацію відповідно до стандартів, включених до рівня 3 (далі – діяльність з оцінки відповідності). Це, як правило, визначається у схемі сертифікації. Для сертифікації кібербезпеки в цій Системі, 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-го рівня. Рівень 4 застосовується лише там, де існують документи, що доповнюють стандарти 3-го 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 (далі – галузеві стандарти); галузеві схеми, як зазначено у Регламенті (ЄС) 765/2008 Статті 2 (10) та 13; схеми оцінки відповідності згідно з ЕА-1/22 (далі – схеми).

Так, галузевим стандартом, який без сумнівів буде у 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 у 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. Може включати, наприклад, конкретні методи випробувань та конкретні вимоги до системи управління (наприклад: ISO/IEC 27001), критерії кібербезпеки (ISO/IEC 15408), методику оцінки кібербезпеки (ISO/IEC 18045) тощо.

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 [13].

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

Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки повинна відображати рівні й обсяг визнання з боку міжнародних організацій з акредитації, досяжність яких Національним органом України з акредитації ООВ визначає й обсяг визнання результатів сертифікації кібербезпеки, формуючи механізми взаємного визнання сертифікатів для Системи сертифікації кібербезпеки.

На рис 4. зображена чотирирівнева Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки (MLA для IAF і MRA ILAC), де на національному рівні представлений Національний орган України з акредитації – Національне агентство з акредитації України (далі – НААУ).

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

Для оперування моделлю при розробці Системи 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.

Рисунок 4 – Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки

Для створення ефективної Системи Оцінки Відповідності Кібербезпеки ІКТ України доцільним є аналіз Угод, які є чинними для НААУ у системі ЕА та IAF/ILAC. Слід зазначити, що такий аналіз може дати наступні важливі сценарії для імплементації Системи сертифікації в Національну систему кібербезпеки України:

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

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

– наявність Угод недостатня і потребує створення Системи на національному чи галузевому рівнях 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, показані на рис. 5 та 6. Там же надані витяги з сайтів ILAC та IAF з зазначенням сфер акредитації, які охоплені відповідними Угодами.

Аналіз діючого статусу Угод НААУ та сфер акредитації, в яких ці Угоди діють, надає можливість виділити можливі оціночні стандарти та інші стандарти для наповнення Моделі Стандартів та формування Системи сертифікації кібербезпеки.

Рисунок 5 – Угода MRA та сфера в ILAC

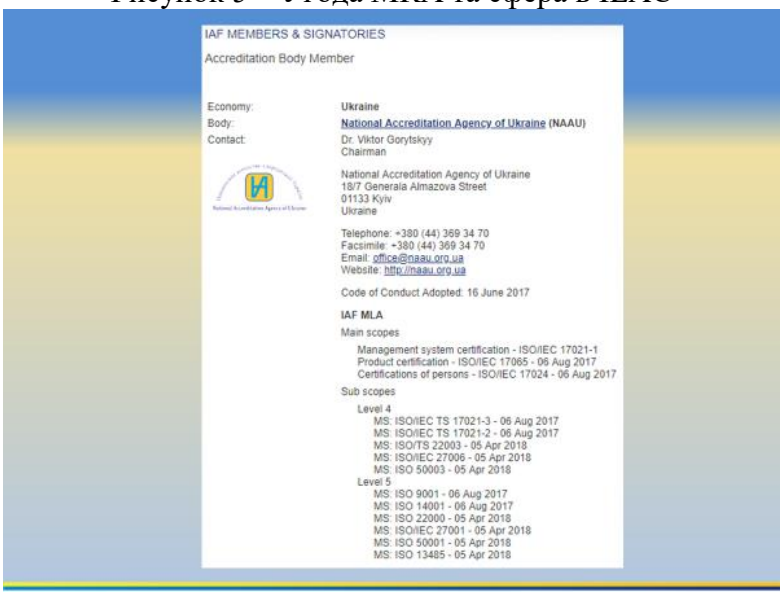

Рисунок 6 – Угода MRA та сфера в IAF

Цей проект Системи сертифікації кібербезпеки ІКТ для України побудований на попередньому аналізі та баченні ЄС з цього питання, яке викладено в Акті з кібербезпеки ЄС [14]. Як зазначено вище, Система сертифікації формується з 7 основних елементів.

1. Вимоги для оцінювання (стандарти чи інші нормативні документи). Сертифікат кібербезпеки повинен надаватися після успішної оцінки належним чином з застосуванням відповідних Схем сертифікації. Це може бути сертифікація органом, акредитованим на відповідність вимогам стандарту ISO/IEC 17065 та з залученням лабораторії, акредитованої згідно зі стандартом ISO/IEC 17025. Залежно від рівня гарантій, схема сертифікації кібербезпеки повинна вказувати, чи слід видавати сертифікат кібербезпеки приватним чи державним органом.

Схеми сертифікації кібербезпеки базуються (сфера сертифікації) на загальних Критеріях та розглядають питання сертифікації кібербезпеки на основі: загальних Критеріїв - ISO/IEC 15408; загальній Методології Оцінки Безпеки Інформаційних Технологій – ISO/IEC 18045. Схеми сертифікації кібербезпеки можуть передбачати проведення оцінки відповідності під виключною відповідальністю виробника або постачальника продуктів ІКТ. 2. Акредитація органів з оцінки відповідності (сертифікації). Після того, як буде прийнята схема сертифікації кібербезпеки, виробники або постачальники продуктів ІКТ повинні мати можливість подавати заявки на сертифікацію своїх продуктів ІКТ до ООВ на їх вибір. ООВ повинні бути акредитовані національним органом з акредитації. Національні органи з акредитації повинні обмежувати, призупиняти або анулювати акредитацію ООВ, якщо умови акредитації не виконуються.

3. Механізми взаємного визнання сертифікатів (угоди про визнання). З метою подальшого сприяння торгівлі та визнання того, що ланцюжки постачання ІКТ є глобальними, Україна може укласти угоди про взаємне визнання сертифікатів кібербезпеки. Кожна схема сертифікації кібербезпеки даної Системи сертифікації кібербезпеки повинна передбачати конкретні умови для таких угод про взаємне визнання з третіми країнами. Тому, система сертифікації кібербезпеки України повинна передбачати участь в Угоді про взаємне визнання результатів оцінки відповідності, яка базується на Регламенті ЄС № 2019/881 [14].

4. Управління системою сертифікації кібербезпеки. Управління Системою сертифікації кібербезпеки враховує належне залучення зацікавлених сторін та встановлює роль органу чи органів управління (далі – Орган управління) під час планування та пропонування, запитування, підготовки, прийняття та перегляду схем сертифікації кібербезпеки. Орган управління системою сертифікації кібербезпеки створюється регулятором (національним органом влади) чи за його погодженням. Орган управління повинен створити Робочу програму для створення та, за необхідністю, адаптацію розроблюваних Схем сертифікації кібербезпеки. Робоча програма повинна бути базовим документом, який дозволяє промисловості, національним органам влади та органам стандартизації заздалегідь підготуватися до майбутніх Схем сертифікації кібербезпеки.

5. Рівні гарантій сертифікатів кібербезпеки. Для забезпечення узгодженості системи сертифікації кібербезпеки схема сертифікації кібербезпеки повинна мати можливість визначати рівні гарантій сертифікатів кібербезпеки та декларацій про відповідність, виданих відповідно до цієї схеми. Кожен сертифікат кібербезпеки може посилатися на один із рівнів гарантій: *базовий*, *суттєвий* чи *високий*, тоді як декларація відповідності може стосуватися лише рівня *базового*.

6. Національні органи з сертифікації кібербезпеки. Цей елемент системи не є обов’язковим, але його доцільність полягає в гармонізації з вимогами Регламенту ЄС 2019/881 [14]. Необхідно призначити один або кілька національних органів з сертифікації кібербезпеки для нагляду за дотриманням зобов'язань, що містяться у Системі сертифікації кібербезпеки. Національним органом з сертифікації кібербезпеки може бути існуючий (за наявності) або новий орган. Національний орган з сертифікації кібербезпеки як мінімум повинен: контролювати виконання зобов’язань про відповідність кібербезпеці; допомагати національним органам з акредитації у моніторингу та нагляді за діяльністю органів з сертифікації, надаючи їм досвід та відповідну інформацію; призначати ООВ виконувати свої

завдання, якщо такі органи відповідають додатковим вимогам, встановленим схемою сертифікації кібербезпеки; слідкувати за відповідним розвитком у галузі сертифікація кібербезпеки.

7. Призначення органів з сертифікації кібербезпеки. Призначення – надання органом, що призначає, ООВ (в тому числі визнаній незалежній організації) права виконувати як третій стороні певні завдання з оцінки відповідності згідно з відповідним технічним регламентом [7]. Вимоги до призначених органів з сертифікації кібербезпеки повинні бути відповідними вимогам закону України «Про технічні регламенти та оцінку відповідності», який, у свою чергу, гармонізований *acquis* до законодавства ЄС щодо нотифікованих ООВ. Органи з сертифікації кібербезпеки можуть бути призначені для виконання ними як третіми сторонами певних завдань з оцінки відповідності згідно з відповідними технічними регламентами за умови, що вони відповідають додатковим вимогам, встановленим схемою сертифікації кібербезпеки чи технічним регулятором [15]. Наприклад, мають власні акредитовані випробувальні лабораторії для проведення принаймні деяких видів випробувань продукції ІКТ в межах сфери призначення.

Робочі версії схем сертифікації кібербезпеки ІКТ. Методологічною базою для розробки схем сертифікації кібербезпеки є міжнародний стандарт ISO/IEC 17067:2013 Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes [10]. Повна версія схеми сертифікації, згідно зі стандартом, повинна мати у своєму складі 17 елементів. У статті досліджено та визначені найбільш важливі та системоутворюючі елементи деяких схем сертифікації кібербезпеки. Такі версії схем будемо називати робочими (далі – Схема П1, Схема Х1). Також зазначимо, що дослідження спрямовано на гармонізацію національних схем сертифікації кібербезпеки з імовірними схемами сертифікації кібербезпеки ЄС [16,17].

Спочатку розглянемо робочу версію Схеми сертифікації кібербезпеки продукції ІКТ (Схема П1). В цій версії визначимо 4 елементи:

1. Предмет та обсяг схеми сертифікації. Схема сертифікації кібербезпеки базується на Загальних Критеріях (Common Criteria або CC) та повинна дозволяти сертифікацію продуктів ІКТ згідно зі стандартом ISO/IEC 15408.

Схема може охоплювати будь-який тип ІКТ-продукту.

Схема повинна охоплювати оцінку вразливостей криптографічних реалізацій до функціональних можливостей безпеки продукту ІКТ відповідно до вимог критеріїв оцінки та методології, визначених у стандарті ISO/IEC 15408.

2. Оціночні стандарти. Оцінки повинні базуватися за такими стандартами:

– загальні Критерії Оцінки Безпеки Інформаційних Технологій, відповідно до їх відповідної версії стандарту ISO/IEC 15408 (відомі ще як Загальні Критерії або Common Criteria - CC);

– загальна Методологія Оцінки Безпеки Інформаційних Технологій (відома ще як Загальна Методологія Оцінки або Common Evaluation Methodology - CEM) згідно з її відповідною версією стандарту ISO/IEC 18045.

Оцінка також враховує допоміжні елементи, створені для забезпечення гармонізованого тлумачення цих стандартів. Такі елементи повинні бути або обов'язковими допоміжними елементами, інтегрованими як додатки до цієї схеми, або допоміжними документами, що надаються Національним органом з сертифікації кібербезпеки.

Крім того, для акредитації ООВ, які виконують діяльність з оцінки та сертифікації, застосовуються такі стандарти:

– ISO/IEC 17065 для ООВ або національного органу, що відповідає за діяльність із сертифікації, надалі визначений органом з сертифікації;

– ISO/IEC 17025 для сторонніх ООВ або національних органів влади, або

субпідрядника ООВ або національних органів, які відповідають за діяльність з оцінки, надалі визначена випробувальною лабораторією.

3. Самооцінка відповідності. Схема не дозволяє проводити самооцінку відповідності.

4. Конкретні вимоги, що застосовуються до ООВ. Орган з сертифікації має бути акредитований відповідно до стандарту ISO/IEC 17065. Випробувальна лабораторія, включаючи її персонал, що проводить оцінки для органу з сертифікації повинна бути технічно компетентною для відповідних завдань. Для рівня гарантій *суттєвий* – ця технічна компетентність повинна оцінюватися шляхом акредитації випробувальної лабораторії відповідно до стандарту ISO/IEC 17025. Додатково для діяльності лабораторій слід визначити як керівництво схемою та використовувати такі потенційно відповідні стандарти:

– ISO / IEC 19896-3: 2018 Методи IT-безпеки – Вимоги до компетентності для тестувальників та оцінювачів інформаційної безпеки - Частина 3: Вимоги до знань, навичок та ефективності для оцінювачів ISO/IEC 15408;

– ISO/IEC DTS 23532-1 Інформаційна безпека, кібербезпека та захист конфіденційності – Вимоги до компетентності лабораторій випробувань та оцінки IT-безпеки – Частина 1: Оцінка за ISO/IEC 15408.

Робоча версія схеми сертифікації кібербезпеки хмарних сервісів (Схема X1) обмежується 1 елементом – визначенням оціночних стандартів. Схема X1 буде базуватись на акредитації органу з сертифікації, використанні Ієрархічних моделей оціночних стандартів Системи сертифікації кібербезпеки і Угод про взаємне визнання сертифікатів кібербезпеки та спиратись на наступну низку стандартів і технічних специфікацій сфери акредитації:

- міжнародні стандарти ISO/IEC 17788, ISO/IEC 17000 та ISO/IEC 27000;
- міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017 [19];
- міжнародний стандарт ISO/IEC 15408-3;
- міжнародний стандарт ISO/IEC ISO/IEC 27032 [18].

Методологія акредитації органу з сертифікації для Схеми X1 буде базуватись на міжнародному стандарті ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and services.

Висновки:

1. Сертифікація кібербезпеки ІКТ в Україні потребує вдосконалення шляхом створення національної системи кібербезпеки України на основі міжнародних стандартів, практик та глобальної системи технічного регулювання.

2. Для створення національної системи кібербезпеки на основі стандартів та систем, які застосовуються для сертифікації продукції у системі ILAC/IAF розроблена Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки.

3. Для створення національної системи кібербезпеки на основі Угод про визнання, які існують у системі ILAC/IAF/EA розроблена Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки.

4. Досліджено стан та міжнародний статус Національного органу України з акредитації ООВ щодо транскордонного визнання сертифікації інформаційної та кібербезпеки.

5. На основі Ієрархічної моделі оціночних стандартів, єрархічної моделі Угод про взаємне визнання та аналізу міжнародного статусу Національного органу України з акредитації запропонована версія Системи сертифікації кібербезпеки, яка встановлює процедуру створення схем сертифікації кібербезпеки України.

6. Розроблені робочі версії схем сертифікації кібербезпеки продукції ІКТ та хмарних сервісів.

ЛІТЕРАТУРА:

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України; від 17.01.2018 № 67-р. – Режим доступу : https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi

2. Conformity assessment - Vocabulary and general principles : ISO/IEC 17000:2020. – [Чинний від 2020-01-06]. – International Organization for Standardization/International Electrotechnical Commission, 2020. – 30 P.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45.

4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР// Відомості Верховної Ради України. – 1994. – № 31.

5.Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України від 15.03.2016 № 96/2016. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016#Text

6. Economic and Social Council Report. On the sectoral initiative on cyber security. – United Nations: Geneva, 20–22 November 2019. – Режим доступу : https://unece.org/DAM/trade/wp6/documents/2019/ECE_CTCS_WP.6_2019_9E.pdf

7. Про технічні регламенти та оцінку відповідності: Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.

8. International Accreditation Forum [Електронний ресурс]. – Режим доступу : https://www.iaf.nu/.

9. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу : https://ilac.org/.

10. Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes : ISO/IEC 17067:2013. – [Чинний від 2013-08-07]. – International Organization for Standardization/International Electrotechnical Commission, 2013. – 13 P.

11. Conformity assessment - Requirements for bodies certifying products, processes and services : ISO/IEC 17065:2012. – [Чинний від 2012-09-21]. – International Organization for Standardization/International Electrotechnical Commission, 2012. – 27 P.

12. EA-1/06 A-AB: 2017 EA Multilateral Agreement. Criteria for signing. – [Чинний від 2017-06]. – The European cooperation for Accreditation. – Paris, 2017.

13. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.

14. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 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) – [Чинний від 2019-04-17]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

15. Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання Постанова Кабінету Міністрів України від 16.12.2015 № 1057. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1057-2015-%D0%BF#Text

16. European Union Agency for Cybersecurity [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

17. European Union Agency for Cybersecurity [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

18. Information technology – Security techniques – Guidelines for cybersecurity: ISO/IEC 27032:2012. – [Чинний від 2012-07-15]. – International Organization for Standardization/International Electrotechnical Commission, 2012.

19. Information technology – Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: ISO/IEC 27017:2015. – [Чинний від 2012-12]. – International Organization for Standardization/International Electrotechnical Commission, 2015.

REFERENCES:

1. Ukraine. Cabinet of Ministers of Ukraine. On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation, Valid from January 17, № 67-p. Kyiv. Web <https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi>

2. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 17000:2020 Conformity assessment – Vocabulary and general principles. 2020.

3. Law of Ukraine. Verkhovna Rada of Ukraine. On the basic principles of cybersecurity of Ukraine. Valid from October 05, 2017, № 2163-VIII. Kyiv, Information of the Verkhovna Rada of Ukraine № 45 (2017). Print.

4. Law of Ukraine. Verkhovna Rada of Ukraine. On the protection of information in information and telecommunication systems. Valid from July 05, 1994, № 80/94-ВР. Kyiv, Information of the Verkhovna Rada of Ukraine № 31 (1994). Print.

5. Ukraine. Decree of the President of Ukraine. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine". Valid from March 15, 2016, № 96/2016. Web <https://zakon.rada.gov.ua/laws/show/96/2016#Text>

6. United Nations. Economic and Social Council Report. On the sectoral initiative on cyber security. Geneva: United Nations, 20–22 November 2019. Print.

7. Law of Ukraine. Verkhovna Rada of Ukraine. On technical regulations and conformity assessment. Valid from January 15, 2015, № 124-VIII. Kyiv, Information of the Verkhovna Rada of Ukraine № 14 (2015). Print.

8. International Accreditation Forum. Home page. Web <https://www.iaf.nu/>

9. International Laboratory Accreditation Cooperation. Home page. Web <https://ilac.org/.

10. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 17067:2013 Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes. 2013.

11. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services. 2012.

12. France.The European cooperation for Accreditation. EA-1/06 A-AB: 2017 EA Multilateral Agreement. Criteria for signing. Paris, 2017.

13. Law of Ukraine. Verkhovna Rada of Ukraine. On accreditation of conformity assessment bodies. Valid from May 17, 2001, № 2407-III. Kyiv, Information of the Verkhovna Rada of Ukraine № 32 (2001). Print.

14. European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 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). Web <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

15. Ukraine. Cabinet of Ministers of Ukraine. On determining the areas of activity in which the central executive bodies and the Security Service of Ukraine perform the functions of technical regulation, Resolution. Valid from December 16, 2015, № 1057. Web < https://zakon.rada.gov.ua/laws/show/1057-2015-%D0%BF#Text>

16.European Union Agency for Cybersecurity. Web <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>

17.European Union Agency for Cybersecurity. Web <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

18. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity, 2012.

19. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, 2015.

DOI 10.33243/2518-7139-2020-1-2-121-134