Розділ 3

Інноваційний менеджмент

УДК 005.9:004.738.5:342.738 **JEL Classification: D04, D81, L86, O32**

Ірина Миколаївна Сотник,
д-р екон. наук, професор, професор кафедри економіки і бізнес-адміністрування, Сумський державний університет (м. Суми, Україна);
Костянтин Юрійович Завражний,
аспірант кафедри економіки і бізнес-адміністрування, Сумський державний університет (м. Суми, Україна)

ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ НА ПІДПРИЄМСТВІ[1]

У статті обґрунтовані перспективи розвитку Інтернету речей та промислового Інтернету речей, акцентована увага на економічних ефектах упровадження масштабних інформаційних систем управління виробництвом сучасних підприємств шляхом використання системних рішень класу ERP. Доведено, що погіршення інформаційної безпеки діяльності підприємств та організацій є однією з важливих проблем, що супроводжують розбудову промислового Інтернету речей. Проаналізовано підходи до забезпечення інформаційної безпеки промислового Інтернету речей у суб'єктів господарювання з урахуванням сучасних досягнень у сфері інформаційних технологій. Визначено основні підходи до економічного обґрунтування інвестицій у цей напрямок діяльності.

Ключові слова: інформаційна безпека, підприємство, інформаційні технології, промисловий Інтернет речей, програмне забезпечення, інвестиції, економічна ефективність.
DOI: 10.21272/mmi.2017.3-17

Постановка проблеми. Сучасний розвиток інформаційних технологій (ІТ) істотно розширює можливості ефективного ведення бізнесу, створює інноваційні конкурентні переваги, відкриває перед компаніями нові ринки. Водночас розвиток ІТ супроводжують і певні вади, що полягають у загостренні проблем інформаційної безпеки суб'єктів господарювання, зростанні кіберзлочинності. Вплив інформаційних ризиків реалізується через уразливість інформаційних систем, що підтримують різні види господарської діяльності промислових підприємств, та виникнення збитків компаній унаслідок витоків конфіденційної інформації, збоїв у роботі інформаційних мереж і систем. У зв'язку з цим, виникає необхідність забезпечення інформаційної безпеки суб'єктів господарювання як соціально-економічних систем у цілому.

Згідно з дослідженнями [3] для фірм, які активно використовують новітні ІТ, функціональна

[1] Публікація підготовлена в рамках НДР «Розроблення фундаментальних основ відтворювального механізму «зеленої» економіки в умовах інформаційного суспільства» (№ д/р 0115U000684), яка фінансується за рахунок державного бюджету України.

сумісність і безпека є основними обмеженнями на шляху до забезпечення прогресу. Керівництво таких підприємств вживає певних заходів щодо захисту важливої інформації. Однак основною причиною проблем у сфері забезпечення інформаційної безпеки є відсутність ефективної управлінської політики, що базується на організаційних, економічних і технічних рішеннях із подальшим контролем їх реалізації та оцінюванням ефективності. Це визначає необхідність і актуальність розвитку систем забезпечення інформаційної безпеки промислових підприємств [17].

Аналіз останніх досліджень і публікацій. Над проблемами інформаційної безпеки суб'єктів господарювання працює багато вітчизняних та зарубіжних вчених. У цьому контексті серед українських науковців необхідно виділити праці А. Е. Архипова [9], К.П. Боримської [1], Л.Ф. Єжової [5], С.В. Казмирчук [9], А.Г. Корченко [9], С.В. Ленкова [11], Л.Г. Мельника [12], Д.А. Перегудова [11], Л.А. Поливаної [13], В.А. Хорошко [11] та ін. Серед зарубіжних вчених доцільно відзначити праці П. Брукса [2], М. Витмана [22], В.А. Галатенко [3], В.І. Завгороднього [6], Р.С. Каплан [8], Д.П. Нортона [8] тощо.

Науковий доробок учених охоплює дослідження технічних й організаційно-економічних аспектів формування систем інформаційної безпеки промислових підприємств, їх теоретичне та методичне обґрунтування. Науковцями розроблено технічні, програмні методи і засоби інформаційного захисту, а також підходи до створення комплексних систем захисту інформації. Водночас питанням забезпечення інформаційної безпеки такого нового напряму ІТ, як промисловий Інтернет речей, оцінюванню економічної ефективності інвестицій промислових підприємств в його інформаційну безпеку приділяється недостатньо уваги.

Метою статті є дослідження перспектив розвитку промислового Інтернету речей, проблем та підходів до забезпечення його інформаційної безпеки в суб'єктів господарювання, а також визначення підходів до економічного обґрунтування інвестицій у цей напрямок діяльності.

Результати дослідження. Реалії сучасного бізнесу є такими, що в умовах ринку практично будь-яка компанія зосереджена на підтриманні своєї конкурентоспроможності. Бурхливий розвиток ІТ останніми десятиліттями, поява і розповсюдження глобальних та локальних інформаційних мереж, вдосконалення і збільшення доступності програмного забезпечення та комп'ютерної техніки обумовили широке впровадження ІТ у практику господарювання підприємств і організацій, забезпечуючи отримання ними додаткових конкурентних переваг. Особливої популярності у цьому контексті сьогодні набувають «розумні» системи, які управляють речами без втручання людини і становлять основу концепції Інтернету речей.

Інтернет речей (*англ*. Internet of Things, IoT) – це мережа, що складається із взаємопов'язаних фізичних об'єктів (речей) або пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу й обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку [8]. Крім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові й бездротові мережі. Ці взаємопов'язані об'єкти (речі) мають можливість зчитування та приведення в дію, функцію програмування й ідентифікації, а також дозволяють виключити необхідність участі людини за рахунок використання інтелектуальних інтерфейсів [16].

Відповідно до [19] існують такі прогнози розвитку ринку Інтернету речей:

– консалтингова компанія Bain передбачає, що до 2020 року річний дохід постачальників IoT, які продають обладнання, програмне забезпечення та комплексні рішення, може перевищити 470 млрд дол. США;

– за оцінюваннями консалтингової компанії McKinsey, загальна місткість ринку IoT, що у 2015 році становила близько 900 млн дол. США, зросте до 3,7 млрд дол. США у 2020 році із середньорічними темпами приросту на рівні 32,6 %;

– компанія IHS Markit прогнозує, що ринок IoT-пристроїв зростатиме з 15,4 млрд пристроїв у

2015 році до 30,7 млрд у 2020 році та 75,4 млрд пристроїв у 2025 році.

Отже, виходячи з прогнозів компаній-світових лідерів, Інтернет речей поступово завойовуватиме всі сфери життєдіяльності суспільства.

Поряд з IoT на цьому етапі розвитку IT надзвичайно потужним драйвером підвищення продуктивності і зростання бізнесу стає промисловий Інтернет речей. Нова хвиля інновацій у світі цифрових технологій прискорює реорганізацію цілої низки секторів економіки, на частку яких у сукупності припадає майже дві третини світового виробництва [11-12].

За визначенням [3], промисловий Інтернет речей (*англ*. The Industrial Internet of Things, IIoT) – це мережа фізичних об'єктів, систем, платформ і стосунків, які містять вбудовані технології для комунікації та обміну інформацією один з одним, зовнішнім середовищем і людьми. Основною метою IIoT є покращення ефективності, безпеки, продуктивності виробництва з особливим акцентом на поверненні інвестицій.

Динаміка збільшення кількості споживачів IoT та IIoT останніми роками відображає зростаючий попит на аналітичну інформацію, одержану з використанням даних датчиків на основі створення та аналізу великих інформаційних масивів. Це свідчить про те, що коли виникає IoT, то й IIoT набуває важливого значення, зокрема, під час вирішення складних завдань матеріально-технічного забезпечення, виробництва, сервісу, формування оптимального ланцюжка поставок [19]. Отже, ера паперових систем і фізичного контролю бізнес-процесів поступово добігає кінця. Замість великої кількості друкованих документів і графіків технічного обслуговування пристрої з функцією повідомлення про існуючі потреби та проблеми за допомогою промислового Інтернету речей перетворюються на один із найважливіших компонентів ефективних процесів виробництва.

Управління ланцюжками поставок ілюструє поточне використання IIoT у процесах постачань. Такі системи управління можуть охоплювати програмне забезпечення, прогресивну техніку й передбачати застосування хмарних технологій для обчислення необхідних даних. Так, застосовуючи звичайні інструменти календарного планування, такі як Google, ми використовуємо IoT, водночас залучення IIoT означатиме використання пов'язаних між собою інтелектуальних пристроїв, які дозволяють вирішувати проблеми неефективності, затримок і помилок упродовж усього життєвого циклу продукту, включаючи закупівлі [21].

Промисловий Інтернет речей реалізує можливості використання Інтернету речей у різних секторах промисловості, таких як виробництво, транспорт, енергетика, житлово-комунальне господарство, гірничо-металургійний, авіаційний комплекси тощо. IIoT зосереджується як на оптимізації ефективності операційних систем, їх раціоналізації, автоматизації й покращенні обслуговування, так і відкриває безліч можливостей для моделювання попиту на послуги, створення нових шляхів обслуговування клієнтів й отримання доходів, причому іноді досить несподіваними способами. Часто промисловий Інтернет речей застосовуються при міжгалузевому використанні IoT, прикладом чого є «розумні» будівлі та поєднані транспортні засоби [20].

Варто зазначити, що сьогодні промисловий Інтернет речей перебуває на ранніх стадіях розвитку, але вже стає зрозумілим, що його розбудова може привести до великих перетворень. За прогнозами компанії General Electric інвестиції в IIoT упродовж наступних 15 років зростуть до 60 трлн дол. США [19], відкриваючи нові можливості для його користувачів.

Промисловий Інтернет речей здатний змінити основи конкуренції, визначити нові межі галузей і створити наступне покоління конкурентоспроможних компаній, тому більшість національних економік наразі намагаються визначити можливі наслідки впливу IIoT на підприємства та галузі [8]. Проявами промислового Інтернету речей є практика активного використання провідними компаніями світу у своїй роботі аналітики великих даних (big data). Цей напрям швидко набирає обертів і потребує нових технічних управлінських знань та навичок, створення суб'єктами господарювання інноваційних фінансових і управлінських моделей для одержання спільної вигоди

від використання загальних даних.

Одним із прикладів реалізації концепції IIoT та застосування аналітики великих даних (big data) є впровадження масштабних інформаційних систем управління виробництвом – віртуальних підприємств. У цьому контексті у вітчизняній практиці та практиці країн близького зарубіжжя останнім часом набувають популярності системні рішення класу ERP (від англ. *Enterprise Resource Planning* – планування ресурсів підприємства) [10], що істотно підвищують економічну ефективність господарювання. За оцінюваннями [10], основними ефектами використання систем класу ERP в компаніях є:

– підвищення продуктивності праці;

– зниження витрат (собівартості);

– значне поліпшення якості процесів.

У табл. 1 наведено усереднені показники економічної ефективності проектів з впровадження ERP-рішень, отримані на основі статистики більше ніж 60 кейсів.

Таблиця 1 – **Економічна ефективність проектів упровадження інформаційних систем класу ERP на підприємствах України і близького зарубіжжя** [10]

Напрям діяльності	Характеристика результату	Значення	
		середнє	діапазон
Запаси і виробництво	Збільшення обсягу продукції, що випускається	28 %	25-30 %
	Скорочення витрат на матеріальні ресурси	9 %	6-10 %
	Зниження виробничих витрат	7 %	5-10 %
	Зниження собівартості продукції, що випускається	8 %	3-10 %
	Зниження обсягів матеріальних запасів	21 %	12-30 %
Оборотні кошти	Зростання оборотності складських запасів	18 %	15-21 %
Ефективність та оперативність	Скорочення термінів виконання замовлень	33 %	10-75 %
	Скорочення операційних та адміністративних витрат	15 %	10-25 %
	Зростання прибутку	11 %	10-12%
Трудовитрати та звітність	Скорочення трудовитрат у різних підрозділах	30 %	10-70 %
	Прискорення отримання управлінської звітності	у 3,8 раза	у 2-5 разів
	Прискорення підготовки регламентованої звітності	у 2,8 раза	у 2-4 рази

Виходячи з даних таблиці 1, упровадження системних рішень класу ERP дозволяє в середньому на 20 % і більше підвищити загальну ефективність діяльності підприємства, тим самим зміцнивши і розширивши його конкурентні позиції.

Незважаючи на високі економічні результати імплементації напрямів IIoT, із поширенням таких проектів загострюються проблеми забезпечення інформаційної безпеки компаній в умовах інтенсивного вдосконалення технологій та інструментів захисту даних. Про актуалізацію цих питань свідчить зростання порушень інформаційної безпеки і посилення тяжкості їх наслідків. Так, загальна кількість інформаційних злочинів у світі щорічно збільшується більше ніж на 100 % [14]. Постійно підвищується кількість інформаційних загроз і ризиків, водночас недостатнім залишається рівень забезпечення інформаційної безпеки існуючих інформаційних систем. Зокрема, компанія Hewlett Packard у 2015 році провела масштабне дослідження, в результаті якого було виявлено, що 70 % електронних пристроїв мають уразливість щодо безпеки своїх паролів, існують проблеми з шифруванням інформації та дозволом доступу, тому 50 % додатків для мобільних пристроїв не обмінюються даними [17].

За даними страхової компанії Allianz, у 2013 році збитки глобальної економіки від кіберзлочинності становили 445 млрд дол. США. Топ-10 провідних національних економік, які потерпають від загроз інформаційній безпеці бізнесу, подані у табл. 2 [14].

Таблиця 2 – **Збитки від кіберзлочинності для найбільших економік світу у 2013 році** [14]

Країна	Розмір втрат від кіберзлочинності	
	млрд дол. США	частка від валового внутрішнього продукту (ВВП), %
США	108,00	0,64
Китай	60,00	0,63
Німеччина	59,00	1,6
Бразилія	7,70	0,32
Великобританія	4,30	0,16
Індія	4,00	0,21
Франція	3,00	0,11
Росія	2,00	0,1
Японія	0,98	0,02
Італія	0,90	0,04

Виходячи з даних таблиці, найбільший збиток (у відносних показниках) інформаційні загрози завдають економіці Німеччині (1,6 % від ВВП), а найменший – економіці Японії (0,02 % від ВВП). Найбільших втрат в абсолютному вимірі у 2013 році зазнала економіка США (108 млрд дол. США), найменших – економіка Італії (900 млн дол. США), що були включені до рейтингу. Таким чином, зважаючи на невтішні прогнози щодо темпів щорічного зростання кіберзлочинності, питання підвищення інформаційної безпеки компаній набувають неабиякої актуальності з точки зору як забезпечення безперебійності проходження бізнес-процесів, так і попередження значних фінансових втрат суб'єктів господарювання внаслідок витоків конфіденційної інформації.

Із погляду управління інформаційною безпекою підприємство повинне гарантувати, що конфіденційність, цілісність і доступність (*confidentiality, integrity, availability*) його активів, інформації, даних та IT-послуг завжди відповідають вимогам, узгодженим із бізнесом. У зв'язку з цим здатність компанії забезпечувати інформаційну безпеку стає ключовим джерелом вартості, а необхідність вбудовувати безпеку в дизайн продукту набуває важливого значення [7].

У черговій щорічній доповіді Global Risks Report 2017 виділено кілька важливих технологій, пов'язаних з інформаційною безпекою суб'єктів господарювання [15]:

1. Штучний інтелект та робототехніка (Artificial intelligence and robotics), тобто розроблення машин, які можуть замінити людей усе більше і більше в завданнях, пов'язаних із мисленням, багатоваріантністю і дрібною моторикою.

2. Нові комп'ютерні технології (New computing technologies), а саме нові архітектури для обчислювальної техніки, такі як квантові, біологічні обчислення або оброблення нейронних мереж, а також інноваційні розширення існуючих обчислювальних технологій.

3. Віртуальна і доповнена реальність (Virtual and augmented realities) – інтерфейси між людьми і комп'ютерами за участі середовища, імерсивні голографічні відліки і в цифровому вигляді, вироблені накладками для змішаної реальності.

4. Всюдисущі пов'язані датчики (Ubiquitous linked sensors), також відомі як Інтернет речей, що передбачають використання мережевих датчиків для віддаленого підключення, відстеження та управління продуктами, системами й мережами.

Зважаючи на значні інвестиції, необхідні для впровадження вищезазначених технологій, виникає потреба у визначенні економічно доцільної межі інвестування в інформаційну безпеку промислового Інтернету речей на підприємстві та підходах до оцінювання досягнутого результату. Щодо критеріїв оцінювання, то вони, на нашу думку, визначаються ступенем виконання основного завдання процесів управління інформаційною безпекою IIoT-захистом інтересів усіх тих, хто залежить від інформації, систем і комунікацій, які надають інформацію. Вимоги до цих процесів досягаються, якщо:

– інформація видима або доступна лише тим, хто має на це право (принцип конфіденційності – *confidentiality*);

– інформація є повною, точною і захищена від несанкціонованої зміни (принцип цілісності – *integrity*);

– інформація доступна і придатна до використання, коли це потрібно (принцип доступності – *availability*);

– переданій інформації можна довіряти (принципи автентичності і «неможливості відмови» – *authenticity* та *nonrepudiation*) [4].

Цілі процесів управління інформаційною безпекою повинні бути визначені в бізнес-термінах, а також співвідноситися з бізнес-цілями та відповідати принципу SMART:

– Specific – конкретні;

– Measurable – вимірні;

– Achievable – досяжні;

– Relevant – значущі [4].

Крім того, для успішності IT-послуги, процесу або іншої діяльності обов'язково повинні реалізуватися критичні фактори успіху (Critical Success Factors – CSF) [18]. З метою оцінювання та контролю досягнення кожного фактора, на нашу думку, доцільно використовувати ключові показники ефективності (Key Performance Indicators – KPI) [4]. Необхідно зазначити, що ці показники працюють лише тоді, коли існує процес, який необхідно оцінити. За його відсутності вимірювання не дозволить виявити проблемні місця і знайти правильний спосіб поліпшення ситуації. Тому основною метою управління безперервністю надання IT-послуг є підтримання загального процесу управління безперервністю бізнесу, забезпечення відновлення працездатності необхідного обладнання та служб IT (включаючи комп'ютерні системи, мережі, додатки, телекомунікації, технічну підтримку і службу Service Desk) в необхідні для бізнесу і обумовлені з ним терміни [2].

Іншим інструментом оцінювання та обґрунтування доцільності інвестування в інформаційну безпеку IIoT на підприємстві є збалансована система показників (Balanced Scorecard – BSC) як елемент контролінгу в рамках комплексної системи управління підприємством. Використання BSC дозволяє досліджувати ефективність інвестицій у безпеку промислового Інтернету речей у напрямі розвитку основних функцій IT, виробництва, логістики, маркетингу, продажів і післяпродажного обслуговування.

Безпосередньо для оцінювання економічної ефективності інвестиційних проектів у безпеку IIoT доцільно застосовувати загальноприйняті показники проектного аналізу, наприклад, показник чистої поточної вартості (Net Present Value – NPV), внутрішню норму дохідності (Internal Rate of Return – IRR), індекс рентабельності (Profitability Index – PI) та ін. [1, 5, 13]. Вони дозволяють урахувати всі потоки грошових коштів, пов'язаних із реалізацією проектів та здійснених у різні періоди часу.

Зауважимо, що відповідно до нової ідеології виробництва – IIoT – інвестиційні процеси повинні здійснюватися згідно з новими вимогами економіки результату: якщо підприємства конкурують не за можливість продати продукт або послугу, а за надання кількісно вимірюваного результату, необхідного клієнтові в певний час і в певному місці [7]. При цьому основним економічним ефектом, якого прагне компанія, створюючи систему захисту інформації, є помітне зменшення матеріальних збитків унаслідок реалізації існуючих загроз інформаційній безпеці підприємства. Безумовно, віддача від таких інвестицій у розвиток компанії повинна бути цілком прогнозованою.

Необхідно зазначити, що інформаційні системи з плином часу зазнають істотних суттєвих змін, виникають нові загрози. Таким чином, забезпечення інформаційної безпеки − це процес, який необхідно відстежувати, оцінювати та вдосконалювати постійно.

Висновки. Промисловий Інтернет речей як сучасний напрям ІТ на підприємстві дозволяє не лише розвивати робочі процеси, а й обумовлює створення нових варіантів робочого середовища, більш віртуальних і націлених на співпрацю, а також принципово нових категорій робочих місць, істотно підвищуючи продуктивність виробництва [17].

Починаючи свій шлях до змін із використанням технологій на базі промислового Інтернету речей, компаніям необхідно планувати кожний свій крок із метою зростання ефективності та стимулювання створення продуктово-сервісних гібридних рішень, орієнтованих на кінцевий результат [17]. Наприклад, спроби змінити ситуацію щодо підвищення ефективності використання активів можуть стати основою для створення нових сервісів.

Для стимулювання поширення промислового Інтернету речей підприємствам необхідні як технічні ресурси − ІТ-інфраструктура, так і трудові – фахівці з певними технічними навичками. Наявність необхідних ресурсів залежить від активності інвестування фірм в інфраструктуру збирання, зберігання і аналізу даних, а також в персонал [23]. Крім того, з розвитком ІТ зростають вкладення компаній у забезпечення їх інформаційної безпеки.

На сучасному підприємстві якість й ефективність його інформаційної системи впливають на кінцеві фінансові показники через якість бізнес-процесів. Програють ті компанії, де фінансування захисту інформації проводиться за залишковим принципом. При цьому кожна фірма постає перед питанням, яким чином ставитися до вкладень в інформаційну безпеку − як до витрат чи інвестицій та які підходи до їхньої оптимізації слід застосовувати. Як правило, якщо у компанії є довгострокова стратегія розвитку, пов'язана з ІТ, вона розглядає вкладення в інформаційну безпеку як інвестиції і прагне зробити їх перспективними, вдаючись до оцінювання економічної ефективності та оптимізації структури вкладень за допомогою, зокрема, розглянутих підходів.

Ураховуючи актуальність розбудови ІТ-систем промислових підприємств та забезпечення їх інформаційної безпеки, у **подальших наукових дослідженнях** ефективності інвестиційних процесів із застосуванням ІТ доцільно приділити увагу обґрунтуванню використання збалансованої системи показників як системи стратегічного управління компанією, побудованої на основі вимірювання та оцінювання її ефективності за набором оптимально підібраних показників, що відображають усі аспекти діяльності підприємства (фінансові, виробничі, маркетингові, інноваційні, інвестиційні, управлінські тощо).

1. Боримська К.П. Оцінка ефективності інвестиційних проектів в системі контролінгу бізнес-процесів підприємства: проблеми безпеки бізнесу [Електронний ресурс] / К.П. Боримська // Ефективна економіка. – 2014. – № 5. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=3065.

2. Брукс П. Метрики для управления ИТ-услугами / П. Брукс ; пер. с англ. − М. : Альпина Бизнес Букс, 2008. − 283 с.

3. Галатенко В.А. Основы информационной безопасности : учеб. пособ. / В.А. Галатенко; под ред. В.Б. Бетелина, 3-е изд. − М. : Интуит.ру "Интернет-университет Информационных Технологий", 2006. – 208 с.

4. Глоссарий терминов и определений [Электронный ресурс] / V 3 Glossary, v 0.92, 30 April 2009. – Режим доступа : http://www.wikiitil.ru/books/ITIL_Glossary(rus)-2009.pdf.

5. Єжова Л.Ф. Доцільність забезпечення захисту інформаційних ресурсів [Електронний ресурс] / Л.Ф. Єжова // Східноукраїнський національний університет імені Володимира Даля, 2012. – № 8 (179), Ч. 1. – Режим доступу : http://www.nbuv.gov.ua/old_jrn/Soc_Gum/VSUNU/2012_8_1/title/17.pdf.

6. Завгородний В.И. Комплексная защита информации в компьютерных системах / В. И. Завгородний. – М. : Логос, 2013. – 264 с.

7. Использование IIoT для увеличения эффективности работы производства [Электронный ресурс]. – Режим доступа : http://controleng.ru/wp-content/uploads/CE_IoT_Listalka.pdf.

8. Каплан Р.С. Сбалансированная система показателей. От стратегии к действию / Р.С. Каплан, Д. П. Нортон. – 2-е изд. – М. : ЗАО "Олимп-Бизнес", 2003. – 320 с.

9. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К. : ООО "Лазурит-Полиграф", 2013. – 275 с.

10. К вопросу об оценке экономической эффективности внедрения ERP системы [Электронный ресурс]. – Режим

доступа : http://bitfactor.ru/methods/k-voprosu-otsenki-ekonomicheskoj-effektivnosti-vnedreniya-erp-sistemy.html.

11. Ленков С.В. Методы и средства защиты информации : монография : в 2 т. – Т. 2 : Информационная безопасность / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – 344 с.

12. Мельник Л.Г. Четвертая промышленная революция: предпосылки и содержание / Л.Г. Мельник // Актуальні проблеми економіки. – 2016. – № 9 (183). – С. 26–30.

13. Поливана Л.А. Методичні підходи до оцінки ефективності проекту впровадження інформаційних технологій на підприємствах торгівлі [Електронний ресурс] / Л.А. Поливана. – Режим доступу : http://www.khntusg.com.ua/files/sbornik/vestnik_149/38.pdf.

14. A Guide to Cyber Risk. Managing the Impact of Increasing Interconnectivity [Electronic resource] / Allianz Global Corporate & Specialty, 2014. – Mode of access : http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

15. Global Risks Report 2017 [Electronic resource]. – Mode of access : http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-1-understanding-the-risk-landscape/.

16. How Smart, Connected Products Are Transforming Companies [Electronic resource]. – Mode of access : https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.

17. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services [Electronic resource] / World Economic Forum, 2015. – Mode of access : http://reports.weforum.org/industrial-internet-of-things/.

18. Intel Solution Summit 2014: Интернет вещей, будущие ПК и новый маркетинг [Электронный ресурс]. – Режим доступа : http://itc.ua/articles/ intelsolution -summit-2014-internet-veshhey-budushhie-pk-i-novyiy-marketing/.

19. Roundup Of Internet Of Things Forecasts And Market Estimates, 2016 [Electronic resource]. – Mode of access : https://www.forbes.com/sites/ louiscolumbus /2016/11/27/ roundup-of-internet-of-things-forecasts-and-market-estimates-2016/.

20. The Industrial Internet of Things (IIoT): benefits, innovations and barriers [Electronic resource]. – Mode of access : https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/.

21. The Industrial Internet of Things, Manufacturing, Supply Chain & Logistics: Where Are We & Where Are We Going? [Electronic resource]. – Mode of access : http://cerasis.com/2016/11/09/the-industrial-internet-of-things/.

22. Whitman M. Management of information security / M. Whitman, H. Mattord. – Gengage Learning, 2010. – 592 p.

23. Winning with the Industrial Internet of Things: How to accelerate the journey to productivity and growth. Accenture, 2015 [Electronic resource]. – Mode of access : https://www.accenture.com/pl-en/insight-industrial-internet-of-things.

1. Boryms'ka, K.P. (2014). Otsinka efektyvnosti investytsiynykh proektiv v systemi kontrolinhu biznes-protsesiv pidpryyemstva: problemy bezpeky biznesu [Estimation of investment projects efficiency in the system of business processes controlling: business security issues]. *Efektyvna ekonomika – Effective economy, 5*. Retrieved from http://www.economy.nayka.com.ua/?op=1&z=3065 [in Ukrainian].

2. Bruks, P. (2008). *Metriki dlya upravleniya IT-uslugami [Metrics for IT Service Management]* (Trans). Moscow: Alpina Biznes Buks [in Russian].

3. Galatenko, V.A., & Betelin, V.B. (Ed.) (2006). *Osnovyi informatsionnoy bezopasnosti [Fundamentals of Information Security]*. Moscow: Intuit.ru "Internet-universitet Informatsionnyih Tehnologiy" [in Russian].

4. *Glossariy terminov i opredeleniy [Glossary of Terms and Definitions]* (2009). V 3 Glossary, v 0.92, 30 April. Retrieved from http://www.wikiitil.ru/books/ITIL_Glossary(rus)-2009.pdf [in Russian].

5. Yezhova, L.F. (2012). Dotsil'nist' zabezpechennya zakhystu informatsiynykh resursiv [The feasibility of providing protection of information resources]. *Skhidnoukrayins'kyy natsional'nyy universytet imeni Volodymyra Dalya – Vladimir Dal Eastern National University, 8 (179)*. Retrieved from http://www.nbuv.gov.ua/old_jrn/Soc_Gum/VSUNU/2012_8_1 /title/17.pdf [in Ukrainian].

6. Zavgorodniy, V.I. (2013). *Kompleksnaya zaschita informatsii v kompyuternyih sistemah [Comprehensive protection of information in computer systems]*. Moscow: Logos [in Russian].

7. Ispolzovanie IIoT dlya uvelicheniya effektivnosti rabotyi proizvodstva [Use of IIoT to increase the efficiency of production] (n.d.). controleng.ru. Retrieved from http://controleng.ru/wp-content/uploads/CE_IoT_Listalka.pdf [in Russian].

8. Kaplan, R.S., & Norton, D.P. (2003). *Sbalansirovannaya sistema pokazateley. Ot strategii k deystviyu [Balanced Scorecard. From strategy to action]*. Moscow: ZAO "Olimp-Biznes" [in Russian].

9. Korchenko, A.G., Arhipov, A.E., & Kazmirchuk, S.V. (2013). *Analiz i otsenivanie riskov informatsionnoy bezopasnosti [Analysis and evaluation of information security risks]*. Kyiv: OOO "Lazurit-Poligraf" [in Russian].

10. K voprosu ob otsenke ekonomicheskoy effektivnosti vnedreniya ERP sistemyi [On issue of assessing the cost-effectiveness of introducing ERP system] (n.d.). *bitfactor.ru*. Retrieved from http://bitfactor.ru/methods/k-voprosu-otsenki-ekonomicheskoj-effektivnosti-vnedreniya-erp-sistemy.html [in Russian].

11. Lenkov, S.V., Peregudov, D.A., & Horoshko, V.A. (2008). *Metodyi i sredstva zaschityi informatsii [Methods and means of information protection]*. (Vols. 1-2). Kyiv: Ariy [in Russian].

12. Melnik, L.G. (2016). Chetvertaya promyishlennaya revolyutsiya: predposyilki i soderzhanie [The fourth industrial revolution: preconditions and content]. *Aktual'ni problemy ekonomiky – Actual Problems of Economics, 9 (183),* 26–30 [in Russian].

13. Polyvana, L.A. (n.d.) Metodychni pidkhody do otsinky efektyvnosti proektu vprovadzhennya informatsiynykh tekhnolohiy na pidpryyemstvakh torhivli [Methodological approaches to assessing the effectiveness of the information technology

implementation project at trade enterprise]. *khntusg.com.ua*. Retrieved from http://www.khntusg.com.ua/files/sbornik/vestnik_149/38.pdf [in Ukrainian].

14. Allianz Global Corporate & Specialty (2014). A Guide to Cyber Risk. Managing the Impact of Increasing Interconnectivity. *agcs.allianz.com*. Retrieved from http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
15. Global Risks Report 2017 (n.d.). *reports.weforum.org*. Retrieved from http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-1-understanding-the-risk-landscape/.
16. How Smart, Connected Products Are Transforming Companies (n.d.). *hbr.org*. Retrieved from https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.
17. World Economic Forum (2015). Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. *reports.weforum.org*. Retrieved from http://reports.weforum.org/industrial-internet-of-things/.
18. Intel Solution Summit 2014: Internet veschey, buduschie PK i novyiy marketing [Internet of things, the future PCs and new marketing] (n.d.). *itc.ua*. Retrieved from http://itc.ua/articles/ intelsolution -summit-2014-internet-veshhey-budushhie-pk-i-novyiy-marketing/ [in Russian].
19. Roundup Of Internet Of Things Forecasts And Market Estimates (2016). *forbes.com*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/.
20. The Industrial Internet of Things (IIoT): benefits, innovations and barriers (n.d.). *i-scoop.eu*. Retrieved from https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/.
21. The Industrial Internet of Things, Manufacturing, Supply Chain & Logistics: Where Are We & Where Are We Going? (n.d.). cerasis.com. Retrieved from http://cerasis.com/2016/11/09/the-industrial-internet-of-things/.
22. Whitman, M., & Mattord, H. (2010). *Management of information security*. Gengage Learning.
23. Accenture (2015). Winning with the Industrial Internet of Things: How to accelerate the journey to productivity and growth. *accenture.com*. Retrieved from https://www.accenture.com/pl-en/insight-industrial-internet-of-things.

И.Н. Сотник, д-р экон. наук, профессор, профессор кафедры экономики и бизнес-администрирования, Сумский государственный университет (г. Сумы, Украина);

К.Ю. Завражный, аспирант кафедры экономики и бизнес-администрирования, Сумский государственный университет (г. Сумы, Украина)

Подходы к обеспечению информационной безопасности промышленного Интернета вещей на предприятии

В статье обосновываются перспективы развития Интернета вещей и промышленного Интернета вещей, акцентировано внимание на экономических эффектах внедрения масштабных информационных систем управления производством современных предприятий путем использования системных решений класса ERP. Доказано, что ухудшение информационной безопасности в деятельности предприятий и организаций является одной из важных проблем, сопутствующих развитию промышленного Интернета вещей. Проанализированы подходы к обеспечению информационной безопасности промышленного Интернета вещей у субъектов хозяйствования с учетом современных достижений в сфере информационных технологий. Определены основные подходы к экономическому обоснованию инвестиций в данное направление деятельности.

Ключевые слова: информационная безопасность, предприятие, информационные технологии, промышленный Интернет вещей, программное обеспечение, инвестиции, экономическая эффективность.

I.N. Sotnyk, Doctor of Economics, Professor, Professor of the Department of Economy and Business Administration, Sumy State University (Sumy, Ukraine);

K.Yu. Zavrazhnyi, PhD Student of the Department of Economy and Business Administration, Sumy State University (Sumy, Ukraine)

Approaches to provide information safety of the Industrial Internet of Things at the enterprise

The aim of the article *is investigation of prospects of Industrial Internet of Things development, analyzing problems and approaches to provide its information safety for economic agents, as well as determining approaches to the economic substantiation of investments in this direction of activity.*

Results of the research. *Modern development of information technology (IT) significantly enhances the effective business activity, creates innovation competitive advantages for companies. In this context, the spread of "smart" production systems becomes especially popular. These systems manage things without human intervention and form the basis of concepts of Internet of Things and Industrial Internet of Things.*

As the current direction of IT at the enterprise, Industrial Internet of Things enables operation processes

developing and creates new options for the working environment as well as entirely new categories of jobs with their significant productivity increasing. In particular, it is confirmed by the economic results of implementation of large-scale information systems for production management at modern enterprises by using system solutions of ERP-class. As a result of such projects' implementation, the overall efficiency of the company may be increased by 20% or more.

Starting using technology based on the Industrial Internet of Things, companies need to plan every step to increase efficiency and to stimulate the creation of product-service hybrid solutions, focused on the result. For example, attempts to change the situation for improving assets' efficiency can become the basis for the creation of new services.

To encourage the spread of Industrial Internet of Things, enterprises need technical resources like IT infrastructure and labour resources like professionals with specific technical skills. Availability of necessary resources depends on firms' investments in the infrastructure for collecting, storing and analysing data, as well as in staff. In addition, the development of IT causes companies to increase investment in information security provision due to rising number of information security violations and increased severity of their consequences.

In terms of information security management, the company must ensure that the confidentiality, integrity and availability of its assets, information, data and IT services always meet the requirements agreed with the business. In this regard, the company's ability to ensure information security is a key source of value, and the need to embed security into product design becomes important.

Today the quality and efficiency of enterprise's information system affect the final financial results through the quality of business processes. Companies that finance information security by residual principle can lose their competitive advantages. In addition, each firm has to solve the problem of how to consider expenditures in information security - as costs or investments and which approaches should be applied to their optimization. Typically, if the company has a long-term development strategy related to IT, it considers the information security expenses as investments and seeks to make them promising, resorting to assess their economic efficiency and optimize the structure of investments. The criterion of economically expedient limits of investment in Industrial Internet of Things information security at the enterprise can be defined as a degree of protection of interests of all persons and objects who are dependent on information and communications systems that provide information.

***Conclusions and directions of further researches**. Modern development of IT provides companies with innovation competitive advantages and exacerbates the problems of information security provision for economic agents and cybercrime growth. The impact of information risks is realized through vulnerability of information systems that support different types of economic activities of industrial enterprises and through the companies' losses due to leaks of confidential information, failures in information networks and systems. To prevent losses from cybercrime, companies should increase their investment in information security, guided by the criterion of economic expedient limits of investment, which provides sufficient protection from unauthorized access.*

Given the urgency of IT systems development and ensuring their information security for the industrial enterprises, further scientific researches should be devoted to the justification for the use the Balanced Scorecard as a system of company's strategic management. The Balanced Scorecard should be based on the measurement and evaluation of enterprise's efficiency with the help of the set of optimally matched indicators that reflect all aspects of the company.

Keywords: information safety, enterprise, information technologies, Industrial Internet of Things, software, investments, economic efficiency.

Отримано 06.02.2017 р.