УДК 657

Шигун Марія Михайлівна,
д.е.н., професор кафедри бухгалтерського обліку та консалтингу,
Фурда Віктор Олександрович,
аспірант кафедри бухгалтерського обліку та консалтингу,
Київський національний економічний університет імені Вадима Гетьмана,
м. Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА НА ПІДПРИЄМСТВІ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

У 2022 році Україна через війну стикнулася з ракетними обстрілами цивільних об'єктів та критичної інфраструктури. Не рідко постраждалими від ракетних ударів виявилися не тільки адміністративні будівлі, медичні заклади, заклади освіти, об'єкти критичної інфраструктури, але також й житлові будинки й приміщення юридичних осіб. При цьому фізично постраждали як виробничі підрозділи, так й адміністративні будівлі з місцями, де зберігаються паперові документи. Також руйнуванню піддаються приміщення, де розміщені сервери або структура, яка поєднує ці сервери, з інформацією підприємств, в тому числі й обліковою. Відповідно, питання фізичної безпеки інформації і документації отримує особливу роль і в 2022-2023 роках буде одним з найбільш актуальних в Україні.

Як правило під безпекою інформації мається на увазі збереження її конфіденційності, запобігання її витоку, запровадження заходів, за яких дані не потраплять до конкурентів або суб'єктів, які можуть нашкодити підприємству [1, с.87]. Разом з тим, безпека даних також означає і забезпечення цілісності інформації та її фізичне збереження. В умовах військового стану заходи із забезпечення інформаційної безпеки набувають ключового значення для підтримання безперервної діяльності підприємств, і облікова інформація при цьому не є винятком.

Виходячи з типів носіїв облікову інформацію можна умовно поділити на цифрову та паперову [2]. До цифрової відносяться бази даних, їх резервні копії, електронні документи, скан-копії документів, цифрові ключі доступу до різних систем тощо [3]. До паперової інформації відносять документи різного типу, наприклад: фінансова та податкова звітність, договори, накладні, звіти про витрати, касові документи, банківські виписки, різні види регістрів бухгалтерського обліку тощо [3]. Кожен із перелічених типів даних необхідно захищати.

Проблеми фізичного захисту інформації мають декілька шляхів вирішення, які залежать від розміру підприємства, його ресурсів та рівня діджиталізації. Разом з тим, можуть бути застосовані рекомендації, які можуть бути універсальними для різних типів організацій і передбачають систему правил поводження з документами.

Перш за все, на підприємстві повинна бути розроблена система електронного документообігу, яка має визначати терміни та умови зберігання

оцифрованих копій документів та вимоги до якості зображень. Усю необхідну документацію за останні періоди потрібно оцифрувати, зробити скан-копії. Таку інформацію можна зберігати в хмарних сховищах із достатньою для роботи пропускною здатністю або в бухгалтерській програмі відповідно до операції, як наприклад в IT-Enterpise, однак тоді варто створювати резервну копію бази даних і зберігати її у хмарі. Щодо неактуальних документів, за якими минув термін зберігання, їх доречно зберігати в архіві, розміщеному у підвальному приміщенні або на відносно захищеній території.

Якщо підприємство відноситься до мікро- чи малого, має низький рівень діджиталізації, працює з відносно невеликими обсягами інформації, яку зберігає на фізичному комп'ютері, тоді варто перейти на застосування хмарних технологій для підвищення ступеня захисту даних. Розрахунки, виконані в MS Excel, можуть бути перенесені до його хмарної версії – Office 365 або до Google Sheets, які є безкоштовними для використання, і хоча мають певні обмеження щодо обсягів даних і дещо менший, але як правило достатній функціонал.

Малі та середні підприємства як правило використовують повноцінні бухгалтерські програми або ERP-системи. Якщо бухгалтерська програма, яка використовується, розміщена на локальному сервері, тоді необхідно створювати резервні копії бази даних у хмарному сховищі, яка буде оновлюватися з певною періодичністю. Також можливим варіантом може бути застосування бухгалтерської програми інтегрованої з хмарою, наприклад, "Діловод", який крім того має відносно нижчу вартість у порівнянні з популярними програми з ведення бухгалтерського обліку. Важливим для керівництва підприємства перед переміщенням управлінських та облікових даних в хмару є отримання інформації щодо того, де знаходяться дата-центри хмарного сервісу та сформувати відповідний план дій на випадок несправності одного з центрів, якщо їх декілька.

Вирішення проблеми фізичної безпеки даних для великих підприємств має свої особливості. В Україні такі суб'єкти часто мають власні сервери для обробки та збереження інформації, оскільки в довгостроковій перспективі це надає цінову перевагу. З початком бойових дій на території України у 2022 році такий підхід виявився небезпечним з точки збереження даних. Яскравим прикладом є АТ "Райффайзен Банк", який мав дата-центр у Херсоні, що на початку вторгнення став недоступним.

Альтернативним способом захисту інформації для великих підприємств є переміщення їхніх баз даних до хмарних сервісів, проте з точки зору обсягу таких даних використання хмар є досить вартісним. Це пов'язано передусім зі складною структурою потоків даних та необхідним розширеним функціоналом для її підтримання. На сьогодні існує як мінімум три хмарних сервіси, які здатні забезпечити нормальне функціонування та обмін даними для великих підприємств: Amazon Web Services (AWS), Azure, Google Cloud. Кожен із них представлений корпорацією техно-гігантом з великою кількістю розробок та надійною репутацією. Зокрема, АТ "Райффайзен Банк" переходить до використання хмарного сервісу AWS [4]. За попередніми оцінками вартість використання серверів компанії Амазон буде щонайменше вдвічі більшою ніж

утримання власних серверів, однак безпека інформації для суб'єкта такого масштабу є важливішою.

Таким чином, в період війни, коли мають місце високі ризики фізичного пошкодження місць зберігання носіїв даних та інформації, жодне підприємство не може знаходитися у безпеці і вимушене шукати альтернативні способи зберігання інформації, в тому числі облікової, з надійним рівнем її захисту, який може бути забезпечений хмарними сервісам. Безумовно такі послуги потребують значних витрат коштів і прийняття рішення щодо вибору хмарного сервісу повинно враховувати економічність такого переходу. Також необхідно розуміти, що завжди буде можливість повернутися до власної інфраструктури, тобто вийти із хмари, коли ситуація з безпекою даних стабілізується.

Список використаних джерел:

1. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека: навчальний посібник частина 2, Харків: ХНЕУ, 2008

2. Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16.07.1999 р. № 996-XIV. Дата оновлення 18.09.2018. URL: https://zakon.rada.gov.ua (дата звернення 20.11.2022).

3. Про інформацію: Закон України від 02.10.1992 No 2758-XII Дата оновлення 03.11.2022. URL: https://zakon.rada.gov.ua (дата звернення 21.11.2022).

4. Офіційний сайт продукту "Amazon Web Services" компанії Amazon. URL: https://aws.amazon.com/en/solutions/case-studies/RaiffeisenBankInternational/