ун-т ім. Вадима Гетьмана» ; [редкол.: І. М. Рєпіна (голов. ред.) та ін.]. – Київ : КНЕУ, 2019. – № 43. – С. 104–114.
4. Катрусяк Х. Забезпечення ефективності діяльності підприємства в сучасних умовах / Катрусяк Христина // Матеріали Ⅳ Міжнародної науково-практичної конференції „Формування механізму зміцнення конкурентних позицій національних економічних систем у глобальному, регіональному та локальному вимірах“, 31 березня 2020 року. — Т., 2020. — С. 48–50.

УДК: 658.012.8

Володимир Кузьомко
к.е.н., доцент кафедри бізнес-економіки та підприємництва,
ДВНЗ «КНЕУ ім. Вадима Гетьмана»,
volodymyr.kuzomko@kneu.ua

ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

INFORMATION SECURITY OF BUSINESS IN THE CONTEXT OF DIGITAL TRANSFORMATION OF THE ECONOMY

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ

Анотація. Розглянуто актуальні загрози інформаційній безпеці бізнесу, які формуються в умовах цифрової трансформації економіки, висвітлено першочергові напрями, методи та інструменти їх подолання.
Abstract. The current threats to the information security of business, which are formed in the context of the digital transformation of the economy, are considered, the priority areas, methods and tools for overcoming them are highlighted.
Аннотация. Рассмотрены актуальные угрозы информационной безопасности бизнеса, формирующиеся в условиях цифровой трансформации экономики, освещены первоочередные направления, методы и инструменты их преодоления.

Нарощування темпів цифрової трансформації економічних процесів, спричинене переходом до нової економіки 4.0, має на меті прискорення запровадження принципово нових методів та моделей поведінки економічних суб’єктів. На перший план виходять завдання комп’ютеризації, автоматизації і інтелектуалізації господарських процесів, віртуалізації господарської діяльності, впровадження та розвитку різних видів комунікаційних ресурсів та технологій. Відповідно, цифровізація, як об’єктивна реальність нової інституціональної економіки, формує перед господарюючими суб’єктами різних форм власності та організаційно-правових форм принципово нові, складні виклики, успішність реагування на які в найкоротші строки стає головною передумовою їх виживання на ринку, забезпечення конкурентоспроможності та довгострокового розвитку.

Цифровізація стає проривною технологією, яка забезпечує стрімкий розвиток бізнесу. За даними консалтингової компанії McKinsey, успішна цифровізація призводить до підвищення продуктивності праці на 55% і скорочує час виходу на ринок на 40% [1].

Можна погодитися з фахівцями у сфері інформаційних технологій [2], що цифрову трансформацію не варто розглядати спрощено, лише як автоматизацію і комп’ютеризацію окремих процесів чи підрозділів підприємств, а слід розуміти як повне переосмислення методів ведення бізнесу, формування додаткових компетентностей, впровадження нових і реконструкцію існуючих бізнес-процесів, їх інтеграцію, як в межах підприємства, так і з зовнішніми контрагентами на засадах сучасних ІТ-технологій (хмарні обчислення, штучний інтелект, машинне навчання тощо).

В цифровій економіці традиційні матеріальні чинники і ресурси господарської діяльності поступово поступаються місцем інтелектуальним і інформаційно-комунікаційним ресурсам і технологіям, що висуває перед суб'єктами бізнесу актуальні завдання ефективного формування, використання і захисту таких видів ресурсів, підвищуючи роль і значення інформаційної безпеки бізнесу як в теоретичній, так і в практичній площині.

Як відомо, під інформаційною безпекою бізнесу розуміється такий стан інформаційних ресурсів і пов'язаних з ними інформаційних засобів і систем суб'єкта господарювання, який гарантує якісне і безперебійне забезпечення його діяльності необхідною інформацією за умови високого рівня її захищеності від внутрішніх і зовнішніх загроз[3, с. 213]. Відповідно, можемо виокремити 2 проблемних поля забезпечення інформаційної безпеки бізнесу: а) діагностика і протидія загрозам інформації та б) створення передумов ефективного її використання в контексті тих викликів і актуальних завдань, які стоять перед бізнесом в даний час.

В контексті першого аспекту, варто, перш за все, враховувати, що цифровізація економіки поряд з традиційними (промислове шпигунство, навмисне і ненавмисне розголошення конфіденційної інформації та комерційної таємниці працівниками, недобросовісні дії конкурентів, включаючи шкоду діловій репутації, втручання сторонніх осіб в інформаційні системи і мережі, порушення цілісності баз даних тощо), генерує множину додаткових загроз інформаційним ресурсам і технологіям бізнесу, методи діагностики і протидії яким поки що відпрацьовані не в повній мірі. Мова йде, перш за все, про загрози, які пов'язані з кібератаками, розкриттям персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерних програм тощо.

Другий аспект інформаційної безпеки спрямований, головним чином, на постійне забезпечення відповідності інформаційних ресурсів бізнесу потребам в них, що обумовлює безперебійність і високу ефективність процесу прийняття та реалізації рішень в межах організації. В результаті досягається цілісність, захищеність і доступність інформації для користувачів бізнесу.

Різнобічний характер та зростаюча кількість загроз інформаційній безпеці бізнесу в умовах формування цифрової економіки обумовлює необхідність розробки та впровадження комплексного характеру дій, спрямованих на її захист. На наш погляд, варто щонайменше виокремлювати взаємопов'язані між собою технічний, організаційний та економічний напрями забезпечення інформаційної безпеки бізнесу.

Заходи технічного характеру пов'язані, в першу чергу, з використанням сучасних технічних засобів і технологій, які, з одного боку, дозволяють ефективно накопичувати, зберігати, обробляти і передавати інформацію, а, з іншого, – забезпечувати її високий рівень захищеності (розподілені бази даних, блокчейн-технології, мережеві екрани, хмарні сервіси, захищені сервери, антивірусні програми тощо). Ключовими суб'єктами в цій сфері є фахівці з інформаційних систем і технологій, системні адміністратори, які вживають заходів щодо безперебійності функціонування інформаційних мереж організації і забезпечують їх захист. Не будемо детально зосереджуватися на цьому аспекті, оскільки він є технічним і вузькоспеціалізованим. Зазначимо лише, що на сьогодні активно впроваджуються системи ранньої діагностики вторгнення і діагностики в режимі реального часу (SIEM), штучний інтелект, удосконалюється архітектура IT-рішень в межах організації, створюються єдині центри забезпечення безпеки (SOC), системи розгортання розподіленої інфраструктури хибних цілей (DDP)[2]тощо.

Не зважаючи на важливе значення техніко-технологічної складової забезпечення інформаційної безпеки бізнесу, дослідження, яке було проведене у 2017 році американським Центром інтернет безпеки (CIS) [4], переконливо довело, що головною дієвою особою і найслабшою ланкою в системі інформаційної безпеки є якраз не технічні системи і використовувані технології, а працівники самого підприємства. Саме через навмисні або ненавмисні дії персоналу здійснюється найбільший відсоток витоку конфіденційної інформації, відбувається втручання в захищені мережі і системи.

У зв’язку з цим важливого значення набуває обізнаність персоналу про можливі дії, які можуть призвести до такого витоку (розголошення) інформації Відповідно одним з пріоритетних напрямів забезпечення інформаційної безпеки бізнесу має стати постійне підвищення рівня інформаційної (цифрової) грамотності працівників та усебічне організаційно-документальне врегулювання процесів збору, накопичення, обробки використання і зберігання інформації в системі положень і інструкцій поводження з інформацією, які можуть імплементуватися в їх посадові інструкції. Такі завдання відповідають організаційному напряму забезпечення інформаційної безпеки бізнесу, який додатково охоплює такі дії, як визначення відповідальних за дотримання тих або інших заходів інформаційної безпеки, формування спеціалізованих на інформаційному захисті підрозділів в рамках організаційної структури організації, імплементацію положень нормативно-правових актів держави щодо кібербезпеки та захисту інформації в діяльність суб’єктів бізнесу тощо.

Важливою проблемою забезпечення інформаційної безпеки бізнесу є також застосування розгалуженої системи економічних заходів. Перш за все, варто усвідомлювати, що проблема захисту інформації має витратний аспект, який необхідно враховувати, порівнюючи позитивний ефект від захищеності інформаційних ресурсів і розмір витрат, які мають бути понесені на забезпечення такого захисту. Крім того, реалізація окремих заходів має проводитися на підставі співставлення вигід від захисту інформації і можливих втрат, які можуть бути понесені в результаті відсутності такого захисту. Цілком зрозуміло, що в разі відсутності економічної доцільності окремі заходи щодо захисту інформації не варто реалізовувати.

Особливо це стосується суб’єктів малого бізнесу, в яких через брак ресурсів організувати повноцінну ефективну систему інформаційної безпеки з формуванням спеціалізованих підрозділів може виявитися надто складним завданням. В такому разі, на наш погляд, варто використовувати переваги, які може надати субконтрактна система забезпечення безпеки бізнесу, в межах якої окремі функції по забезпеченню інформаційної безпеки бізнесу можуть виконуватися сторонніми суб’єктами на підставі укладених договорів. В контексті вищенаведеного, принципово важливим є формування спеціалізованого бюджету (кошторису) на забезпечення економічної безпеки бізнесу і інформаційної безпеки, зокрема.

Крім того, економічні методи забезпечення інформаційної безпеки бізнесу мають охоплювати мотиваційні заходи та інструменти, спрямовані на заохочення працівників до дій, спрямованих на зміцнення захисту інформації, підвищення рівня своєї цифрової грамотності і, навпаки, протидіючі тим діям, які уможливлюють витік конфіденційної інформації, сприяють порушенню цілісності баз даних, шкодять іміджу бізнесу тощо.

Підбиваючи підсумки, варто зазначити, що проблема інформаційної безпеки бізнесу в умовах цифровізації економіки набуває особливої актуальності, а ті загрози, які породжує цифрова трансформація можуть бути успішно подолані лише взаємопов’язаною дією технічних, організаційних та економічних методів та засобів.

Література

1. Савченко М. Цифровая трансформация бизнеса : кому нужна и с чего начать. URL :https://www.epravda.com.ua/rus/columns/2020/10/27/666627/
2. Крилов И. Угрозы информационной безопасности в эпоху цифровой трансформации. URL :https://habr.com/ru/post/544932/
3. Кузьомко В. М. Концептуальні підходи до виокремлення функціональних складових економічної безпеки підприємства. Формування ринкової економіки : зб. наук. пр.Вип. 26. У 2-х ч.Ч.І. К. : КНЕУ, 2011. С. 206-216.
4. CIS Controls Implementation Guide for SMEs. URL :CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org)