КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.6774
УДК 316.776:004.58

**Рой Яніна Володимирівна**
кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-8353-1856
*Y.roi@kubg.edu.ua*

**Рябчун Олена Петрівна**
аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-4400-0112
*Santalen@bigmir.net*

**Єрмошин Валерій Віталійович**
кандидат технічних наук, начальник департаменту інформаційної безпеки
НЕК "Укренерго", Київ, Україна
ORCID: 0000-0003-3747-0471
*Y.roi@kubg.edu.ua*

# МОДЕЛЬ ЗРІЛОСТІ МОЖЛИВОСТЕЙ СИСТЕМИ КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЕНЕРГЕТИЧНОГО СЕКТОРУ ES-C2M2

**Анотація.** В даний час як для комерційних, так і для державних організацій і установ доступний великий набір моделей оцінки зрілості ІБ, побудованих на схожих принципах. При цьому реальне використання таких моделей досить обмежено, в першу чергу через слабку прив'язку до особливостей конкретних організацій. Частково дана проблема вирішується адаптацією існуючих підходів у вигляді галузевих моделей (наприклад, ES-C2M2 для компаній енергетичного сектору, ONG-C2M2 для компаній нафтогазового сектора). Більш того, дуже вірогідним виглядає поява нової моделі, що включає не тільки якісний аналіз через набір характеристик/доменів, а й кількісну оцінку стану кібербезпеки, що дозволить використовувати оцінку як для стратегічного, так і для оперативного планування, а також створити просунуту експертну аналітичну систему. Оптимальним рішенням на сьогодні виглядає початок впровадження будь-якої з існуючих моделей оцінки з подальшою адаптацією і розширенням під власні потреби. Схожі принципи побудови моделей дозволять в майбутньому досить безболісно мігрувати на більш відповідну, при цьому накопичений досвід в оцінці, а також статистичні дані дозволять судити про прогрес розвитку процесів ІБ на підприємстві, причому, що важливо, в зручною та зрозумілою для вищого менеджменту формі. Модель зрілості можливостей системи кібербезпеки ES-C2M2 може суттєво допомогти організаціям енергетичного сектору оцінювати та вдосконалювати свої напрямки з питань кібербезахисту. Модель зрілості можливостей ES-C2M2 є частиною програми зрілості можливостей кібербезпеки DOE (C2M2) та була розроблена для вирішення унікальних характеристик енергетичного підсектору. Модель зрілості можливостей являється інструментарієм самооцінки для вимірювання та вдосконалення своїх напрямків з питань кібербезпеки. Міжнародні стандарти та практики в області інформаційної безпеки рекомендують організаціям при плануванні діяльності по забезпеченню ІБ проводити оцінку поточного стану ІБ і встановлювати цільову планку на найближче майбутнє, досягнення якої дозволить компанії ефективно протистояти існуючим загрозам і своєчасно реагувати на нові виклики і загрози ІБ.

**Ключові слова:** інформаційна безпека, модель зрілості можливостей, енергетична система, ES-C2M22

## 1. ВСТУП

Сучасна енергетична система - дуже складний технічний об'єкт, унікальний за своїми масштабами і своєю значимістю для забезпечення людської життєдіяльності. З огляду на фізичні особливості електроенергії і швидкоплинності електричних процесів управління роботою і безпечна експлуатація такого об'єкту є складною організаційно-технічним завданням. Високий рівень відкритості та інтегрованості систем електроенергетики поряд з широким розвитком і проникненням інформаційних і інтернет технологій в усі сфери життя людства привели до появи нових викликів для галузі. Автоматизовані системи захисту і управління об'єктів електроенергетики нашого часу являють собою інтегровану розподілену обчислювальну систему, що комунікує відкритими, добре документованим протоколам, які були розроблені насамперед з фокусом на забезпечення функціональних технологічних переваг і зручність експлуатації. Оцифрування енергетичних мереж, використання інтелектуальних технологій, датчиків і сенсорів інтернету речей в роботі, а також автоматизація бек-офісних процесів підвищили ризики в області кібербезпеки енергетичних підприємств. А неодноразові кібервторгнення в організації енергетичного сектору демонструють потребу в удосконалення кібербезпеки. Кіберзагрози продовжують зростати і на сьогоднішній день є найсерйознішими викликами, з якими стикається енергетичний сектор. Модель зрілості можливостей системи кібербезпеки ES-C2M2 може суттєво допомогти організаціям енергетичного сектору оцінювати та вдосконалювати свої напрямки з питань кібербезахисту.

## 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

У відкритому доступі майже відсутня статистика стосовно використання підприємствами і організаціями моделей зрілості можливостей в області інформаційної безпеки. На сьогоднішній день найбільш застосованими є моделі зрілості можливостей наведені в табл.1.

*Таблиця 1*

| Модель зрілості | Розробник | К-сть рівней моделі |
|---|---|---|
| COBIT (Control Objectives for Information and) | ISACA | 5 |
| CSF – NIST (Cybersecurity Capability Maturity Model) | Національний інститут стандартів і технологій США (NIST) | 5 |
| C2M2 (Cybersecurity Capability Maturity Model) | Енергетичне агентство Сполучених Штатів Америки (ЕА США) | 5 |
| ISEM (Information Security Evaluation Maturity Model) | City Group | 5 |
| ISM2 (Information Security Maturity Model) | Національних інститут стандартів і технологій США (NIST) | 5 |
| ISM3 (Information Security Management Maturity) | Консорціум ISM3 | 5 |
| NICE-CMM (National Initiative for Cybersecurity Education – Capability Maturity Model) | Національних інститут стандартів і технологій США (NIST) | 3 |
| SSE-CMM (Systems Security Engineering Capability Maturity Model) | АНБ (Агенство національної безпеки США) | 5 |

Модель зрілості можливостей ES-C2M2 є частиною програми зрілості можливостей кібербезпеки DOE (C2M2) та була розроблена для вирішення унікальних характеристик енергетичного підсектору. Модель зрілості можливостей являється інструментарієм самооцінки для вимірювання та вдосконалення своїх напрямків з питань кібербезпеки. Області моделі зрілості можливостей ES-C2M2 наведені на Рис. 1.


*Рис.1 Області ES-C2M2*

RM – Управління ризиками: створення, функціонування та підтримка переліку ризиків кібербезпеки підприємства, наявність програми виявлення, аналізу та зменшення кіберизиків.

ACM – Управління активами, змінами і конфігураціями: управління змінами та конфігурацією технологічних активів, включаючи технологію експлуатації, інформаційні технології, апаратне та програмне забезпечення.

IAM – Управління ідентифікацією та доступом: створення та управління унікальними ідентифікаторами, які можуть надаватися для логічного і фізичного доступу до активів.

TVM – Управління загрозами та вразливостями: створення та підтримування в актуальному стані планів, методологій, та процедур для виявлення, ідентифікації, аналізу, управління та реагування на загрози та вразливості кібербезпеки.

SA – Ситуаційна обізнаність: встановлення технологій збору подій та підтримка діяльності з аналізування, сповіщення, представлення подій з кібербезпеки для формування загальної операційної картини (ЗОК).

ISC – Обмін інформацією та зв'язками: встановлення та підтримка зав'язків із внутрішніми та зовнішніми суб'єктами, які збирають та надають інформацію про стан кібербезпеки включаючи загрози та вразливості, для зменшення ризиків та підвищення експлуатаційної стійкості.

IR – Реагування на події та інциденти, неперервність операцій: створення та підтримка планів, процедур та технологій для виявлення, аналізування та реагування подій кібербезпеки.

EDM – Управління системою поставок та зовнішніми сторонами: встановлення та постійний контроль для управління ризиками кібербезпеки, що пов'язані з послугами які надаються третіми сторонами.

WM – Управління людськими ресурсами: створення та підтримування планів, процедур, технологій для створення культури з кібербезпеки та забезпечення її постійної придатності та компетенції персоналу.

CMP – Керування програмами кібербезпеки: створення та підтримка в актуальному стані програми кібербезпеки підприємства, яка забезпечує управління, стратегічне планування, фінансування та діяльність з кібербезпеки

Модель зрілості можливостей ES-C2M2 використовує чотирьохрівневу структуру для оцінки стану безпеки кожної області. Ці рівні можуть бути представлені у вигляді трьохетапного процесу. Перший етап являє собою відправну точку з відсутніми процесами менеджменту інформаційної безпеки і невизначеними політиками безпеки. На другому етапі акцент робиться на впровадження стандартів безпеки і формалізованих процесів управління. Останній етап передбачає практично повністю автоматизоване управління безпекою підприємства. На даному етапі досягається максимально можливий рівень захисту від кіберзагроз, а сама організація знаходить стійкість до кібератаки. Архітектурна модель зрілості можливостей ES-C2M2 представлена на Рис.2.

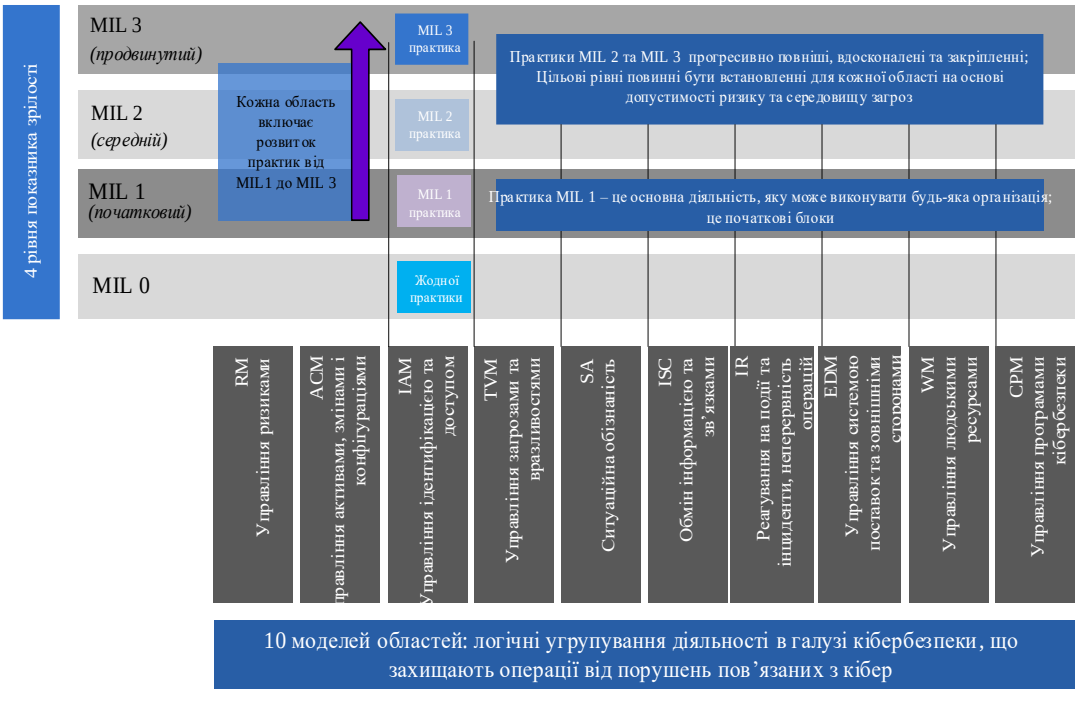


*Рис. 2 Архітектурна модель ES-C2M2*

Міжнародні стандарти та практики в області інформаційної безпеки рекомендують організаціям при плануванні діяльності по забезпеченню ІБ проводити оцінку поточного стану ІБ і встановлювати цільову планку на найближче майбутнє, досягнення якої дозволить компанії ефективно протистояти існуючим загрозам і своєчасно реагувати на нові виклики і загрози ІБ.

Зрілість процесів ІБ безпосередньо впливає на ступінь захищеності інформаційних ресурсів компанії. Детальне планування, моделювання інформаційних потоків, виконання відповідно до заданих умов і обмежень, оцінка ефективності з використанням відповідних метрик і подальше вдосконалення процедур - всі ці дії в сукупності дозволяють гарантувати ефективне виконання процесу ІБ і забезпечити всеосяжний контроль над критичними інформаційними потоками організації.

Наведена вище модель зрілості можливостей ES-C2M2 показує, що енергетичним компаніям слід сконцентрувати свою увагу на завданнях по оцінці ефективності процесів ІБ. Перший крок в цьому напрямку, який необхідно зробити в компанії, - розробка та затвердження стратегії ІБ, що визначає:

- ціль і завдання в частині забезпечення ІБ. Цілі і завдання повинні бути прив'язані до структури бізнесу і спрямовані на досягнення існуючих бізнес-целей. Кожна ціль повинна мати кількісне вираження і часовий горизонт для її досягнення, що дозволить в подальшому детально визначити метрики для регулярної оцінки ефективності виконуваних завдань;
- можливі сценарії розвитку ІБ з урахуванням можливих зовнішніх і внутрішніх факторів, що впливають на реалізацію стратегії ІБ;
- основні напрямки розвитку ІБ, що базуються на загальній ідеології розвитку Компанії і враховують можливі обмеження і ризики в залежності від обраного сценарію розвитку.

Далі, на підставі розробленої стратегії керівництву компанії слід ініціювати розробку метрик ІБ, за допомогою яких буде проводитися оцінка ефективності діяльності ІБ і ступеня реалізації стратегії. Для зниження навантаження на підрозділ ІБ при формуванні та оцінці метрик ІБ в компанії рекомендується використовувати спеціалізовані програмні рішення класу GRC. Системи подібного класу призначені для управління:

- ризиками;
- відповідністю внутрішнім політикам, стандартам, кращим практикам і вимогам регуляторів;
- внутрішнім аудитом;
- безперервністю бізнесу;
- інцидентами;
- конфігураціями

Використання подібних систем дозволить підвищити прозорість процесів ІБ для керівництва за рахунок широкого набору звітних інструментів, забезпечити безперервний моніторинг діяльності по ІБ і підготувати базу для подальшого вдосконалення процесів ІБ

## 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В даний час як для комерційних, так і для державних організацій і установ доступний великий набір моделей оцінки зрілості ІБ, побудованих на схожих принципах. При цьому реальне використання таких моделей досить обмежено, в першу чергу через слабку прив'язку до особливостей конкретних організацій.

Частково дана проблема вирішується адаптацією існуючих підходів у вигляді галузевих моделей (наприклад, ES-C2M2 для компаній енергетичного сектора, ONG-C2M2 для компаній нафтогазового сектора). Більш того, дуже вірогідним виглядає поява нової моделі, що включає не тільки якісний аналіз через набір характеристик/доменів, а й кількісну оцінку стану кібербезпеки, що дозволить використовувати оцінку як для стратегічного, так і для оперативного планування, а також створити просунуту експертну аналітичну систему.

Оптимальним рішенням на сьогодні виглядає початок впровадження будь-якої з існуючих моделей оцінки з подальшою адаптацією і розширенням під власні потреби.

Схожі принципи побудови моделей дозволять в майбутньому досить безболісно мігрувати на більш відповідну, при цьому накопичений досвід в оцінці, а також статистичні дані дозволять судити про прогрес розвитку процесів ІБ на підприємстві, причому, що важливо, в зручною та зрозумілою для вищого менеджменту формі.

## СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ

[1] Department of Energy: Cybersecurity Capability Maturity Model (C2M2): Version 1.1, Department of Homeland Security, 2014.
[2] M. Lessing: Best practices show the way to Information Security Maturity. [Electronic resource]. Accecc: http:// researchspace. Csir. Co. Za/ dspace/ bitstream/handle/10204/3156/Lessing6_2008.pdf?Sequence=1&isallowed=y.
[3] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.
[4] Уровень зрелости организации http://www.elitarium.ru/2007/04/09/uroven_zrelosti_organizacii.html
[5] Best practices show the way to Information Security Maturity. MM Lessing. Council for Scientific and Industrial Research, South Africa http://researchspace.csir.co.za/dspace/bitstream/10204/3156/1/Lessing6_2008.pdf
[6] The Community Cyber Security Maturity Model http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550099b-abs.html
[7] CMMI® for Development, Version http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

**Yanina Vl. Roy**
Phd, Associate Professor of the Department of Information and cyber security Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-8353-1856
*Y.roi@kubg.edu.ua*

**Olena Pt. Riabchun**
Aspirant Department of Information and cyber security Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-4400-0112
*Santalen@bigmir.net*

**Valeriy V. Yermoshin**
Phd, Head of the Information Security Department
NEC Ukrenergo, Kyiv, Ukraine
ORCID: 0000-0003-3747-0471
*Y.roi@kubg.edu.ua*

# MATURITY MODEL OF CYBER SECURITY SYSTEM OPPORTUNITIES AT CRITICAL INFRASTRUCTURE FACILITIES OF THE ES-C2M2 ENERGY SECTOR

**Abstract.** Currently, a large set of IS maturity assessment models based on similar principles is available for both commercial and government organizations and institutions. At the same time, the actual use of such models is quite limited, primarily due to the weak attachment to the characteristics of specific organizations. This problem is partially solved by adapting existing approaches in the form of industry models (for example, ES-C2M2 for companies in the energy sector, ONG-C2M2 for companies in the oil and gas sector). Moreover, the emergence of a new model is very likely, which includes not only qualitative analysis through a set of characteristics / domains, but also a quantitative assessment of cybersecurity, which will use the assessment for both strategic and operational planning, as well as create an advanced expert analytical system .
The best solution today is to start implementing any of the existing evaluation models with further adaptation and expansion for your own needs. Similar principles of model building will allow in the future to migrate painlessly to a more appropriate, while the experience gained in the assessment, as well as statistics will judge the progress of IS processes in the enterprise, and, importantly, in a convenient and understandable for senior management. The ES-C2M2 Cyber Security Maturity Model can significantly help energy sector organizations to assess and improve their cybersecurity areas. The ES-C2M2 Capability Maturity Model is part of the DOE Cybersecurity Capability Maturity Program (C2M2) and was developed to address the unique characteristics of the energy subsector. The opportunity maturity model is a tool for self-assessment to measure and improve their cybersecurity areas. International standards and practices in the field of information security recommend that organizations when planning IS activities to assess the current state of IS and set a target for the near future, the achievement of which will allow the company to effectively address existing threats and respond to new challenges and threats of IS.

**Keywords:** information security, opportunity maturity model, energy system, ES-C2M2

## REFERENCES

[1] Department of Energy: Cybersecurity Capability Maturity Model (C2M2): Version 1.1, Department of Homeland Security, 2014.
[2] M. Lessing: Best practices show the way to Information Security Maturity. [Electronic resource]. Accecc: http:// researchspace. Csir. Co. Za/ dspace/ bitstream/handle/10204/3156/Lessing6_2008.pdf?Sequence=1&isallowed=y.

[3] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.
[4] Уровень зрелости организации http://www.elitarium.ru/2007/04/09/uroven_zrelosti_organizacii.html
[5] Best practices show the way to Information Security Maturity. MM Lessing. Council for Scientific and Industrial Research, South Africa http://researchspace.csir.co.za/dspace/bitstream/10204/3156/1/Lessing6_2008.pdf
[6] The Community Cyber Security Maturity Model http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550099b-abs.html
[7] CMMI® for Development, Version http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm