DOI: 10.32347/2412-9933.2025.61.66-75
УДК 005.334

Максимов Антон Євгенійович
Викладач кафедри комп'ютерних наук та системного аналізу,
https://orcid.org/0009-0002-0411-8164
Черкаський державний технологічний університет, Черкаси

АНАЛІЗ СТАНДАРТІВ УПРАВЛІННЯ РИЗИКАМИ ТА ЇХ ВИКОРИСТАННЯ В ІТ-ПРОЄКТАХ

Анотація. *Управління ризиками є важливим аспектом успішної реалізації проєктів у сфері інформаційних технологій, оскільки ІТ-проєкти схильні до високого рівня невизначеності та складності. Недостатній рівень управління ризиками може призвести до суттєвих втрат, перевищення бюджету, затримок у термінах реалізації проєктів та зниження якості кінцевого продукту. У зв'язку з цим виникає потреба у застосуванні надійних стандартів, які б забезпечили ефективне виявлення, аналіз і моніторинг ризиків протягом усього життєвого циклу ІТ-проєкту. У дослідженні представлено взаємозв'язок між стандартами, методологіями та методами управління ризиками в проєктах. Також у межах дослідження здійснено порівняння стандартів управління ризиками ISO 31000, ISO 27001, PMBOK, NIST SP 800-53 за ключовими параметрами, такими як: сфера застосування, процеси управління ризиками, підходи до ідентифікації та оцінки ризиків, а також рівень гнучкості та можливість адаптації під конкретні проєкти. Проаналізовано переваги і недоліки сучасних стандартів управління ризиками в ІТ-проєктах, що відображено за допомогою діаграм. У результаті дослідження встановлено, що стандарт ISO 31000 і PMBOK підходять для широкого кола ІТ-проєктів завдяки своїм гнучким підходам до управління ризиками та чітким методологічним рекомендаціям. Водночас стандарт NIST SP 800-53 більше орієнтований на кібербезпеку і детальніше розглядає ризики інформаційної безпеки, що робить його корисним для проєктів у цій галузі. Для ефективного управління ризиками в ІТ-проєктах слід використовувати комплексний підхід, що включає адаптацію елементів різних стандартів. Поєднання гнучких і детальних рекомендацій дає змогу розробити надійну стратегію для зменшення ймовірності та впливу ризиків на проєкт, забезпечуючи, тим самим, його успішну реалізацію. У висновках зазначено, що стандарт ISO 31000 є найбільш адаптивним з проаналізованих стандартів, оскільки на початкових етапах його впровадження він легше інтегрується в наявні системи. Отже, цей стандарт може слугувати основою для подальшого впровадження інших стандартів, які будуть доповнювати один одного завдяки наявності різногалузевих норм у рамках ISO.*

Ключові слова: управління ризиками; ІТ-проєкти; стандарти управління ризиками; ISO 31000; ISO 27001; NIST SP 800-53; PMBOK; аналіз ризиків; інформаційні технології

Вступ

У сучасних умовах глобальної економічної нестабільності перспективи будь-якого підприємця або підприємства залежать від вирішення двох головних питань: як запобігти потенційним загрозам та як ефективно управляти негативними наслідками невизначеності. У контексті аналізу ризиків, невизначеність розглядається як первинний фактор, у той час як ризик є вторинним фактором. Існує прямий зв'язок між рівнем невизначеності та рівнем ризику: зі зростанням невизначеності зростає й ризик. Проте обидва ці фактори відіграють ключову роль у підприємницькій діяльності. Згідно з думкою дослідників основна відмінність між цими явищами полягає у можливості їх вимірювання і оцінювання: невизначеність вимірювати неможливо або вкрай складно, в той час як ризик можна оцінити [1]. Більш важливою відмінністю між цими двома явищами є можливість впливу, оскільки ризиком, на відміну від невизначеності, яка не є об'єктивним явищем, можна і потрібно управляти.

Управління ризиками включає в себе прогнозування перспектив розвитку діяльності підприємства, аналіз можливих відхилень від запланованих результатів і керування цими відхиленнями за допомогою вдосконалення бізнес-процесів та мінімізації негативних наслідків. Слід зауважити, що оскільки невизначеність є неодмінною частиною реальності, повне уникнення

ризику неможливе. Отже, ризик завжди присутній, і прийняття рішень повинно базуватися на стратегії управління ризиками.

За даними досліджень, проведених Федерацією європейських асоціацій з ризик-менеджменту, зарубіжна практика свідчить про те, що значна частина компаній активно впроваджує системи управління ризиками. Згідно з проведеним опитуванням, 79% опитаних підприємств здійснюють управління ризиками, а з них 44% виділяють управління ризиками як окрему підсистему менеджменту підприємства. Ці дані вказують на тенденцію до поширення інструментів ризик-менеджменту та на усвідомлення важливості систематичного підходу до контролю та мінімізації ризиків у бізнесі [1].

Впровадження системи управління ризиками на підприємстві передусім ґрунтується на дотриманні національних та міжнародних стандартів. У випадку можливого виникнення негативних сценаріїв, ці стандарти визначають алгоритми дій для зменшення їх впливу на діяльність підприємства.

Мета статті

Метою дослідження є аналіз наявних стандартів управління ризиками і пошук ефективних підходів до їх використання для управління ризиками в IT-проєктах. Мета обумовлена необхідністю подальшого розроблення методів управління ризиками, відповідно до наявних стандартів, які можна застосовувати в IT-проєктах.

Об'єктом дослідження є стандарти управління ризиками в контексті інформаційних технологій та управління проєктами в IT-сфері. Предметом дослідження є специфіка використання стандартів управління ризиками для IT-проєктів, зокрема їх переваги та недоліки.

Аналіз літературних джерел і постановка проблеми

Процес стандартизації управління ризиками розпочався у 90-х рр. XX ст. У цей час різноманітні організації працювали над створенням національних та міжнародних стандартів. У табл. 1 подано аналіз основних актуальних міжнародних стандартів управління ризиками для IT-проєктів, які діють на сьогодні.

Стандарт – це документ, що встановлює вимоги, настанови або характеристики, які повинні бути дотримані у певній сфері чи галузі. Він визначає що потрібно зробити, щоб відповідати певному рівню якості, безпеки або ефективності [2]. Приклад стандарту – ISO 31000 (стандарт управління ризиками) [3], який визначає принципи та вимоги до ефективного управління ризиками, які організації можуть застосовувати.

Таблиця 1 – ***Міжнародні стандарти управління ризиками для IT-проєктів***

№	Стандарт	Основні характеристики стандарту	Розробник
1	Стандарт ISO 31000 та ISO 31010	Визначають загальні принципи та настанови для ефективного управління ризиками в будь-якій організації, надаючи засоби для ідентифікації, оцінки, обробки та моніторингу ризиків. Стандарт дає огляд основних методів оцінювання ризиків [3].	МЕК (IEC)
2	Стандарт ISO 27001	Встановлює вимоги до систем управління інформаційною безпекою, зокрема, управління ризиками, контроль доступу, неперервність діяльності та постійну оцінку та вдосконалення [4].	МЕК (IEC)
3	Стандарт NIST 800-53	Стандарт для управління безпекою та конфіденційністю інформаційних систем через набір контрольних заходів і управління ризиками [5].	Національний інститут стандартів і технологій США (NIST)
4	Стандарт PMBOK	Стандартизований набір кращих практик і процесів для управління проєктами, що охоплює ініціацію, планування, виконання, моніторинг і завершення проєктів, з акцентом на управління ресурсами, ризиками та досягнення проєктних цілей [6].	Інститут управління проєктами (Project Management Institute, PMI)

Мета стандарту – забезпечити відповідність певним вимогам і забезпечити стандартизацію процесів на міжнародному або національному рівні.

Природа стандарту полягає в обов'язкових або добровільних вимогах, які організації можуть впроваджувати для підвищення якості та безпеки своїх процесів і продуктів.

Наразі існує понад 23000 стандартів, розроблених Міжнародною організацією зі стандартизації, що охоплюють широкий спектр тем –

від технологій до управління якістю, охорони здоров'я та безпеки. ISO постійно займається розробкою нових стандартів та оновленням наявних, щоб відповідати сучасним технологічним змінам і вимогам ринку.

Виклад основного матеріалу

Стандарт управління ризиками – це нормативний офіційний документ, що затверджуються організаціями, такими як ISO, ANSI, IEC, NIST тощо, який визначає загальні принципи, рамки, процеси та рекомендації щодо ідентифікації, оцінки, моніторингу, контролю та мінімізації ризиків [3; 5; 6]. *Методологія управління ризиками* – це систематизований підхід, який включає набір принципів, методів і процесів, призначених для управління ризиками в організації або проєкті [3; 5; 6]. *Метод управління ризиками* – це конкретні інструменти та підходи, які застосовуються для ідентифікації, аналізу, оцінки, мінімізації або моніторингу ризиків [3; 5; 6].

На рис. 1 зображено діаграму взаємозв'язку між стандартами, методологіями та методами управління ризиками. При цьому застосовано логічне зіставлення, оскільки стандарти – це ширші рамки або правила, які можуть містити різні методології, а методології включають конкретні методи для розв'язання задач.

Рисунок 1 – Діаграма взаємозв'язку між стандартами, методологіями та методами управління ризиками

Стандарт ISO 31000 [3] «Менеджмент ризиків. Принципи та керівні вказівки» (Risk Management – Principles and guidelines on implementation) є розробкою Міжнародної організації зі стандартизації (International Organization for Standardization, ISO) та Технічного комітету «Надійність Міжнародної електротехнічної комісії» – МЕК (International Electrotechnical Commission, IEC). Цей стандарт є достатньо універсальним, оскільки його можна використовувати будь-яким суб'єктом господарювання, незалежно від їх організаційної форми чи виду діяльності. Цей стандарт можна використовувати протягом всього життєвого циклу організації, в ньому відображені принципи, структури та процеси управління ризиками. Слід зауважити, що цей стандарт є найбільш поширеним у практиці управління ризиками українських підприємств. ISO 31000 та ISO 31010 – це два пов'язаних стандарти, проте вони мають різні фокуси. ISO 31000 встановлює загальні принципи та настанови для управління ризиками в будь-якому виді діяльності, надаючи загальний фреймворк для ідентифікації, оцінки та обробки ризиків. З іншого боку, ISO 31010 надає конкретні методи та підходи для оцінки ризиків, які можуть бути використані в рамках системи управління ризиками, встановленої згідно з ISO 31000. Значною перевагою стандарту ISO 31010 є опис методів оцінювання ризиків з урахуванням сфери їх використання, переваг та недоліків кожного з них. Отже, ISO 31010 доповнює ISO 31000, вказуючи на можливі методи й інструменти для конкретизації процесів управління ризиками.

ISO 31000 пропонує системний підхід до управління ризиками, що містить такі складові: Контекст управління ризиками (визначення цілей і обмежень проєкту), Ідентифікація ризиків (виявлення можливих загроз), Оцінка ризиків (ймовірність і вплив), Моніторинг і контроль (оцінка ефективності заходів з управління ризиками). Цей підхід є особливо цінним для складних ІТ-проєктів, які можуть стикатися з постійними змінами технологій, вимог і термінів реалізації.

Застосування стандарту ISO 31000 дає змогу не лише зменшити технічні ризики (наприклад, збої в системах або кіберзагрози), але й мінімізувати ризики бізнесу, такі як порушення строків або перевищення бюджету, що критично важливо для успішного завершення ІТ-проєктів. Цей стандарт включає процес постійного вдосконалення управління ризиками. В ІТ-проєктах, де ризики та виклики можуть швидко змінюватися, така адаптивність сприяє постійному аналізу і коригуванню стратегії управління. Стандарт акцентує увагу на важливості прозорості й ефективної комунікації між усіма учасниками процесу управління ризиками. Це допомагає залучити до процесу управління ризиками як технічних фахівців, так і зацікавлених сторін на вищому рівні, забезпечуючи більш цілісний підхід до прийняття рішень. ISO 31000 легко інтегрувати з іншими міжнародними стандартами, такими як ISO/IEC 27001 (управління інформаційною безпекою), що часто є необхідним в ІТ-середовищі для забезпечення захисту і конфіденційності даних. Отже, ISO 31000 є ефективним інструментом для

управління ризиками в IT-проєктах завдяки своїй гнучкості, системності та можливості адаптації до специфіки технологічної сфери.

Серед IT-компаній, які використовують ISO 31000, можна навести: Microsoft, що активно використовує цей стандарт для управління ризиками у своїй операційній діяльності та розвитку продуктів [7]; IBM, що застосовує стандарти ISO для забезпечення управління ризиками у хмарних сервісах та консалтингових послугах [8]; Deloitte (міжнародна консалтингова компанія), яка використовує стандарт для своїх послуг із управління ризиками [9].

ISO 31000 є гнучким стандартом для управління ризиками, і його можна адаптувати до потреб різних організацій, включно з малим і середнім бізнесом. Цей стандарт не вимагає впровадження конкретних додаткових процесів чи модулів, що дає змогу компаніям будувати свою систему управління ризиками поступово. За потреби можна інтегрувати інші стандарти, такі як ISO 27001 для управління інформаційною безпекою, що робить ISO 31000 гарною основою для подальших розширень.

З іншого боку, стандарт NIST, зокрема його підходи до кібербезпеки й управління ризиками (наприклад, NIST Cybersecurity Framework), більш інтегрований та широкий, що дійсно може створювати складнощі при спробі виключити певні його компоненти. Це може вплинути на загальну структуру звітів або процесів, якщо компанія не має наміру використовувати всі передбачені компоненти.

ISO 31000 може слугувати гарним початком, який не обтяжує середній бізнес процесами, які не завжди присутні в їх діяльності. Отже, цей стандарт можна використовувати як основу для подальших надбудов за потребою, наприклад, інтегрувати ISO 27001. У стандарті NIST цей модуль інтегрований за замовчуванням, що може стати проблемою, якщо компанія не збирається його використовувати – вирізати його досить важко, щоб не порушити структуру звітів.

ISO 31000 надає гнучку методологічну основу для впровадження управління ризиками, що є особливо актуальним для малого та середнього бізнесу, який не завжди потребує складних і деталізованих процесів. Завдяки своїй універсальності, цей стандарт дає змогу організаціям адаптувати його під власні потреби, поступово інтегруючи додаткові стандарти, такі як ISO 27001 для управління інформаційною безпекою. Така модульна структура сприяє еволюційному розвитку системи управління ризиками без надмірного адміністративного навантаження.

На відміну від цього, стандарти NIST, зокрема NIST Cybersecurity Framework, мають більш жорстко інтегровану архітектуру, де елементи, такі як управління інформаційною безпекою, зазвичай є невід'ємною частиною загальної системи. Це може створювати виклики для компаній, які не мають потреби в цих компонентах, оскільки їх вилучення без порушення структури документації та процесів може бути складним завданням.

Переваги ISO 31000 [10; 11]:

1. ISO 31000 підходить для різних галузей, зокрема й IT, і охоплює різні типи ризиків: фінансові, операційні, стратегічні тощо.

2. Стандарт може бути адаптований до специфіки організації і уможливлює вибудовувати процеси управління ризиками на індивідуальних засадах.

3. Стандарт використовує систематичний підхід до оцінювання, моніторингу та реагування на ризики, включаючи процеси прийняття рішень на основі аналізу ризиків.

Недоліки ISO 31000 [12]:

1. Стандарт не надає детальних специфічних інструкцій саме для IT-сфери.

2. Відсутність чітких метрик для оцінки успішності впровадження та відповідні труднощі у порівнянні різних підходів до управління ризиками, через що виникає складність у вимірюванні ефективності.

3. Для комплексного управління IT-ризиками необхідно інтегрувати його з іншими стандартами, наприклад, ISO 27001.

Стандарт ISO 27001 – міжнародний стандарт в галузі IT, назва якого «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». Стандарт встановлює вимоги щодо розроблення, впровадження, підтримки та постійного удосконалення системи управління інформаційною безпекою в межах організації, включаючи оцінку та обробку ризиків інформаційної безпеки відповідно до потреб організації. Вимоги стандарту є загальними і призначені для всіх організацій, незалежно від їх типу, розміру і характеру. Він входить до групи стандартів, що стосуються систем управління інформаційною безпекою, тісно пов’язаний із стандартом ISO/IEC 27002 [13].

Як і у випадку із ISO 31000, багато IT-компаній використовують цей стандарт, зокрема: Microsoft застосовує ISO 27001 для забезпечення безпеки своїх хмарних сервісів, таких як Azure, Microsoft 365 і Dynamics 365. Компанія має сертифікацію ISO 27001 для багатьох своїх продуктів і послуг; Amazon Web Services (AWS) використовує ISO 27001 для своєї хмарної платформи, що охоплює управління інформаційною безпекою на всіх рівнях — від фізичної безпеки центрів обробки даних до захисту

даних клієнтів у хмарі; Google Cloud: сертифікований за ISO 27001, що гарантує надійну систему управління безпекою для своїх хмарних сервісів та продуктів, таких як Google Workspace і Google Cloud Platform; IBM має сертифікацію ISO 27001 для своїх дата-центрів та хмарних сервісів. IBM використовує цей стандарт для забезпечення інформаційної безпеки у своїх рішеннях для підприємств; Oracle Cloud також сертифікований за ISO 27001, що підтверджує відповідність їхніх продуктів високим стандартам інформаційної безпеки; Dropbox – одна з компаній, яка отримала сертифікацію ISO 27001 для забезпечення надійного зберігання та передачі даних у своїх хмарних рішеннях; Salesforce використовує ISO 27001 для управління інформаційною безпекою своїх хмарних сервісів CRM та забезпечення безпеки даних клієнтів. Cisco має сертифікацію ISO 27001 для низки своїх продуктів та сервісів, які стосуються мережевих і безпекових рішень.

Переваги ISO 27001 [14; 15]:

1. ISO 27001 забезпечує систематичний підхід до виявлення, оцінювання та управління ризиками, що знижує ймовірність інцидентів, пов'язаних з витоком даних, кіберзагрозами та порушенням конфіденційності.

2. Сертифікація ISO 27001 показує партнерам, клієнтам та регуляторам, що компанія дотримується строгих стандартів інформаційної безпеки, що сприяє підвищенню довіри до неї.

3. Сертифіковані за цим стандартом компанії часто отримують перевагу в тендерах та угодах, де інформаційна безпека є ключовим аспектом.

4. Впровадження ISO 27001 допомагає організаціям відповідати національним і міжнародним законодавчим вимогам щодо безпеки даних.

Недоліки ISO 27001 [15]:

1. Процес впровадження стандарту потребує значних фінансових та людських ресурсів, особливо для малих і середніх підприємств.

2. Компаніям необхідно проходити через складні процеси підготовки, внутрішнього аудиту та зовнішніх перевірок для отримання сертифікації.

3. ISO 27001 вимагає значних зусиль для ведення й оновлення документації, що може відволікати ресурси від оперативної роботи.

Стандарт NIST 800-53 – це стандарт інформаційної безпеки, який містить каталог контролів конфіденційності та безпеки для інформаційних систем [5]. Спочатку призначений для федеральних агенцій США, за винятком тих, що пов'язані з національною безпекою, з п'ятого перегляду став стандартом загального використання. Виданий Національним інститутом стандартів і технологій (NIST), який є нерегуляторним агентством Міністерства торгівлі США. NIST розробляє і публікує стандарти, керівництва та інші матеріали, щоб допомогти федеральним агентствам у впровадженні Закону про модернізацію інформаційної безпеки федерального уряду 2014 р. (FISMA) та для сприяння управлінню ефективними за витратами програмами захисту їхньої інформації та інформаційних систем. Є два пов'язані документи – 800-53A та 800-53B, які надають рекомендації та базові норми на основі стандарту NIST 800-53.

Переваги NIST 800-53 [5]:

1. Структурований підхід до інформаційної безпеки. NIST 800-53 пропонує добре організовану систему контролю та заходів безпеки, що покриває різні аспекти безпеки, такі як: управління ідентифікацією, доступом, шифруванням, безпекою мережі тощо.

2. Гнучкість для різних організацій. Рекомендації NIST 800-53 є адаптивними та масштабованими для різних типів організацій, незалежно від розміру чи сфери діяльності. Вони дають змогу організаціям налаштовувати підходи під свої конкретні ризики та загрози.

3. Стандарт орієнтований на управління ризиками на стратегічному рівні, допомагаючи організаціям розробити системи, що мінімізують вплив інцидентів інформаційної безпеки.

4. NIST 800-53 можна поєднувати з іншими стандартами безпеки, такими як ISO 27001, що уможливлює організаціям використовувати декілька підходів для зміцнення інформаційної безпеки.

Недоліки NIST 800-53 [5]:

1. Через велику кількість деталей, які необхідно врахувати, впровадження NIST 800-53 може бути важким завданням для малих і середніх підприємств. Стандарт включає сотні контролів, що потребують значних ресурсів для належного виконання.

2. Зосередження стандарту на федеральних потребах. Хоча стандарт є гнучким, його початкова орієнтація на державні установи може ускладнити впровадження в приватному секторі. Деякі модулі для контролю можуть бути надмірними або непридатними для компаній з іншими потребами.

3. Необхідність частих оновлень. Стандарти NIST регулярно переглядаються та оновлюються для врахування нових загроз і змін у технологіях, що вимагає постійної адаптації з боку організацій, які їх використовують.

4. Трудомістке документування. Як і в ISO 27001, NIST 800-53 вимагає ретельного документування процесів та контролів, що може бути ресурсозатратним і потребувати від організацій залучення додаткових спеціальних фахівців.

Стандарт PMBOK (Project Management Body of Knowledge) – це один із найвідоміших і найпоширеніших стандартів для управління проєктами, розроблений Інститутом управління проєктами (PMI) [6]. Він містить узагальнення найкращих практик і методологій для управління проєктами, які застосовуються в різних галузях. PMBOK є основою для сертифікаційних програм PMI, таких як PMP (Project Management Professional), і часто використовується як керівництво для розроблення планів управління проєктами в реальному середовищі.

PMBOK також приділяє значну увагу управлінню ризиками, що є критично важливим аспектом для успішного виконання проєктів. У рамках управління ризиками виокремлюють такі ключові кроки: Ідентифікація ризиків; Аналіз і оцінка ризиків (кількісний і якісний аналіз); Розробка планів реагування на ризики; Моніторинг та контроль ризиків.

Переваги PMBOK [16; 17]:

1. Стандартизований та структурований підхід. PMBOK забезпечує єдину термінологію та методологію управління проєктами, що полегшує комунікацію між учасниками проєкту і сприяє плануванню, організації та контролю всіх етапів проєкту.

2. Комплексність і універсальність. Методологія охоплює всі аспекти управління проєктами, містить перевірені практики, які можуть бути адаптовані під різні типи проєктів незалежно від їх розміру або сфери діяльності.

3. Гнучкість у застосуванні. PMBOK уможливлює адаптувати свій підхід до різних галузей та підтримує використання різних методологій, включаючи agile і waterfall.

4. Стандарт служить основою для сертифікації PMP, що сприяє кар'єрному зростанню менеджерів проєктів і підвищує їх конкурентоспроможність на ринку праці.

5. PMBOK надає інструменти для ефективного управління людськими, фінансовими та матеріальними ресурсами, що допомагає знизити витрати й оптимізувати роботу команди.

6. Стандарт забезпечує інструменти для ефективного моніторингу прогресу проєкту, що допомагає менеджерам виявляти проблеми та вживати корегувальних заходів учасникам проєкту.

Недоліки PMBOK [17; 18]:

1. Складність впровадження. PMBOK може бути занадто бюрократичним і вимагати значних ресурсів для повного впровадження, що особливо помітно у малих проєктах, де він може бути надто громіздким, також опанування стандартом може бути доволі складним, особливо для новачків.

2. Надмірна формалізація і залежність від документування. Стандарт вимагає значних зусиль на документування та дотримання формальних процесів, що може відволікати від оперативного управління та збільшувати адміністративне навантаження

3. Обмежена гнучкість у деяких аспектах. Хоча стандарт підтримує адаптацію, він може бути менш ефективним для дуже малих проєктів або в умовах, що швидко змінюються, і може конфліктувати з agile-підходами.

4. Методологія не завжди враховує культурні відмінності в управлінні проєктами, що може стати викликом для глобальних проєктів, оскільки її рекомендації можуть не відповідати специфічним вимогам різних регіонів.

Відомі також інші вузькогалузеві стандарти, які можуть бути суміжними до напрямку діяльності IT-компанії.

Стандарт Health Insurance Portability and Accountability Act (HIPAA) – це постанова (закон) федерального органу, розроблена Міністерством охорони здоров'я та соціальних служб США. Цей закон призначений для захисту конфіденційності та забезпечення безпеки інформації про стан здоров'я (Protected Health Information, PHI) людини. Крім того, він встановлює стандарти і вимоги до використання, розкриття та захисту цих даних. Дія HIPAA поширюється на відповідні організації та ділові партнери, які створюють, отримують, обслуговують або надсилають PHI, а також мають доступ до такої інформації.

Стандарт SASB (Sustainability Accounting Standards Board) може бути застосований для управління ризиками в IT-проєктах, хоча SASB спочатку був орієнтований на звітність щодо сталого розвитку, екологічних, соціальних і управлінських факторів (ESG) для різних галузей.

Також можна навести *стандарт SAE J1739* – стандарт для FMEA (Failure Mode and Effects Analysis), розроблений товариством автомобільних інженерів (SAE), що використовується в автомобільній промисловості для оцінки ризиків відмов. Зокрема, можна навести IATF 16949 – Глобальний стандарт для систем управління якістю в автомобільній промисловості, який також охоплює управління ризиками, розроблений International Automotive Task Force (IATF). Також можна навести Стандарти OHSAS 18001, на заміну яким прийшов ISO 45001:2018, що забезпечує міжнародно визнану систему управління охороною здоров'я і безпекою праці (OH&S) British Standards Institution. Існує безліч інших спеціалізованих на конкретній галузі стандартів, які побудовані на основі глобальних ISO-стандартів.

Виокремлюють також *національні стандарти з управління ризиками*, що базуються на ISO 31000: BS 31100:2021 – британський стандарт; AS/NZS ISO 31000:2009 – австралійський стандарт та SA/SNZ HB 436:2013 – австралійське керівництво; ONR 49000:2021 – австрійський стандарт; CSA Q 850:2009 – канадський стандарт; JIS Q 31000 – японський стандарт.

Більш ніж 50 національних органів зі стандартизації, а також деякі організації ООН, прийняли стандарти ISO як національні. Україна приєдналася до цього процесу з 2009 р. – на сьогодні в країні впроваджені та діють стандарти, зазначені у табл. 2.

У зв'язку з різноманітним тлумаченням термінів було введено в дію стандарт ДСТУ ISO Guide 73:2013 «Керування ризиком. Словник термінів». З метою забезпечення інструментарію для оцінювання та управління ризиками був також впроваджений стандарт ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» [19]. Обидва ці стандарти розроблені Науково-дослідним інститутом метрології вимірювальних і управляючих систем (ДП «НДІ "Система"») та введені в дію з 01.07.2014 р. за наказом Мінекономрозвитку України від 29.11.2013 р. № 1423. Сутність цих документів відповідає їхнім аналогам ISO (табл. 2), які були розглянуті раніше.

У 2018 р. були представлені оновлений стандарт ISO 31000:2018 [20] та вперше введений ISO/TR 31004:2018. Ці стандарти, у беззмінному вигляді англійською мовою, були прийняті Наказом ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») № 446 від 29.11.2018 р. та набули чинності на території України з 01.01.2019 р.

Слід зазначити, що згідно з правилом ISO, стандарти мають переглядатись кожні п'ять років, проте попередні методи управління ризиками не завжди ефективні в умовах сучасних загроз.

Таблиця 2 – ***Стандарти управління ризиками, впроваджені в Україні***

№	Назва	Аналог ISO
1	ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів	ISO Guide 73:2009, IDT
2	ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику [19]	IEC/ISO 31010:2009, IDT
3	ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови [20]	ISO 31000:2018, IDT
4	ДСТУ ISO/TR 31004:2018 Менеджмент ризиків. Настанова з впровадження ISO 31000	ISO/TR 31004:2013, IDT

Використання національних стандартів управління ризиками в ІТ-проєктах може мати певні обмеження, через що вони не завжди є найкращим вибором для управління ризиками у цій сфері.

1. Обмежена міжнародна сумісність. ІТ-проєкти часто залучають команди та клієнтів з різних країн, тому використання національних стандартів може створювати проблеми через відсутність узгодженості з міжнародними нормами. Наприклад, національні стандарти можуть не бути підтримувані міжнародними партнерами чи клієнтами; або у проєктах з глобальними командами національні стандарти можуть ускладнити інтеграцію, оскільки вони не враховують культурні, правові або технічні відмінності інших країн.

2. Менша актуальність для швидкозмінних галузей. ІТ-сектор є однією з найбільш динамічних галузей, де технології, загрози та інструменти управління ризиками постійно змінюються. Національні стандарти, особливо якщо вони не оновлюються регулярно, можуть не встигати за цими змінами. Наприклад, ризики, пов'язані з кібербезпекою, новими технологіями (хмарні обчислення, блокчейн) чи штучним інтелектом, можуть не бути належним чином враховані в національних стандартах.

3. Вузька спрямованість національних стандартів, оскільки вони можуть бути розроблені з урахуванням специфіки економіки або правової системи певної країни, що робить їх менш ефективними для проєктів з міжнародним або мультигалузевим контекстом. Наприклад, деякі національні стандарти можуть фокусуватися на промислових ризиках або регуляторних аспектах, які не є ключовими для ІТ-проєктів. Також, вузький підхід національних стандартів може обмежувати можливість управління ризиками, які виникають на стику різних галузей і технологій, як це часто буває в ІТ-проєктах.

4. Національні стандарти можуть бути жорсткішими або менш адаптивними до специфіки ІТ-проєктів порівняно з міжнародними стандартами, такими як ISO 31000 або PMBOK. Міжнародні стандарти частіше пропонують більш гнучкі та універсальні підходи, що уможливлюють адаптувати їх до конкретних потреб ІТ-проєкту. Наприклад, у рамках ІТ-проєктів можуть з'являтися нові ризики протягом проєкту, і гнучкість стандарту є важливим критерієм для можливості застосування швидкого реагування. Зокрема, національні стандарти можуть не надавати достатньо варіантів для адаптації під конкретні вимоги проєкту або технологій.

5. Більшість національних стандартів управління ризиками не спеціалізуються на ІТ-секторі і можуть не враховувати специфіку управління ризиками в технологічних проєктах.

Наприклад, в IT-проєктах велика увага приділяється управлінню ризиками, пов'язаними з кібербезпекою, даними, швидкими змінами вимог замовників та технологій. Національні стандарти часто загальні і не враховують такі специфічні проблеми. Вони можуть не враховувати сучасні інструменти та методи управління ризиками, які є стандартом для IT-галузі, наприклад Agile.

6. Міжнародні стандарти, такі як ISO, збирають найкращі практики з усього світу, тоді як національні стандарти можуть бути обмежені досвідом і підходами тільки певної країни. Це може бути недоліком, оскільки IT-проєкти часто потребують глобальних підходів і гнучких методологій управління ризиками. Наприклад, Національні стандарти можуть бути більш консервативними й орієнтованими на традиційні підходи, тоді як міжнародні стандарти швидше впроваджують інновації.

Використання національних стандартів управління ризиками в IT-проєктах може бути менш ефективним через обмежену міжнародну сумісність, вузьку спрямованість, недостатню гнучкість і відсутність спеціалізації для IT-сфери. Натомість міжнародні стандарти, такі як ISO 31000, пропонують більш гнучкий, актуальний і спеціалізований підхід, що краще відповідає вимогам IT-індустрії та допомагає більш ефективно управляти ризиками в глобальному та технологічно змінному середовищі.

Вибір стандарту для управління ризиками в IT-проєктах. Оскільки ISO 31000 зазвичай використовується в комбінації з ISO 27001, тому окремо для порівняння цей стандарт не розглядається.

Серед унікальних переваг стандартів можна навести: для ISO 31000 – «Широке застосування»; для NIST 800-53 – «Покращене управління ризиками інформаційної безпеки»; для PMBOK – «Покращене управління ресурсами» та «Підтримка процесів моніторингу та контролю».

Спільними перевагами між ISO 31000, NIST 800-53 та PMBOK є: «Гнучкість» та «Структурований підхід».

Серед унікальних недоліків стандартів можна навести: для ISO 31000 – «Відсутність специфічних інструкцій для IT», «Складність вимірювання ефективності», «Вимога інтеграції з іншими стандартами»; для NIST 800-53 – «Зосередження на федеральних потребах в інформаційній безпеці» та «Необхідність частих оновлень»; для PMBOK – «Обмежена гнучкість у деяких аспектах» та «Культурні обмеження регіонів».

Спільними недоліками між NIST 800-53 та PMBOK є: «Складність впровадження», «Трудомістке документування».

Наведені переваги і недоліки стандартів можна відобразити за допомогою діаграм, представлених на рис. 2 та 3.

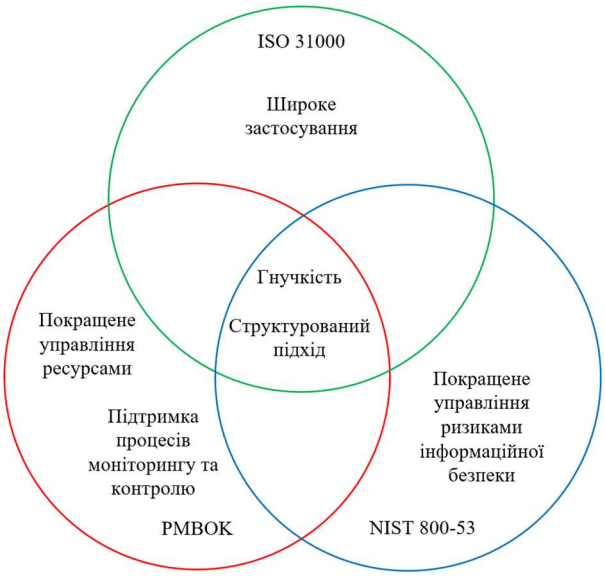

Рисунок 2 – Переваги стандартів ISO 31000, NIST 800-53 та PMBOK

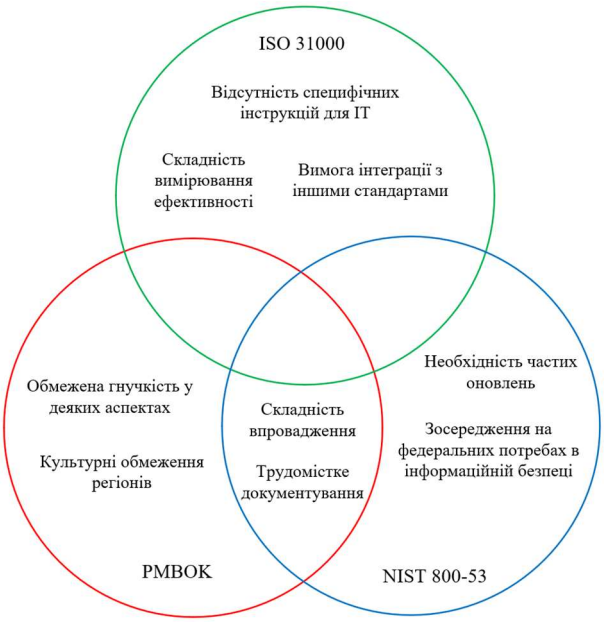

Рисунок 3 – Недоліки стандартів ISO 31000, NIST 800-53 та PMBOK

Висновки

У результаті аналізу визначено, що для управління ризиками в IT-проєктах найбільше підходить стандарт ISO 31000. Цей стандарт у комбінації зі стандартом ISO 31010 є найбільш адаптивним, оскільки на початкових етапах його впровадження він легше інтегрується в наявні системи. Цей стандарт може слугувати основою для подальшого впровадження інших стандартів, які будуть доповнювати один одного завдяки наявності різногалузевих норм у рамках ISO.

Список літератури

1. Сосновська О. О., Деденко Л. В. Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності. *Європейський науковий журнал Економічних та Фінансових інновацій*. 2019. № 1 (3). С. 70–79. DOI: 10.32750/2019-0106.

2. US Department of Homeland Security. A Guide to the Cost-Effective and Efficient Communication of Needs. 2008. 353. URL: https://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.

3. ISO 31000 – Risk management. URL: https://www.iso.org/iso-31000-risk-management.html.

4. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001.

5. National Institute of Standards and Technology Special Publication 800-53. Rev. 5. 2020. 492. DOI: 10.6028/NIST.SP.800-53r5.

6. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK Guide) (7th ed.). Project Management Institute. 2021. 250. URL: https://www.pmi.org/standards/pmbok.

7. Microsoft Compliance Offerings. URL: https://learn.microsoft.com/en-us/microsoft-365/compliance/offering-home.

8. IBM Cloud ISO 31000 compliance. URL: https://www.ibm.com/cloud/compliance/iso-31000.

9. Internal Audit Services | Deloitte SEA | Risk Advisory. URL: https://www2.deloitte.com/sg/en/pages/risk/solutions/internal-audit-services.html.

10. Purdy, G. ISO 31000:2009 – Setting a New Standard for Risk Management. Risk Analysis. 30(6), 2010. P. 881–886. DOI: 10.1111/j.1539-6924.2010.01442.x.

11. Luko, S. N. Risk Management Principles and Guidelines. Quality Engineering. 25(4), 2013. P. 451–454. DOI: 10.1080/08982112.2013.814508.

12. Leitch, M. ISO 31000:2009 – The New International Standard on Risk Management. *Risk Analysis*. 30 (6), 2010. P. 887–892. DOI: 10.1111/j.1539-6924.2010.01397.x.

13. Calder, A., ISO27001/ISO27002 A Pocket Guide: 2013 Second Edition by IT Governance Publishing (Editor). 2013. 86.

14. Von Solms, R., & Van Niekerk, J. From information security to cyber security. *Computers & Security*, 38, 2013. P. 97–102. DOI: 10.1016/j.cose.2013.04.004.

15. Peltier, T. R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press. 2013. 408. DOI: 10.1201/9780203488737.

16. Morris, P. W. G. Reconstructing Project Management. Wiley-Blackwell. 2013. 319. DOI: 10.1002/9781118536698.

17. Kerzner, H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. John Wiley & Sons. 2022. 880.

18. Fernandes, G., Ward, S., & Araújo, M. Improving and embedding project management practice in organisations – A qualitative study. *International Journal of Project Management*, 33(5), 2015. P. 1052–1067. DOI: 10.1016/j.ijproman.2015.01.012.

19. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014-07-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2015. 80 с.

20. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT) [Чинний від 2019-01-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2018. 23 с.

Стаття надійшла до редколегії 03.03.2025

Maksymov Anton
Lecturer at the Department of Computer Science and Systems Analysis,
https://orcid.org/0009-0002-0411-8164
Cherkasy State Technological University, Cherkasy

ANALYSIS OF RISK MANAGEMENT STANDARDS AND THEIR APPLICATION IN IT PROJECTS

Abstract. *Risk management is a critical aspect of successful project implementation in the field of information technology, as IT projects are often subject to high levels of uncertainty and complexity. Insufficient risk management can lead to significant losses, budget overruns, delays in project timelines, and reduced quality of the final product. Consequently, there is a need for the application of reliable standards to ensure effective identification, analysis, and monitoring of risks throughout the entire lifecycle of an IT project. The objective of this study is to analyze existing risk management standards and explore effective approaches to their use in managing risks in IT projects. The research presents the interrelation between standards, methodologies, and methods for risk management in projects. Additionally, the research compares the risk management standards ISO 31000, ISO 27001, PMBOK, and NIST SP 800-53 based on key parameters, including scope of application, risk management processes, approaches to risk identification and assessment, as well as the level of flexibility and adaptability for specific projects. The advantages and disadvantages of contemporary risk management standards in IT projects are analyzed and visualized using diagrams. The findings indicate that ISO 31000 and PMBOK are suitable for a wide range of IT projects due to their flexible approaches to risk management and clear methodological guidelines. Meanwhile, NIST SP 800-53 focuses more on cybersecurity, providing detailed insights into information security risks, making it particularly useful for projects in this domain. For effective risk management in*

IT projects, a comprehensive approach is recommended, combining elements of various standards. The integration of flexible and detailed recommendations enables the development of a robust strategy to mitigate the likelihood and impact of risks on a project, thereby ensuring its successful implementation. The conclusions highlight that ISO 31000 is the most adaptable standard among those analyzed, as its initial implementation is relatively easy to integrate into existing systems. This makes it a suitable foundation for the subsequent adoption of complementary standards, leveraging the cross-industry norms provided within the ISO framework.

Keywords: risk management; IT projects; risk management standards; ISO 31000; ISO 27001; NIST SP 800-53; PMBOK; risk analysis; information technology

References

1. Sosnovska, O., Dedenko, L. (2019). Risk management as an instrument for providing the stable functioning of the enterprise in understanding condition. *European scientific journal of Economic and Financial innovation*, 1 (3), 70–79. DOI: 10.32750/2019-0106.

2. US Department of Homeland Security. A Guide to the Cost-Effective and Efficient Communication of Needs. 2008. 353. URL: https://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.

3. ISO 31000 – Risk management. URL: https://www.iso.org/iso-31000-risk-management.html.

4. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001.

5. National Institute of Standards and Technology Special Publication 800-53 (2020). Rev. 5. 492. DOI: 10.6028/NIST.SP.800-53r5.

6. Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK Guide) (7th ed.). Project Management Institute. URL: https://www.pmi.org/standards/pmbok.

7. Microsoft Compliance Offerings. URL: https://learn.microsoft.com/en-us/microsoft-365/compliance/offering-home.

8. IBM Cloud ISO 31000 compliance. URL: https://www.ibm.com/cloud/compliance/iso-31000.

9. Internal Audit Services | Deloitte SEA | Risk Advisory. URL: https://www2.deloitte.com/sg/en/pages/risk/solutions/internal-audit-services.html.

10. Purdy, G. (2010). ISO 31000:2009 – Setting a New Standard for Risk Management. *Risk Analysis*, 30 (6), 881–886. DOI: 10.1111/j.1539-6924.2010.01442.x.

11. Luko, S. N. (2013). Risk Management Principles and Guidelines. *Quality Engineering*, 25(4), 451–454. DOI: 10.1080/08982112.2013.814508.

12. Leitch, M. (2010). ISO 31000:2009 – The New International Standard on Risk Management. *Risk Analysis*, 30 (6), 887–892. DOI: 10.1111/j.1539-6924.2010.01397.x.

13. Calder, A. (2013). ISO27001/ISO27002 A Pocket Guide: 2013 Second Edition by IT Governance Publishing (Editor). 86.

14. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. DOI: 10.1016/j.cose.2013.04.004.

15. Peltier, T. R. (2013). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press. 408. DOI: 10.1201/9780203488737.

16. Morris, P. W. G. (2013). Reconstructing Project Management. Wiley-Blackwell. DOI: 10.1002/9781118536698.

17. Kerzner, H. (2022). Project Management: A Systems Approach to Planning, Scheduling, and Controlling. John Wiley & Sons, 880.

18. Fernandes, G., Ward, S., & Araújo, M. (2015). Improving and embedding project management practice in organisations – A qualitative study. *International Journal of Project Management*, 33(5), 1052-1067. DOI: 10.1016/j.ijproman.2015.01.012.

19. DSTU IEC/ISO 31010:2013 Risk Management. (2015). Methods of Risk Assessment (IEC/ISO 31010:2009, IDT). [Effective from 2014-07-01]. Official publication. Kyiv: Ministry of Economic Development of Ukraine, 80.

20. DSTU ISO 31000:2018 Risk Management. (2018). Principles and Guidelines (ISO 31000:2018 Risk Management – Principles and Guidelines on Implementation, IDT). [Effective from 2019-01-01]. Official publication. Kyiv: Ministry of Economic Development of Ukraine, 23.

Посилання на публікацію

APA Maksymov, A. (2025). Analysis of risk management standards and their application in IT projects. *Management of Development of Complex Systems*, 61, 66–75, dx.doi.org\10.32347/2412-9933.2025.61.66-75.

ДСТУ Максимов А. Є. Аналіз стандартів управління ризиками та їх використання в ІТ-проєктах. *Управління розвитком складних систем.* Київ, 2025. № 61. С. 66 – 75, dx.doi.org\10.32347/2412-9933.2025.61.66-75.