УДК 004.056

**А.Б. Гребенніков, Ю.М. Щебланін**

# АНАЛІЗ ВИКОРИСТАННЯ МОДЕЛЕЙ ЗРІЛОСТІ ПРОЦЕСІВ В ХОДІ ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розвиток технологій та методів незаконного заволодіння інформацією, у свою чергу, потребує створення нових систем інформаційної безпеки та розробки методичного апарату оцінки їх якості. В роботі проаналізовано методику оцінки інформаційної безпеки підприємства на базі моделей зрілості процесів інформаційної безпеки та запропоновано рекомендації щодо їх впровадження.

*Ключові слова:* інформаційна безпека, модель зрілості, IT- процеси.

**Постановка проблеми**

Діяльність будь-якого підприємства (організації) спрямована в першу чергу на отримання прибутку. На досягненні цієї мети сфокусовані основні бізнес-процеси організації (виробництво, продаж, логістика). Також існує ряд підтримуючих процесів, до яких відносяться інформаційні технології та інформаційна безпека, які спрямовані на забезпечення інфраструктури для функціонування основних процесів. Логічно припустити, що керівництво підприємства зацікавлене в тому, щоб процеси всередині організації були їм підконтрольні, функціонували так, як були задумані, а кількість помилок або зловмисних дій з боку співробітників організації, бізнес-партнерів, а також інших сторін, залучених в бізнес - процеси організації, була мінімальною.

Зневага питаннями оцінювання інформаційної безпеки та захисту інформації може призвести до повного банкрутства. Тому аналіз загроз і ризиків є визначальним при створенні ефективної системи інформаційної безпеки. Встановлено, що витік 20% комерційної інформації в 60 випадках зі 100 призводить до банкрутства підприємства [1].

Постановка завдання щодо впровадження та просування будь-якого процесу управління в організації повинна відповідати рівню організаційного та технологічного розвитку підприємства, і зокрема, процесів забезпечення інформаційної безпеки. Вимоги до реалізації заходів з безпеки повинні формулюватися з урахуванням рівня зрілості цих процесів в конкретній організації. При цьому не доцільно намагатися вимагати потужну сучасну технологію, якщо рівень організації не відповідає рівню технології.

Для визначення стадії організаційного та технологічного розвитку організації та її процесів у світовій практиці існує поняття «модель зрілості».

**Метою статті** є аналіз використання моделей зрілості процесів в оцінюванні рівня інформаційної безпеки.

**Виклад основного матеріалу**

Модель зрілості використовується як інструмент вимірювання стану процесу на основі набору метрик, які являють собою певні характеристики. Оцінка цих метрик за певною шкалою дозволяє зрозуміти стан процесів організації, яка і буде характеризувати рівень зрілості. Після отримання оцінки зрілості можна виробити необхідні заходи для підвищення рівня зрілості процесів і організації в цілому.

У зарубіжній практиці застосування моделей зрілості як інструменту управління широко розвинене, в тому числі моделі зрілості використовуються і для оцінки рівня інформаційної безпеки підприємства.

В українській практиці не склалася необхідність використання моделей зрілості, проте в цьому існує необхідність. Наприклад, в стандарті ISO 27001:2017 існують вимоги до наявності в організації процедури аналізу ризиків. Завжди виникає питання, як же виконати ці вимоги, в якому обсязі і на якому рівні деталізації для різних за величиною компаній. Дуже часто менеджери з інформаційної безпеки звертають увагу саме на розмір організації і майже ніколи на рівень її організаційного та технологічного розвитку. Відповідь на це

питання допоможе дати модель зрілості, на основі оцінки рівня зрілості процесів інформаційної безпеки підприємства.

Якщо рівень зрілості організації низький, детальне опрацювання процедури оцінки ризиків не має сенсу, і може полягати в експертній оцінці ризиків та визначенні пріоритетних напрямків безпеки. В організаціях, де рівень зрілості процесів інформаційної безпеки на високому рівні, процедура оцінки ризиків повинна не тільки функціонувати, а й мати детальне опрацювання методики, шкал, і т.ін.

В світовій практиці відомо більше 10 моделей зрілості оцінки рівня інформаційної безпеки, однак в рамках статті розглянемо деякі з них:

- 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.

**Модель «Open Information Security Management Maturity Model** (O-ISM3)», розроблена незалежним консорціумом The Open Group, повністю враховує вимоги ISO/IEC 27000:2013.

Модель O-ISM3 оцінює зрілість функціонування існуючих процесів системи управління інформаційною безпекою організації. Модель розроблялася як методика, яка допоможе менеджерам з інформаційної безпеки оцінити своє власне робоче середовище і спланувати процеси управління інформаційною безпекою [2].

Модель O-ISM3 вимагає, щоб процеси системи управління інформаційною безпекою (СУІБ) були задокументовані, вимірювалися і керувалися. Також O-ISM3 вимагає, щоб були зафіксовані бізнес-цілі організації, і на їх основі визначено мету і завдання інформаційної безпеки. Відмінною особливістю моделі O-ISM3 є те, що вона заснована на оцінці зрілості кожного з використаних в СУІБ процесів (заходів безпеки). Тобто щоб управляти контролем (згідно процесного підходу) необхідно оцінювати рівень його зрілості.

Модель O-ISM3 розглядає 4 рівні управління СУІБ організації, за якими проводиться оцінка зрілості [2]:

- базовий, для загального управління - 3 контролі;
- стратегічний (керівництво і забезпечення), на якому встановлюються стратегічні цілі, здійснюється координація діяльності та забезпечення ресурсами - 4 контролі;
- тактичний (впровадження і оптимізація), який має справу з розробкою і реалізацією СУІБ, встановленням специфічних цілей та управлінням ресурсами - 12 контролів;
- операційний (виконання і звітність), який має справу з досягненням певних цілей за допомогою технічних процесів - 26 контролів.

У моделі O-ISM3 процеси системи управління класифікуються за 5 рівнями зрілості:

Рівень зрілості 1 - Початковий (Initial);

Рівень зрілості 2 - Керований (Managed);

Рівень зрілості 3 - Описаний (Defined);

Рівень зрілості 4 - Контрольований (Controlled);

Рівень зрілості 5 - Оптимізований (Optimized).

Метрики поділяються на сім можливих типів (Activity, Scope, Unavailability, Effectiveness, Load, Quality, Efficiency) і описують витратність і ефективність обраного методу управління. З точки зору аудитора рівень, досягнутий процесом, залежить від документації, і метрики використаної для управління ним.

Таким чином модель O- ISM3 розроблена для будь-яких типів організацій, комерційних фірм, неурядових організацій, виробничих підприємств:

- може бути застосовна до будь-якої організації незалежно від розміру, контексту і ресурсів;

- вимагає високої кваліфікації менеджерів з інформаційної безпеки і високої деталізації процесів інформаційної безпеки;

- дозволяє організаціям розташувати по пріоритетах і оптимізувати свої інвестиції в безпеку;

- дозволяє безперервно покращувати СУІБ на основі використання метрик.

**Модель зрілості NISTIR - 7358** методологія PRISMA, розроблена National Institute of Standards and Technology, заснована на Capability Maturity Model (CMM) Software Engineering Institute (SEI).

Методологія PRISMA [3] розроблена для проведення дослідження та ідентифікації слабких місць інформаційної безпеки, забезпечення рентабельності ІБ, оцінки комерційних технологій безпеки і можливості застосування їх в IT- системах Федеральними агентствами і відомствами США.

Модель являє собою систематизований підхід, заснований на оцінці ризиків та оцінці ефективності управління ІБ.

Відмінною особливістю моделі PRISMA є те, що вона основана на оцінці документації ІБ за певними 9 -ти основними областями ІБ. В результаті на виході PRISMA маємо оцінну таблицю, яка оцінює зрілість цих областей ІБ:

- інформаційне управління безпекою та культура;
- інформаційне планування безпеки;
- розуміння безпеки, навчання та освіта;
- бюджет і ресурси;
- управління життєвим циклом безпеки;
- сертифікація та акредитація;
- захист критичної інфраструктури;
- інциденти і екстрене реагування на них;
- засоби безпеки, контролі.

PRISMA використовує п'ять рівнів зрілості, де п'ятий рівень зрілості представляє найвищий рівень забезпечення інформаційної безпеки:

Рівень зрілості 1 - Політики (Policies);

Рівень зрілості 2 - Процедури (Procedures);

Рівень зрілості 3 - Впровадження (Implementation);

Рівень зрілості 4 - Тестування (Test);

Рівень зрілості 5 - Інтеграція (Integration).

Більш високий рівень зрілості може бути досягнутий тільки, якщо попередній рівень зрілості вже досягнутий.

Визначення зрілості інформаційної безпеки організації будується на розгляді документації з ІБ, інтерв'ювання персоналу організації і виконання аналізу розбіжності кожної з 9 -ти областей ІБ.

Оцінка кожної з 9 –ти областей здійснюється за відповідними критеріями, які повинні бути зафіксовані документально. Ці критерії і є метриками моделі. Для кожного критерію проводиться оцінка на кожному з рівнів зрілості (Політики (Policies) - Процедури (Procedures) - Впровадження (Implementation) - Тестування (Test) - Інтеграція (Integration)).

Оцінка виконання критерію, тобто оцінка метрики, може бути наступна: «Відповідний», «Частково відповідний», «Не відповідний».

Оцінювання починається з самого нижнього рівня (Політики (Policies)), якщо для всіх розглянутих документів критерію оцінка «Не відповідний», то весь рівень отримує таку ж оцінку за вказаним критерієм. Якщо в критерії для деяких документів оцінка «Відповідний», але оцінка одного або більше документа «Частково відповідний» / «Не відповідний», тоді загальна оцінка критерію для рівня буде «Частково відповідний».

Таким чином методологія PRISMA може бути застосована для оцінки процесів СУІБ:

- в будь-якій організації незалежно від розміру і ресурсів;

- оцінка рівня зрілості СУІБ організації ґрунтується на затверджених документах, тобто

якщо процеси не задокументовані, то для моделі їх використовувати неможливо;

- рівень оцінки «Частково відповідний» визначається у відсотку реалізації.

**Модель оцінки зрілості процесів забезпечення інформаційної безпеки Community Cyber Security Maturity Model.** Державним та комерційним організаціям США було потрібно розробити програму безпеки, яка дозволила б їм спільно ефективно попереджати, виявляти, реагувати і відновлювати свої процеси після кібератак. Стояло завдання знати не тільки, де вони в даний час знаходяться в плані їх підготовки, але де вони мають знаходитись, щоб мати можливість покращити свій поточний стан. Саме для цієї мети була розроблена суспільна модель зрілості кібербезпеки - Community Cyber Security Maturity Model [3, 4].

Модель створена на основі досвіду використання двох моделей зрілості Capability Maturity Model (CMM або SW- CMM) для програмного забезпечення та інженерних систем безпеки Systems Security Engineering Capability Maturity Model (SSE - CMM) для побудови взаємодії різних організацій між собою в напрямку ефективної протидії кіберзлочинності [4].

Модель враховує не тільки метрики, а й технології, вразливості, тести, які можуть бути використані разом з метриками для вимірювання поточного стану рівня інформаційної безпеки.

Рівням зрілості в моделі були присвоєні назви, які характеризують типи загроз і діяльність, які вирішуються на кожному з рівнів:

Рівень зрілості 1 - Про безпеку відомо (Security Aware);

Рівень зрілості 2 - Розвиток процесів (Process Development);

Рівень зрілості 3 - Встановлено інформування (Information Enabled);

Рівень зрілості 4 - Розвиток тактики (Tactics Development);

Рівень зрілості 5 - Повна безпека експлуатованих можливостей (Full Security Operational Capability).

Визначення рівня зрілості оцінюватиметься за розробленими в моделі критеріям, а саме:

- загрози, які слід розглядати (The Threat Addressed);
- метрики: Керівництво, Виробництво, Громадяни (Metrics: Government, Industry, Citizens);
- інформаційний обмін (Information Sharing);
- технології безпеки (Technology);
- навчання (Training);
- тестування (Test).

Розглянуті моделі зрілості розроблені і застосовуються в основному в США та Європі. В Україні застосування таких моделей ускладнено в силу ряду причин.

Зокрема, розвиток інформаційної безпеки в українських організаціях знаходиться на низькому рівні і часто вимоги, які розглядаються в зазначених моделях не реалізовані. Наприклад, моделі не враховую забезпеченість ресурсами для організації процесів інформаційної безпеки. Так само, розвиненість і стабільність процесів управління зарубіжних організацій і українських сильно відрізняється.

Розглянувши описані вище моделі зрілості, стає очевидним той факт, що кожна з них розроблялася для вирішення конкретних завдань і на основі певної постановки задачі (назвемо її базовою моделлю). Інакше кажучи, представлені моделі зрілості вирішували деякі завдання, які стояли перед виконавцями. А для цього проблематику потрібно представити у вигляді моделі.

У випадку з моделлю зрілості О- ISM3, стояло питання оцінки стану існуючих процесів СУІБ, і хоча модель повністю сумісна з вимогами ISO 27001, COBIT, ITIL немає чіткого розуміння яка базова модель процесу використовувалася. Таке ж зауваження висувається і до решти моделей зрілості.

Модель NIST методологія PRISMA розроблена для проведення дослідження та ідентифікації слабких місць інформаційної безпеки, забезпечення рентабельності ІБ, оцінки

комерційних технологій безпеки і можливості їх застосування в IT- системах Федеральними агентствами і відомствами США.

Модель CC SMM розроблена як суспільна модель зрілості кібер-безпеки для побудови механізмів взаємодії різних організацій співтовариства між собою в напрямку ефективної протидії кіберзлочинності.

Таким чином, для розуміння можливості застосування будь-якої з моделей зрілості на практиці, без розуміння базової моделі, однозначно сказати чи можна її застосовувати для наших завдань, складно. Вбачається, що для вирішення власних завдань з безпеки слід врахувати досвід створення моделей зрілості і розробити власну модель.

У розглянутих моделях кількість рівнів оцінки зрілості становить 5, за винятком моделі Gartner, в якій 6 рівнів.

Назва рівнів, говорить про розвиток стану організацій від початкового стану, на якому процесами не займаються взагалі або займаються слабо, до верхнього рівня, де в бізнес повністю інтегровані і оптимізовані оцінювані процеси. Цікавим винятком є модель NIST методологія PRISMA, в якій рівні названі відповідно до загальної теорії стратегічного управління, і відображають еволюцію управління в організації.

Метрики в кожній моделі свої, збігів практично не виявлено. Це й зрозуміло, кожна модель зрілості розроблялася під конкретні цілі, вирішує конкретні завдання. Відсутність збігів може бути наслідком того, що в основі лежать різні базові моделі.

В наступних дослідженнях доцільно провести аналіз використання моделі зрілості процесів міжнародного стандарту COBIT в процесі оцінки рівня інформаційної безпеки підприємства (організації).

**Висновок**

Розглянувши кілька моделей зрілості можна зробити наступні висновки:

- єдиного трактування поняття зрілості немає, кожна модель вирішує власну проблематику;
- застосування розроблених моделей зрілості без розуміння базової моделі (тобто для вирішення яких питань вона розроблялася і на основі якої постановки задачі) - важко;
- модель зрілості повинна враховувати цілком конкретний набір метрик, через які розкривається рівень зрілості організації;
- слід розробляти власну модель зрілості, на основі власної базової моделі з необхідними для конкретного об'єкту метриками.
- розглянуті варіанти моделей зрілості корисно використовувати як зразок.

**Список використаної літератури**

1. Втрати великих компаній Британії від хакерських атак за 4 роки становили 52 млрд. доларів. [Електрон. ресурс]: - Режим доступу: https://www.rbc.ua/ukr/news/poteri-krupnyh-kompaniy-britanii-hakerskih-1492003702.html.

2. The Open Group Releases Maturity Model for Information Security Management, SAN FRANCISCO. April 11, 2011. [Електрон. ресурс]: - Режим доступу: http://www.opengroup.org/.

3. Computer security resource center. [Електрон. ресурс]: - Режим доступу: https://csrc.nist.gov/Publications.

4. The Community Cyber Security Maturity Model. [Електрон. ресурс]: - Режим доступу: https://pdfs.semanticscholar.org/c76f/bfde67b7afcbae58ee7f2323fa9746d32f80.pdf.

5. The Systems Security Engineering Capability Maturity Model. [Електрон. ресурс]: - Режим доступу: https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf/.

6. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [Електрон. ресурс]: - Режим доступу: http://www.isaca.org/COBIT/Pages/default.aspx?utm_source=informz-25-January-2013-COBIT-Focus-Vol-1&utm_medium=email&utm_campaign=cobit-focus 30.01.2013, 15-00 13.

7. Cobit® 4.1. Framework. Control Objectives. Management Guidelines. MaturityModels. IT GovernanceInstitute. (Методология. Цели контроля. Руководство по управлению. Модели зрелости процессов. Институт управления ИТ) ISBN 1-933284-72-2. USA, 2011, 196 p.

Надійшла: 22.01.2018 Рецензент: к.т.н. Довбешко С.В.