

Тульчинська Світлана Олександрівна,
д.е.н., професор, професор кафедри економіки та підприємництва,
Солосіч Олександр Сергійович,
аспірант кафедри економіки та підприємництва,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ОБЛІКОВОЇ ДІЯЛЬНОСТІ ЯК БАЗОВА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ВОЄННОГО СТАНУ

Однією із ключових особливостей функціонування сучасних економічних систем є їх першочергова орієнтація на інтелектуальну компоненту розвитку, зокрема інформацію як її невід'ємний елемент. Активний розвиток інформаційних технологій відкрив нові управлінські та ресурсні можливості до нарощення господарської ефективності підприємницьких структур, разом з тим, спричинивши появу загроз принципово нового рівня, ігнорування або нехтування якими може завдати значних економічних втрат та підставити під сумнів можливості подальшого функціонування підприємства. Особливої актуальності дані питання набувають в умовах дії воєнного стану та активізації кіберзагроз.

Інформаційна безпека підприємницької структури нерозривно пов'язана із сформованою на його базі системою обліку та відповідними інформаційно-технічними засобами, що забезпечують її перманентне функціонування. Адже, саме система обліку є джерелом найбільш важливої та комерційно чутливої інформації для підприємства, при цьому активні процеси діджиталізації формують нові безпекові виклики та потребують адекватного управлінського реагування безпосередньо у контексті забезпечення загальної економічної безпеки.

Виходячи з цього, пропонуємо ідентифікувати ключові безпекові виклики, які постають перед господарськими структурами у сфері забезпечення інформаційної безпеки облікової діяльності: (1) вразливість віртуальної інфраструктури підприємства в контексті потенційних кібератак та підірвної діяльності ворожих країн; (2) відсутність комплексної інтеграції облікових процесів у цифрову інфраструктуру підприємства; (3) застосування конкуруючими структурами неправомірних інструментів економічної розвідки (інформаційного шпіонажу); (4) відсутність повноцінно сформованої управлінської політики у сфері інформаційної безпеки системи обліку; (5) високий рівень залежності інформаційної інфраструктури від надійності електропостачання; (6) низький рівень цифрової компетентності працівників, залучених до роботи з інформаційними системами обліку; (7) ризики порушення

конфіденційності як відносно комерційно чутливої інформації підприємства, так і щодо особистої інформації працівників (порушення меж цифрового контролю); (8) наявність комунікаційного розриву між технічними спеціалістами та безпосередньо суб'єктами ведення обліку, що значно ускладнює процес системної інтеграції програмних продуктів.

Окреслені вище безпекові виклики становлять значну загрозу стабільному функціонуванню підприємницьких структур в умовах воєнного стану, саме тому пропонуємо сформулювати перелік основних напрямків посилення інформаційної безпеки систем обліку в контексті забезпечення загальної економічної безпеки підприємства в сучасних умовах: (1) забезпечення цілісності та інформаційної ізольованості внутрішніх систем обліку (включає в себе провадження відповідних контрольних та режимних процедур) (2) формування та чітка регламентація базових положень інформаційної політики підприємства у її тісному взаємозв'язку із прийнятою системою обліку; (3) забезпечення резервних засобів підтримки електрифікованості ключових елементів інформаційної інфраструктури та її захисту (серверні, відеоспостереження тощо); (4) перманентний моніторинг кіберзагроз, формування індивідуалізованого підходу до управління кібер-ризиками; (5) ізоляція фізичного доступу до найбільш важливих технічних елементів інформаційних систем (серверні приміщення, інформаційні носії), фіксація та контроль віртуального доступу до облікових даних; (6) забезпечення безперервного підвищення кваліфікації працівників, що здійснюють обробку облікових даних [1, с. 18]; (7) здійснення постійного вдосконалення безпекових елементів віртуальної інформаційної інфраструктури [2, с. 57]; (8) налагодження дієвої системи комунікації між ключовими відповідальними технічними та обліковими фахівцями в процесі інтеграції інформаційних систем.

Підсумовуючи вищевикладене, можна стверджувати, що в умовах активних процесів інформатизації соціально-економічних відносин підприємства стикаються з широким спектром загроз пов'язаних із забезпеченням інформаційної безпеки облікових систем, як екзогенного, так і ендогенного походження, водночас, рівень спроможності підприємства до їх ефективної елімінації напряму залежить від можливостей підприємства організувати комплексну управлінську політику інформаційної безпеки облікових процесів як у сфері підтримки захищеності програмного забезпечення та відповідної віртуальної інфраструктури, так і щодо фізичної захищеності відповідних технічних засобів та інформаційних носіїв.

Список використаних джерел:

1. Легенчук С. Ф., Городинський М. П., Майстренко Н. М. *Захист бухгалтерських даних в умовах використання Інтернету речей: проблеми і перспективи діджиталізації обліку. Облік і фінанси. 2021. №1 (91). С. 12-19.*
2. Тульчинська С. О., Солосіч О. С., Чорній В. В. *Вплив діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства. Інвестиції: практика та досвід. 2021. № 9. С. 54–58.*