УДК 004.056
DOI: https://doi.org/10.17721/ISTS.2024.7.24-30

Олександр ТОРОШАНКО, канд. техн. наук, асист.
ORCID ID: 0000-0002-2354-0187
e-mail: toroshanko@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Юрій ЩЕБЛАНІН, канд. техн. наук ст. наук. співроб.
ORCID ID: 0000-0002-3231-6750
e-mail: y.shcheblanin@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Олег КУРЧЕНКО, канд. техн. наук , доц.
ORCID ID: 0000-0002-3507-2392
e-mail: kurol@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

ПОРІВНЯННЯ МОДЕЛЕЙ ЗРІЛОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ (КОМПАНІЇ)

Вступ. *Зростання зловмисної активності в інформаційному та кібернетичному просторах ставить перед керівниками підприємств (організацій) і власниками компаній додаткові завдання та вимоги щодо захисту своїх активів. Втрата активів, наприклад, фінансового або технологічного, може призвести до неможливості виконання компанією своєї базової функції – приносити прибуток.*

Методи. *Використано методи аналізу ризиків інформаційної безпеки.*

Результати. *Організації витрачають значні фінансові ресурси на придбання й експлуатацію технологій захисту, створюють відповідні структурні підрозділи, завданнями яких є оцінювання та забезпечення відповідного рівня інформаційної безпеки підприємства (компанії). Водночас існує ризик настання ситуації, коли, використовуючи сучасніші технології, зловмисники зможуть подолати систему захисту компанії та завдати неповоротних втрат як фінансових, так і репутаційних.*

Висновки. *Одним із напрямів розв'язання цієї проблеми є створення системи управління інформаційною безпекою (СУІБ), яка є складовою загальної системи управління організації (компанії) і ґрунтується на оцінюванні бізнес-ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки організації (підприємства). СУІБ містить організаційну структуру організації (компанії), її політики, питання планування, контроль за дотриманням вимог посадових обов'язків, впровадження сучасних практик, контроль та супроводження процесів ресурсів. Кращі світові практики, для оцінювання рівня інформаційної безпеки організації, рекомендують використовувати підхід, що базується на можливостях моделей зрілості процесів. Отримані результати можна використовувати для вдосконалення або оптимізації створеної системи інформаційної безпеки організації (компанії). Нині для організацій (компаній) доступний великий набір моделей оцінювання зрілості інформаційної безпеки, побудованих на схожих принципах. Причому реальне використання таких моделей досить обмежене, в першу чергу через слабке прив'язування до особливостей конкретних організацій.*

В роботі розглянуто моделі зрілості процесів, їхню структуру та можливості використання у процесі оцінювання рівня інформаційної безпеки.

Ключові слова: *модель, оцінювання зрілості, загроза, інформаційна безпека.*

Вступ

Зростання зловмисної активності в інформаційному та кібернетичному просторах ставить перед керівниками підприємств (організацій) і власниками компаній додаткові завдання та вимоги, щодо захисту своїх активів. Втрата активів, наприклад, фінансового або технологічного, може призвести до неможливості виконання компанією своєї базової функції – приносити прибуток.

Для досягнення зазначеної мети доцільно впроваджувати й активно використовувати сучасні інформаційні технології та рішення з інформаційної та кібернетичної безпеки. Саме такий підхід створює основу для якісного забезпечення безпеки основних процесів компанії

(організації). Керівники компаній зацікавлені, щоб реалізовані бізнес-процеси відповідали концепції захисту своїх активів, що полягає у зменшенні ймовірності кількості помилок або зловмисних дій із боку працівників компанії та бізнес-партнерів.

Ненадання належної уваги оцінюванню рівня інформаційної безпеки та захисту інформації в компанії може призвести до репутаційних ризиків і банкрутства. Відповідно діяльність, орієнтована на аналіз загроз і ризиків, є визначальною у побудові ефективної системи інформаційної та кібернетичної безпеки. Відповідно до статистики, витікання 20 % інформації з обмеженим доступом, що належить компанії, в 60 випадках зі 100 призводить до банкрутства підприємства (Гребенніков, & Щебланін, 2018).

Прийняття рішення щодо розроблення та впровадження системи управління інформаційною безпекою в організації має відповідати рівню організаційного та технологічного розвитку компанії, а саме її процесів забезпечення інформаційної безпеки. Вимоги до впровадження рішень з інформаційної та кібернетичної безпеки мають враховувати рівні зрілості процесів у конкретній організації (компанії).

Нині гостро постає питання підвищення рівня інформаційної безпеки підприємства, яка напряму впливає на залучення інвестицій і впровадження сучасних технологій.

Використання "моделей зрілості" дозволяє визначити рівень технологічного й організаційного розвитку компанії та, відповідно, її бізнес-процесів, розвиток інформаційних технологій (ІТ) компанії значно впливає на конкурентоспроможність, а забезпечення її базових показників інформаційної безпеки – на неперервну діяльність.

Мета статті **–** порівняти можливості використання моделей зрілості ІТ-процесів під час оцінювання рівнів інформаційної безпеки організації (компанії).

Методи

В роботі використано методи аналізу ризиків інформаційної безпеки.

Результати

Оцінювати та вдосконалювати свої розробки з питань інформаційної та кібернетичної безпеки компаніям може суттєво допомогти використання моделей зрілості процесів інформаційної безпеки.

Інструментом вимірювання стану процесу на основі набору метрик, які являють собою певні характеристики, є модель зрілості. Використання метрик, запропонованих у моделях, дає змогу оцінити стан процесів інформаційної безпеки (ІБ), що у свою чергу є характеристикою рівня зрілості. Після завершення оцінювання зрілості процесів, керівництво ухвалює відповідні рішення щодо впровадження заходів із підвищення рівня зрілості процесів інформаційної безпеки організації (компанії).

У практиці зарубіжних країн широко розвинене застосування моделей зрілості, які є як інструментом управління, так і інструментом оцінювання рівня інформаційної безпеки компанії.

Національні компанії зрідка використовують підхід оцінювання та забезпечення інформаційної безпеки, оснований на моделях зрілості, хоча в цьому є необхідність. Наприклад, стандарт ДСТУ ISO/IEC 27001 вимагає наявності в організації процедури аналізу ризиків. Тому виникає актуальне питання, яким чином забезпечити виконання вимог стандарту, з урахуванням обсягу робіт, рівня деталізації та масштабів організації (компанії). В більшості випадків фахівці з інформаційної безпеки орієнтуються на масштаб організації і дуже рідко аналізують рівень її організаційного та технологічного розвитку. Саме відповідь на це питання допоможе надати модель зрілості, яка враховує рівень зрілості процесів інформаційної безпеки організації (компанії).

Залежно від того, який рівень зрілості мають процеси інформаційної безпеки організації, є сенс впроваджувати ту чи іншу діяльність, наприклад, якщо рівень низький, то реалізація процедури оцінювання ризиків із залученням значних ресурсів є недоцільною і може полягати у експертному оцінюванні ризиків та визначенні найпріоритетніших напрямків безпеки. Якщо рівень зрілості процесів інформаційної безпеки в організації на високому рівні, тоді має бути реалізована процедура оцінювання ризиків з урахуванням спеціалізованих методів, шкал тощо.

Для оцінювання рівня інформаційної безпеки відомо більше 10 моделей, які мають свої переваги й недоліки, в межах статті розглянемо найвідоміші з них:

- Business Process Management Maturity Model (BPMM) – розроблена компанією Gartner Group;
- Open Information Security Management Maturity Model (O-ISM3) – розроблена незалежним консорціумом The Open Group;
- NISTIR-7358 методологія PRISMA – розроблена National Institute of Standards and Technology;
- Community Cyber Security Maturity Model (CCSMM) – розроблена The Center for Infrastructure Assurance and Security The University of Texas;
- Cybersecurity Capability Maturity Model (C2M2) – розроблена Міністерством енергетики (DOE) США (Department of Energy…, 2014).

ISSN 2707-1758

Модель Business Process Management Maturity Model (BPMMM) – це модель, розроблена фахівцями аналітичної компанії Gartner Group, яка виділяє чотири рівні – з нульового до третього.

Нульовий рівень – необхідність забезпечення інформаційної безпеки організацією належним чином не усвідомлена і формально таке завдання не ставиться. Служба ІБ не створена. Підрозділ інформаційних технологій використовує традиційні механізми й засоби захисту інформації в локальній обчислювальній мережі та сервісах інтернету, а також операційного середовища та додатків (операційні системи, СУБД, системи підтримки та прийняття рішень тощо).

Перший рівень – проблему забезпечення ІБ керівництво організації розгдядає лише у технічній площині. Службу ІБ не створено. Організаційні заходи підтримки ІБ не вживаються. Фінансування здійснюється в межах єдиного бюджету на ІТ. Підрозділ ІТ додатково до засобів рівня 0 може залучати засоби відмовостійкості, резервного копіювання інформації, джерела безперебійного живлення, міжмережні екрани, віртуальні приватні мережі, антивірусні засоби, засоби шифрування тощо.

Другий рівень – важливість забезпечення ІБ керівництвом організації усвідомлено та розглядається як взаємопов'язаний комплекс організаційних і технічних заходів. В організації впроваджено методики аналізу ризиків ІБ, які відповідають мінімальному рівню захищеності інформаційної системи. Визначено склад і структуру штатної служби ІБ. Розроблено політику безпеки організації. Фінансування, створення та підтримку системи забезпечення ІБ ведуть з окремого бюджету. Служба ІБ додатково до засобів рівнів 0 та 1 упроваджує засоби захисту від несанкціонованого доступу, системи виявлення вторгнень, засоби шифрування, а також організаційні заходи, які відповідають прийнятій політиці безпеки (зовнішній та внутрішній аудит ІБ, плани захисту та безперервності бізнесу, план дій у позаштатних ситуаціях тощо).

Третій рівень – проблему забезпечення ІБ організацією усвідомлено повною мірою. Поряд із бізнес-культурою існує поняття культури ІБ. Активно застосовуються методики повного кількісного аналізу ризиків ІБ та відповідні інструментальні засоби. Введено штатну посаду – керівника служби ІБ (CISO). Визначено склад і структуру групи внутрішнього аудиту ІБ (CISA), групи попередження та розслідування комп'ютерних злочинів, групи економічної безпеки. Керівництвом організації затверджено концепцію та політику ІБ, план захисту й інші нормативно-методичні матеріали та посадові інструкції. Фінансування виділяють виключно у межах окремого бюджету. Служба ІБ додатково до засобів рівнів 0–2 звертається до засобів централізованого управління ІБ і засобів інтеграції з платформами управління мережними ресурсами.

Отже, модель BPMMM є багатовимірна й дозволяє аналізувати процеси організації за такими критеріями: керівництво, персонал, стратегія, методики, IT тощо.

Модель Open Information Security Management Maturity Model розроблена незалежним консорціумом The Open Group і враховує вимоги ISO/IEC 27000.

Модель оцінює рівень зрілості функціонування процесів системи управління інформаційною безпекою організації (компанії) та орієнтована допомагати фахівцям з інформаційної безпеки оцінювати власну робочу інфраструктуру та планувати процеси управління інформаційною безпекою компанії (The Open Group Releases Maturity Model for Information Security Management).

Головною вимогою O-ISM3 є задокументованість, вимірюваність і керованість процесами управління інформаційною безпекою, також мають бути зафіксовані бізнес-цілі компанії, на основі яких визначають мету й основні завдання управління інформаційною безпекою. Модель O-ISM3 відрізняється від інших тим, що вона передбачає оцінювання зрілості всіх процесів (заходів безпеки), які використовують у системі управління інформаційною безпекою. Тому керувати контролем (згідно з процесним підходом) можливо за допомогою оцінювання рівня його зрілості.

В моделі O-ISM3 застосовано чотири рівні управління інформаційною безпекою, саме вони дозволяють оцінити зрілість процесів ІБ (The Open Group Releases Maturity Model for Information Security Management):

- базовий, який належить до загального управління та включає три види контролю;
- стратегічний (керівництво і забезпечення) рівень, де встановлюють стратегічні цілі, здійснюють координаційні дії та розробляють механізм забезпечення ресурсами, який містить чотири види контролю;
- тактичний (впровадження й оптимізація) рівень, на якому розробляють і впроваджують систему управління інформаційною безпекою за допомогою встановлення специфічних цілей та управління ресурсами, включає 12 видів контролю;
- операційний (виконання і звітність) рівень, цілей якого досягають технічними процесами та передбачають 26 видів контролю.

Процеси управління за моделлю O-ISM3 класифіковано на п'ять рівнів зрілості:

1-й рівень зрілості – Initial (початковий);

2-й рівень зрілості – Managed (керований);

3-й рівень зрілості – Defined (орієнтований);

4-й рівень зрілості – Controlled (контрольований);

5-й рівень зрілості – Optimized (оптимізований).

Метрики моделі розділено на такі типи: діяльність, масштаб, відсутність, результативність, навантаження, якість, ефективність (Activity, Scope, Unavailability, Effectiveness, Load, Quality, Efficiency) й описують ресурсовитратність обраного методу управління. Поточний рівень процесу, залежить від наявної документації та метрик, які використовують для управління ним.

Отже, модель O-ISM3 розроблена для різних типів організацій (компаній), комерційних фірм, неурядових організацій та

- може бути використана в організації (компанії) незалежно від розміру, контексту та її ресурсів;
- вимагає високої професійної підготовки фахівців з інформаційної безпеки та потребує високої деталізації процесів інформаційної безпеки;
- дозволяє організаціям (компаніям) визначати пріоритетність інвестицій у безпеку та оптимізувати їх за потреби;
- дозволяє безперервно покращувати систему управління інформаційною безпекою на основі використання метрик (Рой, Рябчун, & Єрмошин, 2020).

Модель зрілості NISTIR 7358 – методологія PRISMA, яку розроблено National Institute of Standards and Technology, засновано на Capability Maturity Model (CMM) Software Engineering Institute (SEI).

Методологія PRISMA (Гребенніков, & Щебланін, 2018) створена з метою виявлення й оцінювання слабких місць у процесах управління інформаційною безпекою, забезпечення рентабельності впровадження СУІБ, оцінювання комерційних пропозицій у вказаній сфері та встановлення можливості їхнього застосування в державних ІТ-системах США.

Запропонована модель представляє собою підхід, оснований на процесах оцінювання ризиків та оцінювання ефективності управління ІБ.

Особливістю моделі PRISMA є те, що документи з ІБ оцінюють за такими основними напрямами ІБ (Computer security resource center):

- управління інформаційною безпекою та культура;
- інформаційне планування безпеки;
- розуміння процесів безпеки, навчання й освіти;
- ресурси та бюджет;
- управління життєвим циклом системи безпеки;
- сертифікація та акредитація системи інформаційної безпеки;
- захист критичної інфраструктури;
- інциденти та реагування на них;
- засоби безпеки та контролю.

В результаті використання моделі PRISMA користувач отримує таблицю, яка відображає оцінку зрілості процесів ІБ. В моделі PRISMA застосовано п'ять рівнів, а саме:

1-й рівень зрілості – Policies (політики);

2-й рівень зрілості – Procedures (процедури);

3-й рівень зрілості – Implementation (впровадження);

4-й рівень зрілості – Test (тестування);

5-й рівень зрілості – Integration (інтеграція).

Вищого рівня зрілості ІБ досягають лише тоді, коли попереднього рівня зрілості вже досягнуто. П'ятий рівень зрілості являє собою найвищий рівень забезпечення інформаційної безпеки.

Для оцінювання зрілості ІБ організації (компанії), проводять розгляд та аналіз документації з ІБ, беруть інтерв'ю у працівників організації та оцінюють розбіжності кожного з напрямів ІБ.

Для оцінювання напрямів ІБ вводять критерії, які мають бути документально зафіксовані. Ці критерії являють собою метрики моделі й застосовуються на кожному з рівнів зрілості.

Оцінка виконання організацією критерію, тобто оцінка метрики, може мати таку класифікацію: "Відповідний", "Частково відповідний", "Невідповідний".

Оцінка зрілості ІБ починається з першого рівня (Policies (політики)), якщо для всіх розглянутих документів критерію оцінка "Невідповідний", то весь рівень отримує ту саму оцінку за вказаним критерієм. Однак, якщо у критерії для деяких документів є оцінка "Відповідний", але оцінка одного або більшої кількості документів "Частково відповідний" / "Невідповідний", тоді загальна оцінка критерію для рівня буде "Частково відповідний".

Отже, методологію PRISMA, як варіант, можна застосовувати в оцінюванні процесів СУІБ:

- незважаючи на масштаби організації (компанії) та її ресурси;
- коли основою для оцінювання рівня зрілості СУІБ компанії є документи, в яких описано та затверджено відповідні бізнес-процеси;
- коли рівень оцінювання процесів має значення "Частково відповідний" і визначається у відсотках виконаної реалізації.

ISSN 2707-1758

Модель оцінювання зрілості процесів забезпечення інформаційної безпеки (Community Cyber Security Maturity Model). Зусилля урядових організацій і приватних компаній у США були зосереджені на розробленні програми безпеки, яка надала б їм інструмент спільного прогнозування кібератак, їх виявлення, реагування на них і відновлення процесів організацій (компаній).

Завдання полягало не лише в тому, щоб мати інформацію, де вони в даний час перебувають у плані їхньої підготовки до відбиття кібератаки, але і де вони мають перебувати, щоб покращити свій поточний стан. Для розв'язання поставленого завдання була створена суспільна модель зрілості кібербезпеки – Community Cyber Security Maturity Model .

Модель розробляли з урахуванням досвіду використання моделей зрілості програмного забезпечення Capability Maturity Model (CMM або SW-CMM) та інженерних систем безпеки Systems Security Engineering Capability Maturity Model (SSE-CMM), що дозволяло розробити варіанти взаємодії різних організацій (компаній) між собою, спрямовані на підвищення ефективності протидії кіберзлочинності (The Systems Security Engineering Capability Maturity Model). Така модель враховує не лише метрики, а й технології, відомі вразливості та методи тестування, спільне використання яких дозволить оцінити поточний стан рівня інформаційної безпеки організації (компанії).

В розробленій моделі виділено рівні зрілості, які враховують типи загроз і діяльність із рівнів (The Systems Security Engineering Capability Maturity Model):

1-й рівень зрілості – Security Aware (про безпеку відомо);

2-й рівень зрілості – Process Development (розвиток процесів);

3-й рівень зрілості – Information Enabled (встановлено інформування);

4-й рівень зрілості – Tactics Development (розвиток тактики);

5-й рівень зрілості – Full Security Operational Capability (повна безпека експлуатованих можливостей).

Для оцінювання рівня зрілості процесів організації (компанії) в моделі запропоновано такі критерії:

- перелік загроз, які слід розглядати та які можуть бути усунені (The Threat Addressed);
- метрики: громадяни, керівництво, виробництво (Citizens, Government, Industry);
- інформаційний обмін (Information Sharing);
- технології безпеки (Technology);
- навчання (Training);
- тестування (Test).

Cybersecurity Capability Maturity Model (C2M2) – модель зрілості можливостей кібербезпеки є інструментом для оцінювання й покращення рівня кібербезпеки. Була розроблена 2012 р. енергетичним сектором Міністерства енергетики США.

Використання C2M2 дозволяє організаціям усіх секторів, типів і розмірів оцінити та вдосконалити свої програми кібербезпеки та підвищити їхню операційну стійкість. C2M2 зосереджено на впровадженні й управлінні методами кібербезпеки, пов'язаними з активами IT та операційних технологій (OT), а також із середовищами, в яких вони працюють.

Модель зрілості можливостей ES-C2M2 використовує чотирирівневу структуру для оцінювання 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 й невизначеними політиками безпеки. На другому етапі акцент роблять на впровадження стандартів безпеки і формалізованих процесів управління. Останній етап передбачає практично повністю автоматизоване управління безпекою підприємства. На цьому етапі досягають максимально можливого рівня захисту від кіберзагроз, а сама організація отримує стійкість до кібератаки.

В таблиці наведено порівняльний аналіз розглянутих моделей зрілості за такими критеріями як: тип моделі, кількість рівнів зрілості, масштаб моделі та рівень професійної підготовки працівників.

Розглянуті моделі зрілості створено з метою розв'язання конкретних задач і завдань. Вони використовують процесний підхід для визначення рівня зрілості, причому відсутнє єдине трактування поняття зрілості, в силу того, що кожна модель орієнтована на розв'язання конкретного завдання.

Для визначення рівня інформаційної безпеки необхідно враховувати конкретний набір метрик, які дозволяють розкрити рівень зрілості процесів інформаційної безпеки. Кожна модель пропонує використовувати свій набір метрик для оцінювання зрілості процесів, збігів серед яких практично немає.

Таблиця

Порівняння моделей зрілості оцінювання рівня ІБ

Критерії оцінювання моделей	BPMMM	O-ISM3	NISTIR 7358	CCSMM	C2M2
Тип моделі	Описова	Описова	Описова	Описова	Описова
Кількість рівнів зрілості	4	5	5	4	4
Масштаб моделі	Уся структура організації	СУІБ організації	Документація ІБ організації	Процеси ІБ організації	ІТ-активи підприємства
Рівень професійної підготовки працівників	Середній	Високий	Середній	Низький	Середній

До недоліків можна віднести такий: розглянуті моделі не враховують рівень забезпеченості ресурсами процесів інформаційної безпеки організації. Водночас такі критерії, як розвиненість і стабільність процесів управління українських і зарубіжних компаній мають значні відмінності, що вимагає проведення адаптації моделей зрілості для їхнього використання.

Дискусія і висновки

Розглянуті моделі зрілості процесів рекомендуються до використання кращими світовими практиками у сфері інформаційної безпеки. Вони дозволяють керівникам компаній контролювати стан інформаційної безпеки, своєчасно реагувати на інциденти інформаційної безпеки й розробляти напрями модернізації ІБ та СУІБ організації (компанії).

Результати оцінювання зрілості процесів СУІБ відповідають на такі важливі питання:

- рівень документування бізнес-процесів і процесів ІБ;
- яким способом і з використанням яких ресурсів забезпечуються вимоги до підтримки того чи іншого процесу на заданому рівні;
- чи дотримується організація (компанія) рекомендацій кращих практик зі створення та підтримки функціонування СУІБ тощо.

Проведені дослідження показали, що для оцінювання можливості впровадження розглянутих моделей зрілості на практиці є потреба глибокого розуміння базової моделі організації (тобто треба знати, для якого переліку завдань вона розроблялась), не можливо впевнено стверджувати, чи можна її застосовувати для розв'язання наших завдань.

Досліджені в роботі моделі зрілості процесів доцільно використовувати як еталон для розроблення моделі зрілості, беручи за основу власну базову модель з урахуванням метрик, властивих конкретному об'єкту. Оптимальним рішенням нині виглядає впровадження будь-якої з існуючих моделей оцінювання з подальшою її адаптацією і розширенням під власні потреби.

Подальші дослідження доцільно проводити, створюючи модель оцінювання, яка враховуватиме національну нормативно-правову базу, рівень підготовки фахівців організації (компанії) та обсяг фінансування процесів ІБ.

Внесок авторів: Олександр Торошанко – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Юрій Щебланін – збір емпіричних даних та їхня валідація; Олег Курченко – емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Гребенніков, А., & Щебланін, Ю. (2018). Аналіз використання моделей зрілості процесів у ході оцінювання рівня інформаційної безпеки. *Сучасний захист інформації*, 1(33), 33–37.

Рой, Я. В., Рябчун, О. П., & Єрмошин, В. В. (2020). Модель зрілості можливостей системи кібербезпеки на об'єктах критичної інфраструктури енергетичного сектору ES-C2M2. *Кібербезпека: освіта, наука, техніка*, 2(10), 67–72.

Department of Energy: Cybersecurity Capability Maturity Model (2014). Version 1.1, Department of Homeland Security. https://www.energy.gov/ceser/cybersecurity-capability-maturity-/model-c2m2

REFERENCES

Department of Energy: Cybersecurity Capability Maturity Model (2014). Version 1.1, Department of Homeland Security. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

Grebennikov, A., Shcheblanin, Yu. (2018). Analysis of the use of process maturity models during the assessment of the level of information security. *Modern information protection*, 1(33), 33–37 [in Ukrainian].

Roy, Y. V., Ryabchun, O. P., & Yermoshin, V. V. (2020). Maturity model of cyber security system capabilities at critical infrastructure facilities of the energy sector ES-C2M2. *Cyber security: education, science, technology*, 2(10), 67–72 [in Ukrainian].

Отримано редакцією журналу / Received: 17.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24

Oleksandr TOROSHANKO, PhD (Engin.), Assist.
ORCID ID: 0000-0002-2354-0187
e-mail: toroshanko@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Yurii SHCHEBLANIN, PhD (Engin.), Senior Researcher
ORCID ID: 0000-0002-3231-6750
e-mail: y.shcheblanin@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Oleh KURCHENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-3507-2392
e-mail: kurol@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

COMPARISON OF ORGANIZATION (COMPANY) INFORMATION SECURITY PROCESS MATURITY MODELS

Background. *The increase in malicious activity in the information and cyberspace poses a challenge to the leaders of enterprises (organizations) and the leaders of companies with additional tasks and benefits to protect their assets. The loss of assets, for example, financial or technological, can make it impossible for the company to achieve its basic function - to generate profits.*

Methods. *The work used the information security risk analysis method.*

Results. *Creation and promotion of current information security systems. Organizations spend significant financial resources on the development and operation of technology protection, create various structural subdivisions, such as the assessment and provision of a similar level and information security of the enterprise (company). At the same time, there is a real risk of the current situation if malicious and more current technologies are able to rig the system to protect the company and cause irrevocable costs, both financial and reputational.*

Conclusions. *One of the main directions of this problem is the creation of an information security management system (ISMS), which is a warehouse management system for an organization (company) and is assessed without bears the risks of creating, implementing, operating, operational monitoring, review, support and thorough information security organizations (enterprises). The ISMS includes the organizational structure of the organization (company), its policies, nutritional planning, monitoring of labor costs, promotion of daily practices, control and support of resource processes. As a best practice, to assess the level of information security of an organization, it is recommended to use a different approach that is based on the capabilities of process maturity models. The extracted results can be used to thoroughly and optimize the created information security system of the organization (company). There are currently a wide range of information security maturity assessment models available to organizations based on similar principles. In this case, it is realistic to select such models to be limited, first and foremost through a weak connection to the characteristics of specific organizations.*

The work examines models of the maturity of processes, their structure and the ability to evolve in the course of assessing the level of information security.

Keywords: *model, maturity assessment, threat, information security.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.