

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ І УПРАВЛІННІ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 2



**Одеса
2020**

РИЗИКИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ПІДПРИЄМСТВАХ

Браїла Г. В.¹, Орлик О. В.²

1 — студентка 3 курсу 35 гр., факультет міжнародної економіки,

2 — канд. екон. наук, доцент, кафедра економічної кібернетики та інформаційних технологій
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Браїла Г. В., Орлик О. В. *Ризики впровадження і використання інформаційних технологій на підприємствах.* В статті розглянуто важливість та переваги впровадження на підприємствах сучасних інформаційних технологій. Визначено основні ризики, якими може супроводжуватися процес впровадження і використання інформаційних технологій. Розкрито принципи управління ІТ-ризиками, а також шляхи запобігання ризикових ситуацій на підприємствах.

Ключові слова: підприємство, інформаційні технології, ІТ-ризики, принципи управління ІТ-ризиками.

Браила А. В., Орлик О. В. *Риски внедрения и использования информационных технологий на предприятиях.* В статье рассмотрены важность и преимущества внедрения на предприятиях современных информационных технологий. Определены основные риски, которыми может сопровождаться процесс внедрения и использования информационных технологий. Раскрыты принципы управления ИТ-рисками, а также пути предотвращения рискованных ситуаций на предприятиях.

Ключевые слова: предприятие, информационные технологии, ИТ-риски, принципы управления ИТ-рисками.

Braila A. V., Orlyk O. V. *Risks of the introduction and use of information technology in enterprises.* The article discusses the importance and advantages of introducing modern information technologies at enterprises. The main risks that may accompany the process of implementation and use of information technology are identified. The principles of IT risk management are disclosed, as well as ways to prevent risk situations in enterprises.

Keywords: company, information technology, IT risks, principles of IT risk management.

Браїла Г. В., Орлик О. В. *Ризики впровадження і використання інформаційних технологій на підприємствах* // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2020. Вип. 2. С. 58–67.

Постановка проблеми у загальному вигляді. У сучасному світі майже неможливо уявити собі підприємство, яке здатне працювати ефективно без використання новітніх інформаційних технологій (ІТ). В цьому полягає цільове призначення ІТ – допомагати підприємствам вести свою діяльність продуктивно, відповідати стандартам держави ХХІ століття, і що найважливіше – вимогам споживачів. Але процес впровадження і використання інформаційних технологій часто тягне за собою виникнення певних проблем, які можуть погано вплинути на діяльність компанії. Мова йде про ризики використання ІТ на підприємствах. Зараз, у вік інформаційних технологій, ці проблеми, як ніколи, дуже поширені. Адже витік конфіденційної інформації здатен назавжди зруйнувати репутацію компанії, яка будувалася роками. І ця проблема частково викликана саме використанням на підприємстві інформаційних технологій. Все це підтверджує про актуальність даної проблеми.

Аналіз досліджень і публікацій останніх років. При написанні статті проаналізовано публікації ряду науковців, серед яких А. П. Баранов [1], К. І. Свіріденков [2], І. В. Ісаєв [3], А. О. Сінгіна і М. В. Набока [4], Н. Н. Грінчар [5] та ін., які досліджували різні аспекти вирішення проблеми ризиків впровадження та використання інформаційних технологій на сучасних підприємствах.

Виділення невирішених раніше частин загальної проблеми. Велика увага вчених до розгляду цієї проблеми дає підставу вважати, що проблема виникнення ризиків при впровадженні і використанні ІТ на підприємствах є дуже поширеною. Незважаючи на те, що вже існують певні методи управління ризиками, підходи щодо їх запобігання, питання щодо вирішення проблем ІТ-ризиків продовжують виникати. Це пов'язано з тим, що впровадження нових технологій, у т.ч. інформаційних, що дають нам більше нових можливостей, супроводжується і виникненням нових ризиків. Саме тому ця проблема потребує більш детального розгляду.

Мета статті полягає у визначенні найбільш поширених ризиків, пов'язаних із впровадженням і використанням інформаційних технологій на підприємствах, а також виділенні принципів управління цими ризиками і запобігання їх виникнення.

Виклад основного матеріалу дослідження. У сучасному світі, як усім нам відомо, дуже широку популярність здобула обчислювальна техніка. Майже кожна людина може похвалитися наявністю навиків використання ПК, і крім того, майже у всіх зараз є багатофункціональний смартфон, планшет, ноутбук, стаціонарний комп'ютер і т. д. Це одна з характерний рис нашого часу: формування глобального інформаційного суспільства, широке розповсюдження на комерційній основі засобів обчислювальної техніки і зв'язку, програмних засобів, впровадження комп'ютерних інформаційних технологій в різні сфери людської діяльності. Логічним наслідком цього процесу стало впровадження інформаційних технологій на підприємствах різних форм бізнесу.

Інформаційні технології приносять користь та надають підприємству величезну кількість переваг, серед яких:

- полегшення процесу управління усіма видами ресурсів;
- сприяння ефективному здійсненню комерційної діяльності; збільшення доходів підприємства;
- підвищення продуктивності;
- скорочення часу випуску продуктів;
- зменшення штатної кількості співробітників, що дозволяє скоротити витрати на оплату праці;
- зниження ризиків виникнення помилок і дублювання інформації при роботі тощо.

Ці переваги ведуть до підвищення конкурентоспроможності підприємства на ринку.

Згідно з даними, наведеними у [6] та представленими на рис. 1, вигод від використання ІТ на підприємствах багато, серед яких можна виділити такі:

- ІТ сприяють скороченню паперової праці, адже набагато краще, коли уся інформація знаходиться в одному місці, і легше можна отримати доступ до будь-яких даних;
- збільшення швидкості доступу до інформації також свідчить на користь ІТ. У працівників з'являється більше вільного часу. Відповідно його можна використовувати більш ефективно, що дозволяє збільшити прибуток підприємства;
- зниження витрат також відносять до плюсів використання ІТ, адже це дозволяє зменшити собівартість;
- знижується вплив людського чиннику. Людина від природи здатна допускати помилки, які іноді можуть кардинально вплинути на усю документацію.
- зменшується штат працівників та ін.

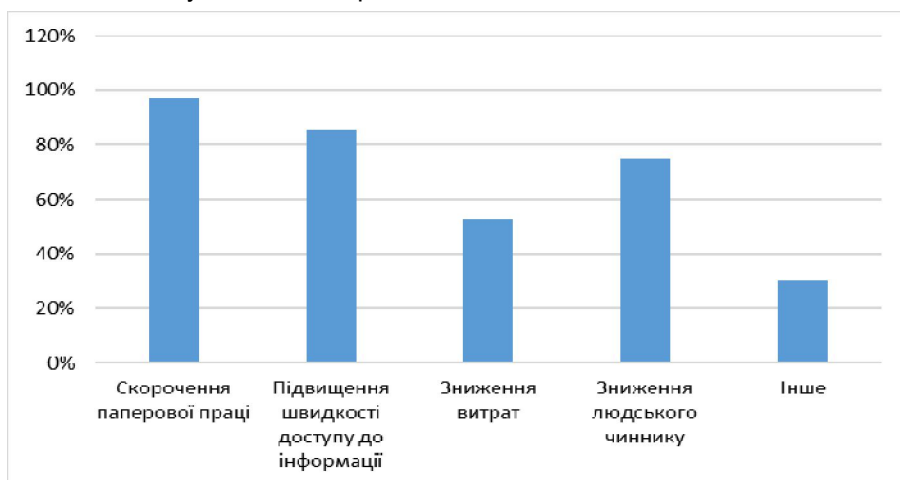


Рис.1. Вигоди від використання ІТ (побудовано на основі [6])

Це все дає підставу стверджувати, що зараз використання інформаційних технологій є обов'язковою умовою розвитку підприємства.

Ризики, пов'язані з впровадженням і використанням ІТ на підприємстві.

Інформаційні технології виконують величезну кількість функцій, серед яких: пошук, збір, зберігання, обробка, надання, розповсюдження інформації тощо. Саме завдяки цьому вони є настільки популярними у світі.

Незважаючи на величезні переваги використання інформаційних технологій на будь-якому підприємстві, є і певні ризики. У ті часи, коли людство тільки починало працювати з обчислювальною технікою, воно бачило у цьому лише можливість полегшити підприємницьку діяльність, можливість підвищити ефективність праці в компанії за рахунок використання ІТ. Але зараз варто усвідомлювати, що впровадження інформаційних технологій на підприємстві може супроводжуватися також виникненням певних ризиків, які пов'язані з використанням інформаційних систем, що підтримують місію та бізнес-функції організації.

З точки зору інформаційної безпеки ризик розглядають як добуток втрат від порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів на імовірність такого порушення [7].

Варто зазначити, що на даний період часу існує багато визначень поняття «інформаційний ризик», як і класифікацій інформаційних ризиків.

Так, Гринчар Н. Н. у [5] зазначає, що існують два види ризиків: селективний і операційний. На думку автора, селективний ризик є ризиком неправильного вибору інформаційної системи, і пов'язаний, перш за все, зі стратегією автоматизації підприємства. І консервативна стратегія, що використовує принцип мінімуму, і агресивна стратегія, яка навпаки орієнтована на максимальний ефект, тягнуть за собою виникнення певних проблем. Операційні ризики у більшій мірі пов'язані з управління персоналом. Адже часто зустрічаються випадки, коли робітники чинять опір впровадженню нових інформаційних технологій на підприємстві. Одні бояться не впоратися з новітніми системами, інші – взагалі не бажають нічого змінювати, адже звикли до існуючих порядків.

Іншу класифікацію пропонує Свіріденков К. І. На його думку [2], слід розрізняти технічні і корпоративні ІТ-ризики.

Технічні ризики включають порушення проектування самої інформаційної системи. Тобто, обрана система може не підходити даному підприємству, може бути несумісна з іншими системами, присутніми в організації. Відомі випадки, коли впровадження системи призводить до виникнення помилок функціонування, а також зниження продуктивності і т. п. А це, в кінцевому підсумку, веде до виникнення збитків. У випадку виникнення таких ризиків слід проводити деякі заходи, як на етапі впровадження, так і на етапі використання ІТ. А саме: дотримання певних технічних вимог, попереднє тестування інформаційних технологій, боротьба з відмовою інформаційних систем. Але не слід забувати, що причиною

виникнення технічних ризиків, може бути також неправильно підібраний ІТ-постачальник, який забезпечив підприємство неякісними технологіями.

До корпоративних ризиків, перш за все, відноситься витік інформації, що є найпоширенішою проблемою, яка призводить до непередбачених ситуацій в компанії, а іноді – навіть до втрати репутації, іміджу, імені, які будувалися роками. Витік конфіденційної інформації може бути здійснений у декількох напрямках: несанкціоноване копіювання інформації і поширення її за межі організації; друк інформації і поширення її за межі організації; передача інформації по мережі на інші сервери, розташовані поза організації; розкрадання носіїв, які містять конфіденційну інформацію.

Також ризики у сфері інформаційних технологій класифікуються за: властивостями інформаційних ресурсів, які порушуються при реалізації ризику (конфіденційність, цілісність, доступність, автентичність, спостережність); видами втрат внаслідок реалізації ризиків (фінансові втрати, репутаційні втрати, порушення законодавства/контрактів, шкода продуктивності персоналу, загроза життю і здоров'ю людей) [7].

Зі зростаючою роллю інформації у світі, зростають і випадки, коли люди отримують несанкціонований доступ до секретної інформації і використовують її у своїх цілях. Саме тому підбір якісної інформаційної технології дуже сильно впливає на підтримку рівня конфіденційності інформації підприємства.

За результатами глобального дослідження Аналітичного центру компанії InfoWatch у світі в 2018 році було зареєстровано 2263 публічних випадків витоку конфіденційної інформації. У 86% інцидентів були скомпрометовані персональні дані і платіжна інформація – всього близько 7,3 млрд записів даних проти 13,3 млрд записів даних у 2017 році. У 2018 році суттєво скоротився обсяг даних, скомпрометованих в результаті витоків з організацій сфери високих технологій, фінансово-кредитного та страхового сектора, а також підприємств промисловості [8].

Кількість витоків інформації та обсяг скомпрометованих записів даних у світі за 2011–2018 рр. наведено на рис. 2.

Згідно з даними, наведеними у [8], найбільш привабливими для зловмисників у 2018 р. залишалися дані з організацій фінансово-кредитної та страхової сфери, де близько 64,9% витоків були вчинені навмисно, з промислових і транспортних систем, компаній сфер торгівлі і HoReCa, а також високотехнологічного бізнесу. Як свідчать дані, наведені на рис. 3, більше половини витоків у цих галузях носили умисний характер.

У 2017–2018 рр. серед каналів передачі даних, лідерами за витоками даних, призначених для користувача, залишалися: мережа (браузер, Cloud), електронна пошта та паперові документи, про що свідчать дані на рис. 4. При цьому виток інформації через паперові документи зріс, а електронної пошти – навпаки, зменшився.



Рис.2. Кількість витоків інформації та обсяг скомпрометованих записів даних у світі за 2011–2018 рр. (побудовано на основі [8])



Рис.3. Частка умисних витоків записів даних від загального числа витоків за галузями у 2018 р. (побудовано на основі [8])

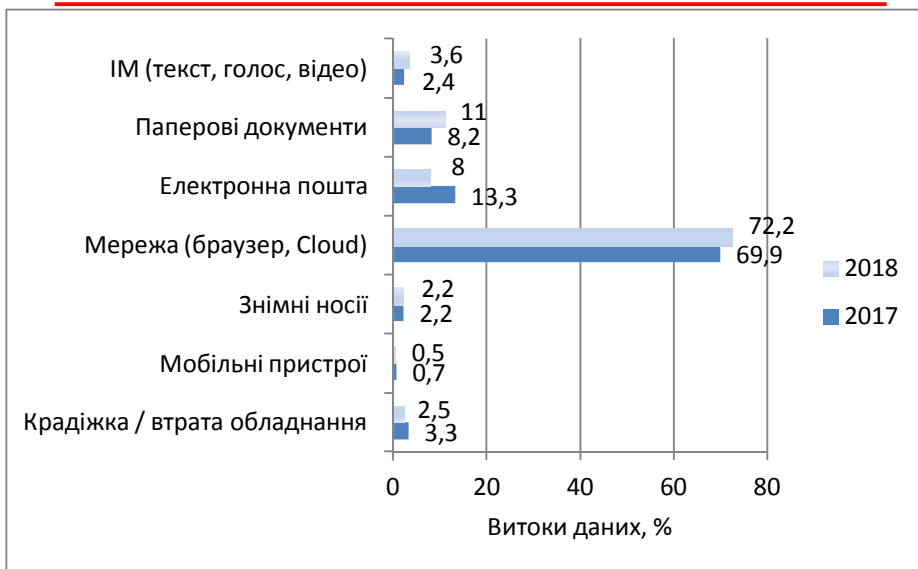


Рис.4. Розподіл витоків за каналами передачі даних у 2018 р.
(побудовано на основі [8])

У 2018 р. 69,5% складали витоки персональних даних, 16,9% – витоки платіжної інформації, 8,1% – комерційні секрети та виробничі ноу-хау, 5,4% – державні таємниці [8].

За цей період 40% інцидентів відбулося з хмарних сховищ, що належать компаніям сфери високих технологій. Високотехнологічні компанії найбільш сприйнятливі до сучасних трендів і охоче перекладають свої бази у зовнішні сховища, при цьому не завжди враховуючи всі правила інформаційної безпеки при роботі з хмарними серверами. Порівняно з 2017 р. зросла частка витоків з серверів, що належать медичним організаціям і освітнім установам. Частка витоків з фінансової сфери, промисловості та державного сектору, навпаки, скоротилася.

Дані на рис. 5 ілюструють галузевий розподіл витоків інформації з хмарних серверів за 2017–2018 рр.

Серед витоків з хмарних серверів у 2018 р. переважали витоки персональних даних – 81,6% випадків, порівняно з 77,7% у 2017 р. За цей період зросла частка витоків платіжної інформації, а також комерційних секретів і виробничих ноу-хау. Так, якщо у 2017 р. витоки комерційних секретів і ноу-хау склали 8,9%, а платіжної інформації – 6,7%, то у 2018 р. обидва показники зросли до 9,2%.

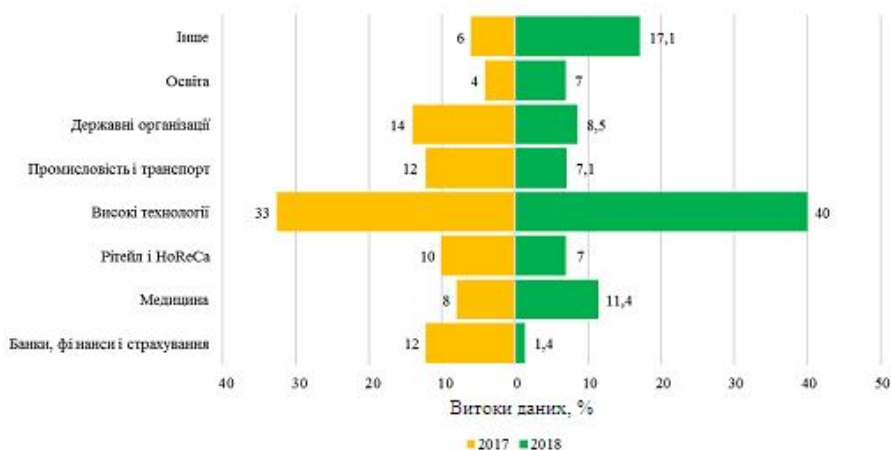


Рис.5. Галузевий розподіл витоків інформації з хмарних серверів за 2017–2018 рр. (побудовано на основі [8])

Принципи управління ІТ-ризиками на підприємстві.

З вищевикладеного матеріалу можна зрозуміти, що інформаційні ризики пов'язані з виникненням негативних наслідків впровадження і використання інформаційних технологій на підприємстві. Вони можуть бути у вигляді вірусів, різних методів розкрадання інформації, хакерських атак тощо. З цього слідує, що виникнення ІТ-ризиків призводить до збитків підприємства, до втрати репутації та конкурентоспроможності на ринку. Але цього не можна допускати. Саме тому зараз дуже поширена проблема пошуку методів та принципів управління ІТ-ризиками.

Ризики у сфері інформаційних технологій розглядають як частину бізнес-ризиків та обробляють схожим чином.

Щоб уникнути виникненню проблем, пов'язаних із впровадженими інформаційними технологіями, кожне підприємство повинно мати комплексну систему, яка має відповідати певним вимогам [5]:

- Система управління ризиками повинна мати необхідне навчально-методичне забезпечення.

- В основу концепції розробки системи повинна бути покладена методика, яка буде забезпечувати підприємство достатньою кількістю інформації, необхідною для прийняття рішень.

- Технічні засоби реалізації цього методу повинні бути відносно простими, універсальними, високотехнологічними, і мати прийнятну ціну.

- Система оцінки ризиків повинна допускати можливість модернізації, враховуючі сучасні тенденції розвитку інформаційних систем.

- Система повинна бути повністю забезпечена інформаційно, тобто вся необхідна інформація повинна бути доставлена в систему з належною повнотою і якістю з уже сформованих джерел.

– Система повинна бути забезпечена організаційно, тобто повинно існувати забезпечення як новими спеціалістами, так і забезпечена можливість використання існуючого на підприємстві високоякісного інженерно-технічного персоналу.

З метою уникнення ІТ-ризиків, кожне підприємство має проводити певні заходи:

– визначити коло осіб, які будуть нести відповідальність за інформаційну безпеку, а також скласти звіт правил, спрямованих на уникнення ІТ-ризиків;

– розробити єдині стандарти інформаційних систем в рамках організації;

– класифікувати дані за ступенем конфіденційності і розмежувати права доступу до них;

– слідкувати за тим, щоб будь-які документи, що мають відношення до діяльності підприємства, складалися за допомогою систем, централізовано встановлених на комп'ютерах;

– розробити і створити систему, що дозволяє оперативно відновити працездатність ІТ-інфраструктури при технічних збоях;

– впровадити засоби контролю, які будуть дозволяти слідкувати за станом усіх корпоративних систем, і у разі несанкціонованого доступ система повинна або автоматично забороняти вхід, або сигналізувати про небезпеку, щоб персонал міг вжити заходів [3].

Крім цього, треба бути готовим до наслідків виникнення можливих кризових ситуацій через ІТ. Необхідно підготувати документ з певною послідовністю дій для персоналу у таких випадках.

Варто також зазначити, що із вдосконаленням інформаційних технологій, повинні вдосконалюватися методи інформаційної безпеки, модернізуватися системи, спрямовані на уникнення ІТ-ризиків.

Наприкінці слід зазначити, що отримати плюси можна тільки при грамотному впровадженні та використанні інформаційних технологій на підприємстві, а це не просте завдання, адже спочатку потрібно виявити і усунути всі причини, що перешкоджають їх впровадженню, а це відповідно вимагає значних витрат часу і досвіду фахівців в даній області.

Висновки з даного дослідження. Інформаційні технології є невід'ємною складовою будь-якого підприємства. Але поряд із перевагами, існують і ризики від їх впровадження і використання. Для того, щоб їх уникнути, треба виконувати певну послідовність дій, спрямовану на інформаційну безпеку підприємства, а саме: захищати конфіденційну інформацію, впроваджувати лише високоякісну техніку, правильно обирати персонал, що буде з нею працювати і т. д.

ЛІТЕРАТУРА

1. Баранов А. П. Современное состояние философии управления информационной безопасностью // Бизнес-информатика. 2014. № 2 (28). С. 7–14.

2. Свириденков К. И. IT-риски: особенности идентификации и управления // Экономика и предпринимательство. 2015. № 9-2 (62). С. 993–997.
3. Исаев И. В. IT риски и информационная безопасность // Современные наукоемкие технологии. 2014. № 7-1. С. 184. URL: <http://www.top-technologies.ru/ru/article/view?id=34276> (дата звернення: 03.11.2019).
4. Сингина А. А., Набока М. В. Управление IT-рисками при эксплуатации информационных систем // Технические науки в России и за рубежом : материалы Междун. науч. конф. (м. Москва, май 2011 г.). М. : Ваш полиграфический партнер, 2011. С. 22–25. URL: <https://moluch.ru/conf/tech/archive/3/722/> (дата звернення: 03.11.2019).
5. Гринчар Н. Н. Особенности управления рисками при внедрении новых информационных технологий // Экономика и управление: проблемы и решения (Часть II) : материалы междун. заочной научно-практической конференции (21 ноября 2011 г.). Новосибирск : Сибирская ассоциация консультантов, 2011. С. 124–127.
6. Двойцова И. Н., Барановская Е. Г., Зырянова Н. Ю. Преимущества и недостатки внедрения информационных технологий. URL: http://www.rusnauka.com/14_ENXXI_2009/Economics/46078.doc.htm (дата звернення: 03.11.2019).
7. Ризик (інформаційна безпека). URL: [https://uk.wikipedia.org/wiki/Ризик_\(інформаційна_безпека\)#cite_note-0-1](https://uk.wikipedia.org/wiki/Ризик_(інформаційна_безпека)#cite_note-0-1) (дата звернення: 07.11.2019).
8. Утечки данных. URL: http://www.tadviser.ru/index.php/Статья:Утечки_данных (дата звернення: 06.11.2019).
9. Орлик О. В. Інформаційні технології забезпечення безпеки електронного бізнесу // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. (Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 167–169.
10. Орлик О. В. Проблеми забезпечення інформаційної складової економічної безпеки сучасних підприємств // Кібербезпека в Україні: правові та організаційні питання : матеріали III Всеукр. наук.-практ. конф. (Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 79–81.
11. Фінансово-економічна безпека підприємств та інформаційні технології забезпечення безпеки : монографія / О. В. Орлик, О. О. Кюне, О. Г. Єсіна, А. Ю. Вакула. Одеса : ФОП Гуляєва В. М., 2018. 140 с.
12. Сохадзе Т. Т., Орлик О. В. Методи забезпечення безпеки інформації в інформаційних системах // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2019. Вип. 1. С. 84–88.