DOI: 10.18372/2410-7840.21.13954
УДК 004.056.5

ФУНКЦІОНАЛЬНА МОДЕЛЬ ОЦІНЮВАННЯ РІВНЯ ЗРІЛОСТІ SOC НА ОСНОВІ МОДЕЛІ ЗРІЛОСТІ

Артем Жилін, Ганна Голич, Микола Худинцев

Розвинуті сучасні організації, що у своїх бізнес-процесах застосовують передові технології, потребують висококласного підходу до управління процесом кіберзахисту, незалежно від призначення застосовуваних технічних засобів - інформаційних технологій (IT), систем промислового управління (ICS), кібер-фізичних систем (CPS) або пристроїв IoT. Тому основним завданням фахівці з ІБ вбачають вибір стандартів та фреймворків у сфері інформаційних технологій, що містять вимоги, настанови та рекомендації стосовно організації актуальних процесів з кіберзахисту та менеджменту інформаційної безпеки. Компанії, під керівництвом яких функціонують центри оперативного реагування на кіберінциденти (SOCs), при їх створенні та підтримці експлуатації аналогічно керуються визнаними задокументованими стандартами та рекомендаціями. Станом на сьогодні проблематичним є питання опису як інструкцій із впровадження власних SOC в міру різності їх функціональних елементів залежно від цілей і масштабів впровадження, наявних фінансових ресурсів, так і моделі оцінки зрілості і можливостей оперативних центрів безпеки, більшість із яких пропонуються лідерами IT індустрії у якості комерційної послуги. Метою даної роботи є аналіз функціонування моделей оцінки зрілості і можливостей у керуючій стратегії розвитку ІБ організації та створення функціональної моделі задачі оцінювання рівня зрілості SOC на основі обраної моделі зрілості. Результати впровадження такої моделі дозволяють використовувати єдиний підхід у процесі оцінки рівня зрілості як окремих доменів, так і SOC у цілому незалежно від вибору моделі зрілості, аналізуючи обрахунки від простих метрик досягнення цілей до бізнес-орієнтованих метрик. У подальшій декомпозиції модель дає змогу сформувати конкретні вимоги до простих метрик результативності, на яких ґрунтується обчислення комплексних метрик, а також конкретніше визначати методи аналізу проведених підрахунків.

Ключові слова: *кібербезпека, центр оперативного реагування на кіберінциденти, оцінка, ефективність, модель зрілості та можливостей, метрика, функціональна модель.*

Постановка проблеми. На сьогодні, кіберзлочинність за своєю методологією та стратегічним планом значно просунулась в перед у способах здійснення атак із застосуванням інформаційних технологій. Через це сфера бізнесу вимагає професійного та обдуманого підходу у захисті від подібних інцидентів. Одним із варіантів його забезпечення є покладання обов'язків із забезпечення кібербезпеки організації на окремий підрозділ – центр оперативного реагування на кіберінциденти (SOC).

Таким чином, інформаційні системи підприємства підлягають постійному моніторингу, захисту та контролю стану захищеності. Це, у свою чергу, створює оптимальні умови для виявлення поточних недоліків у конфігурації систем, ідентифікації наявних і потенційних загроз. Ефективність вказаних функціональних обов'язків SOC не опосередковано залежить від рівня повноти його впровадження в організацію, що визначається моделлю зрілості і можливостей SOC аналогічно до контролю ефективності функціонування інших організаційних структур підприємства.

Зважаючи на відносно нещодавній початок приросту зацікавленості у створенні повнофункціонального SOC та пов'язану з цим фактом низьку кількість досліджень у даній сфері, компанії пропонують платні індивідуальні рішення із впровадження та комплексної організації діяльності центру оперативного реагування. Тому **актуальним** є питання розробки нових доступних обґрунтованих моделей оцінки зрілості та можливостей SOC, а також підбору методики визначення рівнів зрілості та можливостей в цих моделях.

Аналіз останніх досліджень і публікацій. Публікації [1]-[12] підтверджують наявність задокументованих настанов та рекомендацій з побудови та підтримки центру реагування на кіберінциденти. Перераховані в [13] моделі оцінки рівня зрілості та можливостей можуть бути застосовані до оцінки ефективності впровадження SOC, а вказана в [14] модель SOC-CMM – навіть інтегрована з фреймворком з кібербезпеки, про який йдеться в контексті забезпечення ІБ організації в цілому, попри наявність описаного алгоритму аналізу даних для визначення рівня зрілості та можливостей SOC, а також його продуктивності.

Метою даної роботи визначено створення функціональної моделі оцінювання рівня зрілості SOC на основі обраної моделі зрілості, а також аналіз ролі самих моделей оцінки зрілості у загальному фреймворку з ІБ організації.

Виклад основного матеріалу дослідження. Вважається, що для здійснення системного управління, аналізу ефективності дійсних політик безпеки, управління активами, створення SOC/NOC Service desk, необхідним є впровадження і вимірювання метрик ІБ. Тому часто питання оцінки рівня зрілості, можливостей, ефективності певного процесу помилково вирішується підрахунком стандартних метрик:

– Key Result Indicator (KRI) – метрики досягнення цілі, наприклад, загальним об'єм даних, що циркулює корпоративною мережею, кількість користувачів із правами доступу «super user», число подій від певного пристрою за годину, кількість коректних або помилкових спрацювань;

– Key Performance Indicator (KPI) – метрики результативності виконання процесу, наприклад, MTTR (Mean Time to Resolve/Repair/Recovery) – середній час відновлення після збою в роботі системи; MTTA (Mean Time to Acknowledge) – середній час прийняття інциденту в обробку; MTTI (Mean Time to Identify) – середній час визначення інциденту; MTBF (Mean Time Between Failures) – середній час між збоями в роботі системи, інтегральна характеристика стабільності системи;

– Critical Success Factors (CSF) – бізнес-орієнтовані метрики, наприклад, число інцидентів ІБ, що знижують продуктивність бізнес-операцій; частка бюджету служби ІБ від бюджету організації; частка операцій ІБ, які відхиляються від SLA; частка персоналу, що підвищують кваліфікацію.

У відповідності до стандартних обраховуваних метрик формують стратегічний план із поліпшення кількісних і якісних показників ефективності компанії, що конкретизує і пришвидшує процес впровадження фреймворку в організацію.

Обчислення метрик будь-якого рівня складності є одним із основних етапів загального процесу оцінювання рівня зрілості певних процесних областей, який демонструє визначальні аспекти поточного функціонування процесів, а тому повинен бути обов'язково контрольованим і включеним до переліку планової діяльності з управління процесами ІБ.

На рис. 1 зображена ієрархія метрик в масштабі підприємства, представлена бізнес-консультантом з безпеки Cisco – Олексієм Лукацьким.

Рис. 1. Ієрархія метрик ІБ підприємства [15]

Вирішення питання оцінки рівня зрілості, можливостей та ефективності шляхом підрахунку стандартних метрик є актуальним і загальноприйнятим у контексті оцінювання згідно моделей зрілості і можливостей (Capability Maturity Models), які визначаються відповідно до сфери функціонування проблемного процесу. Більше того, такі моделі можуть бути інтегровані з загальним фреймворком з ІБ, що є своєрідним алгоритмом покращення менеджменту діяльності в організації. Самі поодиноко обчислювані метрики представляють собою лише один з етапів оцінювання рівня зрілості, можливостей і ефективності.

Підбір оптимального фреймворку з ІБ є стратегічним кроком у вирішенні питання ефективного управління бізнес-процесами за рахунок коригування виконуваних процесів і процедур компанії у напрямку відповідності стандартів, серед яких найчастіше прийнятими до уваги є SOC2, CISv7, GDPR, HIPAA, ISO 27001, NIST CSF 1.1, NIST 800-53, NIST 800-171, NYDFS 500, PCI і SEC [16].

До прикладу, у 2018-му році Національним інститутом стандартів і технологій (NIST) було запропоновано удосконалену версію фреймворку з кібербезпеки [17] для оцінювання організацій за рівнем забезпечення конфіденційністю як персоналу, так і клієнтів, а також визначення недоліків у поточному підході до оцінювання ризиків з питання кібербезпеки. (див. рис. 2) Таким чином, удосконалений фреймворк може бути впроваджений в організації як незалежний процес з детектування, оцінки та управління ризиками кібербезпеки.

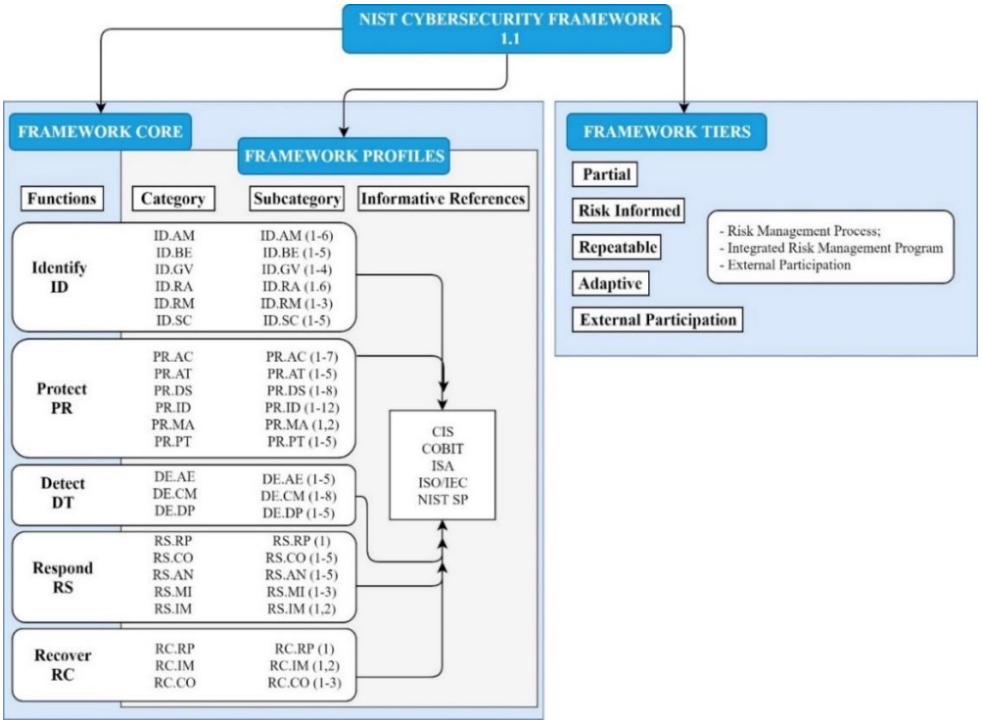


Рис. 2. NIST Cybersecurity Framework 1.1

Для визначення ефективності процедур, задіяних у встановленні відповідності процесів, які виконуються організацією, до описаних в NIST Cybersecurity Framework цільовим профілям (Target Profiles), використовують підхід самооцінки одного з трьох компонентів фреймворку - Framework Core [17] шляхом аналізу наступних процесів:

– поточний рівень впровадження Cybersecurity Framework;

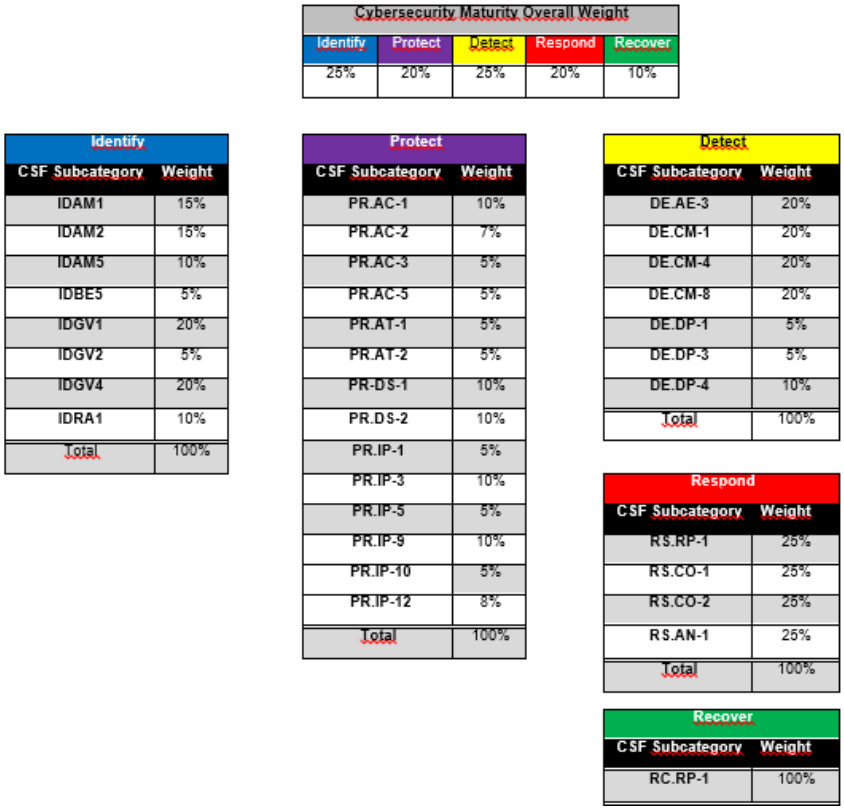
– встановлення пріоритетів діяльності організації, спрямованій на забезпечення кібербезпеки шляхом розробки Target Profile;

– визначення ступеня опрацювання кроків, описаних у категоріях забезпечення п'яти основних функцій Framework Core (визначення Current Profile);

– визначення ступеня впровадження інформаційних посилань (Informative References) в діяльність організації, що пов'язані з функціями, описаними в Framework Core.

Згідно з моделлю зрілості NIST CSF, офісом OIS (Office of Information Security) в Технологічному департаменті штату Каліфорнія був розроблений інструмент з обрахунку загального рівня зрілості процесу кіберзахисту в будь-якій компанії [18] шляхом оцінювання зрілості підкатегорій (subcategories) фреймворку за 4-бальною шкалою, кожна з яких співвідноситься з відповідною категорією, та функцією, які мають визначені вагові коефіцієнти (див. рис. 3). Даний спосіб аналізу показника кіберзахищеності є засобом вимірювання повноти досягнення департаментами організації своїх цілей і їх оптимальності (відповідно до ієрархії метрик в масштабі підприємства), так як питанням кібербезпеки зазвичай займається окремий структурний підрозділ компанії.

Провідні організації в міру потреби в уніфікації і оптимізації існуючих формалізованих процесів ІБ, моделюванні спільних процесів з ІТ, підвищенні стійкості бізнес-процесів і бізнес-інфраструктури [19], впроваджують проекти з реалізації Центру оперативного управління ІБ (SOC), який фактично здійснює комплексний процес «моніторингу безпеки для оцінки ризику».



Cybersecurity Maturity Overall Weight				
Identify	Protect	Detect	Respond	Recover
25%	20%	25%	20%	10%

Identify	
CSF Subcategory	Weight
IDAM1	15%
IDAM2	15%
IDAM5	10%
IDBE5	5%
IDGV1	20%
IDGV2	5%
IDGV4	20%
IDRA1	10%
Total	100%

Protect	
CSF Subcategory	Weight
PR.AC-1	10%
PR.AC-2	7%
PR.AC-3	5%
PR.AC-5	5%
PR.AT-1	5%
PR.AT-2	5%
PR.DS-1	10%
PR.DS-2	10%
PR.IP-1	5%
PR.IP-3	10%
PR.IP-5	5%
PR.IP-9	10%
PR.IP-10	5%
PR.IP-12	8%
Total	100%

Detect	
CSF Subcategory	Weight
DE.AE-3	20%
DE.CM-1	20%
DE.CM-4	20%
DE.CM-8	20%
DE.DP-1	5%
DE.DP-3	5%
DE.DP-4	10%
Total	100%

Respond	
CSF Subcategory	Weight
RS.RP-1	25%
RS.CO-1	25%
RS.CO-2	25%
RS.AN-1	25%
Total	100%

Recover	
CSF Subcategory	Weight
RC.RP-1	100%

Рис. 3. Вагові коефіцієнти для підкатегорій NIST CSF [18]

Незважаючи на відсутність конкретних стандартів та керівних принципів для побудови та підтримки функціонування SOC, деякі міжнародні та американські урядові стандарти містять частковий опис настанов та рекомендацій [20], серед яких є:

– NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management [1] надає рекомендації щодо ведення журналювання подій та аудиту підприємства;

– NIST Draft SP 800-94 Revision 1, Guide to Intrusion Detection and Prevention Systems [2] надає рекомендації по плануванню, впровадженню, конфігуруванню, забезпечення безпеки та моніторингу технологій IDPS;

– NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops [3] надає рекомендації щодо вдосконалення заходів із запобігання інцидентам, пов'язаним із розповсюдженням шкідливого програмного забезпечення та існуючих можливостей організації по реагуванню на події ІБ;

– NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide [4] надає рекомендації щодо обробки інцидентів, зокрема, стосовно послідовності аналізу даних, пов'язаних з інцидентами, та визначення відповідного реагування на інциденти;

– Department of Homeland Security Recommended Practice: Creating Cyber Forensics Plans for Control Systems [5] надає вказівки щодо застосування традиційних концепцій кібер-криміналістики в середовищах систем управління;

– Department of Homeland Security Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability [6] містить рекомендації з реагування на кіберінциденти, методи та підходи з покращення захищеності організації від атак;

– The Open Source Security Testing Methodology Manual (OSSTMM) [7] включає в себе процедури для різних процесів SOC, що включають тестування безпеки, метрики оперативності рівня безпеки, аналіз показників довіри;

– Information Security Management Maturity Model (ISM3) [8], опублікована The Open Group, опирається на стандарти ISO 20000, ISO 9001, CMM, ISO/IEC 27001, і може використовуватися як шаблон для побудови систем управління безпекою, сумісних з ISO 9001;

– The Information Security Assurance - Capability Maturity Model (ISA-CMM) [9], що базується на System Security Engineering Capability Maturity Model (SSE-CMM) і INFOSEC Assurance Capability Maturity Model (IA-CMM) і була модифікована для

вирішення процесів забезпечення інформаційної безпеки;

– Information Technology Infrastructure Library (ITIL) [10] представляє собою набір практик для управління IT-послугами, що зосереджується на узгодженні IT-послуг з потребами бізнесу;

– ISO/IEC 27001 [11] є міжнародним стандартом інформаційної безпеки, що містить специфікацію для систем управління інформаційною безпекою (ISMS);

– Control Objectives for Information and Related Technology (COBIT) [12], фреймворк, створений ISACA для менеджменту інформаційних технологій та управління IT, містить інструменти, які дозволяють контролювати технічні питання та бізнес-ризики.

Деякі з передових організацій IT-індустрії пропонують індивідуально розроблені рекомендації із впровадження SOC [21], [22], [23], [24].

Ефективність впровадженого та діючого в організації Центру оперативного управління ІБ в кінцевому рахунку зводиться до обрахунку метрик безпеки. Кожен із рівнів розвитку SOC, згідно однієї із застосовуваних моделей зрілості або можливостей, має визначений набір метрик, які підтверджують досягнення Центром одного з цих рівнів. До таких моделей належать Crosby's Quality Management Maturity Grid (QMMG) Model, Bessant's Continuous Improvement Capability Model, Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), Business Process Maturity Model (BPMM) та ін. [13], до сфери інформаційних технологій та безпеки з яких відносяться CMMI, Easiest Open Source Software Model, Performance Management Maturity Model, CERT-RMM (Resilience Management Model) і ISO/IEC 15504 (Software Process Improvement and Capability Determination, SPICE).

Враховуючи критерії порівняння існуючих моделей зрілості, описаних у статті «Maturity Models for Information Systems - A State of the Art» [13], а також опису моделей [25], [26], [27], [28], [29], було проаналізовано 5 моделей у сфері інформаційних технологій і безпеки (див. рис. 4).

	Структура моделі (Model Structure)				Оцінювання моделі (Model Assessment)		Підтримка моделі (Model Support)		
Назва моделі	Кількість рівнів	Визначення поняття "зрілість" (maturity)	Практичність		Опис методу оцінювання	Вартість оцінювання	Доступність	Підтримка розробників	Впроваджуваність
CMMI	5	+	Конкретно описані кроки		+	Висока	Безкоштовна	+	Висока
EOSS	5	+	Конкретно описані кроки		+	Середня	Безкоштовна	+	Середня
PMMM	5	-	Конкретно описані кроки		+	Середня	Платна	+	Висока
CERT-RMM	5	+	Конкретно описані кроки		+	Висока	Безкоштовна	+	Середня
SPICE	5	+	Конкретно описані кроки		+	Середня	Безкоштовна	+	Висока

Рис. 4. Порівняння моделей зрілості у сфері IT

Моделі зрілості і/або можливостей, розроблені спеціально для SOC, зазвичай представлені у вигляді комерційної пропозиції компаній-розробників (наприклад, HP Security Operations Maturity model (HP SOMM), вимірювання показників зрілості консультаційних послуг IBM SOC), тому опис їх рівнів не знаходиться у вільному доступі.

Загальнодоступна модель для оцінки зрілості (maturity) і можливостей (capabilities) SOC, SOC-CMM, що базується на CMMI, [14] була створена шляхом оцінки літератури для визначення характеристик і особливостей SOC, а також практичного аналізу 16 діючих ситуаційних центрів, які мають різний термін впровадження, сектор використання, програми з визначення ефективності SOC (рис. 5).

Так, як модель SOC-CMM у визначенні рівнів зрілості і можливостей повністю ґрунтується на описі, представленому моделлю CMMI, визначення понять «зрілість» та «можливості» у цьому випадку також збігаються:

– рівень зрілості організації характеризує її продуктивність. Так, як кожен з рівнів зрілості має детальний опис, він дає змогу оцінити ступінь контрольованості діючих функціональних процесів. Проте, незважаючи на загальний стан виконання функцій процесу, йому може бракувати ефективності і бажаного позитивного впливу на бізнес-процеси, що у такому випадку свідчить про недостатній рівень можливостей, якими забезпечений процес;

– рівень можливостей демонструє ступінь повноти реалізації функцій діючих процесів, оцінюючи рівень продуктивності та ефективності від виконання процесів.

Для опису рівнів модель CMMI має 2 варіанти представлення:

– поетапне (staged), що використовується для відображення рівнів зрілості з метою удосконалення загального стану процесів організації згідно з моделлю в цілому;

– безперервне (continuous), що використовується для відображення рівнів можливостей з метою удосконалення виконання функцій процесів певних процесних областей. У цьому випадку організація залишає за собою право вибору послідовності дій, що ведуть до удосконалення бізнес-процесів.

Модель SOC-CMM використовує варіант безперервного представлення як для опису рівнів зрілості, так і можливостей.

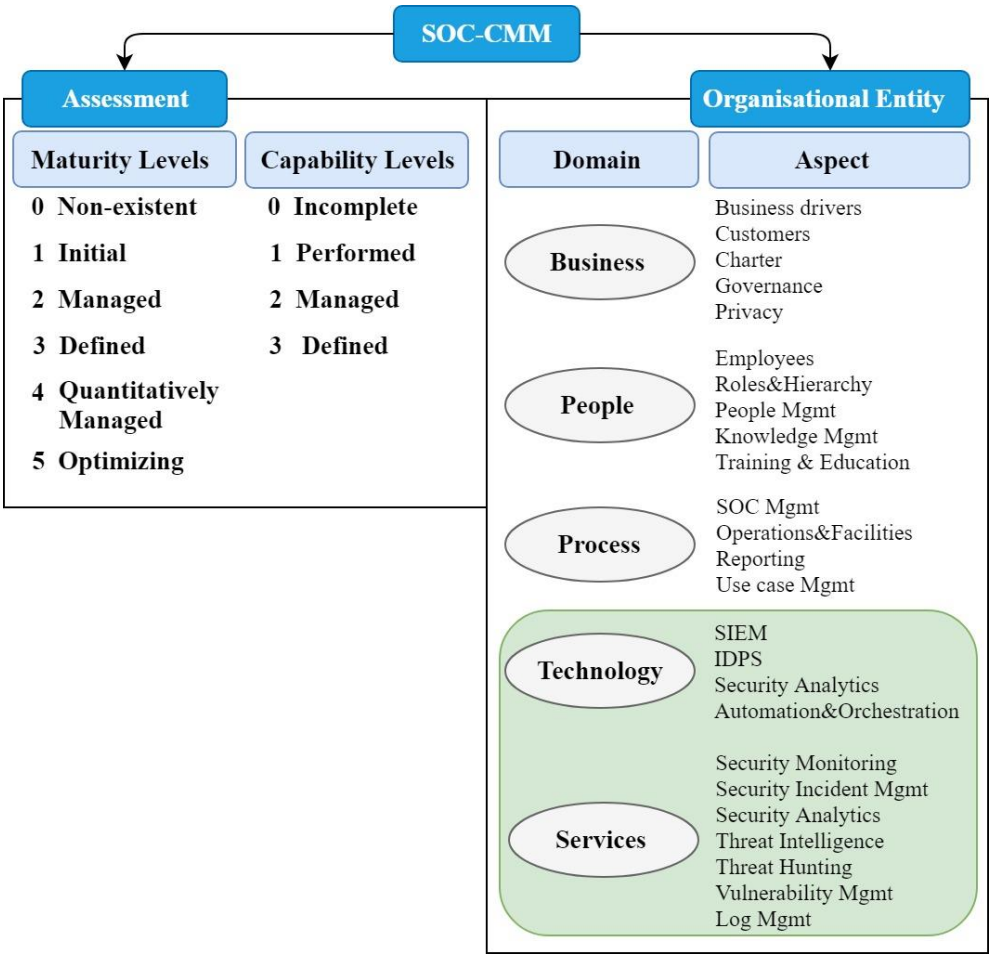


Рис. 5. Модель SOC CMM

За потреби, тестування за моделлю SOC-CMM може бути узгоджене з п'ятьма функціями NIST Cyber Security Framework (CSF): ідентифікація, захист, детектування, відповідь, відновлення (рис. 6).

За результатами покроково проведеного стандартного тестування SOC-CMM відповідно до введених даних серед п'яти доменів, які розглядаються (бізнес, персонал, процеси, технології, сервіси), усі оцінюються за рівнем зрілості, в той час як за зрілістю і можливостями разом – тільки технології і сервіси, після чого вказані дані автоматично заповнюють результуючу таблицю і діаграму радарів з оцінкою SOC за рівнем зрілості (див. рис. 7) і можливостей.

На основі розглянутого підходу до створення фреймворку метрик безпеки на основі моделі зрілості Cyber Security Capability Maturity Model [31], а також методу оцінки рівня зрілості Центру оперативного реагування на кіберінциденти через метрики ІБ на основі моделі SOC-CMM, пропонується контекстна діаграма для задачі оцінювання рівня зрілості SOC за обраною моделлю зрілості за методологією IDEF0 (рис. 8).

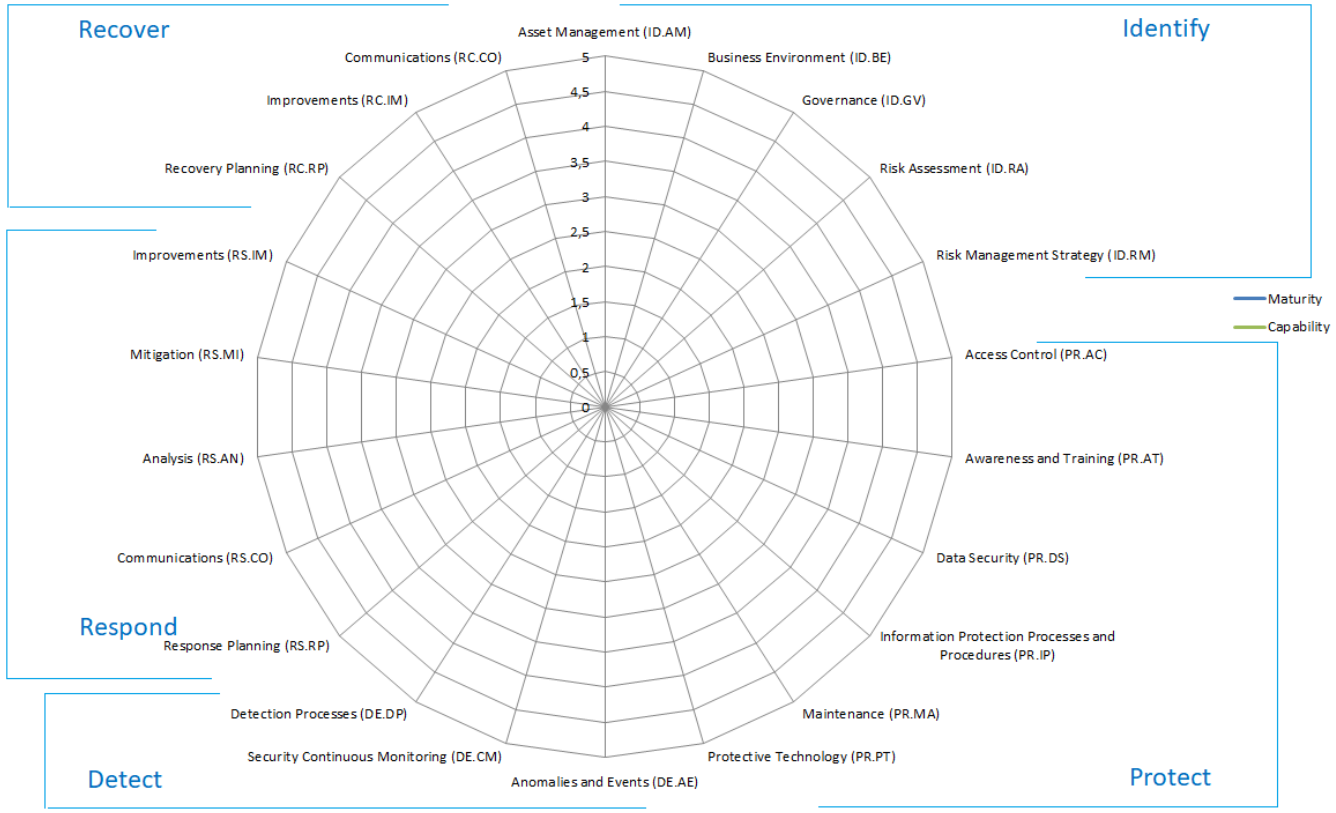


Рис. 6. Діаграма радарів SOC за рівнем зрілості (за SOC-CMM) [30]

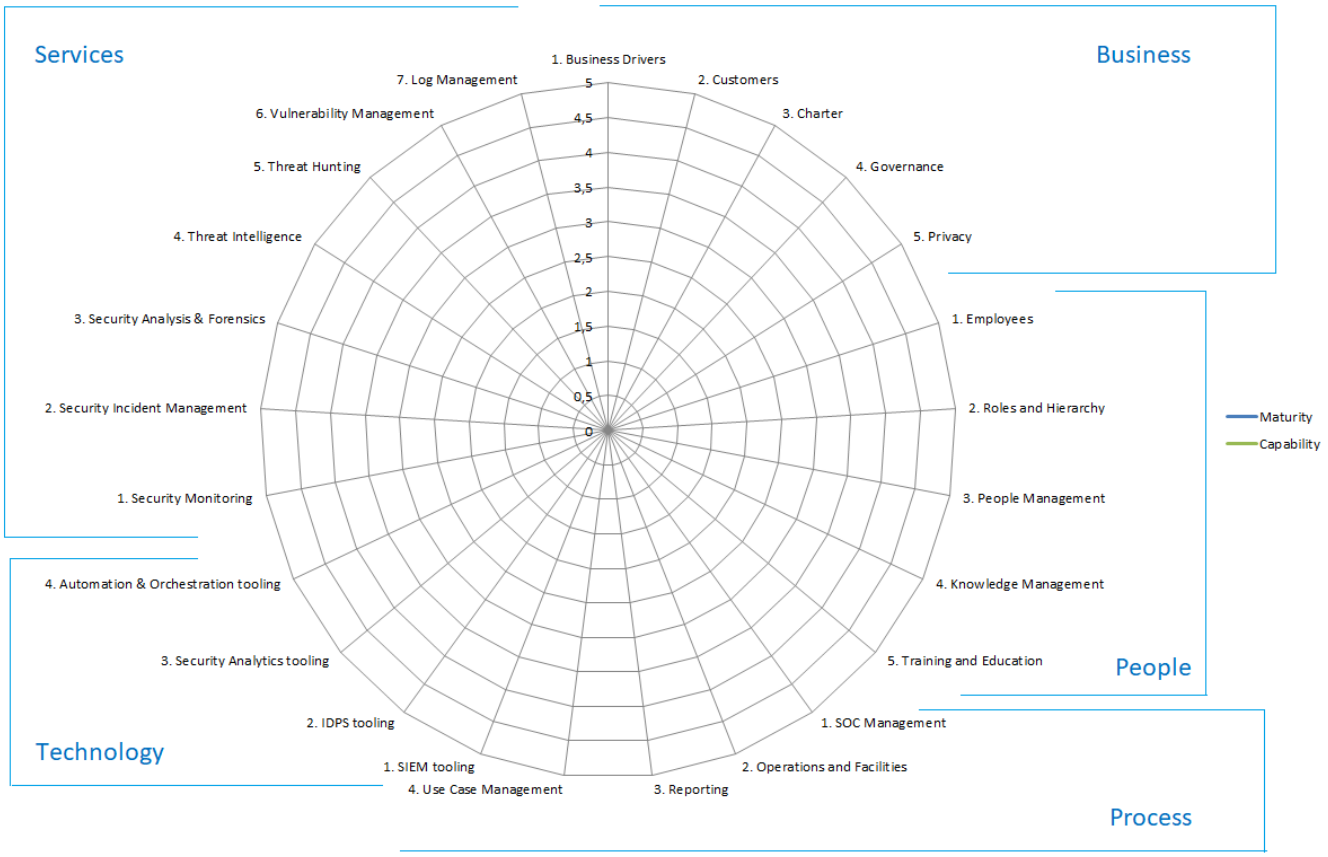


Рис. 7. Діаграма радарів SOC за рівнем зрілості (за SOC-CMM) [30]

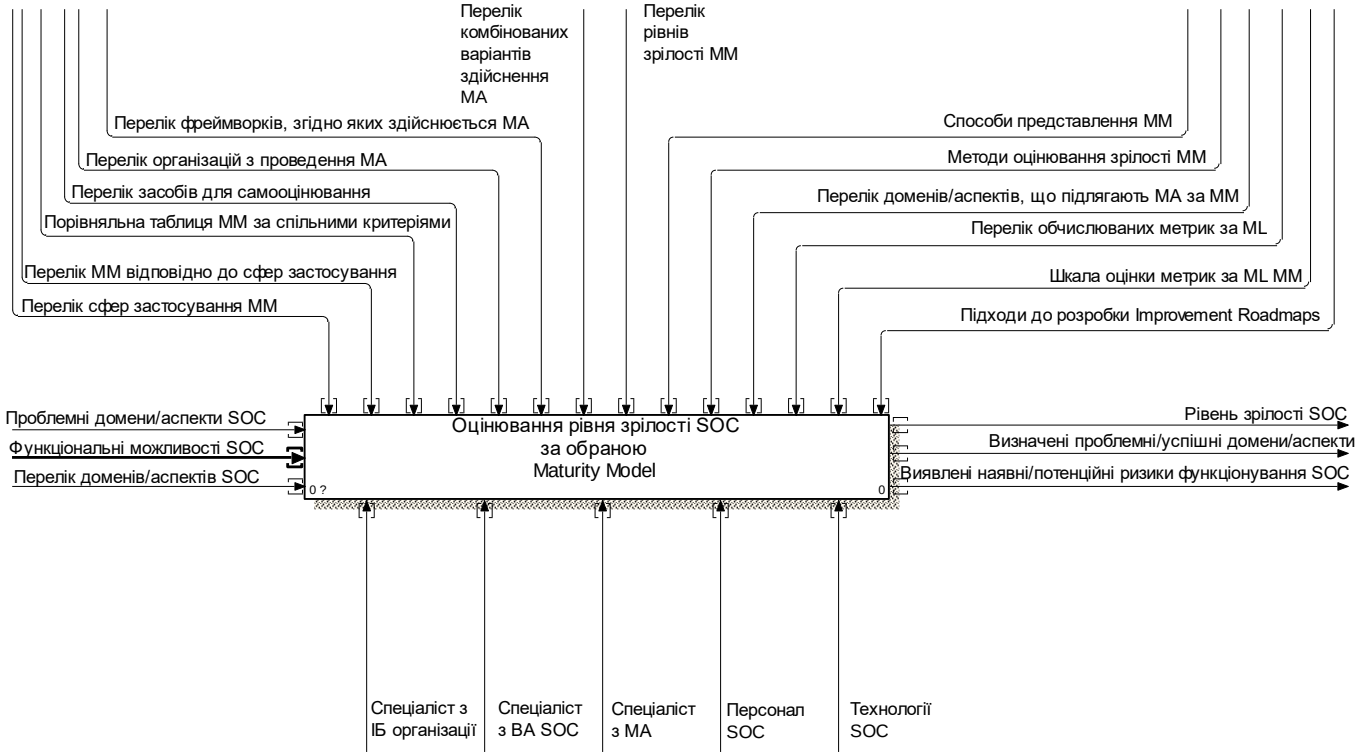


Рис. 8. Контекстна діаграма для задачі оцінювання рівня зрілості SOC за обраною моделлю зрілості (методологія IDEF0)

Контекстна діаграма відображає основні компоненти, які стосуються процесу оцінювання рівня зрілості SOC за обраною моделлю зрілості:

– вхідні дані, необхідні як для вибору самої моделі зрілості, так і здійснення оцінювання (перелік доменів та аспектів SOC організації, визначені проблемні питання стосовно їх функціонування, дані щодо функціональних можливостей SOC);

– вихідні дані, що представляють собою результат виконання процесу (визначений рівень зрілості SOC, підтверджений перелік проблемних/успішних доменів та їх аспектів, ризиків SOC);

– управляюча і регламентуюча інформація, якою керуються на різних етапах проведення оцінювання;

– механізми реалізації процесу, які представлені технологіями SOC і спеціалістами у сфері управління ІБ.

З метою деталізації функціональної моделі виконана функціональна декомпозиція в нотаціях IDEF0 (див. рис. 9). Задачу оцінювання рівня зрілості SOC за обраною моделлю зрілості можна представити у вигляді послідовно виконуваних 4 процесів:

– вибір моделі зрілості для оцінювання SOC організації за її методологією;

– вибір способу реалізації оцінювання за рівнем зрілості (Maturity Assessment, MA);

– визначення архітектури моделі зрілості (Maturity Model, MM);

– проведення оцінювання рівня зрілості SOC (MA).

Процес вибору моделі зрілості базується на визначенні оптимальної ММ, оцінювання за якою дасть висновки з приводу удосконалення процесів певних процесних областей. Вхідними даними повинен слугувати перелік функціональних можливостей і проблемних доменів та аспектів SOC, які дають підстави для проведення оцінювання за моделлю зрілості з метою мінімізації потенційних ризиків, пов'язаних з даною діяльністю.

Процес вибору способу реалізації МА передбачає наявність визначеної ММ, за якою буде проведено оцінювання, і перегляд програмних засобів (для самооцінювання SOC), організацій, які надають послуги зі здійснення МА, можливих комплексних методів, а також фреймворків з ІБ, згідно стратегії яких буде доцільною реалізація МА саме за визначеною моделлю зрілості.

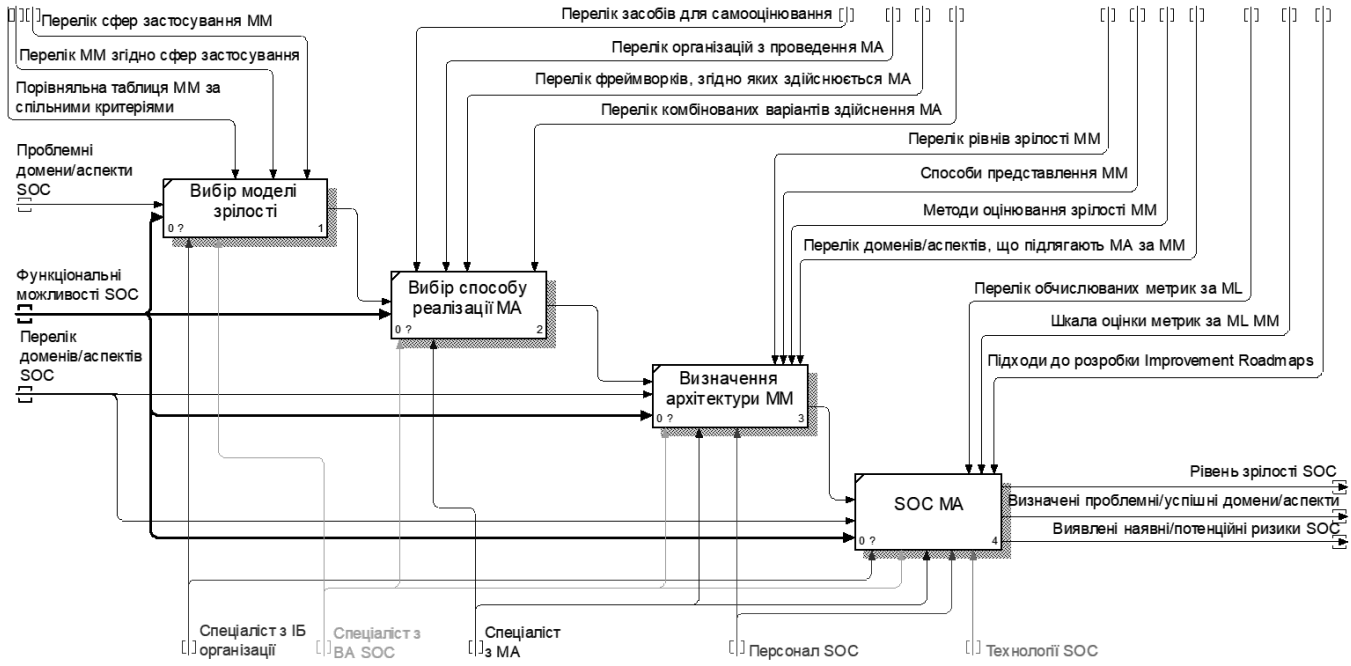


Рис. 9. Діаграма декомпозиції першого рівня (методологія IDEF0)

Процес визначення архітектури ММ базується на маркуванні ключових елементів, спільних для усіх моделей:

– перелік рівнів зрілості моделі (їх кількість та назви рівнів, список вимог по досягненню кожного з рівнів);

– способи представлення (безперервне або поетапне представлення, для визначення рівня зрілості зазвичай застосовують поетапне);

– методи оцінки зрілості за ММ;

– перелік доменів та їх аспектів, оцінювання яких передбачене за обраною ММ (ключові домени і аспекти SOC, наявність і функціонування яких є обов'язковим для реалізації оцінювання).

Процес **SOC MA** підсумовує результати, отримані внаслідок попередніх трьох етапів, шляхом реалізації методу оцінювання зрілості, визначеному при розборі архітектури ММ. За висновками стає зрозумілим рівень зрілості SOC за ММ, вказуються проблемні домени/аспекти SOC організації, діяльність яких необхідно коригувати з метою зниження виявлених ризиків ІБ.

Висновки. Задача оцінювання зрілості є актуальною для будь-якої організації, що розвиває та впроваджує стратегічний план у діяльність з інформаційної безпеки, оскільки це дозволяє виміряти зрілість компанії в одній або декількох процесних областях через визначені методи оцінювання, отримуючи як показник - оцінку зрілості, так і improvement roadmaps - ряд рекомендацій щодо поліпшення цього стратегічного плану. З цією метою спеціалісти з управління ІБ установи згідно процесних областей обирають настанови, рекомендації, стандарти, фреймворки, які і формують стратегію поліпшення тактики компанії, хоча ефективність їх впровадження є невирішеним питанням до оцінювання діяльності з ІБ організації згідно моделі зрілості, що і є перевіркою застосовуваного стратегічного плану на доцільність і продуктивність.

Впровадження Центру оперативного реагування на кіберінциденти в організацію, що є одним із етапів стратегії діяльності з ІБ, як і сама організація, потребують не лише механізмів для розгортання діяльності – технологій, спланованих процесів, процедур, а також персоналу, який буде в цьому задіяний, але й аналогічного виконуваного стратегічного плану, якого дотримується сама установа. У цьому випадку та ж сама задача перевірки ефективності стратегічного плану зводиться до визначення рівня зрілості за однією з ММ.

У зв'язку з низьким рівнем досліджуваності у сфері оцінювання ефективності, зрілості та можливостей SOC незначна кількість моделей була розроблена специфічно для оцінки рівня зрілості SOC, більшість із яких пропонуються у вигляді комерційної послуги. Крім того, наявні моделі не завжди представляють детально задокументований опис методу оцінювання рівня зрілості, тому відкритими залишаються питання:

– розробки оптимальної моделі для оцінювання рівня зрілості, можливостей, ефективності SOC;

– покрокового опису послідовності здійснення процесу оцінювання рівня зрілості SOC, незалежного від вибору моделі зрілості.

З метою деталізації алгоритму дій по вирішенню задачі з оцінювання рівня зрілості SOC на основі обраної моделі зрілості, було запропоновано функціональну модель задачі у вигляді контекстної діаграми за методологією IDEF0, а також її декомпозицію першого рівня.

Подальша декомпозиція функціональної моделі дозволить детально структуризувати кроки з проведення 4 підетапів процесу оцінювання рівня зрілості SOC, даючи підстави для створення покрокового алгоритму застосування обраної моделі зрілості до Центру оперативного реагування на кіберінциденти з метою підвищення ефективності його функціонування.

ЛІТЕРАТУРА

[1]. Guide to Computer Security Log Management. [Електронний ресурс]. Режим доступу: https:// csrc.nist.gov/publications/detail/sp/800-92/final.

[2]. Guide to Intrusion Detection and Prevention Systems (IDPS). [Електронний ресурс]. Режим доступу: https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps.

[3]. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. [Електронний ресурс]. Режим доступу: https://nvlpubs. nist. gov/nistpubs/ SpecialPublications/ NIST.SP. 800-83r1.pdf.

[4]. Computer Security Incident Handling Guide. [Електронний ресурс]. Режим доступу: https:// nvlpubs.nist.gov/ nistpubs/ SpecialPublications/ NIST. SP.800-61r2.pdf.

[5]. Recommended Practice: Creating Cyber Forensics Plans for Control Systems. [Електронний ресурс]. Режим доступу: https:// inldigitallibrary. inl. gov/ sites/sti/sti/4113665.pdf.

[6]. Developing an Industrial Control Systems Cybersecurity Incident Response Capability. [Електронний ресурс]. Режим доступу: https://ics-cert.us-cert.gov/ sites/default/files/ recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.

[7]. Herzog P. Open Source Security Testing Methodology Manual (OSSTMM). [Електронний ресурс]. Режим доступу: http://www. isecom. org/ research/ osstmm.html.

[8]. Information Security Management Maturity Model (ISM3). [Електронний ресурс]. Режим доступу: https://www.ism3.com/.

[9]. Cybersecurity Capability Maturity Model White Paper. Department of Homeland Security. [Електронний ресурс]. Режим доступу: https:// niccs.us-cert.gov/ sites/ default/files/ Capability%20 Maturity%20Model%20White%20Paper.pdf?trackDocs = Capability%20Maturity%20 Model%20 White%20Paper.pdf.

[10]. Information Technology Infrastructure Library (ITIL). [Електронний ресурс]. Режим доступу до ресурсу: https://www.axelos.com/best-practice-solutions/itil.

[11]. ISO/IEC 27001. [Електронний ресурс]. Режим доступу: https://www.iso.org/isoiec-27001-information-security.html.

[12]. Control Objectives for Information and Related Technology. [Електронний ресурс]. Режим доступу: http://www.free-management-ebooks. com/ news/cobit/.

[13]. Proenca D. Maturity Models for Information Systems - A State of the Art. [Електронний ресурс]. Режим доступу: https://www.researchgate. net/ publication/ 313838260_ Maturity_ Models_ for_ Information_Systems_-_A_State_of_the_Art.

[14]. Van Os R. SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers. [Електронний ресурс]. Режим доступу: https://www.soc-cmm.com/.

[15]. А. Лукацкий, *Как посчитать эффективность информационной безопасности?* [Електронний ресурс]. Режим доступу: https:// www. cisco.com/ c/ dam/ global/ ru_ua/ training-events/events/ pdf/security_ metrics-alukatsk.pdf.

[16]. Which Cybersecurity Framework is Right for You? [Електронний ресурс]. Режим доступу: https:// securityboulevard.com/2019/02/which-cybersecurity-framework-is-right-for-you/.

[17]. Framework for Improving Critical Infrastructure Cybersecurity. [Електронний ресурс]. Режим доступу: https:// nvlpubs. nist. gov/ nistpubs/ CSWP/ NIST.CSWP. 04162018.pdf.

[18]. California Cybersecurity Maturity Metrics [Електронний ресурс]. Режим доступу: https:// cdt.ca.gov/wp-content/ uploads/2018/ 05/ Copy-of-SIMM-5300-C_CACybersecurity-Maturity-Metrics_May-2018_REVISED_FINAL0525.xlsx.

[19]. Нужен ли вам SOC? [Електронний ресурс]. Режим доступу: https://www. securitylab. ru/ blog/ compa-ny/AngaraTech/341933.php.

[20]. G. Rasche, *Guidelines for Planning an Integrated Security Operations Center* [Електронний ресурс]. Режим доступу: https://www.smart-energy.com/wp-content/uploads/2014/02/EPRI-Planning-ISOC-report.pdf.

[21]. McAfee® Foundstone® Professional Services, Creating and Maintaining a SOC: The details behind successful Security Operations Centers [Електронний ресурс]. Режим доступу: https://www.mcafee. com/enterprise/en-us/resource-library/publications. html.
[22]. How to Build Security Operations Center (SOC) [Електронний ресурс]. Режим доступу: ftp://ftpeng.cisco.com/cons/workshops/SP-Powersession -Thailand-Jan-2007/SPSEC-610-Security-Operations-Centers-Basics-Version-2.pdf.
[23]. Building an intelligence-driven security operations center. [Електронний ресурс]. Режим доступу: https://www.emc.com/collateral/technical-documentation/h11533-intelligence-driven-security-ops-center.pdf.
[24]. Building a successful security operations center - Business white paper. [Електронний ресурс]. Режим доступу: https://ssl.www8.hp.com/us/en/ssl/leadgen/ secure_ document. html? Objid = 4AA46169ENW& siebelid=23803&parentUrl=https%3A%2F%2F www. google.com%2F.
[25]. S. Albliwi, J. Antony, N. Arshed*, Critical Literature Review on Maturity Models for Business Process Excellence.* [Електронний ресурс]. Режим доступу: https://www.academia.edu/9930188/Business_Process_Excellence_Maturity_Models.
[26]. A. Zahoor, K. Mehboob, S. Natha, *Comparison of open source maturity models.* [Електронний ресурс]. Режим доступу: https:// www. sciencedirect. com/ science/ article/ pii/S1877050917312061.
[27]. OpenSource Maturity Model. [Електронний ресурс]. Режим доступу: https:// en. wikipedia. org/ wiki/OpenSource_Maturity_Model.
[28]. M. Aho, *What is your PMI?* [Електронний ресурс]. Режим доступу: https://www.slideshare.net/mikaaho/ what-is-your-pmi-a-model-for-assessing-the- maturity- of- performance- management- in-organizations.
[29]. CERT Resilience Management Model (CERT-RMM) Version 1.2. [Електронний ресурс]. Режим доступу: https://resources.sei.cmu.edu/library/asset-view.cfm? assetid=508084.
[30]. ISO/IEC 15504. [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_15504.
[31]. T. Le, D. Hoang, *Capability maturity model and metrics frameworkfor cyber cloud security* [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/ 321277007_ Capability_ Maturity_Model_and_Metrics_Framework_for_Cyber_Cloud_Security.

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ОЦЕНИВАНИЯ УРОВНЯ ЗРЕЛОСТИ SOC НА ОСНОВЕ МОДЕЛИ ЗРЕЛОСТИ

Развитые современные организации в своих бизнес-процессах применяют передовые технологии, требуют высококлассного подхода к управлению процессом киберзащиты независимо от назначения применяемых технических средств - информационных технологий (IT), систем промышленного управления (ICS), кибер-физических систем (CPS) или устройств IoT. Поэтому основной задачей специалисты ИБ определяют выбор стандартов и фреймворков в сфере информационных технологий, содержащих требования, установки и рекомендации по организации актуальных процессов киберзащиты и менеджмента информационной безопасности. Компании, под руководством которых функционируют центры оперативного реагирования на киберинциденты (SOCs), при их создании и поддержке эксплуатации аналогично руководствуются признанными задокументированными стандартами и рекомендациями. На сегодня проблематичным является вопрос описания в виде инструкций по внедрению собственных SOC по мере разности их функциональных элементов в зависимости от целей и масштабов внедрения, имеющихся финансовых ресурсов, модели оценки зрелости и возможностей оперативных центров безопасности, большинство из которых предлагаются лидерами IT индустрии в качестве коммерческой услуги. Целью данной работы является анализ функционирования моделей оценки зрелости и возможностей в управляющей стратегии развития ИБ организации и создания функциональной модели задачи оценивания уровня зрелости SOC на основе выбранной модели зрелости. Результаты внедрения такой модели позволяют использовать единый подход в процессе оценки уровня зрелости как отдельных доменов, так и SOC в целом независимо от выбора модели зрелости, анализируя расчеты от простых метрик достижения целей бизнес-ориентированных метрик. В дальнейшей декомпозиции модель позволяет сформировать конкретные требования к простым метрикам результативности, на которых основывается вычисления комплексных метрик, а также конкретно определять методы анализа проведенных подсчетов.

Ключевые слова: кибербезопасность, центр оперативного реагирования на киберинциденты, оценка, эффективность, модель зрелости и возможностей, метрика, функциональная модель.

FUNCTIONAL MODEL OF SOC MATURITY ASSESSMENT BASED ON A MATURITY MODEL

Leading modern organizations that use advanced technologies in their business processes require a high-level approach to managing the cybedefence process, regardless of the appointment of technical means usage - introspection technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or IoT devices. Therefore, the main task of IS specialists lies in the choice of standards and frameworks in the field of information technology, which contain requirements, guidelines and recommendations for the organization of up-to-date processes of cyberdefense and information security management. Security Operations Centers (SOCs), which functionate under the guidance of organizations, operate on the basis of admitted and documented usage of standards and recommendations. As for today, the problematic issue lies either in documenting instructions for the implementation of their own SOCs as they differ in functionality depending on goals and scale of implementation, available financial resources or models for assessing the maturity and capabilities of SOCs, most of which are poorly described and suggested with IT industry leaders as a commercial service. The purpose of this work is to analyze the functioning of maturity and capability assessment models in the management strategy of organization`s information security sphere and to create the functional model of assessing the level of SOC maturity, which is based on the chosen maturity model. The results of a such model`s implementation allow us to use a single approach in the process of assessing the maturity level of both individual domains and SOC in general, regardless of the choice of a maturity model with analyzing the calculations from simple metrics of achieving goals (Key Result Indicators, KRI) to business-oriented metrics. The subsequent model decomposition enables to formulate specific requirements for simple metrics on which the calculation of complex metrics is based, as well as more precisely determine the methods of analysis of the performed calculations.

Keywords: cybersecurity, center of operational response to cyber incidents, assessment, efficiency, capability maturity model, metrics, functional model.

Жилін Артем Вікторович, кандидат технічних наук, доцент кафедри Кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.
E-mail: zhylinartem@gmail.com.
Orcid ID: 0000-0002-4959-612X.

Жилин Артем Викторович, кандидат технических наук, доцент кафедры Кибербезопасности и применения информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Zhylin Artem, candidate of technical sciences, associate professor of the cyber security and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Голич Ганна Степанівна, інженер, Державний центр кіберзахисту, Київ, Україна.
E-mail: dckz_ggs@dsszzi.gov.ua.
Orcid ID: 0000-0003-0849-5127.

Голыч Анна Степановна, инженер, Государственный центр киберзащиты, Киев, Украина.

Holych Ann, engineer, State Centre of Cyberdefence, Kyiv, Ukraine.

Худинцев Микола Миколайович, кандидат фізико-математичних наук, доцент, в.о. начальника Державного центру кіберзахисту, Київ, Україна.
E-mail: dckz_hmm@dsszzi.gov.ua.
Orcid ID: 0000-0001-9659-2984.

Худынцев Николай Николаевич, кандидат физико-математических наук, доцент, и.о. начальника Государственного центра киберзащиты, Київ, Україна.

Khudyncev Mykola, candidate of physical and mathematical sciences, associate professor, the acting head of State Centre of Cyberdefence, Kyiv, Ukraine.