УДК 657.6:008

Муравський В. В.,
д.е.н., доцент, професор кафедри обліку і оподаткування,
Питель С. В.,
к.е.н., доцент, доцент кафедри обліку і оподаткування,
Тернопільський національний економічний університет

ГІПОТЕЗА ПРО ОБЛІКОВУ ПЛАТФОРМУ ОРГАНІЗАЦІЇ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

Важливим елементом запобігання гібридного впливу на національні та державні формації є забезпечення кіберзахисту економічних систем. Кібербезпека підприємств, секторів та галузей економіки країн передбачає реалізацію інформаційного захисту, попередження організаційних, технологічних, іміджевих та інвестиційних втрат. Враховуючи генеративну природу бухгалтерського обліку у сфері продукування економічної інформації, необхідним є залучення облікових фахівців до проблематики кіберзахисту підприємств. Система бухгалтерського обліку як частина управління підприємством є первинною ланкою в інформаційному процесі, а тому потребує першочергового кібернетичного захисту.

Спочатку необхідність забезпечення кіберзахисту розглядалася лише як елемент інформаційного кругообігу на підприємствах з метою запобігання: втрати споживчої цінності облікової інформації, потрапляння облікових даних до сторонніх осіб, несанкціонованого доступу працівників до інформаційних ресурсів тощо. Такий, винятково інформаційний підхід до кіберзахисту, є частковим та не дає змоги системно забезпечити кібернетичну безпеку суб'єктів господарювання, галузей економік чи національних економічних систем.

Активізатором ґрунтовних науково-прикладних досліджень щодо захисту облікової інформації стали активні кіберзагрози на міждержавному рівні як частина гібридних воєн. Глобальність та масштабність проблематики кібербезпеки визначила необхідність забезпечення інформаційної та економічної безпеки країн. На багатьох великих підприємствах національного значення були створені структурні об'єкти або відкриті вакансії для працівників, функціональними обов'язками яких є забезпечення кібернетичної безпеки. Проте, з часом, активні хакерські атаки; викрадення інформації, що містить комерційну таємницю; вбудовування вірусних модулів в програмне забезпечення для отримання вигоди шахрайськими методами і т.д. призвели до актуалізації забезпечення кіберзахисту на мікро-рівні.

Штатні працівники технічних фахових спеціальностей (системні адміністратори, програмісти, корпоративні архітектори, адміністратори баз даних тощо) не здатні забезпечити системний кіберзахист з акцентом на оптимізацію економічних процесів на підприємствах. Якщо великі суб'єкти господарювання можуть формувати проблемні групи з штатного персоналу для врахування економічних та технічних аспектів кіберзагроз або залучати

послуги безпекового аутсорсингу, то суб'єкти малого бізнесу ресурсно обмежені для організації повноцінного інформаційного захисту.

З метою оптимізації інформаційно-безпекових процесів рекомендовано функції кібрзахисту асоціювати з обліковою системою підприємств. Забезпечення кібербезпеки передбачає не лише захист облікової інформації, система обліку стає суб'єктом безпекових процесів. Висувається гіпотеза науково-прикладних досліджень, відповідно до якої бухгалтерський облік є платформою забезпечення кібербезпеки підприємств, інтегратором методичних й організаційних дій з метою реалізації інформаційної та економічної безпеки суб'єктів господарювання, галузей та секторів економіки.

Базовими причинними постулатами сформованої гіпотези, які потребують науково-прикладного доведення, визначено наступне:

- система бухгалтерського обліку є основним генератором економічної інформації, що визначає пріоритетність забезпечення кібербезпеки облікових процесів;
- значна частина облікової інформації (за виключенням даних, продукованих фінансовим обліком) містять комерційну таємницю, оскільки використовуються керівництвом підприємства для оперативного, тактичного і стратегічного управління;
- останні хакерські атаки та шахрайські дії реалізовувалися через обліково-управлінське програмне забезпечення (вірус «Pety.A» у програмі «M.E.Doc», відключення енергопостачання населення через хакерські атаки), що пояснює важливість захисту системи обліку;
- сучасні бухгалтери є мультиквалфікованими фахівцями, які поєднують економічні, технічні, юридичні знання і можуть виконувати функції із кіберзахисту підприємств;
- регуляторною базою бухгалтерського обліку є нормативні документи, які визначають більшість інформаційних процесів на підприємстві, і можуть містити регламенти забезпечення кібербезпеки.

Розробка методики та організації обліку в частині реалізації кіберзахисту підприємства потребує: ідентифікації й класифікації інформаційних ризиків та кіберзагроз, перегляду функціональних повноважень обліково-управлінських фахівців, оновлення професійних навичок та вмінь бухгалтерів, запровадження практики безпекового аудиту на перманентній основі, удосконалення облікової політики та внутрішніх регламентів підприємства, розробки методики стресового реагування на появу кіберзагрози, перегляду методики обліку бізнес-процесів у напрямку захисту конфіденційної інформації, реорганізації облікової служби суб'єкта господарювання, аутсорсингу облікових функцій із значною імовірністю виникнення кіберзагроз, селекції актуального на ринку програмного забезпечення на предмет відповідності безпековим параметрам, вибору найбільш захищених електронних комунікацій облікового призначення.

Системне врахування усіх напрямків забезпечення кібербезпеки підприємств сприятиме попередженню, уникненню та оперативному реагуванню на кіберзагрози незалежно від джерел їх походження.