9. Chaplinskyj, Yu.B. (2021). Approaches to evaluating the effectiveness of loyalty programs. Visnyk Chernivets'koho torhovel'no-ekonomichnoho instytutu [Bulletin of the Chernivtsi Trade and Economic Institute], vol. II (82), pp. 54–65 (in Ukr.).

10. Chaplinskyj, Yu.B., Nikulcha, V.A. (2019). The mechanism of formation of the system of consumer loyalty to the tourist enterprise. Visnyk Chernivets'koho torhovel'no-ekonomichnoho instytutu [Bulletin of the Chernivtsi Trade and Economic Institute], vol. I (73), pp. 122–130 (in Ukr.).

УДК 658.5 : 004.056
JEL Classification: M11, D29, L86
DOI: *http://doi.org/10.34025/2310-8185-2021-3.83.06*

Н. В. Шупрудько, к.е.н., доцент,
https://orcid.org/ 0000-0002-5629-0671
Чернівецький торговельно-економічний інститут КНТЕУ,
м. Чернівці

ДЕТЕРМІНАНТИ УСПІХУ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Анотація

Актуальність. Постановка проблеми. Сьогодення ставить нові виклики у сфері інформаційної безпеки перед бізнесом, в тому числі і малим та середнім. Щораз більшої значущості набувають нематеріальні активи, виникають нові інформаційні загрози. Побудова системи менеджменту інформаційної безпеки дає можливість бізнесу бути готовим до загроз та успішно розвиватися.

Мета дослідження полягає в аналізі та обґрунтуванні факторів успішності системи менеджменту інформаційної безпеки малого та середнього бізнесу в Україні.

Методологія. При побудові логіки і структури статті ми використали метод структурно-логічного аналізу. Для узагальнення підходів до визначення ключових факторів успіху системи менеджменту використано методи групування і систематизування, аналізу й синтезу. Для формування переліку проблем, потреб та загроз інформаційного середовища МСБ – системний метод дослідження та спостереження.

Результати. Дослідження показали нагальну потребу суб’єктів малого та

середнього бізнесу у використанні у своїй діяльності ефективної системи менеджменту інформаційної безпеки, яка має бути органічною частиною загального менеджменту. Потреба у менеджменті інформаційної безпеки продиктована двома типами загроз: загроза власне небезпечної інформації та загроза використання (впливу) небезпечних інформаційних технологій.

Обґрунтовані загальні та конкретні потреби та проблеми в управлінні інформаційною безпекою на вітчизняних підприємствах, серед яких: захист функціональності бізнесу, безпечної роботи програм і додатків, захист даних, захист технологічних активів бізнесу.

Швидке подолання зазначених проблем шляхом побудови системи менеджменту інформаційної безпеки можливе лише за умови розуміння та врахування ключових факторів успіху такої системи. Фактори успіху мають розкривати класичні функції менеджменту: успіх планування, успіх організації, успіх мотивації, успіх контролю. Доповненням ключових факторів успіху може стати врахування чинників, які суттєво впливають на прийняття та формування культури інформаційної безпеки суб'єктами МСБ.

Практичне значення. Побудова системи інформаційної безпеки на підприємстві на основі врахування ключових факторів успіху дає можливість суб'єкту отримати динамічну рівновагу із зовнішнім оточенням та бути готовим до ймовірних ризикових потенційно негативних подій.

Перспективи подальших досліджень. Подальшим напрямом дослідження має стати пошук та обґрунтування конкретних складових зазначених факторів успіху, їх деталізація та вивчення механізмів імплементації у практику господарювання МСБ.

Ключові слова: менеджмент інформаційної безпеки, малий бізнес, інформаційна безпека, фактори успіху.

Кількість джерел: 8.

Nataliia Shuprudko, Candidate of Economic Sciences,
Associate Professor,
https://orcid.org/ 0000-0002-5629-0671
Chernivtsi Institute of Trade and Economic of KNUTE, Chernivtsi

DETERMINANTS OF SUCCESS INFORMATION SECURITY MANAGEMENT OF SMALL AND MEDIUM BUSINESS

Summary

Today poses new challenges in the field of information security for businesses, including

small and medium. Intangible assets are becoming increasingly important, and new information threats are emerging. Building an information security management system allows businesses be prepared for threats and develop successfully.

The purpose of the study is to study and substantiate the success factors of the information security management system of small and medium-sized enterprises (SMEs) in Ukraine.

Constructing the logic and structure of the article, we used the method of structural-logical analysis. Methods of grouping and systematization, analysis and synthesis are used to generalize approaches to determining the key success factors of the management system. A systematic method of research and observation was used to form a list of problems, needs and threats of the information environment of SMEs.

Study has shown that there is an urgent need for small and medium-sized businesses to use an effective information security management system in their activities, which should be an integral part of overall management. The need for information security management is dictated by two types of threats: the threat of actually dangerous information and the threat of using (influencing) dangerous information technologies.

The general and specific needs and problems in information security management at domestic enterprises are substantiated, including protection of business functionality, safe operation of programs and applications, data protection, protection of technological assets of the business.

Rapid overcoming of these problems by building an information security management system is possible only if one understands and takes into account the key success factors of such a system. Success factors should reveal the classic functions of management: the success of planning, the success of the organization, the success of motivation, the success of control. Another key success factor can be taking into account the factors significantly influencing the information security culture formation and adoption by the SMEs.

Building an information security system in the enterprise based on key success factors allows the entity to achieve a dynamic balance with the external environment and be prepared for possible potentially negative events.

A further direction of the research should be the search for and substantiating specific components of these success factors, their detailing and study of the mechanisms of implementation in the SME management practice.

Keywords: information security management, small business, information security, success factors.

Number of sources – 8.

Постановка проблеми. Сьогодні ми спостерігаємо стійку тенденцію перетворень у світовій економіці, що змінюють парадигму ведення бізнесу, де джерела успіху майже кожного виду бізнесу переходять з матеріальних активів на нематеріальні, а

інформація та її вартість стають все більш значущими, особливо в сегменті малого та середнього бізнесу як найбільш чутливого сектору економіки будь-якої країни. У цьому контексті, зважаючи на економічну та соціальну роль малого та середнього бізнесу у суспільстві, можна стверджувати про потребу підвищення уваги до інформаційної безпеки суб'єктів малого та середнього бізнесу (МСБ). Сучасний фокус уваги до цієї проблеми є незначним порівняно з великим бізнесом та потребує не просто ефективного менеджменту, але й визначення тих факторів ефективності, які б забезпечили успішність такого менеджменту.

Складності у вирішенні проблем забезпечення успішності менеджменту інформаційної безпеки МСБ додає те, що зазвичай пріоритетом є глобальна та національна безпека, в тому числі її інформаційна складова. Хоча варто зазначити, що мало хто заперечує проти того, що інформаційна складова за важливістю вийшла на рівень економічної складової.

Тому пошук факторів успішності системи менеджменту інформаційної безпеки суб'єктів МСБ набуває актуальності не лише у контексті ефективності їх господарської діяльності, але й забезпечення досягнення цілей управління інформаційною безпекою на національному та глобальному рівнях.

Аналіз досліджень і публікацій. Актуальність даної проблематики підтверджується низкою досліджень вітчизняних і закордонних вчених. Так, автори [1] безпосередньо досліджують фактори успіху управління інформаційною безпекою в сегменті МСБ Словаччини, серед яких ключовими визначають 4 основні фактори успіху управління інформаційною безпекою: відповідність управління інформаційною безпекою бізнес-діяльності компанії, підтримка вищого керівництва, контроль безпеки та поінформованість організації. Результати дослідження показують, що контроль безпеки та підтримка вищого керівництва є найважливішими факторами загалом, а фактор організаційної обізнаності є найбільш очевидним і важливим

у короткостроковому періоді.

Інформаційну безпеку малих і середніх підприємств у Туреччині порівнювали з даними інших країн автори у своєму дослідженні [2]. Згідно з результатами цього дослідження, пріоритетними напрямами менеджменту інформаційної безпеки є покращення комунікаційного та операційного управління та політики безпеки. Це, своєю чергою, веде до покращення й інших параметрів безпеки в компаніях: організаційних, кадрових, екологічних.

Вітчизняні автори, досліджуючи менеджмент інформаційної безпеки, зосереджуються на питаннях переважно техніко-економічних [3; 4; 5] або загальноуправлінських [6].

Однак питання менеджменту інформаційної безпеки суб'єктів МСБ в Україні залишаються поза увагою науковців загалом, а також аспекти пошуку та обґрунтування факторів успішності зокрема.

Формулювання мети, цілей та завдань. Мета дослідження полягає у дослідженні та обґрунтуванні факторів успішності системи менеджменту інформаційної безпеки малого та середнього бізнесу в Україні.

Для досягнення поставленої мети ми вбачаємо виконання низки завдань, зокрема:

- визначити зміст та особливості інформаційної безпеки суб'єктів МСБ у (як у зовнішньому, так і у внутрішньому середовищі);
- визначити систему менеджменту інформаційної безпеки та потребу в ній з боку МСБ;
- обґрунтувати фактори успіху менеджменту інформаційної безпеки МСБ в Україні.

Виклад основного матеріалу. Традиційно увага у вітчизняній економіці приділялася переважно економічній безпеці загалом, залишаючи безпеку інформаційну поза достатнім фокусом уваги. При цьому державна політика безпеки стосувалася економічної безпеки на рівні національної економіки як системи, де безпека МСБ була лише складовою, і не завжди ключовою. Тому традиційно

рівень економічної безпеки залишається низьким у вітчизняному малому та середньому бізнесі і ми, погоджуючись з авторами [7], констатуємо ще й той факт, що говорити про системність менеджменту інформаційної безпеки поряд із економічною, фінансовою, технологічною та іншими не доводиться.

Інформаційна безпека – це не лише захист інформації від несанкціонованого доступу. Інформаційна безпека – це, в основному, практика запобігання несанкціонованому доступу, використанню, розголошенню, зриву, модифікації, перевірці, запису або знищенню інформації. Інформаційна безпека охоплює такі сфери дослідження, як криптографія, мобільні обчислення, кіберкриміналістична експертиза, онлайн-соціальні медіа тощо.

В епоху суцільної діджиталізації інформаційна безпека виходить на перші місця та потребує адекватної уваги з метою подолання ймовірних загроз, які існують як у зовнішньому середовищі суб'єктів МСБ, так і всередині бізнес-одиниць. На сьогодні можна виділити дві категорії загроз:

1) загроза власне небезпечної інформації;

2) загроза використання небезпечних інформаційних технологій.

Інформація сама по собі може бути небезпечною та призвести до негативних наслідків для бізнесу. Наприклад, використання неперевіреної інформації із сумнівних джерел про контрагентів може мати наслідком укладання невигідних угод або й взагалі отримання прямих збитків.

Використання в господарській діяльності, наприклад, незахищених технологій передачі даних, недотримання цифрової гігієни співробітниками тощо може стати також потенційно загрозливим та завдати збитків бізнесу.

Сьогодні часто цілями кіберзлочинців можуть стати не тільки відомі корпорації, а й будь-які підприємства малого та середнього бізнесу, які обробляють дані кредитних карток або зберігають певну конфіденційну інформацію. Більшість власників МСБ роблять

велику помилку – не приділяють увагу захисту даних, інформаційній безпеці загалом, вважаючи, що їх це ніяк не стосується. Однак інструменти кіберзлочинців удосконалюються, а кількість жертв зростає.

Саме тому постає питання необхідного забезпечення інформаційної безпеки на підприємствах, що передбачає формування повноцінної системи менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки, по суті, є системою управління та захисту інформаційного середовища бізнесу, передусім його інформаційних активів. Ми виходимо з того, що системі менеджменту інформаційної безпеки суб'єкта МСБ притаманні всі загальні для систем менеджменту елементи.

Мета управління інформаційною безпекою даних полягає в тому, щоб забезпечити безперервність бізнесу та зменшити шкоду бізнесу шляхом запобігання та мінімізації впливу загроз безпеки.

Визначимо головні причини або потреби МСБ в інформаційній безпеці (табл. 1).

Загроз інформаційної безпеки може бути багато, наприклад атаки на програмне забезпечення, крадіжка інтелектуальної власності, крадіжка особистих даних, крадіжка обладнання чи інформації, саботаж та вимагання інформації – все це потребує системної уваги, впровадження превентивних заходів, розбудови механізмів реагування на ризикові події та їх наслідки тощо.

Існують деякі інші фундаментальні проблеми в управлінні інформаційною безпекою в МСБ. Вони наведені нижче:

1. Завдання технології: вибухове зростання Інтернету та пов'язаних з ним технологій дозволило МСБ збирати цінну інформацію. Але інформаційні активи ставлять перед МСБ безліч проблем: обробка та зберігання інформації, відсутність ресурсів для розробки та впровадження програмного забезпечення безпеки, а також хмара та пов'язані з нею ризики – усе це посилюється фінансовими обмеженнями та постійно супроводжується ризиком

втрати довіри клієнтів.

2. Відсутність основи для управління інформаційною безпекою. Хоча проблема технології обмежує попередні зусилля щодо управління ризиками інформаційної безпеки, відсутність ефективної структури робить стратегії подолання загроз неефективними. Це створює розрив між тим, де хоче бути бізнес середнього рівня, і тим, де він насправді знаходиться в контексті його здатності керувати ризиками інформаційної безпеки. Відсутність системи управління ризиками також робить МСБ неспроможними протистояти обмеженню ресурсів за допомогою належного планування та стратегії.

Таблиця 1

Необхідність впровадження системи менеджменту інформаційної безпеки малим та середнім бізнесом

Потреба	Характеристика
Захист функціональності бізнесу	Особа, яка приймає рішення в організації, повинна встановлювати політику та керувати своєю організацією відповідно до складного, змінюваного законодавства, ефективних та дієвих програм.
Забезпечення безпечної роботи програм, додатків	Організація перебуває під величезним тиском, щоб придбати і керувати інтегрованими, ефективними та ефективними програмами. Сучасній організації необхідно створити середовище, яке захищає програми з використанням IT-систем організації, особливо тих додатків, які служать важливими елементами інфраструктури організації.
Захист даних, які збирає та використовує бізнес	Дані в організації можуть бути у двох формах: у стані спокою або в русі, рух даних означає, що дані в даний момент використовуються або обробляються системою. Значення даних спонукали зловмисників заблокувати або зіпсувати дані. Це важливо для цілісності та цінності даних організації. Інформаційна безпека забезпечує захист як даних у русі, так і даних у стані спокою.
Захист технологічних активів бізнесу	Організація повинна додати внутрішні послуги на основі розміру та сфери діяльності організації. Організаційне зростання може призвести до необхідності інфраструктури відкритих ключів, інтегрованої системи програмного забезпечення, методологій шифрування. Механізм інформаційної безпеки, який використовується великими організаціями, є складним порівняно з невеликою організацією. Невелика організація зазвичай віддає перевагу симетричному ключовому шифруванню даних.

3. Невиконання стандарту ISO 27001:2013: на відміну від

багатонаціональних компаній, які впроваджують систему управління інформаційною безпекою (СУББ), МСБ часто буває важко комплексно впровадити вимоги стандарту ISO/IEC 27001:2013. Нездатність малих і середніх підприємств, які є вразливими до різноманітних ризиків, що несуть регуляторні, операційні та фінансові загрози, ефективно застосовувати на практиці необхідні керівні принципи, такі як політика та процедури для зменшення ризику інформаційної безпеки.

4. Відсутність політики інформаційної безпеки: хоча деякі малі та середні підприємства прагнуть досягти більшої мети повної інформаційної безпеки, багато з них часто не можуть створити чітко визначену політику інформаційної безпеки. Відсутність цього, очевидно, затуманює ширший зір, заважаючи безпосередньому завданню виявлення будь-якої потенційної шкоди.

5. Непідготовлені ресурси та необслуговування програмних засобів: у той час як малі підприємства не можуть навчати свої критичні кадрові ресурси насамперед через фінансові обмеження, середні підприємства очікують, що їхня робоча сила вже достатньо навчена, щоб визначити та вжити заходів захисту від зростаючих ризиків. З іншого боку, критичний персонал, який обробляє важливу архітектуру програмного забезпечення, повинен періодично проходити навчання протистояти будь-якій новій загрозі. Інакше відсутність навчання призводить до неякісного управління інформаційними системами і навіть повного занедбання систем безпеки.

Швидке подолання зазначених проблем шляхом побудови системи менеджменту інформаційної безпеки можливе лише за умови розуміння та врахування ключових факторів успіху такої системи.

На наш погляд, фактори успіху мають розкривати класичні функції менеджменту:

1) успіх планування;

2) успіх організації;

3) успіх мотивації;

4) успіх контролю.

Доповненням ключових факторів успіху може стати врахування чинників, які суттєво впливають на прийняття та формування культури інформаційної безпеки суб'єктами МСБ.

Критичними факторами успіху культури інформаційної безпеки можуть стати [8]:

- підтримка інформаційної безпеки вищого керівництва;
- створення ефективної політики інформаційної безпеки;
- поінформованість про інформаційну безпеку;
- навчання з інформаційної безпеки;
- аналіз та оцінка ризиків інформаційної безпеки, відповідність вимогам інформаційної безпеки, політика етичної поведінки, організаційна культура.

Фактично реалізація системи менеджменту інформаційної безпеки суб'єкта МСБ може бути організована як сукупність управління головними функціями менеджменту з врахуванням інформаційного аспекту.

Висновки та перспективи подальших досліджень. Таким чином, ми дослідили особливості формування системи менеджменту інформаційної безпеки суб'єктів малого та середнього бізнесу, яка є важливим елементом забезпечення безпеки господарської діяльності у сучасному інформаційному середовищі. Передусім важливо забезпечити безпеку внутрішнього середовища бізнесу та налагодити її динамічну рівновагу із впливом середовища зовнішнього, оскільки загрози можуть бути як від власне самої інформації, так і через недосконалу технологічну складову отримання, обробки, зберігання, використання тощо цієї інформації.

Це завдання могла б виконати дієва система менеджменту інформаційної безпеки МСБ, яку доцільно будувати на основі зазначених вище його особливостей, проблем та потреб.

Дієвість системи зумовлена реалізацією ключових факторів

успіху, які, як ми вважаємо, повинні відповідати базовим класичним функціям менеджменту: успіх планування, успіх організації, успіх мотивації та успіх контролю.

Тому подальшим напрямом дослідження має стати пошук та обґрунтування конкретних складових зазначених факторів успіху, їх деталізація та вивчення механізмів імплементації у практику господарювання МСБ.

Список використаних джерел:

1. Aleksandr Ključnikov & Ladislav Mura & David Sklenár (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues*, VsI Entrepreneurship and Sustainability Center, vol. 6(4), pp. 2081-2094, June.

2. Yildirim, Ebru & Akalp, Gizem & Aytaç, Serpil & Bayram, Nuran (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management - INT J INFORM MANAGE*, vol. 31, pp. 360-365.

3. Панченко В. А. Менеджмент інформаційної безпеки комерційного підприємства. *Центральноукраїнський науковий вісник. Економічні науки.* 2019. Вип. 3(36). С.219-228. URL: http://nbuv.gov.ua/UJRN/Nt_2017_3_6 (дата звернення 08.06.2021).

4. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. *Наукоємні технології*. 2017. №3. С. 215-225. URL: http://nbuv.gov.ua/UJRN/Nt_2017_3_6 (дата звернення 08.06.2021).

5. Турчин О. І. Інформаційна безпека процесів менеджменту інтегрованих систем. *Моделювання регіональної економіки.* 2010. №2. С. 347-352. URL: http://nbuv.gov.ua/UJRN/Modre_2010_2_42 (дата звернення 08.06.2021).

6. Обидєннова Т. С., Гусаров О. О., Антипцева О. Ю. Методи прийняття управлінських рішень в умовах розроблення, впровадження та функціонування системи менеджменту інформаційної безпеки. *Проблеми системного підходу в економіці.* 2019. Вип. 2 (1). С.153-157.

7. Джаман М. О., Гончаров Г. О. Еволюція та напрями вдосконалення державної політики забезпечення економічної безпеки малого підприємництва в Україні. *Економічні науки. Серія: Облік і фінанси.* 2014. Вип. 11(3). С. 34-43. URL: http://nbuv.gov.ua/UJRN/ecnof_2014_11(3)__6 (дата звернення 12.06.2021).

8. Alnatheer, Mohammed (2015). Information Security Culture Critical Success Factors. *Proceedings - 12th International Conference on Information Technology: New Generations*, ITNG 2015, pp. 731-735.

References:

1. Aleksandr Ključnikov & Ladislav Mura & David Sklenár (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues,* VsI Entrepreneurship and Sustainability Center, vol. 6(4), pp. 2081-2094, June.

2. Yildirim, Ebru & Akalp, Gizem & Aytaç, Serpil & Bayram, Nuran (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management - INT J INFORM MANAGE,* vol. 31, pp. 360-365.

3. Panchenko, V.A. (2019). Information security management of a commercial enterprise. *Tsentral'noukrayins'kyy naukovyy visnyk. Ekonomichni nauky [Central Ukrainian Scientific Bulletin. Economic sciences],* №3(36), pp. 219-228. URL: http://nbuv.gov.ua/UJRN/Nt_2017_3_6 (Accessed 08.06.2021) (in Ukr.).

4. Buchyk, S.S., Shalayev, V.O. (2017). Analysis of instrumental methods for determining information security risks of information and telecommunications systems. *Naukoyemni tekhnolohiyi [Science-intensive technologies],* №3, pp. 215-225. URL: http://nbuv.gov.ua/UJRN/Nt_2017_3_6 (Accessed 08.06.2021) (in Ukr.).

5. Turchyn, O.I. (2010). Information security of integrated systems management processes. *Modelyuvannya rehional'noyi ekonomiky [Modeling of the regional economy],* №2, pp. 347-352. URL: http://nbuv.gov.ua/UJRN/Modre_2010_2_42 (in Ukr.).

6. Obydyennova, T.S., Husarov, O.O., Antyptseva, O.Yu. (2019). Methods of making managerial decisions in terms of development, implementation and operation of information security management system. *Problemy systemnoho pidkhodu v ekonomitsi [Problems of system approach in economics],* №2(1), pp.153-157 (in Ukr.).

7. Dzhaman, M.O., Honcharov, H.O. Evolution and directions of improving the state policy of economic security of small business in Ukraine. *Ekonomichni nauky. Seriya: Oblik i finansy [Economic sciences. Series: Accounting and Finance],* № 11(3), pp. 34-43. URL: http://nbuv.gov.ua/UJRN/ecnof_2014_11(3)__6 (Accessed 12.06.2021) (in Ukr.).

8. Alnatheer, Mohammed (2015). Information Security Culture Critical Success Factors. *Proceedings - 12th International Conference on Information Technology: New Generations,* ITNG 2015, pp. 731-735.