ЕКОЛОГІЧНІ ПИТАННЯ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

УДК 504.658:361

ОЦІНЮВАННЯ РИЗИКІВ НЕУПЕРЕДЖЕНОСТІ ОРГАНУ СЕРТИФІКАЦІЇ СИСТЕМ УПРАВЛІННЯ

Горшков Л.І., Яковенко Л.О.
Державна екологічна академія післядипломної освіти та управління
вул. Митрополита Василя Липківського, 35, 03035, м. Київ
dei2005@ukr.net

Досліджено послідовність дій під час визначення, аналізування, оцінювання, моніторингу та документування ризиків щодо конфлікту інтересів, які виникають під час виконання процесу сертифікації. Послідовність процесу оцінювання ризиків розглянуто на прикладі оцінювання ризиків органу сертифікації систем управління. Запропоновано процес оцінювання ризиків з урахуванням вимог міжнародних стандартів серії ISO 31000 та ДСТУ EN ISO/IEC 17021-1:2015. *Ключові слова:* ризики, небезпеки, імовірність, невизначеність, орган сертифікації.

Оценка рисков беспристрастности органа сертификации систем управления. Горшков Л.І., Яковенко Л. О. Исследована последовательность действий во время определения, анализа, оценки, мониторинга и документирования рисков по конфликту интересов, которые возникают во время выполнения процесса сертификации. Последовательность процесса оценки рисков рассмотрена на примере оценки рисков органа сертификации систем управления. Предложено процесс оценки рисков с учетом требований международных стандартов серии ISO 31000 и ДСТУ EN ISO / IEC 17021-1: 2015. *Ключевые слова:* риски, опасности, вероятность, неопределенность, орган сертификации.

Evaluation of the risks of impartiality of the certification body of management systems. Gorshkov L., Iakovenko L. The sequence of actions during the determination, analysis, evaluation, monitoring and documenting risks of conflict of interests that arise during the process of certification process was investigated. The sequence of the risk assessment process is considered in the example of the risk assessment of the certification body of management systems. The risk assessment process is proposed taking into account the requirements of the international standards ISO 31000 and DSTU EN ISO / IEC 17021-1: 2015. *Keywords:* risks, hazards, probability, uncertainty, certification body.

Діяльність органів сертифікації систем управління(далі – ОС) в сучасних умовах передбачає необхідність постійного розвитку, змін та нововведень, що неможливе без ризику. Насамперед, це ризики, що можуть призвести до упередженості процесів аудиту, сертифікації та їх результатів.

Для надання компетентної, послідовної сертифікації, яка заслуговує на довіру, ОС має бути неупередженим. Важливо розпізнати та зрозуміти загрози неупередженості, що можуть виникнути у процесі діяльності ОС, оцінити ризик, який випливає з конкретної та потенційної загрози, а також запровадити заходи щодо усування або зменшення таких загроз. Оцінювання ризиків є найбільш ефективним запобіжним заходом, під час якого враховують не тільки інциденти, що сталися у минулому, але й небезпеки (потенціальні ризики), які ще не викликали негативних наслідків.

Термін «ризик» визначають як вплив невизначеності. Під впливом розуміють відхил, позитивний або негативний, від очікуваного. Невизначеність означає стан нестачі (навіть часткової) інформації стосовно розуміння чи знання події, її наслідку чи ймовірності[1]. Ризик часто характеризують посиланням на можливі події та можливі наслідки чи на їх поєднання і подають з погляду на поєднання наслідків події (охоплюючи зміни в обставинах) та імовірністю її виникнення [2].

Ризик неможливо передбачити чи усунути повністю. Проте його можна досліджувати, визначати його ступінь і природу, оцінювати та аналізувати, обирати ефективні методи управління ним. Відповідно до вимог п. 5.2.3 стандарту [3]ОС повинен оцінити ризики, що пов'язані з його діяльністю, а також визначити заходи з управління ризиками.

Ризики ОС можуть охоплювати, але не обмежуватися такими, що мають відношення до:

– цілей аудиту;

– вибірки, використаної у процесі аудиту;

– реальної та сприйманої неупередженості;

– правових та регуляторних питань, а також питань відповідальності;

– організації-заявника, щодо якої проводять аудит, та середовища, в якому зазначена організація провадить діяльність;

– впливу аудиту на заявника та його діяльність;

– здоров'я та безпеки членів групи аудиту;

– сприйняття зацікавлених сторін;

– заяв сертифікованого заявника, що вводять в оману;

– використання знаків.

Сучасне розуміння процесу керування ризиком базується на концепції прийнятного ризику, згідно з якою основною метою є одержання максимальної стійкості діяльності ОС шляхом утримання очікуваного рівня ризику в заданих межах. Стійкість передбачає гнучке реагування на всі зовнішні й внутрішні впливи для того, щоб не запобігати новим обставинам, властивостям і відносинам, а кваліфіковано використовувати їх для постійного відновлення та самовдосконалення, тобто, здатність системи пристосовуватися до умов управління, що змінюються.

Виклад основного матеріалу

Процес загального оцінювання ризиків щодо конфлікту інтересів, що виникають під час провадження сертифікації через взаємозв'язки ОС та можуть призвести до загрози неупередженості, охоплює такі етапи:

– визначення;

– аналізування;

– оцінювання потенціальних ризиків, що пов'язані з небезпеками і визначення їх прийнятності;

– документування ризиків;

– моніторинг.

Передусім, для визначення ризиків варто створити з числа персоналу ОС робочу групу з експертів та спеціалістів з екологічного управління, сертифікації та ризиків (далі – Група). Федерація асоціації управління ризиками Європейської (FERMA) рекомендує до процесу ідентифікації ризиків залучати незалежних консультантів. Члени Групи регулярно (щонайменше один раз на рік) мають визначати, аналізувати, оцінювати можливі ризики щодо конфлікту інтересів, що виникають під час виконання процесу сертифікації. У своїй діяльності вони можуть використовувати настанови стандарту[4].

Результати оцінювання/повторного оцінювання ризиків використовують для прийняття рішень, які можуть впливати на встановлення та досягнення цілей, адекватність і результативність заходів управління операціями, що є джерелами ризиків. Результати рекомендуємо занести до табл. 1.

Таблиця 1

Результати оцінювання ризиків

№ з/п	Ризик	Опис наслідку ризику	Причина (джерело) ризику	Бальна оцінка		
				імовірність	тяжкість	ризик
1	*2*	*3*	*4*	*5*	*6*	*7*

Оцінювання ризиків можна виконувати у послідовності, що наведена на рис. 1.

Свою діяльність Група має розпочинати з етапу збирання інформації, який передбачає постійний моніторинг факторів зовнішнього середовища та умов діяльності ОС. На цьому етапі здійснюють збирання, оброблення, передавання та аналізування різного роду інформації, що дає можливість оцінити виникнення максимально широкого кола ризиків. Для визначення можливих ризиків члени Групи повинні максимально використовувати усі доступні джерела інформації, зокрема:

– статутні та організаційно-розпорядчі документи ОС;

– нормативно-правові акти та організаційно-розпорядчі документи Мінекономрозвитку України, НААУ, ДП «УкрНДНЦ» тощо;

– Положення про ОС та посадові інструкції персоналу;

– документи системи управління ОС;

– дані, отримані за результатами зворотного зв’язку із заявниками, від персоналу ОС та зацікавлених сторін;

– результати зовнішніх/внутрішніх аудитів;

– інформацію у засобах масової інформації;

– дані за результатами попереднього визначення небезпек і оцінювання ризиків тощо.

Виявлення (ідентифікація) небезпек полягає у визначенні всіх джерел, ситуацій або дій (чи їх поєднання), що притаманні діяльності ОС та несуть потенційну загрозу виникнення конфлікту інтересів.

Джерелами загроз неупередженості ОС можуть бути:

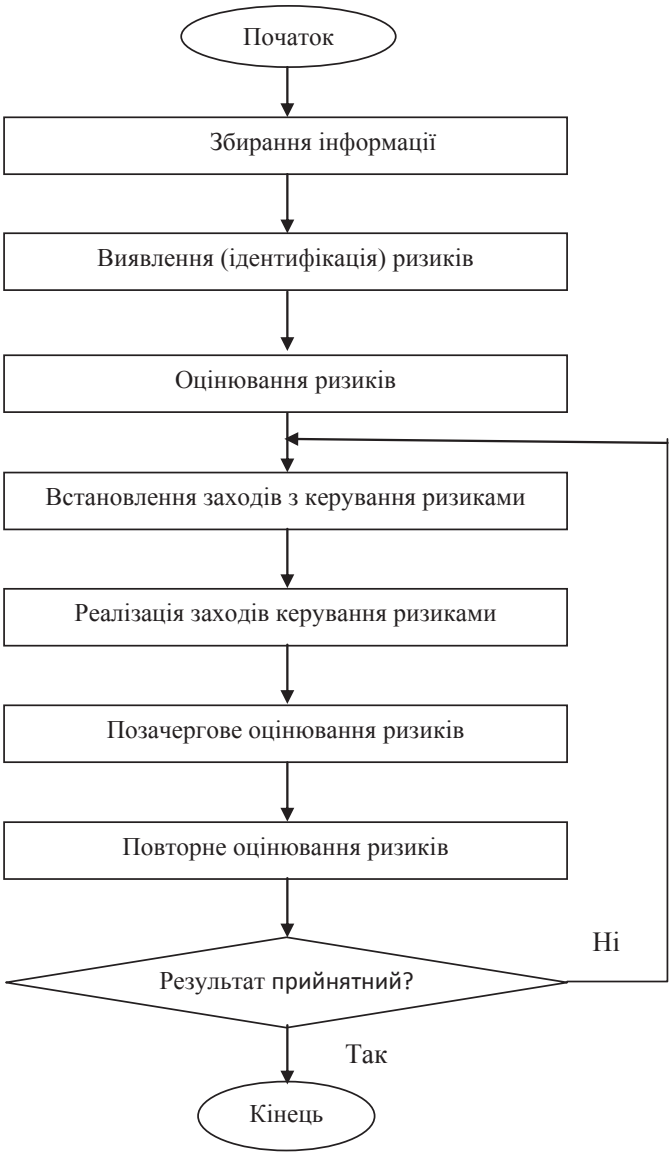

Рис. 1. Схема процесу «Оцінювання ризиків»

– органи влади;
– керівництво;
– права власності;
– персонал;
– розподіл ресурсів;
– фінанси;
– договори та угоди;
– навчання співробітників.

Під час виявлення небезпек потрібно враховувати можливість взаємного зв'язку кількох небезпеку разі одночасного їх виникнення.

Результати ідентифікації вносять у колонки 2-4 табл. 1.

Далі Група(на основі виявлених небезпек та їх причин)має оцінити наслідки кожної небезпеки та її імовірність. Існує багато методів оцінювання ризику. У стандарті [4] дана характеристика 31-му методу та описано, в яких ситуаціях їх найкраще застосовувати. Ми пропонуємо ризики ОС оцінювати за допомогою матриці наслідків/імовірностей, що передбачає поєднання якісних або напівкількісних оцінок наслідків та імовірностей для одержання рівня ризику чи його ранжування. Цей метод застосовний, оскільки у ОС можна ідентифікувати багато ризиків і потрібно визначати, які ризики потребують подальшого чи докладнішого аналізування, які необхідно обробляти насамперед, а які з них на даний час не потребують подальшого розглядання. Матричну оцінку також можна застосовувати для визначення прийнятності чи неприйнятності ризику. Перевагою даного методу також є візуалізація представлення даних.

Оцінювання кожного ризику полягає в аналізуванні імовірності його виникнення, можливих наслідків, визначенні величини та прийнятті рішення стосовно прийнятності чи неприйнятності ризику. Процес оцінювання ризику охоплює визначення відповідних зацікавлених сторін та консультування з ними з метою обговорення факторів, що негативно впливають на неупередженість, зокрема, на відкритість та сприйняття громадськістю. Такими сторонами можуть бути заявники ОС, промислові і торгівельні асоціації, урядові регуляторні органи або інші урядові структури, неурядові організації, в тому числі організації із захисту прав споживачів. Консультування з ними ОС повинен проводити без надання переваг будь-якій стороні.

Головною метою оцінювання ризиків є їх розподіл на прийнятні та неприйнятні. Для неприйнятних ризиків повинні бути розроблені заходи щодо їхнього усунення або переведення до категорії прийнятних.

Вважаємо, що ОС до неприйнятних ризиків ОС потрібно віднести вимоги стандарту [3] щодо заборони:

– проведення сертифікації системи управління іншого органу з сертифікації;

– пропонування або здійснювання консультування щодо систем управління ОС як частиною юридичної особи та будь-якою особою під організаційним контролем ОС;

– пропонування або здійснювання внутрішніх аудитів своїх сертифікованих заявників;

– сертифікування системи екологічного управління (СЕУ) заявника, внутрішні аудити якої ОС здійснював, щонайменше протягом двох років від дати закінчення внутрішніх аудитів;

– сертифікування СЕУ заявника щонайменше протягом двох років після закінчення консультування;

– залучення до здійснення аудитів СЕУ консалтингової організації;

– представлення або пропонування діяльності ОС як такої, що пов’язана з діяльністю організації, яка надає консультування з питань СЕУ;

– заявляння чи натякання, що сертифікація може бути простішою, легшою, швидшою або дешевшою, якщо буде задіяна певна консалтингова організація;

– залучання до аудиту або іншої сертифікаційної діяльності персоналу, зокрема того, який працює на керівних посадах та/або здійснював консультування щодо СЕУ;

– дозволяння комерційному, фінансовому або будь-якому іншому тиску ставити під загрозу неупередженість;

– залучання персоналу, як внутрішнього так і зовнішнього, доки він не зможе продемонструвати відсутність конфлікту інтересів.

Ризик оцінюють як добуток імовірності (колонка 5 табл. 1) та тяжкості наслідків (колонка 6 табл. 1). У колонку 7 табл. 1 заносять бальну оцінку ризику.

Імовірність кожного конкретного ризику визначають відповідно табл. 2, тяжкість наслідків – табл. 3. На підставі даних, одержаних у колонці 7 табл. 1, визначають пріоритетність ризику в залежності від числових критеріїв ризику (табл. 4). Для унаочнення представлення категорій ризику Група може визначити для них певне кольорове маркування, наприклад, зелене, жовте та червоне. Звертаємо увагу, що запропоновані критерії у таблицях 2 -4 наведені як приклад застосування матриці наслідків/імовірностей. Конкретні ситуації повинні враховувати різноманітні чинники, що характерні для даного ОС.

Таблиця 2

Критерії для бальної оцінки можливості виникнення потенціальної причини небезпеки

Оцінка імовірності	Опис	Імовірність виникнення	Бал
Дуже низька	Тільки надзвичайна ситуація	Імовірність виникнення протягом року менша 10%	**1**
Низька	Малоймовірно	Імовірність виникнення протягом року 11- 20%	**2**
Середня	Іноді виникає в особливих випадках	Імовірність виникнення протягом року 21-50%або виникає мінімум один раз на один рік	**3**
Висока	Зазвичай виникаєв ряді випадків	Імовірність виникнення протягом року 51-80%або виникає мінімум один раз на один квартал	**4**
Дуже висока	Виникає в більшості випадків	Імовірність виникнення протягом року більше 81%або виникає мінімум один раз на один місяць	**5**

Рішення щодо рівнів оцінювання ризиків приймає керівник ОС, наприклад, (табл. 4):

– ризики в діапазоні від 1 до 5 – зона низьких ризиків, їх вважають прийнятними, вони не потребують вжиття заходів керування;

– ризики в діапазоні від 6 до 12 – зона середніх ризиків, їх вважають значними, вони потребують вжиття заходів керування;

– ризики в діапазоні від 15 до 25 –зона високих ризиків, їх вважають неприйнятними, вони потребують обов'язкового вжиття заходів керування.

Члени групи розробляють заходи керування ризиками, що належать

Таблиця 3

Критерії для бальної оцінки тяжкості наслідків

Оцінка тяжкості наслідків	Опис				Бал
	Грошовий еквівалент	Законодавчий/ нормативно-правовий аспект	Задоволеність зацікавлених сторін	Репутаційний ефект	
Дуже мала	Невеликі проблеми, величина збитків до 1000 грн	Незначні порушення (адміністративна відповідальність), що підлягають коригуванню	Незначні проблеми за відсутності скарг та апеляцій	Незначний вплив на репутацію (1-2 статті у ЗМІ)	**1**
Мала	Невеликі проблеми, величина збитків до 5000 грн	Порушення (адміністративна відповідальність), що підлягають коригуванню	Негативна реакція деяких зацікавлених сторін, наявність 1 скарги та 1 апеляції за рік	Втрата репутації, яку можна відновити (3-5 статей у ЗМІ)	**2**
Середня	Фінансові проблеми, величина збитків до 10000 грн	Порушення (адміністративна відповідальність), що може призвести до призупинення діяльності	Негативна реакція деяких зацікавлених сторін, наявність 1 скарги та 1 апеляції за півроку	Втрата репутації, яку можна відновити	**3**
Велика	Серйозні фінансові проблеми, величина збитків до 20000 грн	Грубе порушення (адміністративна відповідальність), що може призвести до призупинення діяльності	Дуже негативне відношення, наявність 1скарги та апеляції за квартал	Втрата репутації, яку складно відновити	**4**
Дуже велика	Фінансові проблеми, величина збитків більше 20000 грн (максимальна страхова сума)	Загроза подальшому існуванню, втрата атестату акредитації	Дуже негативне відношення, наявність 1 скарги та 1 апеляції за місяць	Непоправна втрата репутації	**5**

до зон середніх та високих ризиків (пріоритетного керування), для зниження значення ризику або переводу значення в менш небезпечну зону. Визначені заходи можуть охоплювати:

Таблиця 4

Числові критерії для оцінювання ризиків

Тяжкість наслідків, бали	Імовірність виникнення, бали				
	1	*2*	*3*	*4*	*5*
1	**1**	**2**	**3**	**4**	**5**
2	**2**	**4**	**6**	**8**	**10**
3	**3**	**6**	**9**	**12**	**15**
4	**4**	**8**	**12**	**16**	**20**
5	**5**	**10**	**15**	**20**	**25**

– реалізацію визначених заходів зниження (пом'якшення) ризику;

– оптимальне прийняття рівнів ризиків, що забезпечує відповідність політиці ОС та критеріям ризиків;

– повне уникнення ризиків;

– перенесення ризиків на інші сторони (страхування тощо).

Для демонстрації повноти та завершеності аналізування ризикуможна вести перелік виключених на момент даного оцінювання ризиків.

Під час визначення заходів необхідно використовувати всі можливі ресурси ОС(адміністративні, навчальні, технічні тощо). Вибір заходів базується на значенні ризику до і після їх втілення. За наявності кількох варіантів рішення розглядають кожен і приймають той, що дозволить суттєво знизити ризик. Заходи заносять в ієрархічному порядку від найбільшого до найменшого рівня ризику до колонки 4 Плану впровадження заходів керування ризиками (табл. 5).

Таблиця 5

План впровадження заходів керування ризиками

№ з/п	Номер цілі СУ ОС	Опис ризику	Значення ризику до прийняття заходів	План робіт				Ризик після прийняття заходів (залишковий)			Аналіз результативності	
				Найменування заходу	Термін виконання	Відповідальні особи	Запланований об'єм витрат, грн	Імовірність	Тяжкість	Значення	Позитивно $K_п$	Негативно $K_п$
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*

Варто зауважити, що керування ризиком не зводиться виключно до дії на джерело ризику з метою зниження рівня. Управляти можна не лише внутрішніми, але й зовнішніми ризиками, наприклад, це може бути ухилення від ризику, страхування ризику тощо.

Для реалізації кожного заходу призначають відповідальну особу, встановлюють терміни та забезпечують ресурсами. У План впровадження можна вносити зміни. У такому випадку їх документують (фіксують версію та дату внесення змін). Визначена особа повинна

проводити моніторинг виконання заходів, а керівник ОС повинен контролювати реалізацію заходів у встановлені терміни.

При виявленні небезпек, що не враховані під час попереднього аналізування, проводять позачергове оцінювання ризиків. Такі небезпеки можуть спричинити:

– зміни у законодавчих та інших нормативно-правових актах;

– суттєві зміни в системі управління (СУ), зокрема, в організаційній структурі ОС;

– аналізування інцидентів, апеляцій та скарг;

– надходження інформації від персоналу ОС про виявлені ними нові або невраховані раніше небезпеки.

Щодо нових ризиків члени Групи оформляють додатковий протокол до основного. Якщо такі ризики підлягають пріоритетному керуванню, то для них розробляють заходи керування.

Повторне оцінювання ризиків проводять за необхідності або не менше ніж раз на рік під час підготування даних для щорічного аналізування з боку керівництва. У випадку, коли заходи щодо зниження ризиків не виявилися результативними (ризик не переведено до категорії «прийнятний»), проводять повторну процедуру встановлення заходів керування.

Результативність процесу виконання заходів керування ризиками оцінюють за коефіцієнтом $К_n$, де n приймає значення від 1 до 2:

$К_1$ – кількість оцінених ризиків/ загальна кількість ризиків. Прийнятне значення 0,9 – 1,0;

$К_2$ – кількість ризиків доведених до рівня прийнятних ризиків/загальна кількість ризиків. Прийнятне значення 0,9 – 1,0.

Процес оцінювання ризику має бути неперервним, тому Група повинна проводити регулярний моніторинг усіх видів ризику та переглядати записи в реєстрі ризиків. Для цього проводять регулярне аналізування кожного ризику та правильність опису і розрахунку, відповідність існуючим небезпекам, наслідкам, оцінці імовірності виникнення, вибраних заходів керування, що спрямовані на зменшення ризику. Діяльність з моніторингу обов'язково перевіряють під час внутрішнього аудиту.

Висновки

Для отримання та підтримки довіри ОС вкрай важливо демонструвати свою неупередженість, зокрема, показати, що його дії з оцінювання ризиків стосовно конфлікту інтересів, який виникає під час провадження сертифікації та може призвести до загрози неупередженості, є достатніми для усунення або мінімізації таких ризиків. Розгляд практичної послідовності виявлення та опису ризиків ОС дозволяє зробити певні висновки. По-перше, розглядання ризиків ОС як добутку імовірності та тяжкості наслідків можливої події дозволяє використовувати матрицю як зручний формат для їх відображення. По-друге, така послідовність виявлення та описування враховує вимоги основних міжнародних стандартів з ризик-менеджменту. По-третє, застосування спеціальної матриці ризик-аналізу суттєво полегшує та візуалізує процес виявлення та оцінювання ризиків. Отже, використання міжнародних стандартів

надає можливість керівникам ОС досягти припустимого рівня ризику за допомогою системного підходу до небезпечних подій і використання послідовності оцінки ризиків та результативно керувати ними.

Література

1. ДСТУ ISO 14001:2015Системи екологічного управління. Вимоги та настанови щодо застосовування
2. ДСТУ ISO Guide 73:2013Керування ризиком. Словник термінів
3. ДСТУ EN ISO/IEC17021-1:2015 Оцінка відповідності. Вимоги до органів, які проводять аудит і сертифікацію систем менеджменту. Частина 1. Вимоги
4. ДСТУ IEC/ISO 31010:2013Керування ризиком. Методи загального оцінювання ризиків