ЗАХИСТ ОБЛІКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Григоревська Олена Олександрівна,
к.е.н., доцент, доцент кафедри обліку і аудиту
Київський національний університет технологій та дизайну
м. Київ, Україна
lenazelenina@ukr.net

Вступ./Introductions. Інформаційна захищеність є одним з найважливіших аспектів загальної безпеки на різних рівнях – національному, галузевому, корпоративному, персональному. Це пов'язано з тим, що в сучасному світі експонентний приріст кількості інформації перетворив її з другорядного ресурсу в чинник, який вирішальним чином впливає практично на всі сфери суспільного життя, відображаючи тим самим зростаючу інформаційну залежність суспільства.

В свою чергу, інформаційна система бухгалтерського обліку формується з конфіденційної та приватної інформації, яка може бути порушена, якщо її не захистити. Несанкціоноване використання інформації, сформованої в системі бухгалтерського обліку, може призвести до згубних наслідків, ризикуючи втратою інформації, неправильним введенням даних та зловживанням конфіденційною інформацією. Неадекватна інформаційна безпека збільшує можливість маніпулювання, фальсифікації або зміни бухгалтерських записів. Тому питання захисту інформації, сформованої в системі бухгалтерського обліку, є надзвичайно актуальними, а забезпечення її безпеки є пріоритетом у багатьох фірмах.

Мета роботи./Aim. Полягає в узагальненні існуючих підходів та окресленні перспективних напрямів до організації захисту облікової інформації в умовах забезпечення кібербезпеки.

Матеріали та методи./Materials and methods. У процесі дослідження використано методи спостереження, порівняння, аналізу, синтезу, узагальнення.

Результати та обговорення./Results and discussion. Несанкціонований або невідповідний доступ до інформаційної системи бухгалтерського обліку або нездатність встановити і підтримувати поділ обов'язків в рамках системи внутрішнього контролю може ускладнити забезпечення реєстрації, обробки та подання достовірних і точних транзакцій.

За підрахунками, інциденти з кібербезпекою загрожують деяким людям на десятки тисяч доларів. Кібератака, яка призводить до значного порушення даних, може мати згубні наслідки не тільки для операційної сторони фірми, але також матиме юридичні наслідки для директорів бізнесу, коли вищий менеджмент може зіткнутися з регуляторним розслідуванням або судовим розглядом.

Порушення даних також може спричинити значний ризик довіри та репутації, що може призвести до втрати доходу / зниження ціни акцій публічно зареєстрованих компаній

Щодо виділення ризиків загрози безпеці бухгалтерських даних, то дослідниками виділяється цьому питанню достатньо уваги. Проте цікавим є підхід до виділення груп ризиків виходячи із процесів, що включає у себе бухгалтерський облік: процесу збору, накопичення, систематизації, узагальнення облікової інформації.

Так, об'єктивно, що наявність виділених загроз продукує розробку методів їх мінімізації. На нашу думку, захист облікової-інформації та уникнення «гачка» кібератаки можливий лише у випадку дотримання комплексних заходів та спільних дій керівного персоналу, облікового персоналу, аудиторів та, як не дивно, закладів освіти при навчанні майбутніх фахівців.

На нашу думку, захист облікової-інформації та уникнення «гачка» кібератаки можливий лише у випадку дотримання комплексних заходів та спільних дій керівного персоналу, облікового персоналу, аудиторів та, як не дивно, закладів освіти при навчанні майбутніх фахівців.

Так, наприклад, керівник підприємства повинен володіти такими знаннями та компетенцією, щоб розуміти порядок документування та вміти протестувати систему внутрішнього контролю.

Бухгалтери повинні бути інформовані про загрози безпеки і відповідних методах контролю, щоб захистити свої власні інформаційні системи і консультувати підприємства щодо ризиків безпеки. Важливим є забезпечення бухгалтерів встановленими найсучаснішими антивірусними програмами. Актуальним є вміння розпізнавати шахрайство по електронній пошті, що не адресована напряму.

Важливим суб'єктом забезпечення уникнення загроз кібератак підприємства є аудитор (зовнішній, внутрішній). Аудитор повинен мати достатні знання в області ІТ, щоб довести до відома ІТ-фахівця мету аудиту, оцінити, чи будуть процедури відповідати цілям аудитора, а також оцінити результати процедур, оскільки вони пов'язані з характером, термінами і обсягом інших аудиторських процедур.

Науковці і викладачі при підготовці фахівців повинні робити акцент на розуміння ними необхідності ІТ-безпеки і важливість спільної роботи з іншими над розробкою політик, процесів і технологій для усунення загроз.

Висновки./Conclusions. Таким чином, ефективна комунікація та стратегії між керівництвом, бухгалтерами та аудиторами важливі для зменшення або захисту від виникаючих загроз інформаційній системі бухгалтерського обліку. Щоб правильно оцінити потенційні ризики, бухгалтери та аудитори повинні бути знайомі з поточними і новими технологіями. Контроль несанкціонованого доступу до бухгалтерських записів є важливим компонентом внутрішнього контролю. Політика доступу і паролів, шифрування, цифрові підписи, блокування дисків, міжмережеві екрани і цифрові сертифікати є прикладами заходів контролю, які повинні бути ідентифіковані, задокументовані, повідомлені і піддані перевірці при оцінці ефективності контролю.