ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 004:316.4:005.334

[0000-0001-5657-9144] **О. Б. Данченко,** *д.т.н., професор,*
e-mail: elen_danchenko@rambler.ru
[0000-0003-3389-5720] **Є. В. Ланських,** *к.т.н., доцент,*
e-mail: yevhenlanskykh@gmail.com
[0000-0002-4309-3556] **О. В. Семко,** *магістр*
e-mail: semkoinga77@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ІНФОРМАЦІЙНІ РИЗИКИ ЦИФРОВОГО ФОРМАТУ

Стаття присвячена питанню надійності та захисту інформаційних ресурсів, аналізу можливих негативних наслідків при настанні ризикових ситуацій. Автори визначили сутність та зміст поняття «інформаційний ризик» в умовах цифрової революції і нових технологій, відзначили необхідність комплексного підходу до ідентифікації, аналізу інформаційних ризиків та розробки плану управління інформаційними ризиками. Особливу увагу приділено інформаційним ризикам як окремій групі ризиків, що виникають при застосуванні інформаційних технологій.

Важко уявити, з якими ще ризиками на шляху діджиталізації зіткнеться організація та суспільство в найближчому майбутньому. У цьому сенсі цілком перспективною виглядає спроба пошуку шляхів та можливостей для безпечного подолання потенційних загроз, спираючись на тенденції та пріоритети, які диктує ринок і суспільство.

Ключові слова: *інформаційний ризик, цифрова трансформація, управління ризиками, класифікація, інформаційні технології.*

Вступ. Розвиток інформаційних технологій нині розглядається через призму створення глобальних промислових мереж з використанням штучного інтелекту (AI), поширенням Інтернету речей (Internet of things), впровадженням кіберфізічних систем та нейротехнологій з принципово новим механізмом взаємодії (пристроєм) «людина–машина», поширенням сервісів автоматичної ідентифікації, збору та обробки глобальних баз даних (big data), хмарних сервісів (cloud computing), розумних пристроїв та промислових об'єктів (smart everything), розвитком соціальних мереж, різноманітних платформ, сервісів цифрового середовища Інтернету [1].

Цифровий формат сучасного життя змінює традиційні уявлення про способи і механізми зберігання, обігу та захисту інформації, відкриває дорогу до інноваційного розвитку підприємств, що дає можливість поєднати всі виробничі процеси в єдину цифрову систему та максимально автоматизувати управління цією системою:

– використовуючи стратегію Mobile First, компанії отримують і монетизують мобільний трафік, який за своїми показниками вже наздогнав трафік зі стаціонарних пристроїв;

– готові рішення дають змогу економити час на вирішення завдань. Різні програми, розширення та конектори оптимізують роботу компанії і вимагають мінімальних витрат часу на їх впровадження та адаптацію;

– масове впровадження інтелектуальних датчиків в обладнання та виробничі лінії (технології індустріального Інтернету речей);

– перехід на безлюдне виробництво і масове впровадження роботизованих технологій;

– перехід на зберігання інформації та проведення обчислювань із власних потужностей на розподілені ресурси («хмарні» технології);

– наскрізна автоматизація та інтеграція виробничих і управлінських процесів у єдину інформаційну систему («від обладнання до міністерства»);

– використання всієї маси збираних даних (структурованої та неструктурованої інформації) для формування аналітики (технології «великих» даних);

– перехід на обов'язкову оцифровану технічну документацію та електронний документообіг («безпаперові» технології»);

– цифрове проектування та моделювання технологічних процесів, об'єктів, виро-

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

бів протягом усього життєвого циклу від ідеї до експлуатації (застосування інженерного програмного забезпечення);

– застосування технологій нарощування матеріалів взамін зрізання («адитивні» технології, 3D прінтинг);

– застосування сервісів із автоматичного замовлення витратних матеріалів і сировини для виробництва продукції й автоматичного постачання готової продукції споживачу, оминаючи посередницькі ланцюжки;

– застосування безпілотних технологій у транспортних системах, у т. ч. для постачання промислових товарів;

– застосування мобільних технологій для моніторингу, контролю процесів та управління ними у житті та на виробництві;

– перехід на реалізацію промислових товарів через Інтернет [2].

Цифрова революція, яка охопила світову економіку, вражає масштабом, темпами і географією. З кожним роком зростає інтенсивність впровадження нових технологій у виробництво й обслуговування людських потреб [3].

Однак інший бік масштабної цифровізації сфер життя веде до того, що громадяни України та бізнес усе більше потерпатимуть від зростання кіберзлочинності. Найнебезпечнішими для економіки та громадян є кібератаки на критичну інфраструктуру (енергозабезпечення, транспортне управління, банківський і телекомунікаційний сектори, медичне обслуговування, водопостачання тощо) України [4].

Мета дослідження – ідентифікувати та класифікувати інформаційні ризики; проаналізувати сучасні методи та засоби управління інформаційними ризиками в процесі цифрової трансформації.

Виклад основного матеріалу. В дослідженнях провідних фахівців у галузі контролю та управління ризиками О. Окишева та Г. Городової зазначено, що функція управління ризиками допомагає організаціям домогтися успіхів при впровадженні цифрових ініціатив. Сьогодні організації стрімко освоюють цифрові технології в умовах, коли обсяг даних збільшується, рівень автоматизації збільшується, кібератаки стають більш витонченими. На теперішній час ідентифіковано й описано більшість ризиків, але впровадження цифрових технологій «створює» передумови появи нових, ще не відомих ризиків.

«Готовність функції управління ризиками до цифрової трансформації» має дві складові:

– наявність навичок і компетенцій для надання стратегічних консультацій стейкхолдерам, проведення аудиту ініціатив, які пов’язані з цифровою трансформацією організації;

– зміни процесу та інструментарію управління ризиками повинні відбутися таким чином, щоб робота функції управління ризиками максимально базувалася на використанні даних і цифрових технологій для прогнозування ризиків та реагування на них з тим об’ємом і швидкістю, які необхідні при цифровій трансформації організації [5].

Фахівець відділу безпеки компанії Infopulse О. Дячук наголошує, що потреби клієнтів, які постійно змінюються, посилюють тиск на компанії, що мають застарілі системи і процеси; організації, що зволікають із впровадженням цифрових трансформацій, змушені поступатися своєю сферою впливу іншим конкурентним компаніям, які вже «народжені цифровими». Крім того, організаціям потрібно враховувати можливі ризики внаслідок використання технологій і ресурсів, які їм не належать або які вони не контролюють повністю.

Основна мета програмного забезпечення з управління ризиками та дотримання нормативних актів (GRC) (або будь-якого з його модулів) – автоматизувати більшість робочих процесів, пов’язаних зі звітуванням, моніторингом та документообігом [6].

В роботі І. А. Кораблінової зазначено, що вітчизняні компанії, які ще не мають достатньої захищеності від загроз зовнішнього середовища, можуть, скориставшись наполегливою рекомендацією здійснити «цифрову трансформацію», зробити такі кроки, які нанесуть збитки не тільки їм, а й вітчизняній економіці взагалі. Тобто, якщо організація прагне долучитися до всебічної цифровізації, то слід розуміти, чи може ця організація гідно прийняти нові загрози, які за своєю природою будуть залежати від інформації з нових цифрових систем, до яких вона інтегрується.

Оскільки цифрові перетворення пов’язують із розробкою та впровадженням інформаційно-комунікаційних технологій, під якими розуміють сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збору, обробки, збереження, поширення, відображення та викорис-

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

тання інформації в інтересах її користувачів, ризики, що виникають у процесі цих перетворень, отримали назву «інформаційні» [7].

У дослідженні [8] автори розкривають суть «інформаційних ризиків», які виникають на різних ієрархічних рівнях (держави, економіки в цілому, корпорацій, окремих підприємств тощо), і свій склад ризиків, що утворюють обсяг поняття «інформаційний ризик», який відбиває особливості його прояву на цьому рівні та враховує певні умови його функціонування. Так, наприклад, незважаючи на те, що проблема ризиків, пов'язаних з використанням інформації та інформаційних технологій, є відносно новою у загальній теорії ризиків, деякі з них вже включено до переліку глобальних ризиків, які загрожують людству та з якими воно поки що не в змозі впоратися [9].

У роботі Г. Мельника розроблено економіко-математичну модель, яка дає змогу точніше оцінювати ступінь інформаційних ризиків на підприємстві [10]. Також автор відзначає, що аналіз інформаційних ризиків є основою для побудови підсистеми управління інформаційною безпекою підприємства, і підкреслює необхідність виконувати такі кроки:

– ідентифікація інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику, можливих загроз активу, та визначення рівня загроз безпеці КІС підприємства;

– оцінювання рівня дієвості засобів контролю безпеки корпоративної системи; оцінювання вразливості корпоративної системи, що розглядається як результат впливу факторів вірогідного рівня сили загрози та рівня дієвості засобів контролю;

– оцінювання частоти подій втрат від інформаційних ризиків як результату впливу факторів частоти виникнення загрози та вразливості корпоративної системи; оцінювання величини можливих збитків від інформаційних ризиків у корпоративній системі;

– оцінювання рівня інформаційних ризиків у корпоративній системі як результуючої двох факторів: частоти подій втрат та величини можливих втрат від інформаційних ризиків.

Діджиталізація – неоднозначна модель розвитку суспільства, економіки і виробництва, при всіх її позитивних ефектах необхідно прогнозувати, ідентифікувати та управляти негативними загрозами, викликами.

Результати досліджень. Ризик – невизначена подія або умова, настання якої негативно або позитивно позначається на цілях проекту [11].

На сьогодні ще немає однозначного поняття «інформаційний ризик». Деякі фахівці розглядають інформаційний ризик як подію, яка безпосередньо впливає на інформацію: її видалення, спотворення, порушення її конфіденційності або доступності. Інші розглядають це поняття, обмежуючи зону інформаційного ризику лише комп'ютерними системами [12].

Можливість настання випадкової події в інформаційній сфері (інформаційній системі) підприємства, в результаті якої підприємству буде завдано збитку, називають інформаційним ризиком [13].

Інформаційна система організації охоплює всі сфери її діяльності (адміністративну, виробничу, фінансову), є сполучною ланкою при розробці стратегії бізнесу та якості управління організацією і персоналом. Вона містить відомості, що стосуються планів, стану матеріальних та фінансових потоків, договірної діяльності, дані фінансового і управлінського обліку.

Така інформація має цілісний, конфіденційний характер, а її втрата може виявитися критичною для роботи всієї організації. Тому передбачається, що побудова роботи користувачів з інформацією, яка міститься в системі, вимагає спеціальних заходів захисту, які забезпечують конфіденційність, цілісність і доступність даних [14].

За останній час почав активно розвиватися науковий напрям з ефективного управління IT-ризиками. Сучасний рівень інформатизації в організаціях дає змогу використовувати визначення рівня ризику з метою ефективного управління інформаційними технологіями та забезпечення економічної безпеки організації за допомогою підвищення надійності бізнес-процесів. Тобто, ідентифікацію ризиків з їх подальшим аналізом та оцінкою необхідно розглядати як основу сталого функціонування організації. Управлінські рішення по створенню і модернізації інформаційних технологій мають ґрунтуватися на регулярному оцінюванні інформаційних ризиків [11, 13].

Обговорення результатів. Для проведення цілісного аналізу інформаційних ризиків необхідно створити класифікаційну базу ризиків. Якщо інформаційні ризики згрупува-

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

ти відповідно за окремими критеріями, то можна застосувати індексовану схему класифікації. Пропонуємо цю схему у вигляді схеми Ісікави (рисунок 1).

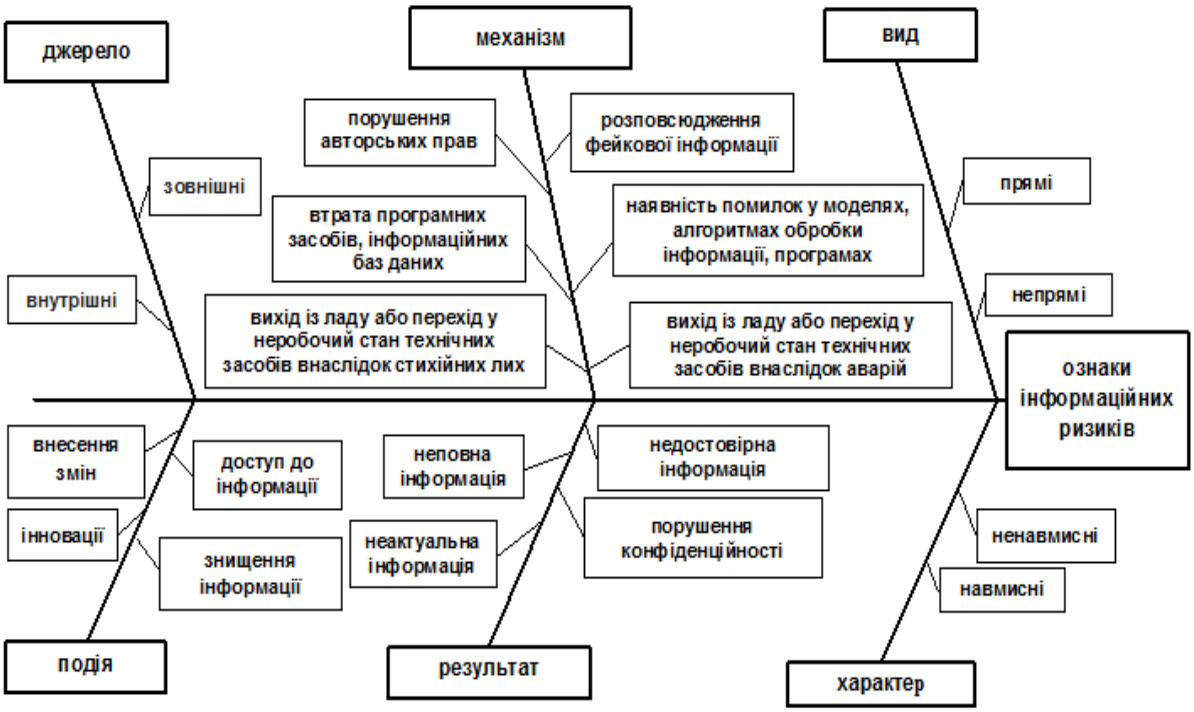

Рисунок 1 – Індексована схема класифікації інформаційних ризиків

Складено за: [13]

Методологія управління ризиками базується на якісному та кількісному оцінюванні ідентифікованих ризиків, не винятком є й інформаційні ризики. Завданням якісного оцінювання є визначення можливих видів ризиків, оцінювання принципового рівня пріоритетності загроз, а також виділення чинників, які впливають на рівень обґрунтування різних можливих контрзаходів [15]. Якісне оцінювання часто супроводжується кількісним, яке визначає імовірність виникнення ризиків та наслідків, що несуть ризикові події. Автор роботи [15] відзначає, що на початкових етапах аналізу інформаційних ризиків, як правило, використовується якісне, а на кінцевому – кількісне оцінювання.

Однозначної загальної методики, за якою можна було б визначити кількісну величину ризику, на сьогоднішній день не існує, що обумовлено відсутністю достатнього обсягу статистичної інформації про можливість виникнення будь-якої конкретної загрози. Крім того, визначити величину вартості конкретного інформаційного активу досить важко (рисунок 2).

Рисунок 2 – Фактори оцінювання інформаційних ризиків

Складено за: [10, 16]

Виділяють наступні етапи аналізу інформаційних ризиків (таблиця 1).

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

Таблиця 1 – **Етапи аналізу інформаційних ризиків**

№	Етап	Складові етапу
1	Ідентифікація	інформаційні ресурси (активи) організації як об'єкт ризику
		можливі загрози (комбінації загроз) активу та ідентифікація можливих небезпек, які загрожують
2	Оцінювання частоти виникнення загрози можливих втрат від настання ризикової ситуації	експертне оцінювання рівня загроз за набором показників, які характеризують можливість доступу порушника відповідного класу до інформаційних ресурсів
		очікуване реагування засобів контролю впродовж відведеного часового інтервалу
		вразливість як результат впливу факторів можливого рівня сили загрози та реагування засобів контролю на загрозу
		частота виникнення загрози як можлива частота реалізації чинників ризику (агентів загрози) в межах певного часового інтервалу
		частота виникнення подій втрат – можлива частота протягом визначеного часового інтервалу, з якою агент загрози завдає шкоди активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості
3	Оцінювання величини можливих втрат від настання ризикової ситуації	ввизначення можливої дії кожного з агентів загрози інформаційному активу
		оцінювання величини кожної з можливих форм втрат, що пов'язані з дією певного агента загрози
		оцінювання величини всіх можливих форм втрат
4	Результат аналізу та контрзаходи	оцінювання загального рівня інформаційних ризиків у корпоративній системі; план реагування на ризики із зазначенням пріоритетів рішень по ризиках
5	Моніторинг та контроль	контроль поточного стану захищеності інформаційних систем та планування заходів із захисту
		моніторинг дій та результатів проведення заходів, спрямованих на підвищення ефективності захисту інформації

Складено за: [10, 16]

Результати якісного оцінювання використовуються для формування зв'язку між імовірністю та наслідками події для ключових ризиків. З його допомогою можна вимірювати та описувати профіль ризику організації. Приклад наведено в таблиці 2, яка містить інформацію на основі даних рисунка 1.

Оцінювання важливості ризиків, тобто пріоритетності для обробки, здійснюється за допомогою матриці імовірності та впливу настання ризикових подій (таблиця 3).

В дослідженні [5] автори відзначають, що чим більше функція управління ризиками відповідає планам діджиталізації, тим вища імовірність досягнення мети організації, передбаченої цифровими ініціативами, і пропонують наступні характеристики управління ризиками, які допомагають у прийнятті обґрунтованих рішень, що, в свою чергу, збільшують шанси на успіх у цифровізації:

– повна залученість у план цифрової трансформації організації;

– підвищення кваліфікації спеціалістів задля відповідності темпам розвитку організації;

– визначення балансу компетенцій для роботи з новими технологіями;

– активна взаємодія з особами, що приймають рішення з питань основних цифрових ініціатив;

– комунікація та синхронізація з метою створення єдиної думки про ризик.

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

Таблиця 2 – **Якісне оцінювання груп інформаційних ризиків**

№ п/п	Найменування групи ризиків	Усереднена імовірність виникнення ризиків (0 ÷ 1)	Усереднений вплив на інформаційні активи від настання ризиків (0 ÷ 1)
1.	Ризики за механізмом виникнення	0,8	0,9
2.	Ризики за характером виникнення	0,7	0,7
3.	Ризики за видами виникнення	0,5	0,6
4.	Ризики за джерелом виникнення	0,5	0,6
5.	Ризики за характером події	0,8	0,8
6.	Ризики за результатом	0,6	0,5

Складено з урахуванням [13]

Таблиця 3 – **Матриця імовірності та впливу настання ризикових подій**

Вплив	Імовірність				
	0,1	0,3	0,5	0,7	0,9
0,8 ÷ 1,0				5	1
0,6 ÷ 0,8			7	2	
0,4 ÷ 0,6			3, 4		
0,2 ÷ 0,4					
0,0 ÷ 0,2					

– зона помірних ризиків;
– зона високих ризиків;
– зона низьких ризиків.

За результатами ідентифікації та оцінювання інформаційних ризиків приймають рішення щодо можливості уникнення або зниження рівня наслідків інформаційних ризиків. Реагування на настання ризикових подій базується на розробці методів і технологій зниження негативного впливу ризиків. Тому готують кілька варіантів стратегій (сценаріїв) реагування, головна мета яких спрямована, в першу чергу, на виключення умов виникнення ризиків.

На ринку інформаційних технологій існує велика кількість програмних засобів, впровадження яких забезпечує ефективне управління інформаційними потоками та виявлення інформаційно-технологічних ризиків, що пов'язані з діяльністю організації, для якої застосовуються ті чи інші методи управління.

До якісних методик управління ризиками на основі вимог ISO 17999 відносяться методики Risk Advisor, COBRA, КОНДОР+, Proteus Enterprise, OCTAVE, а також Digital Security Office, РискМенеджер, Oracle Crystal Ball, @Risk, Risk Watch [17].

До основних результатів автори статті відносять узагальнення аналізу інструментальних засобів оцінювання ризиків.

Висновки. На основі проведеного в статті аналізу можна зробити наступні висновки. По-перше, цифрова трансформація виробництва, суспільного життя неминуча. Її здійснення веде як до розширення можливостей організацій у мережі, так і до небезпек. По-друге, інформаційні ризики, які часто супроводжують процес цифровізації, підпорядковуються стандартам управління ризиками, головним інструментарієм для «боротьби» з ними є ідентифікація та оцінювання ризиків інформаційних активів компанії. По-третє, формулювання та здійснення політики без-

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

пеки усунення ризиків не буде ефективним, якщо існуючі стандарти використовуються не за правилами. Саме тому роботи із забезпечення інформаційної безпеки повинні бути комплексними.

Управління інформаційними ризиками – досить суб'єктивний та складний процес у діяльності організацій, особливо, якщо діяльність пов'язана з конфіденційною інформацією або прихованою інформацією, або просто з великими обсягами інформації, коли імовірність її непередбаченого витоку є досить великою.

Тому ця проблематика на сьогодні є досить актуальною, а задачі захисту інформації від можливих ризиків – перспективними, які потребують вдосконалення вже існуючих методів протидії чи розробки нових, що дає необхідність продовжити роботу в цьому напрямі.

Подальші дослідження полягають в ідентифікації й якісному та кількісному оцінюванні окремих ризиків серед запропонованих груп інформаційних ризиків з подальшою розробкою протидій у процесі ризик-менеджменту. Також у сучасних умовах цифрової трансформації суспільства актуальною є розробка нових методів управління саме інформаційними ризиками, які б інтегрували в собі процеси інформаційного менеджменту та управління ризиками в компанії в цілому, елементи ризик-менеджменту в проектах, а також засоби інформаційної безпеки.

Список використаних джерел

[1] А. А. Карцхия, "Цифровая революция: новые технологии и новая реальность", *Правовая информатика,* № 1, 2017.

[2] І. Г. Яненкова, "Цифрова трансформація промисловості України: ключові акценти", *Економіка та управління національним господарством. Проблеми економіки,* № 4, с. 179-184, 2017.

[3] И. Н. Макаров, О. В. Широкова, В. А. Арутюнян, и Е. Э. Путинцева, "Цифровая трансформация разномасштабных предприятий, вовлеченных в реальный сектор российской экономики", *Экономические отношения*, т. 9, № 1, с. 313-326, 2019. doi: 10.18334.

[4] Валерій Фіщук, Володимир Матюшко, Єгор Чернєв, Олександр Юрчак, Яна Лаврик, та Анатолій Амелін, "2030 E – країна з розвинутою цифровою економікою". [Електронний ресурс]. Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-10. Дата звернення: Берез. 2020.

[5] А. Окишев, и А. Городова, "Разумное управление рисками в ходе цифровой трансформации", *Исследование из серии "Взгляд на риски" за 2019 год*. [Электронный ресурс]. Режим доступа: http://pwc.com/us/RiskStudy. Дата обращения: Март 2020.

[6] О. Дячук, "Як вирішити проблеми в системі безпеки під час цифрової трансформації бізнесу". [Електронний ресурс]. Режим доступу: https://ain.ua/2020/02/08/yak-virishiti-problemi-v-sistemi-bezpeki-pid-chas-cifrovoï-transformacii-biznesu/. Дата звернення: Берез. 2020.

[7] І. А. Кораблінова, "Цифрова трансформація" як джерело ризику компаній у сучасних умовах", *Інноваційна економіка*, № 1-2, с. 217-223, 2018.

[8] В. М. Гранатуров, та І. А. Кораблінова, "Інформаційний ризик підприємства: щодо вирішення проблеми qui pro quo у визначенні поняття", *Інноваційна економіка,* № 5-6 (69), с. 199-206, 2017.

[9] The Global Risks Report 2017. Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf.

[10] Г. Мельник, "Модель оцінювання рівня інформаційних ризиків в корпоративних системах", *Вісник Київського національного університету ім. Тараса Шевченка. Економіка*, № 6 (171), с. 48-54, 2015.

[11] "A guide to the project management body of knowledge (PMBOK guide)", *BISAC: Business & Economics / Project Management*, 6 th. edition, Newtown Square, PA, USA: Project Management Institute, pp. 395-458, 2017.

[12] И. А. Киселева, и С. О. Искаджян, "Информационные риски: методы оценки и анализа", *ИТпортал*, № 2, 2017 [Электронный ресурс]. Режим доступа: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/. Дата обращения: Март 2020.

[13] М. И. Левина, и В. Ю. Петров, "Управление информационными рисками при

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

внедрении информационных систем", *Международный студенческий научный вестник*, № 2, с. 1-5, 2014.

[14] О. Б. Кузнецова, "Оценка информационных рисков в обеспечении экономической безопасности предприятия", *Труды ИСА РАН*, т. 31, с. 77-98, 2007.

[15] О. Архипов, та А. Скиба, "Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації", *Захист інформації*, т. 15, № 4, с. 366-375, жовтень-грудень, 2013.

[16] J. A. Jones, "An introduction to FAIR", *Trustees of Norwich University,* p. 67, 2005.

[17] Б. Я. Корнієнко, Ю. О. Максімов, та Н. М. Марутовська, "Прикладні програми управління інформаційними ризиками", *Захист інформації*, № 4, с. 60-64, 2012.

References

[1] A. A. Kartshia, "The digital revolution: new technologies and the new reality", *Pravovaya informatika,* no. 1, 2017. [in Russian].

[2] I. G. Yanenkova, "Digital transformation of the Ukrainian industry: key highlights", *Ekonomika ta upravlinnia natsionalnym hospodarstvom. Problemy ekonomiky,* no. 4, pp. 179-184, 2017. [in Ukrainian].

[3] I. N. Makarov, O. V. Shirokova, V. A. Arutyunyan, and E. E. Putintseva, "Digital transformation of large-scale enterprises involved in the real sector of Russian economy", *E`konomicheskie otnosheniya,* vol. 9, no. 1, pp. 313-326, 2019. doi: 10.18334. [in Russian].

[4] Valeriy Fishchuk, Volodymyr Matyushko, Yehor Chernev, Oleksandr Yurchak, Yana Lavryk, and Anatolii Amelin, "2030 E is a country with developed digital economy". [Online]. Available: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-10. Accessed on: Mar. 2020.

[5] A. Okishev, and A. Gorodova, "Reasonable risk management in the course of digital transformation. Risk Sight Survey. 2019 [Online]. Available: http://pwc.com/us/RiskStudy. Accessed on: Mar. 2020

[6] O. Dyachuk, "How to solve security problems during digital business transformation". [Online]. Available: https://ain.ua/2020/02/08/yak-virishiti-problemi-v-sistemi-bezpeki-pid-chas-cifrovoï-transformacii-biznesu/. Accessed on: Mar. 2020.

[7] I. A. Korablinova, "Digital transformation as a source of risk for companies in today's environment", *Innovatsiina ekonomika,* no. 1-2, pp. 217-223, 2018. [in Ukrainian].

[8] V. M. Granaturov, and I. A. Korablinova, "Enterprise information risk: to solve the qui pro quo problem in defining a concept", *Innovatsiina ekonomika,* no. 5-6 (69), pp. 199-206, 2017. [in Ukrainian].

[9] The Global Risks Report 2017. [Online]. Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf. Accessed on: Mar. 2020.

[10] G. Melnyk, "A model for assessing the level of information risks in corporate systems", *Visnyk Kyivskoho natsionalnoho universytetu im. Tarasa Shevchenka. Ekonomika,* no. 6 (171), pp. 48-54, 2015. [in Ukrainian].

[11] "A guide to the project management body of knowledge (PMBOK guide)", *BISAC: Business & Economics / Project Management*, 6 th. edition, Newtown Square, PA, USA: Project Management Institute, pp. 395-458, 2017.

[12] I. A. Kiseleva, and S. O. Iskadzhian, "Information risks: methods of assessment and analysis". *ITPortal,* no. 2, 2017 [Online]. Available: http://itportal.ru/ science/economy/informatsionnye-riski-metody-otsenk/. Accessed on: Mar. 2020.

[13] M. I. Levina, and V. Yu. Petrov, "Information risk management in the implementation of information systems", *Mezhdunarodnyiy studencheskiy nauchnyiy vestnik,* no. 2, pp. 1-5, 2014. [in Russian].

[14] O. B. Kuznetsova, "Assessment of information risks in ensuring the economic security of the enterprise", *Trudyi ISA RAN,* vol. 31, pp. 77-98, 2007. [in Russian].

[15] O. Arkhipov, and A. Skiba, "Information risks: methods and ways of research, risk models and methods for their identification". *Zakhyst informatsii,*

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792

vol. 15, no. 4, pp. 366-375, Oct.-Dec., 2013. [in Ukrainian].

[16] J. A. Jones, "An introduction to FAIR", *Trustees of Norwich University*, pp. 67, 2005.

[17] B. Ya. Kornienko, Yu. O. Maksimov, and N. M. Marutovska, "Information risk management applications", *Zakhyst informatsii,* no. 4, pp. 60-64, 2012. [in Ukrainian].

O. B. Danchenko, *D.Sc., professor,*
e-mail: elen danchenko@rambler.ru
E. V. Lanskykh, *Ph.D., associate professor,*
e-mail: yevhenlanskykh@gmail.com
O. V. Semko, *M.Sc.*
e-mail: semkoinga77@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

INFORMATION RISKS OF THE DIGITAL FORMAT

The article is devoted to the issue of reliability and protection of information resources, possible negative consequences when risk situations arise. The authors have made an attempt to define the essence and content of the concept of information risk in the conditions of the digital revolution and new technologies, noted the need for a comprehensive approach to the identification and analysis of information risks, reducing negative consequences in case of risk events. Particular attention is paid to information risks as a component of risks arising from the use of different information technologies.

Losses from information risks can be material (in the form of damages, lawsuits, etc.), and can be viewed through the prism of intangible losses (in the form of loss of trust or, in general, reputation). The main task of information security professionals is to apply timely and complete assessment of IT risks using methodological bases of risk management. Organizations must determine their strategy in information security in order to further manage their risks effectively.

In the article the authors give an example of analysis, estimation, probability matrix and possible influence of risk events in the process of digitization. To help combat IT risks in the information technology market, software has been developed to provide adequate management by information flows and IT risks, including Risk Advisor, COBRA, KONDOR +, Proteus Enterprise, OCTAVE, as well as Digital Security Office, RiskManager, Oracle Crystal Ball, @Risk, Risk Watch.

It is difficult to imagine what other risks an organization and society will face in the near future in the way of digitization. In this sense, an attempt to find ways and opportunities to safely overcome potential threats, based on trends and priorities which are dictated by the market and society, is quite promising.

Keywords: *information risk, digital transformation, risk management, classification, information technologies.*

Стаття надійшла 14.04.2020
Прийнято 04.09.2020

© О. Б. Данченко, Є. В. Ланських, О. В. Семко, 2020
DOI: 10.24025/2306-4412.3.2020.200792