УДК 341.01(083.71):334-047.37
DOI https://doi.org/10.32837/yuv.v0i2.2315

М. Василенко,
доктор фізико-математичних наук, доктор юридичних наук, професор,
професор кафедри кібербезпеки
Національного університету «Одеська юридична академія»

В. Слатвінська,
викладач кафедри кримінального права, процесу та криміналістики
Міжнародного гуманітарного університету

Т. Шевченко,
кандидат юридичних наук,
доцент кафедри міжнародних відносин та права
Державного університету «Одеська політехніка»

МІЖНАРОДНО-ПРАВОВЕ РОЗУМІННЯ ДЕФІНІЦІЙ ТА ВИЗНАЧЕНЬ В ТЕОРІЇ РИЗИКІВ (АНАЛІЗ ТА УПРАВЛІННЯ РИЗИКАМИ): МІЖДИСЦИПЛІНАРНЕ ДОСЛІДЖЕННЯ

Постановка проблеми. Ризики представляють собою невід'ємну нашого буття і суспільства в якому ми живемо. Вони породжуються невизначеністю, відсутністю достатньо повної інформації про події, явища та неможливістю прогнозувати розвиток цих подій. Ризик виникає тоді, коли рішення вибирається з декількох можливих варіантів і немає впевненості, що воно найефективніше. Фактично ризик характеризується як невизначеність по відношенню можливих втрат на шляху до мети, проявляючи себе як міжгалузеве різнобічне явище з інформаційно-філософським значенням. Поняття «ризик» можна конкретизувати стосовно до мети дослідження, визначаючи його то як «відхилення фактичного результату від очікуваного», то як «ймовірність певної небажаної події». В даний час не існує однозначного тлумачення терміну «ризик». З багатьох публікацій у вітчизняних та іноземних виданнях відомо безліч визначень ризику, що несуть досить широке його тлумачення. Так, тільки у Інтернет-словниках міститься сотні тлумачень ризику у багатьох сферах людської діяльності (див. [1]). В наслідок цього виникають різні неоднозначності, пов'язані з розкриттям сутності самого ризику та пов'язаних з ним понять, які мають бути уніфіковані. Для цього існують певні міжнародні стандарти, які конкретизують ті чи інші поняття і яких існує вже у достатній кількості. В той же час не викликає заперечень той факт, що одним із важливих завдань науки, в цілому, а також правової науки, зокрема, і не тільки стало створення узгодженого і чіткого понятійно-категоріального апарату. Однак, акти інформаційно-правового блоку приймаються законодавцями достатньо важко,

а швидкість формування інформаційних відносин у суспільстві не відповідає швидкості їх нормативного закріплення, спостерігається термінологічний дисбаланс, неузгодженість категорій, багатозначне трактування понять, необґрунтована відсутність дефініцій, важливих для регламентації інформаційно-безпекових відносин. При цьому, як відзначено в роботі [2], інформаційна складова завжди випереджала правову складову. Подібна ситуація зумовлює актуалізацію дослідження проблем лінгвістично-термінологічного змісту категорій та визначення узагальнених понять та узгодженості з міжнародними стандартами. Про якість зазначеного можна говорити лише у тому разі, якщо акти містять у своєму складі норми-дефініції, які визначають базис для упорядкування інформаційних відносин. Значення таких норм дуже вагоме, оскільки «відповідно до системного галузевого і міжгалузевого характеру понять, дефініції інституту, галузі та законодавства в цілому покликані виконувати ієрархічну системо- і структуроутворюючу функцію у викладі регулятивних норм» [3, с. 64]. В першу чергу, це стосується інформаційного права, зокрема інформаційних ризиків, їх аналізу і управління. Так, на наш погляд, все ж таки треба мати корегування відповідних дефініцій з відповідними міжнародними стандартами. Зауважимо, що дефініції досить ґрунтовно вивчалися теорією держави і права (див., наприклад, підручник і роботи О. Ф. Скакун [4]). Стосовно ситуації в інформаційному праві нема суттєвих досягнень через специфіку досліджень, зокрема щодо ризиків, їх аналізу та управління [5]. Так, у роботі [6] розглядаються деякі поняття та онтологічні особливості нормативних дефініцій в інформаційному праві. Автором пропонується певна класифікація функцій нормативних дефініцій. На основі наукового аналізу конкретизуються проблеми понятійно-категоріального апарату інформаційного права та визначаються можливі шляхи їх подолання. Разом з тим, залишаються маловивченими теоретико-онтологічні особливості нормативних дефініцій та виявилося відкритим питання належного формування понятійно-категоріального апарату інформаційного права. При обговоренні ризиків та їх дефініцій слід пам'ятати, що інформаційна складова ризику є найбільш вагомою у випадках використання прогнозної інформації, дефіциту часу на обробку інформації та ухвалення рішення в умовах активної інформаційної протидії конкурентів або супротивника. На відміну від інших складових ризику інформаційна складова обов'язково є присутньою в кожній ризиковій події. Змінюється лише її відносна величина.

Метою статті є встановлення корегування і відповідності дефініцій з інформаційних ризиків з міжнародними стандартами, а також формулювання їх визначення та проведення змістово-правової уніфікації.

Виклад основного матеріалу. Не викликає сумнівів те, що настанню ризикової події можуть сприяти свідомі або неумисні дії людини. Навіть маючи якісну інформацію, фахівець може прийняти неправильне рішення або виконати неприпустиму дію, яка спричинить реалізацію ризикової події. Значна частина ризикових подій пов'язана з технічними системами, технологічними процесами, отриманими людиною речовинами та іншими об'єктами, що стали продуктами людської діяльності. Техногенні аварії, збої і відмови устаткування, екологічні катастрофи далеко не вичерпують повного переліку компонентів цього типу. Природні явища, тваринний та рослинний світ на сьогодні все ще недостатньо добре вивчені людиною, що, безумовно, впливає вірогідність ризиків. Людина безсила перед цілим рядом стихійних лих. Значна частина

з них доки ще не піддається точному і своєчасному прогнозуванню.

Поняття ризику, дане в міжнародному стандарті інформаційної безпеки, який в Україні має назву ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» [7], мабуть, виявилося найповнішим. Цей стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації. Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям і процесам, зазначеним в ISO / IEC 27001. Його рекомендації призначені, щоб допомогти реалізувати достатню інформаційну безпеку, засновану на підході менеджменту ризиками. Для достатнього розуміння цього стандарту важливим виявилося знайомство з поняттями, моделями, процесами і термінологією, описаними в ISO/IEC 27001 (очікується ISO/IEC FDIS 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements) та ISO/IEC 27002 (наразі ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls). Відомий стандарт (ISO/IEC 27005) був і залишається придатним до всіх типів організацій (наприклад, комерційні підприємства, урядові агентства, некомерційні організації), які мають намір здійснювати менеджмент ризиками, які ставлять під загрозу інформаційну безпеку організації. Стандарт не вказує, не рекомендує або навіть не називає конкретного методу управління ризиками. Проте це означає постійний процес, що складається з структурованої послідовності дій, серед яких основними визначаються наступні.

1. Встановити контекст управління ризиками (наприклад, обсяг, зобов'язання щодо дотримання, підходи / методи, що підлягають використанню, а також відповідні політики та критерії, такі як толерантність або апетит до ризику організації).

2. Високоякісно або якісно оцінити (тобто ідентифікувати, аналізувати та оцінювати) відповідні інформаційні ризики, беручи до уваги інформаційні активи, загрози, існуючі контролі та вразливі місця, щоб визначити вірогідність сценаріїв інцидентів або інцидентів, а також очікувані комерційні наслідки, якщо вони мали місце, визначити «рівень ризику».

3. Використовувати (наприклад, змінювати елементи інформаційної безпеки), зберігати (приймати), уникати та / або поділяти (з третіми сторонами) ризики відповідно, використовуючи «рівні ризику» для визначення їх пріоритету.

4. Відслідковувати ризики, ризикові методи лікування, зобов'язання та критерії на постійній основі, виявляючи та відповідаючи на відповідні суттєві зміни. Однак можна оперувати і більш простими визначеннями, що легко запам'ятовуються. Наприклад, ризик можна розглядати як просто потенційну проблему або як можливі втрати організації внаслідок інцидентів.

Аналіз відомих міжнародних стандартів щодо ризиків дозволяє авторам цієї роботи стверджувати те, що започаткування міжнародних стандартів сталося саме з запровадження стандарту управління інформаційною безпекою, що сьогодні відомий як британський стандарт BS 7799. Його перша частина – BS 7799-1 «Практичні правила управління інформаційною безпекою» – була розроблена Британським Інститутом стандартів (BSI) в 1995 р. на замовлення уряду Великобританії. Як випливає з назви, цей документ є практичним керівництвом управління інформаційною безпекою в організації. Він відтворює 10 галузей та 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ), визначених на основі кра-

щих прикладів зі світової практики. У 1998 році з'явилася друга частина цього британського стандарту – BS 7799-2 «Системи управління інформаційною безпекою. Специфікація та посібник із застосування», що визначила загальну модель побудови СУІБ і набір обов'язкових вимог для сертифікації. З появою другої частини BS 7799, яка визначила, що має собою представляти СУІБ, почався активний розвиток системи сертифікації у сфері управління безпекою. У 1999 році обидві частини BS 7799 р було переглянуто та гармонізовано з міжнародними стандартами систем управління ISO 9001 і ISO 14001, а через рік технічний комітет ISO без змін прийняв BS 7799-1 як міжнародний стандарт ISO 17799, який згодом був названо ISO 27002.

Друга частина BS 7799 переглядалася у 2002 р., а наприкінці 2005 р. була прийнята як міжнародний стандарт ISO/IEC 27001:2005 «Інформаційні технології – Методи забезпечення безпеки – Системи правління інформаційною безпекою – Вимоги». У той же час була оновлена і перша частина стандарту. З виходом ISO 27001 специфікації СУІБ набули міжнародного статусу, і тепер роль та престижність СУІБ, сертифікованих за стандартом ISO 27001, значно підвищилися.

BS 7799 та його міжнародні редакції поступово стали одними з найважливіших стандартів для галузі інформаційної безпеки. Проте, коли в серпні 2000 р. в ISO обговорювалася перша редакція міжнародного стандарту ISO 17799 (наразі ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls), важко вдалося досягти консенсусу. Документ викликав масу критичних зауважень з боку представників провідних IT держав, які стверджували, що він не відповідає основним критеріям, що висуваються до міжнародних стандартів. Відразу кілька держав, включаючи США, Канаду, Францію та Німеччину, виступили проти прийняття ISO 17799. На їхню думку, цей документ був гарним як набір рекомендацій, але не як стандарт. У США та європейських країнах до 2000 р. вже було проведено величезну роботу зі стандартизації інформаційної безпеки. Незважаючи на всі заперечення, авторитет BSI, який став засновником ISO, основним розробником міжнародних стандартів та головним органом із сертифікації у світі, переважив. Була запущена процедура прискореного узгодження, і стандарт незабаром був прийнятий. Основною перевагою ISO 17799 та споріднених стандартів є їх гнучкість та універсальність. У стандартах серії ISO 27000 відбилося все, що потрібно для управління інформаційними ризиками. Йдеться насамперед про випущений у 2008 році міжнародний стандарт ISO/IEC 27005:2008 (зараз ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management [8]), а також про його попередника – британський стандарт BS 7799-3:2006, що побачив світ у 2006 році. Заслуговує також на згадку американський стандарт у галузі управління ризиками NIST 800-30, який, у свою чергу, спирається на ISO Guide 73, ISO 16085, AS/NZS 4360. Основні положення цього стандарту були враховані при розробці ISO 27005. Всі ці стандарти у багатьох речах взаємно перегукуються, а деяких питаннях доповнюють одне одного. Такий стан речей дозволив нам провести систематизацію та вибірку основних дефініцій у відповідності з зазначеними вище міжнародними стандартами щодо ризиків, а також аналізу та управління ними. При цьому вказано відповідні стандарти, а результати такої роботи, проведеної нами, наведено нижче.

Конфіденційність – властивість, яка полягає в недоступності інфор-

мації або нерозкритому її змісті для неавторизованих осіб, суб'єктів або процесів (ISO/IEC 13335-1:2004).

Цілісність – властивість, що полягає у забезпеченні точності та повноти ресурсів (ISO/IEC 13335-1:2004).

Доступність – властивість, яка полягає в доступності та застосовності для авторизованих суб'єктів, коли потрібно (ISO/IEC 13335-1:2004).

Інформаційна безпека – забезпечення конфіденційності, цілісності та доступності інформації; додатково також можуть матися на увазі інші властивості, такі як автентичність, підзвітність, невідмовність та надійність (ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls [9]).

Подія інформаційної безпеки – ідентифікований стан системи, сервісу або мережі, що свідчить про можливе порушення політики безпеки або відсутність механізмів захисту, або колись траплялася невідома ситуація, яка може мати відношення до безпеки (ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 1: Guidelines to plan and prepare for incident response [10]).

Інцидент інформаційної безпеки – одна або серія небажаних чи несподіваних подій інформаційної безпеки, які мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки (ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response [11]).

Загроза – потенційна причина інциденту, який може завдати шкоди системі або організації (ISO/IEC 13335-1:2004).

Вразливість – слабкість ресурсу або групи ресурсів, яка може використовуватися при реалізації однієї або кількох загроз (ISO/IEC 13335-1:2004).

Ризик – комбінація ймовірності події та її наслідків (ISO GUIDE 73:2009 Risk management – Vocabulary [12]).

Ризик інформаційної безпеки – потенційна можливість використання певної загрози вразливості активу або групи активів для заподіяння шкоди організації.

Залишковий ризик – ризик, що залишається після обробки ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Ідентифікація ризику – це процес, що спрямований на знаходження, перерахування та опис елементів ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Аналіз ризику – систематичне використання інформації для ідентифікації джерел та оцінки величини ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Розрахунок ризику – процес присвоєння значень ймовірності та наслідків ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Оцінювання ризику – це процес порівняння оцінної величини ризику з встановленим критерієм ризику з метою визначення рівня значущості ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Оцінка ризику – загальний процес аналізу та оцінювання ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Обробка ризику – процес вибору та реалізації заходів щодо модифікації ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Уникнення ризику – рішення не брати участь у ситуації, пов'язаній із ризиком, або дія, спрямована на вихід із неї (ISO GUIDE 73:2009 Risk management – Vocabulary).

Зменшення ризику – заходи, що вживаються для зниження ймовірності або негативних наслідків, пов'язаних з ризиком, або того чи іншого (ISO GUIDE 73:2009 Risk management – Vocabulary).

Збереження (прийняття) ризику – тягар збитку або вигоди від конкретного ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Передача ризику – поділ з іншою стороною тяжкості збитку або вигоди, пов'язаної з ризиком (ISO GUIDE 73:2009 Risk management – Vocabulary).

Контроль ризику – дії, що реалізують рішення щодо управління ризиком (ISO GUIDE 73:2009 Risk management – Vocabulary).

Критерії ризику – показники, за допомогою яких оцінюється значимість ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Управління ризиком – скоординовані дії з управління та контролю організації щодо ризику (ISO GUIDE 73:2009 Risk management – Vocabulary).

Система управління ризиками – це набір елементів системи управління організацією, призначених для управління ризиками (ISO GUIDE 73:2009 Risk management – Vocabulary).

Комунікація ризику – обмін або спільне використання інформації про ризик між особою, яка приймає рішення, та іншими заінтересованими сторонами (ISO GUIDE 73:2009 Risk management – Vocabulary).

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, що ґрунтується на оцінці бізнес ризиків, яка призначена для створення, впровадження, експлуатації, моніторингу, аналізу, супроводу та вдосконалення інформаційної безпеки.

Декларація про застосовність – документована заява, що описує цілі та механізми контролю, які мають відношення та застосовні до СУІБ організації.

До цих визначень (в послідовності викладу) можна зробити деякі коментарі в контексті використання зазначених міжнародних стандартів. Так, ризик інформаційної безпеки визначається в термінах комбінації ймовірності події та її наслідків. Аналіз ризиків є основою для оцінювання ризиків, обробки ризиків та прийняття ризиків, а викладена інформація може включати історичні дані, теоретичний аналіз, компетентні думки та інтереси власників бізнесу. Уникнення ризику розглядається як рішення, що прийняте виходячи з результатів оцінювання ризику. У контексті ризиків інформаційної безпеки в описі збереження ризику враховуються лише негативні наслідки (збитки). Передача ризику сформулювала це положення в контексті ризиків інформаційної безпеки, коли при описах передачі ризику враховуються лише негативні наслідки (збитки), а вимоги законодавства або нормативної бази можуть обмежувати, забороняти або наказувати на передачу певного ризику. Передача ризику може здійснюватися укладанням договорів страхування або інших договорів. Вона може спричинити інші ризики або модифікувати існуючий ризик. Переміщення джерела ризику не є ризиком.

Критерії ризику можуть включати в себе пов'язані з ним витрати і вигоди, вимоги законодавства та нормативної бази, соціально-економічні аспекти та аспекти, пов'язані з навколишнім середовищем, інтереси власників бізнесу, пріоритети та інші вхідні дані для оцінки.

Управління ризиком зазвичай включає оцінку ризику, обробку ризику, прийняття ризику і повідомлення про ризик. Елементи системи управління ризиками можуть включати стратегічне планування, прийняття рішень та інші процеси, що мають справу з ризиками. Культура організації відображається у системі управління ризиками.

Інформація щодо комунікації ризику може стосуватися існування, природи, форми, ймовірності, небезпеки, прийнятності, обробки або інших аспектів ризику.

СУІБ включає організаційну структуру, політики, дії з планування, розподіл відповідальності, практики, процедури, процеси і ресурси.

Декларація про застосовність представляє собою цілі та механізми контролю, що базуються на результатах та висновках, отриманих у процесі оцінки ризиків та обробки ризиків, законодавчих вимогах та вимогах нормативної бази, договірних зобов'язаннях та бізнес-вимогах організації до інформаційної безпеки.

Зазначимо, що функціонування ризиків у форматі ринкових відносин характеризується неповною інформаційною відкритістю, наявністю протиріч та стохастичністю. В таких випадках важливо враховувати вплив ризику, коли негативними наслідками можуть стати втрата частини ресурсів, недоотримання доходів, поява додаткових витрат, збитки, закриття інвестиційних проєктів тощо. Невизначеність обумовлює наступ ситуації, яка не має однозначного результату, і тому, якщо існує можливість кількісно і якісно визначити ступінь ймовірності появи того чи іншого варіанту, це і буде ситуація ризику. Наявність елементів невизначеності обумовлює виникнення ситуацій, які не мають однозначного рішення. При цьому сутність будь-якого підходу до управління ризиками полягає в аналізі факторів ризику та прийнятті адекватних рішень з обробки ризиків. Чинники ризику завжди пов'язані з основними параметрами, якими оперують в оцінці ризиків і які були визначені та викладені нами вище. Отже, основні дефініції та їх визначення, які були сформульовані, виходячи з теорії ризиків, на відміну інших формулювань в правовій науці набули міжнародно-правового характеру й прийняті за основу в багатьох країнах світу.

Висновки. Дефініції відіграють досить суттєву роль щодо системи інформаційного права та відповідного законодавства, мають широке міжнародне використання і закріплені в міжнародних стандартах. Важливо зауважити, що першочергово це стосується тої частини інформатики, де існують суттєві невизначеності, а саме питання щодо невизначеності інформаційних ризиків, а також їх аналізу та управління ними. Слід враховувати, що необхідна їх узгодженість з іншими нормативно-правовими актами, що обумовлює однозначне та адекватне розуміння термінів таким чином, щоб вони відповідали міжнародним стандартам в зазначеній галузі інформатики. Нами була запропонована класифікація нормативних дефініцій у відповідності з міжнародними стандартами в найбільш невизначеній частині інформатики (кібербезпеки) – галузі, що стосується аналізу та управління ризиками.

У роботі приведені результати дослідження на встановлення корегування та відповідності дефініцій з інформаційних ризиків з міжнародними стандартами, а також надано формулювання, визначено та проведено змістово-правову уніфікацію щодо ризиків в цілому та в питаннях їх аналізу та управління. Дефініції відіграють досить суттєву роль в законодавства, а в системі інформаційного права вони мають широке міжнародне використання і закріплені в міжнародних стандартах. В інформаційних ризиках існують суттєві невизначеності. В першу чергу це стосується аналізу та управлінню ризиками. Проаналізовано відомі міжнародні стандарти щодо ризиків, сформульовано дефініції та надано визначення, а саме дефініції таких понять як сам ризик, загроза, вразливість, ризик інформаційної безпеки, залишковий ризик, ідентифікація ризику, аналіз та система управління ризи-

ками, а також все, що пов'язане з їх характеристиками (оцінювання, зменшення, обробка, прийняття, передача тощо), Встановлено критерії ризику і такі показники (властивості) як конфіденційність, цілісність, автентичність, підзвітність, невідмовність та надійність. Подію інформаційної безпеки визначено як ідентифікований стан системи, сервісу або мережі, що свідчить про можливе порушення політики безпеки або відсутність механізмів захисту, або як невідому ситуацію, що може мати відношення до безпеки, а інцидент інформаційної безпеки визначають як одну або серію небажаних (несподіваних) подій інформаційної безпеки, які мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки потенційна причина інциденту, який може завдати шкоди системі або організації. В цьому розумінні система управління інформаційною безпекою представляє собою частину загальної системи управління, що ґрунтується на оцінці бізнес ризиків і призначена для створення, впровадження, експлуатації, моніторингу, аналізу, супроводу та вдосконалення інформаційної безпеки.

У всіх випадках детінізації надано посилання на чинні міжнародні стандарти щодо ризиків. Зазначено, що сутність будь-якого підходу до управління ризиками полягає в аналізі факторів ризику та прийнятті адекватних рішень з обробки ризиків. Чинники ризику завжди пов'язані з основними параметрами, якими оперують в оцінці ризиків і які були визначені та викладені в статті, що пропонується.

Ключові слова: міжнародні стандарти, дефініції, теорія ризиків, класифікація, інформаційні ризики, аналіз, управління.

Vasilenko M., Slatvinskaya V., Shevchenko T. International legal understanding of definitions and definitions in risk theory (risk analysis and management): an interdisciplinary study

The paper presents the results of the study to establish the adjustment and compliance of definitions of information risks with international standards, as well as provided formulation, defined and carried out substantive and legal unification regarding risks in general and in matters of their analysis and management. The definitions play a very significant role in the legislation, and in the system of information law they have wide international usage and are fixed in the international standards. There are significant uncertainties in information risks. First of all, it concerns risk analysis and management. As known, international standards on risks are analyzed, definitions are formulated and definitions are given, namely definitions of such concepts as risk itself, threat, vulnerability, information security risk, residual risk, risk identification, risk analysis and risk management system, as well as everything related to their characteristics (assessment, reduction, processing, acceptance, transfer, etc. An information security event is defined as an identified condition of a system, service or network that indicates a possible violation of security policy or lack of protection mechanisms, or as an unknown situation that may be security-related, and an information security incident is defined as one or a series of unwanted (unexpected) information security events that have a significant probability of disrupting business operations or posing a threat to information security. In this understanding, an information security management system is part of an overall business risk-based

management system designed to create, implement, operate, monitor, analyze, maintain, and improve information security.

In all cases of deteanization a reference to current international standards regarding risks is provided. It is noted that the essence of any approach to risk management is to analyze risk factors and make adequate decisions on risk treatment. The risk factors are always related to the main parameters, which are used in risk assessment and which have been defined and outlined in the proposed article.

Keywords: international standards, definitions, risk theory, classification, information risks, analysis, management.

Література

1. Индеева В.В. К вопросу об определении понятия "риск". Сб. заочних электронных конференций. Электрон. дан. Москва : Российская Академия Естествознания. 2009. URL: http:www.rae.ru/arj/2007/02/Indeeva/pdf

2. Василенко М.Д. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення. Юридичний вісник. Одеса : ВД «Гельветика». 2018. № 4. С. 35–41.

3. Апт Л.Ф., Дорофеева Т.А. Методические рекомендации по формированию понятийного апарата законопроекта. Юридический вестник. 2009. № 3–4. С. 64–70.

4. Скакун О.Ф. Общее сравнительное правоведение. 208. 404 с.

5. Василенко М.Д., Козін О.Б. Право в теорії ризиків: генеза ризиків від правової до інфомаційної складових (інституційний підхід). Юридичний вісник. Одеса : ВД «Гельветика». 2019. № 4. С. 43–51.

6. Селезньова О.М. Нормативні дефініції в інформаційному праві. Правова інформатика. 2014. № 1(41). С. 23–29.

7. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. На заміну ДСТУ ISO/IEC 27005:2015. / Нац. стандарт України. – Вид. офіц. – [Чинний від 2019-11-01]. – Київ : ДП «УкрНДНЦ», 2019. 76 с.

8. ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

9. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

10. ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 1: Guidelines to plan and prepare for incident response. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

11. ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

12. ISO GUIDE 73:2009 Risk management – Vocabulary. URL: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en