DOI: https://doi.org/10.30525/978-9934-26-500-6-12

Serhii Harkusha
Candidate of Economic Sciences, Associate Professor,
Associate Professor at the Department of Accounting and Taxation
Sumy National Agrarian University

INFORMATION PROTECTION IN AUTOMATED ACCOUNTING SYSTEMS: USER ASPECT

Summary

The article addresses key challenges and prospective solutions for securing information in automated accounting systems, emphasizing the growing significance of data protection in modern enterprises. A major concern is the increasing threat of cybercrime, including ransomware attacks and insider risks, prompting organizations to adopt proactive measures like firewalls and security protocols. Another critical factor is compliance with stricter international data protection standards, requiring significant investments to safeguard databases. The research highlights the importance of multilayered security strategies that incorporate user authentication, data encryption, and role-based access control to mitigate unauthorized access risks. Innovative encryption technologies, such as full data encryption and digital signatures, ensure data confidentiality, integrity, and authenticity during storage and transmission. Additionally, the study underscores the value of developing security policies and conducting regular audits to identify vulnerabilities and enhance organizational resilience. Employee training plays a pivotal role in preventing breaches caused by human error. The proposed measures, including automated data backups and rapid recovery systems, ensure business continuity even during cyberattacks. Integrating these advanced security approaches enhances the reliability of accounting software, ensures compliance with regulatory standards, and builds trust among stakeholders.

Вступ

Бухгалтерський облік все більше переходять в цифровий простір. Впровадження цифрових технологій та автоматизованих систем значно спрощує процеси, але водночас збільшує ризики кібербезпеки, такі як витік даних, хакерські атаки та вірусні програми. Ці загрози посилюються через популярність дистанційної роботи у сфері бухгалтерії та податкового обліку, коли підприємства залучають сторонніх працівників, надаючи їм доступ до фінансових даних і своїх інформаційних систем. Забезпечення безпеки даних є ключовим аспектом в бухгалтерському обліку, оскільки воно спрямоване на захист конфіденційної інформації,

запобігання кіберзагрозам та забезпечення стабільної роботи інформаційних систем. Втрата або витік даних може призвести до серйозних наслідків для підприємства, включаючи фінансові збитки та втрату довіри з боку клієнтів, партнерів та органів державної влади.

Основними загрозами, що виникають у процесі обробки даних у бухгалтерських системах, є кіберзлочинність, зокрема хакерські атаки, шкідливе програмне забезпечення, а також внутрішні загрози, пов'язані з людським фактором. Враховуючи це, захист інформації в автоматизованих системах бухгалтерського обліку є не лише технічним завданням, але й частиною стратегії забезпечення конкурентоспроможності та відповідності міжнародним вимогам щодо захисту персональних даних і конфіденційної інформації.

У відповідь на ці виклики розвиваються перспективні напрями захисту інформації в автоматизованих системах бухгалтерського обліку, що включають різноманітні методи і технології для запобігання витоку даних та забезпечення цілісності інформаційних потоків. До таких методів відносяться шифрування даних, багаторівневий контроль доступу, використання цифрових підписів, а також інтеграція з сучасними технологіями хмарного зберігання даних.

Особливу увагу слід приділяти розробці внутрішніх політик безпеки, проведенню регулярних аудитів і навчання персоналу з питань інформаційної безпеки. Комплексний підхід, що поєднує технічні заходи, правові аспекти і освітні ініціативи, сприяє підвищенню рівня захисту бухгалтерських систем, знижуючи ймовірність несанкціонованого доступу та інцидентів безпеки.

Забезпечення інформаційної безпеки в сфері бухгалтерського обліку є складним завданням, але воно критично важливе для захисту фінансових інтересів бізнесу, що допомагає уникнути фінансових ризиків і зберегти ділову репутацію.

У світі, де дані є одним з найбільш цінних активів, кібербезпека в сфері бухгалтерського обліку має бути на першому місці. На перший погляд може здатися, що довіра до професіоналів та відповідальних співробітників повинна бути достатньою для забезпечення кібербезпеки. Однак на практиці навіть найнадійніші спеціалісти можуть помилитися, інколи навіть непередбачено або, що ще гірше, свідомо. Їхні дії можуть призвести до непередбачуваних і негативних наслідків. Тому довіра не повинна бути єдиним фактором; необхідно постійно перевіряти.

Впроваджуючи цифрові технології, бізнес отримує можливість збільшити швидкість, ефективність роботи та контроль над процесами, але водночас стає вразливим до кібератак через появу нових точок уразливості, що виникають через перехід «в цифру». Кіберризики

зростають, якщо нові інформаційні системи не контролюються належним чином.

У цьому контексті перспективні напрями розвитку і вдосконалення захисту інформації стають надзвичайно важливими для забезпечення стабільної та ефективної роботи бухгалтерських систем в умовах цифровізації та глобалізації. Впровадження передових технологій і методів захисту допоможе організаціям не лише мінімізувати ризики, але й відповідати зростаючим вимогам щодо безпеки даних у міжнародному середовищі.

Розділ 1. Законодавче забезпечення захисту інформації в сфері бухгалтерського обліку

Захист бухгалтерської інформації є одним із ключових аспектів забезпечення фінансової стабільності суб'єктів господарювання та держави в цілому. У сучасних умовах цифровізації та стрімкого розвитку інформаційних технологій питання збереження конфіденційності, достовірності та цілісності даних стають особливо актуальними. Бухгалтерська інформація, як стратегічний ресурс, перебуває під постійною загрозою через можливі кібератаки, помилки в автоматизованих системах або недотримання нормативних вимог.

Ефективне забезпечення захисту цієї інформації потребує створення надійного законодавчого підґрунтя та інституційної бази, які регулюють основні принципи та механізми її безпеки. У національному законодавстві України вже сформовано ряд положень, спрямованих на регулювання цього питання, однак їх інтеграція з міжнародними стандартами залишається важливим завданням.

Законодавче забезпечення захисту інформації в сфері бухгалтерського обліку є важливою складовою для забезпечення прозорості, достовірності та безпеки фінансової звітності підприємств. Системи бухгалтерського обліку обробляють величезну кількість чутливої інформації, що включає дані про доходи, витрати, податкові зобов'язання, а також інформацію про фінансові операції. Враховуючи, що ці дані можуть стати об'єктом несанкціонованого доступу або фальсифікацій, захист бухгалтерської інформації має законодавчі та організаційні засади.

Законодавче забезпечення захисту інформації в бухгалтерському обліку полягає в створенні нормативно-правової бази, що регламентує порядок обробки, зберігання та захисту фінансової інформації. Крім того, захист бухгалтерської інформації забезпечується через відповідність її зберігання вимогам щодо конфіденційності та цілісності даних. Законодавство встановлює правила щодо доступу до інформації, що стосується фінансової діяльності організацій. Ці норми вимагають, щоб доступ до облікових даних мали лише уповноважені особи, що є

гарантією запобігання несанкціонованому доступу або змінам в інформації, які можуть вплинути на фінансову звітність.

Особливу увагу законодавство приділяє питанням кібербезпеки та захисту від зовнішніх загроз, оскільки більшість бухгалтерської інформації зберігається в електронному вигляді, на підприємства покладається обов'язок забезпечувати захист від кібератак, які можуть призвести до викрадення або пошкодження фінансових даних, що вимагає впровадження сучасних технологій шифрування та систем виявлення вторгнень.

Крім безпосередньо інформаційної безпеки, законодавство встановлює вимоги щодо зберігання фінансових даних. В Україні існують чітко визначені строки зберігання бухгалтерських документів, що містять важливу інформацію для контролюючих органів, що дає змогу здійснювати належний контроль за правильністю ведення обліку та забезпечує захист даних від несанкціонованого видалення або втрати.

Система контролю також включає в себе обов'язкові процедури щодо аудитів фінансової звітності, де важливим елементом є перевірка наявності належних засобів захисту інформації, що дозволяє виявити недоліки в існуючих системах обліку та своєчасно вжити заходів для усунення потенційних загроз.

Серед основних нормативних актів є Стратегія кібербезпеки України [14]. Національний кіберпростір України стикається зі значними викликами, серед яких швидкий розвиток інформаційно-комунікаційних технологій, мілітаризація кіберпростору, зростання кіберзлочинності та гібридна агресія з боку держав-агресорів. Особливу загрозу становлять кібератаки, спрямовані на критичну інфраструктуру, що мають руйнівні наслідки. Проблеми посилюються відсутністю належного законодавчого врегулювання, недостатньою підготовкою фахівців, низьким рівнем цифрової грамотності громадян та фінансовою обмеженістю заходів із кіберзахисту. Умови цифровізації вимагають комплексного підходу до створення стійкої та захищеної інформаційної інфраструктури.

Україна прагне побудувати ефективну систему кібербезпеки, спираючись на принципи стримування, кіберстійкості та взаємодії. Пріоритетними завданнями є адаптація до нових загроз, посилення міжнародного співробітництва, вдосконалення законодавчої бази та стимулювання державно-приватного партнерства. Важливим є впровадження сучасних підходів до управління кібербезпекою, підвищення обізнаності населення щодо кіберзагроз, розвиток інфраструктури для запобігання та нейтралізації кібератак. Ключову роль у цьому відіграє Національний координаційний центр кібербезпеки, який забезпечуватиме ефективну координацію зусиль усіх зацікавлених сторін [14].

Важливим у формуванні інформаційної безпеки бухгалтерського обліку є Закон України «Про інформацію» [12]. Закон визначає основні терміни, принципи та засади інформаційних відносин, зокрема права і обов'язки суб'єктів у сфері інформації. До ключових понять належать документ, інформація, захист інформації та суб'єкти владних повноважень. Основними принципами є забезпечення права на інформацію, відкритість, доступність, достовірність, свобода обміну інформацією та захист особистого життя. Державна інформаційна політика спрямована на доступність інформації, розвиток інформаційного суспільства та безпеку даних.

Суб'єктами інформаційних відносин є фізичні та юридичні особи, об'єднання громадян і владні органи, а об'єктом – інформація. Закон гарантує право на інформацію, його реалізацію через механізми доступу, зокрема до державних ресурсів, і встановлює обмеження у випадках, передбачених законом. Захист інформації охороняється державою, яка забезпечує рівність доступу до неї, а також регулює основні види діяльності: створення, зберігання, поширення, охорону та захист інформації [12].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [10] визначає засади захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, регулюючи відносини між володільцями інформації, власниками систем, користувачами, а також уповноваженими органами. Встановлюються терміни, такі як «захист інформації», «доступ до інформації», «блокування», «криптографічний та технічний захист», а також особливості комплексної системи захисту інформації. Закон передбачає порядок доступу до інформації, її обробки та умови створення резервних копій державних інформаційних ресурсів.

Суб'єктами правовідносин є власники систем, володільці інформації та користувачі, права й обов'язки яких визначаються законодавством або договорами. Порядок доступу до інформації встановлюється володільцем, але щодо державних інформаційних ресурсів діють окремі норми законодавства. Власник системи забезпечує захист інформації та, за необхідності, інформує володільця про загрози або несанкціоновані дії. Окремо розглядаються відносини між різними власниками систем у разі обробки інформації з інших систем [10].

Обробка інформації з обмеженим доступом передбачає використання сертифікованих технічних і криптографічних засобів та дотримання вимог інформаційної безпеки. Закон деталізує процедури державної експертизи та підтвердження відповідності систем захисту, особливо для державних інформаційних ресурсів. Додатково визначено умови обробки

інформації без комплексного захисту за наявності сертифікованих засобів безпеки та відповідності системи управління інформаційною безпекою [10].

Закон України «Про захист персональних даних» [11] регулює правові відносини, пов'язані із захистом і обробкою персональних даних, спрямований на забезпечення основоположних прав і свобод людини, включаючи право на недоторканність приватного життя. Він охоплює обробку персональних даних як із застосуванням автоматизованих засобів, так і в картотеках чи неавтоматизованих системах. Закон визначає ключові терміни, зокрема «база персональних даних», «володілець», «розпорядник», «згода суб'єкта», «знеособлення», а також обґрунтовує принципи обробки і використання даних.

Суб'єктами відносин є фізичні особи, володільці, розпорядники та треті особи, а також Уповноважений Верховної Ради з прав людини. Об'єктами захисту виступають персональні дані, що можуть бути конфіденційною інформацією. Закон встановлює винятки щодо обмеження доступу до інформації про державних службовців, бюджетні кошти чи боргові зобов'язання фізичних осіб, регламентуючи їх відкритість відповідно до чинного законодавства [11].

У Законі України «Про електронну комерцію» [9] зазначається, що захист персональних даних у сфері електронної комерції забезпечується шляхом створення суб'єктами електронної комерції умов для їх безпеки. Учасники таких відносин зобов'язані дотримуватися норм законодавства, запобігаючи несанкціонованому використанню даних, отриманих під час електронних правочинів. Використання персональних даних допускається виключно для цілей, пов'язаних із правочинами, якщо інше не передбачено законом або домовленістю сторін.

Реєстрація фізичних осіб у системах електронної комерції передбачає їхню згоду на обробку даних, а ідентифікація користувачів здійснюється через електронний підпис. Для посилення захисту облікових записів можуть застосовуватися додаткові унікальні дані, створені під час реєстрації, що запобігає несанкціонованому доступу до інформаційних систем [9].

У свою чергу, в Законі України «Про електронні документи та електронний документообіг» [8] вказується на цілісність електронного документа перевіряється шляхом підтвердження електронного підпису чи печатки, зокрема удосконалених або кваліфікованих, або за допомогою інших методів захисту інформації, відповідно до вимог законодавства. Це забезпечує достовірність та безпеку електронних документів у процесі їх використання.

Обіг електронних документів з конфіденційною інформацією регулюється суб'єктами електронного документообігу на договірній основі, вони встановлюють режими доступу та засоби захисту.

У системах, що забезпечують обмін такими документами, повинно дотримуватися законодавства щодо захисту державних інформаційних ресурсів та інформації з обмеженим доступом [8].

Закон України «Про платіжні послуги» [13] вказує, що надавачі платіжних послуг зобов'язані забезпечувати надійний захист інформації, що обробляється під час виконання платіжних операцій, зберігання та передачі даних. Для цього застосовуються системи захисту інформації, що гарантують цілісність, конфіденційність, доступність і простежуваність даних відповідно до вимог Національного банку України. У разі виявлення порушень законодавства щодо захисту інформації, зокрема із ознаками злочину, відповідні органи мають бути негайно повідомлені. Працівники надавачів послуг зобов'язані дотримуватись конфіденційності, зберігати таємницю користувачів і надавачів послуг, а також забезпечувати безпеку засобів захисту.

Автентифікація користувачів є обов'язковою умовою електронної взаємодії та виконання платіжних операцій. Надавачі платіжних послуг застосовують посилену автентифікацію для забезпечення безпеки дистанційного доступу, ініціювання операцій і запобігання шахрайству. Для цього використовуються незалежні елементи автентифікації, що унеможливлюють компрометацію системи. Обробка персональних даних користувачів здійснюється лише за їхньою згодою, крім випадків, передбачених законодавством, наприклад, під час фінансового моніторингу. Інформація про діяльність користувачів є конфіденційною і охороняється як комерційна таємниця [13].

Положення про документальне забезпечення записів у бухгалтерському обліку [6] вказує, що зберігання первинних документів, регістрів бухгалтерського обліку та іншої звітності є важливим обов'язком, який регламентується нормативно-правовими актами. Документи, які пройшли обробку, передаються до архіву після зберігання в спеціально обладнаних приміщеннях або зачинених шафах під відповідальністю уповноважених осіб. Особлива увага приділяється зберіганню бланків суворої звітності в сейфах або металевих шафах, а також електронним документам, які повинні бути захищені від пошкоджень і зберігатися у формі, що забезпечує їх перевірку.

Перед передачею до архіву документи поточного місяця комплектуються, нумеруються та переплітаються. Визначення строків зберігання в архіві здійснюється відповідно до чинного законодавства. Головний бухгалтер несе відповідальність за оформлення, зберігання та передачу документів до архіву. Доступ до документів з архіву можливий лише за рішенням головного бухгалтера, а вилучення документів регламентується законодавчими нормами [6].

У разі втрати або знищення документів керівник підприємства зобов'язаний повідомити правоохоронні органи та створити комісію для розслідування обставин інциденту. Результати роботи комісії документуються актом, який направляється до відповідних органів. Такі дії спрямовані на забезпечення цілісності та достовірності бухгалтерської звітності та документів [6].

Технічний захист інформації в Україні регулюється Положенням про технічний захист інформації в Україні [7] та спрямований на охорону конфіденційності, цілісності та доступності даних, важливих для держави, суспільства і особи. Положення визначає правові та організаційні засади ТЗІ, яке здійснюється у державних органах, військових формуваннях, підприємствах, установах та організаціях. Основу правового регулювання становлять Конституція України, закони, нормативно-правові акти Служби безпеки та Держспецзв'язку, а також міжнародні договори, що затверджені Верховною Радою України. Організація та контроль у цій сфері покладаються на керівників відповідних установ і здійснюються за допомогою визначених нормативно-правових механізмів.

Захист бухгалтерської інформації є надзвичайно важливим аспектом для забезпечення фінансової стабільності як на рівні окремих підприємств, так і держави в цілому. В умовах швидкого розвитку інформаційних технологій та цифровізації економіки, ефективний захист бухгалтерської інформації набуває все більшої актуальності. Українське законодавство вже має кілька важливих нормативно-правових актів, які забезпечують безпеку цієї інформації, проте є потреба в їх подальшому вдосконаленні та адаптації до сучасних вимог кібербезпеки.

Законодавче забезпечення захисту бухгалтерської інформації в Україні включає низку ключових законів і стратегій, серед яких Стратегія кібербезпеки України, Закон України «Про інформацію», «Про захист персональних даних», а також спеціалізовані нормативні акти, які регулюють захист інформації в інформаційно-телекомунікаційних системах. Однак існує необхідність у більш активному впровадженні міжнародних стандартів у вітчизняну практику та координації зусиль на рівні державних органів, приватного сектору та міжнародних інституцій.

Законодавчі ініціативи, такі як Стратегія кібербезпеки України, зосереджуються на розвитку стійкої інформаційної інфраструктури, підвищенні цифрової грамотності громадян, а також на інтеграції нових технологій для захисту бухгалтерської інформації. Важливим є удосконалення нормативної бази для протидії кіберзагрозам, а також забезпечення належного рівня технічного захисту даних, зокрема через використання сертифікованих криптографічних засобів та систем резервного зберігання даних.

У сфері бухгалтерського обліку важливо звернути увагу на зміцнення захисту електронних документів і платіжних операцій. Законодавчі акти, що регулюють обіг електронних документів та платіжних послуг, повинні забезпечувати безпечний обмін інформацією та мінімізувати ризики шахрайства. Водночас, забезпечення належного захисту бухгалтерських документів потребує вдосконалення процедур їх зберігання та обробки, а також удосконалення правил щодо доступу до архівних матеріалів.

Загалом, для створення стійкої системи захисту бухгалтерської інформації в Україні необхідно посилити законодавчу та інституційну підтримку, впроваджувати новітні технології захисту та посилювати міжнародну співпрацю, що дозволить знизити ризики, пов'язані з втручанням у фінансові дані, та забезпечити стабільність і надійність національної економіки в умовах цифровізації.

Розділ 2. Організація захисту інформації в автоматизованих системах бухгалтерського обліку

У сучасному світі автоматизація бухгалтерського обліку стала невід'ємною частиною діяльності багатьох підприємств і організацій. Впровадження автоматизованих систем бухгалтерського обліку дозволяє значно підвищити ефективність роботи облікових підрозділів, забезпечити швидку обробку великих обсягів інформації та знизити кількість помилок, що виникають при виконанні облікових операцій вручну. Однак, разом з цими перевагами з'являються і нові загрози, пов'язані з безпекою інформації, що обробляється в таких системах.

Однією з основних проблем, з якою стикаються організації, є забезпечення надійного захисту облікової інформації, враховуючи, що автоматизовані системи бухгалтерського обліку містять чутливі дані, такі як фінансові звіти, розрахунки з контрагентами, зарплати працівників, а також інші конфіденційні відомості, безпека цих даних має бути пріоритетом для кожного підприємства.

Протягом останніх півстоліття людство зробило значні зусилля для дослідження поняття «ризик», його видів та методів управління ними, особливо в контексті підприємницької діяльності суб'єктів господарювання [2, с. 111].

Несанкціонований доступ до таких даних може призвести не тільки до фінансових втрат, але й до серйозних правових наслідків, включаючи штрафи, санкції, а також втрату репутації.

Криза в діяльності підприємства не є випадковим процесом, якщо її не викликано форс-мажорними обставинами чи природними катастрофами, такими як повені, пожежі, урагани, війни, вибухи, епідемії та пандемії тощо. Навпаки, криза є наслідком, на який можуть впливати суб'єкти господарювання. Крім того, завдяки постійному моніторингу та

контролю менеджери здатні прогнозувати появу кризи в діяльності організації. Прогнозування банкрутства або виникнення кризових ситуацій у розвитку підприємства, що можуть призвести до банкрутства, має на меті завчасно знизити ймовірність виникнення негативних наслідків, які можуть призвести до повної втрати фінансової платоспроможності підприємства [4, с. 175].

Організація захисту інформації в автоматизованих системах бухгалтерського обліку повинна враховувати різноманітні аспекти безпеки: від захисту від несанкціонованого доступу до фізичних серверів і баз даних до контролю за внутрішнім доступом до системи. Важливим є також захист інформації від можливих помилок або навмисного пошкодження даних, що можуть бути результатом некоректного використання системи або навіть зловмисних дій з боку внутрішніх користувачів.

Один із ключових елементів захисту інформації – це розробка та впровадження ефективних механізмів контролю доступу. Для цього використовуються різноманітні методи автентифікації та авторизації користувачів, що дозволяють визначити, хто має доступ до конкретних даних та операцій в системі. Використання надійних паролів, біометричних даних, а також двофакторної аутентифікації значно знижує ймовірність несанкціонованого доступу до інформації.

Важливим аспектом захисту є також шифрування даних. Воно дозволяє перетворити дані у такий вигляд, що їх неможливо буде прочитати без відповідного ключа. Це особливо важливо при передачі чутливих даних через відкриті канали зв'язку, де існує ризик перехоплення інформації зловмисниками. Шифрування даних на всіх етапах їх обробки – від введення в систему до зберігання і передачі – є основою для забезпечення їх конфіденційності та захисту від несанкціонованого доступу.

Особливу увагу слід приділяти також захисту від помилок користувачів і програмних збоїв, хоча автоматизовані системи значно знижують ймовірність помилок, що виникають внаслідок людського фактору, деякі операції все ж можуть бути виконані некоректно. Щоб мінімізувати такі ризики важливо забезпечити наявність системи моніторингу та логування всіх операцій в системі, що дозволяє вчасно виявляти помилки та проводити їх виправлення. Крім того, створення ефективної системи резервного копіювання дозволяє відновити інформацію у разі її пошкодження або втрати.

Захист від зловмисних дій також є невід'ємною частиною безпеки автоматизованих систем бухгалтерського обліку. Встановлення антивірусного та антишпигунського програмного забезпечення, а також постійне оновлення системи безпеки дозволяють знизити ризики, пов'язані з проникненням зловмисників у систему. Крім того, важливо

обмежити доступ до системи лише для уповноважених осіб і забезпечити належну політику безпеки для користувачів, яка включає регулярну зміну паролів, контроль за використанням привілеїв користувачів, а також інші методи захисту.

Організація захисту інформації в автоматизованих системах бухгалтерського обліку є багатогранним процесом, що включає в себе не лише технічні заходи, але й організаційні аспекти, такі як навчання персоналу, визначення політики доступу та проведення регулярних перевірок. Важливість цієї проблеми важко переоцінити, оскільки від надійного захисту облікових даних залежить не лише ефективність облікових процесів, а й фінансова стабільність і репутація організації в цілому.

Програмне забезпечення «BAS Бухгалтерія» є ефективним інструментом для виконання всіх обов'язків бухгалтерії підприємства, зокрема щодо обліку, виписки первинних документів, продажів та інших аспектів. Воно підходить для повної автоматизації бухгалтерського та податкового обліку, однак для автоматизації інших підрозділів, таких як відділ продажів, можуть використовуватись окремі спеціалізовані системи або рішення [15].

Для забезпечення надійності роботи з BAS важливо уникати пошкоджень бази даних, оскільки її відновлення може бути неможливим. Для цього слід забезпечити стабільну роботу локальної мережі, використовувати джерела безперебійного живлення, подбати про достатню оперативну пам'ять і дисковий простір комп'ютера, регулярно створювати резервні копії та зберігати їх на окремих носіях. Рекомендується обмежити доступ користувачів через «товстий клієнт», віддаючи перевагу «тонкому клієнту» через веб-сервер, а згодом перейти на клієнт-серверний режим, який мінімізує ризики пошкодження та підвищує швидкість роботи. Також важливо захищати базу даних від вірусів, перевіряти всі отримані обробки для BAS і консультуватися з фахівцями.

У разі появи помилки про пошкодження бази даних, насамперед потрібно спробувати відновити її з резервної копії, а відсутню інформацію внести вручну за період між створенням копії та виникненням пошкодження. Метод відновлення залежить від конфігурації BAS і характеру пошкодження. Для відновлення користуються функцією «Завантажити інформаційну базу» через меню «Адміністрування» в Конфігураторі. Якщо резервної копії немає або вона застаріла, доцільно звернутися до фахівців BAS, які зможуть діагностувати проблему та виправити помилки. Самостійні спроби ремонту можуть погіршити ситуацію і зробити відновлення неможливим.

Комплекс ISpro побудований за модульною архітектурою, що включає системи та модулі. Кожна система автоматизує облік певного напряму діяльності підприємства і може використовуватися як окремо, так і у складі комплексу. Основні модулі адміністрування та загальні довідники є обов'язковими для роботи Комплексу, незалежно від його конфігурації. Набір систем і модулів залежить від специфіки підприємства та його потреб, наприклад, для обліку лише заробітної плати можуть бути відсутні модулі Логістики чи Основних засобів. Обов'язкові модулі забезпечують базову функціональність і входять до мінімальної поставки, тоді як додаткові модулі виконують сервісні функції або розширюють можливості для реалізації бізнес-процесів [3].

Для захисту Комплексу ISpro без електронного ключа використовується код конфігурації, сформований на основі комбінації даних картки підприємства: назва, ЄДРПОУ (ОКПО), адреса, поштовий індекс, а також ПІБ та ідентифікаційні номери керівника і керівника фінансової служби. Код конфігурації створюється індивідуально для кожної унікальної комбінації цих даних.

Безключовий захист застосовується лише за умови, що підприємства в Комплексі мають ідентичні ключові дані (наприклад, для роботи з різними базами одного підприємства) та не використовуються кілька серверних інсталяцій з одним ключем. Для активації робочого режиму необхідно підключити файл безключового захисту.

Електронний ключ для програми ISpro – це компактний пристрій, який підключається до USB- або паралельного порту комп'ютера без потреби в електроживленні. Він має унікальний номер ліцензії, вказаний на наклейці, та підключається до комп'ютера із встановленим Сервером застосунків для захисту Комплексу. USB-ключ можна підключати або відключати без вимкнення комп'ютера. Для роботи Комплексу в різних операційних системах необхідно встановити драйвер ключа, що виконується один раз під час початкового налаштування. Драйвери надаються разом із дистрибутивом у каталозі PROTECT серверної частини та мають бути обрані відповідно до типу ключа. Файл конфігурації та електронний ключ створюються для кожного номера ліцензії окремо, і їх не можна використовувати з іншими ключами. У разі відсутності ключа чи файлу конфігурації Комплекс працює в демонстраційному режимі.

Проблеми із захистом ISpro часто зводяться до ситуації, коли ключ і код конфігурації встановлені, але система працює в демонстраційному режимі. Для діагностики необхідно перевірити модуль Адміністратор сервера застосунків, звернувши увагу на поле «Стан». Можливі причини: закінчення терміну дії ліцензії, невідповідність номера ключа і файлу конфігурації, помилка ключа чи драйвера. Для усунення проблем слід

перевірити з'єднання ключа, перевстановити драйвер (використовуючи актуальну версію з дистрибутиву або сайту розробника), протестувати ключ утилітами, що йдуть у комплекті. Якщо ключ не працює навіть після перевірок, варто випробувати його на іншому комп'ютері чи звернутися до постачальника для заміни. У випадку централізованого обліку необхідно, щоб параметр централізованого обліку та кількість структурних одиниць відповідали ліцензії, а реквізити основної СО збігалися з Карткою підприємства. За порушення цих умов система переходить у демо-режим, і потрібна корекція ліцензії.

Програма «M.E.Doc IS» забезпечує високий рівень захисту інформації, гарантуючи конфіденційність та юридичну значущість електронних документів. Для цього використовується засіб криптографічного захисту «Надійний засіб електронного цифрового підпису», що відповідає вимогам українського законодавства. Документи підписуються за допомогою ЕЦП, що підтверджує їх цілісність і авторство, а шифрування забезпечується за допомогою затверджених державних алгоритмів. Захищений обмін інформацією між користувачами та державними органами здійснюється за допомогою спеціальних транспортних контейнерів, що відповідають державним вимогам [5].

Сервер електронного документообігу «M.E.Doc IS» сприяє прискоренню процесу обміну документами між користувачами програми, забезпечуючи високий рівень безпеки. СДО дозволяє аутентифікувати контрагентів за унікальним поєднанням ЄДРПОУ та коду філії, а доступ до документів можливий лише через чинний сертифікат ЕЦП. Пряме з'єднання через HTTP є пріоритетним, що знижує ризики втрати або перехоплення документів під час передачі. Усі документи шифруються і можуть бути розшифровані тільки одержувачем, гарантуючи повну конфіденційність.

SaaS (Software as a Service) – це інноваційна модель в сфері хмарних технологій, яка дозволяє користувачам доступати до програмного забезпечення через Інтернет без необхідності його встановлення чи обслуговування на власних пристроях. Замість покупки ліцензій користувачі підписуються на регулярний сервіс, що забезпечує доступ до хмарних додатків. Плата за використання часто залежить від обсягу споживаних послуг або кількості користувачів [1].

Основною перевагою SaaS є можливість швидкої адаптації до змін на ринку, оскільки підприємства можуть уникнути великих капіталовкладень в програмне забезпечення та інфраструктуру. Завдяки централізованому оновленню, всі користувачі отримують актуальні версії програм і виправлення безпеки без додаткових зусиль.

Ще однією ключовою рисою є масштабованість. Бізнес може коригувати кількість користувачів або послуг залежно від своїх потреб,

що є зручним рішенням для організацій з непередбачуваними навантаженнями або сезонними змінами. SaaS технології користуються великою популярністю серед малого та середнього бізнесу завдяки своїй доступності та гнучкості.

Ведення обліку в онлайн-системі Облік SaaS є безпечним завдяки кільком важливим аспектам. По-перше, дані зберігаються в захищених дата-центрах Європейського Союзу, де вони розподілені на кількох серверах, що унеможливлює фізичний доступ до них. Система забезпечує захист за допомогою двофакторної автентифікації, що обмежує доступ лише авторизованим користувачам. Крім того, розробники сервісу не мають доступу до облікових даних клієнтів, що додає додатковий рівень безпеки.

По-друге, при віддаленій роботі через веб-інтерфейс Облік SaaS використовує HTTPS-протокол для шифрування даних, що забезпечує захист від атак і перехоплення інформації. Усі дані передаються в зашифрованому вигляді, що гарантує їхню безпеку під час обміну.

По-третє, система дозволяє точно налаштовувати доступ до даних за ролями, обмежуючи доступ до документів і звітів залежно від посади співробітника. Це дає змогу контролювати доступ до конфіденційної інформації, зокрема комерційної таємниці. Крім того, система підтримує можливість налаштування обмежень доступу за IP-адресами на рівні корпоративної мережі.

Таким чином, Облік SaaS забезпечує надійний захист даних і зручність для користувачів, дозволяючи вести облік в умовах високого рівня безпеки.

Виходячи з наведеної інформації систематизуємо переваги і недоліки щодо захисту інформації в програмних комплексах (табл. 1).

Програмні продукти бухгалтерського обліку, представлені в таблиці, мають різноманітні переваги та недоліки в контексті захисту інформації. Кожна система забезпечує високий рівень захисту через різні механізми, такі як резервне копіювання, електронні підписи, шифрування даних та двофакторну автентифікацію. Наприклад, BAS Бухгалтерія і M.E.Doc IS забезпечують надійний захист даних завдяки резервному копіюванню і цифровим підписам, тоді як ISpro і Облік SaaS пропонують додаткові рівні безпеки, такі як використання електронних ключів та захищених дата-центрів. Однак, кожна система має свої недоліки, пов’язані з необхідністю регулярного оновлення, налаштування доступу та залежністю від зовнішніх факторів, таких як стабільність мережі чи інтернет-з’єднання.

Таблиця 1

Порівняння переваг та недоліків захисту інформації в програмних продуктах бухгалтерського обліку

Програмне забезпечення	Переваги	Недоліки
BAS Бухгалтерія	1. Повна автоматизація бухгалтерського та податкового обліку. 2. Надійний захист через резервне копіювання. 3. Можливість використання «тонкого клієнта» для підвищення безпеки. 4. Відновлення даних з резервної копії.	1. Ризик втрати даних при пошкодженні бази даних, якщо немає актуальної резервної копії. 2. Залежність від стабільної роботи локальної мережі та наявності безперебійного живлення. 3. Необхідність обмеження доступу через «товстий клієнт».
ISpro	1. Модульна архітектура, що дозволяє адаптувати систему під потреби підприємства. 2. Код конфігурації для захисту доступу. 3. Можливість використання електронного ключа для додаткового захисту.	1. Проблеми із захистом через неправильне налаштування ключа чи ліцензії можуть призвести до переходу в демонстраційний режим. 2. Необхідність постійного перевіряння драйверів та актуальності ліцензії. 3. Висока вартість ліцензій та ключів.
M.E.Doc IS	1. Високий рівень захисту завдяки ЕЦП та криптографічному шифруванню. 2. Конфіденційність документів за допомогою шифрування та цифрових підписів. 3. Використання транспортних контейнерів для обміну з державними органами.	1. Залежність від коректного використання сертифікатів ЕЦП. 2. Можлива складність в налаштуванні для деяких користувачів.
Облік SaaS	1. Захист даних у захищених дата-центрах ЄС. 2. Використання двофакторної автентифікації. 3. Шифрування даних через HTTPS-протокол. 4. Гнучке налаштування доступу до даних.	1. Залежність від сторонніх провайдерів хмарних послуг. 2. Можливі ризики при збої інтернет-з'єднання або недоступності сервісу. 3. Потреба в налаштуванні доступу та ролей для запобігання витоку даних.

Джерело: узагальнено автором на основі [1; 3; 5; 15]

Загалом, вибір програмного забезпечення для бухгалтерії має ґрунтуватися на специфічних потребах підприємства та вимогах до захисту даних. Проблеми, що виникають через неправильне налаштування або відмову обладнання, можуть суттєво вплинути на функціонування системи, тому важливо вибирати програмне забезпечення, яке забезпечує не тільки високу безпеку, але й зручність використання для кінцевих користувачів. Кожен продукт має свої сильні та слабкі сторони, тому необхідно ретельно зважити переваги і ризики перед його впровадженням.

У сучасних умовах цифровізації автоматизація бухгалтерського обліку є важливим елементом, що значно підвищує ефективність роботи підприємств та організацій. Впровадження автоматизованих систем бухгалтерського обліку дозволяє обробляти великі обсяги інформації, знижувати кількість помилок та забезпечувати високу оперативність в облікових процесах. Однак разом із цими перевагами виникають нові загрози для безпеки інформації, які потребують комплексного підходу до захисту даних.

Захист інформації в автоматизованих системах бухгалтерського обліку є багатогранним і включає як технічні, так і організаційні заходи. З одного боку, важливим аспектом є забезпечення захисту від несанкціонованого доступу, використовуючи методи автентифікації та авторизації, шифрування даних, а також ефективне управління доступом до інформації. З іншого боку, потрібно враховувати ризики, пов’язані з внутрішніми загрозами, помилками користувачів і технічними збоями.

У цьому контексті застосування різноманітних методів, таких як двофакторна аутентифікація, антивірусне програмне забезпечення, регулярне оновлення систем безпеки та моніторинг всіх операцій в системі є важливими для забезпечення належного захисту даних. Резервне копіювання та наявність інструментів для відновлення інформації у разі її пошкодження також є невід’ємною частиною надійного захисту.

Зокрема, програмні продукти, такі як BAS, ISpro та SaaS, надають можливості для забезпечення безпеки облікових даних, застосовуючи різні методи шифрування, захисту доступу та резервного зберігання даних. Програми забезпечують високу ступінь конфіденційності, підтримуючи електронний цифровий підпис, що гарантує цілісність і юридичну значущість документів, а також захищають від зовнішніх загроз. Водночас використання хмарних рішень, таких як SaaS, надає підприємствам гнучкість, знижуючи витрати на інфраструктуру, а також дозволяє оперативно оновлювати програмне забезпечення, підтримуючи його відповідність вимогам безпеки.

Також важливим елементом є навчання користувачів і розробка внутрішніх політик безпеки, що дозволяють не тільки знижувати ризики несанкціонованого доступу, але й створювати культуру безпеки серед працівників. Проведення регулярних перевірок систем безпеки та аудитів є необхідними для підтримки високого рівня захисту даних у сучасних умовах.

Отже, організація захисту інформації в автоматизованих системах бухгалтерського обліку є складним і багатогранним процесом, що вимагає постійної уваги до нових загроз і викликів. Однак забезпечення надійної безпеки облікових даних є необхідною умовою для стабільної та ефективної роботи підприємства, що не лише знижує ризики втрат та санкцій, а й сприяє збереженню репутації організації на ринку.

Розділ 3. Перспективні напрями захисту інформації в автоматизованих системах бухгалтерського обліку

Сучасні підприємства та державні установи не можуть функціонувати без використання інформаційних баз, які включають дані про клієнтів, нормативні акти, продукти та фінансову звітність. Такі бази часто містять персональну, корпоративну та конфіденційну інформацію, викрадення якої може призвести до серйозних фінансових втрат і репутаційних збитків.

Зростання витрат на захист баз даних зумовлене двома основними факторами.

Перший – це загроза кіберзлочинності. Зловмисники постійно вдосконалюють свої інструменти, створюють нові програми-вимагачі та застосовують безфайлові методи атак. Ризик виникає також через можливі дії співробітників, які можуть ненавмисно порушити конфіденційність інформації. Щоб протидіяти цим загрозам, підприємства впроваджують превентивні заходи, такі як налаштування брандмауерів для фільтрації трафіку, і створюють процедури реагування на випадки порушень безпеки.

Другий фактор – дотримання нормативних вимог. Міжнародні стандарти захисту персональних даних стають дедалі суворішими, і відповідальність за конфіденційність покладається на організації, які збирають і обробляють такі дані. Для збереження конкурентоспроможності підприємства повинні відповідати цим стандартам, незалежно від галузі та типу інформаційних активів, що вимагає значних інвестицій у забезпечення безпеки баз даних.

Безпека даних є ключовим елементом загальної стратегії захисту інформації, вона охоплює методи виявлення та аналізу загроз, а також мінімізації ризиків, спрямованих на захист конфіденційної інформації в

комп'ютерних системах і мережах. Важливо розрізняти поняття захисту даних і безпеки баз даних, адже вони мають різні аспекти [3].

Захист даних включає активні дії та використання інструментів, які гарантують збереження інформації, запобігаючи її несанкціонованому доступу, модифікаціям, випадковому розкриттю або знищенню. Цей процес досягається через застосування програмного забезпечення, технологій та процедур, які формують цілісну систему захисту.

Безпека баз даних здебільшого базується на пасивних заходах, які спрямовані на реалізацію політики конфіденційності. Вони регламентують управління конфіденційними масивами даних, зокрема інформацією про клієнтів, кредитні картки, медичні записи тощо.

Ефективний захист баз даних вимагає багаторівневого підходу, що означає впровадження системи заходів, яка ускладнює несанкціонований доступ до інформації. Початковий рівень безпеки передбачає контроль доступу на основі розподілу привілеїв і прав. Важливим є не лише запобігання зовнішнім загрозам, але й внутрішнім, оскільки співробітники можуть отримати несанкціонований доступ до даних навмисно або через необережність.

Початковий рівень захисту забезпечується шляхом обмеження доступу через перевірку повноважень користувачів і застосування атрибутів та ролей, зменшення адміністративних привілеїв і контроль взаємодії додатків із базами даних. Таким чином, комплексний підхід дозволяє мінімізувати ризики і гарантувати безпеку інформації.

Основою забезпечення безпеки є – конфіденційність, цілісність та доступність.

Конфіденційність передбачає дотримання принципу мінімальних привілеїв, що означає запобігання несанкціонованому доступу до чутливої інформації.

Цілісність гарантує захист даних від несанкціонованих змін або видалення. Одним із способів забезпечення цілісності є використання цифрових підписів для перевірки автентичності та безпечних транзакцій.

Доступність є критично важливим аспектом, що вимагає від систем і програмного забезпечення належної роботи для забезпечення доступу до необхідних послуг і даних. Прикладом може бути те, що при недоступності фінансової бази даних бухгалтерія не зможе своєчасно обробляти фінансові операції, що може порушити важливі бізнес-процеси.

У сучасних умовах цифровізації організації інформаційної безпеки в автоматизованих системах бухгалтерського обліку є пріоритетним завданням, оскільки такі системи обробляють значні обсяги конфіденційної інформації. Розглянемо ключові перспективні напрями, які сприяють підвищенню рівня безпеки (табл. 2).

Таблиця 2

Впровадження заходів безпеки для бухгалтерського програмного забезпечення

Напрямок	Заходи	Мета
Впровадження багаторівневого захисту доступу	- автентифікація користувачів (біометричні дані, двофакторна автентифікація, смарт-карти або токени); - гранульована авторизація (доступ до даних лише для виконання конкретних завдань); - регулярне оновлення паролів	Забезпечення контрольованого доступу до даних і мінімізація ризиків несанкціонованого доступу.
Використання сучасних технологій шифрування	- повне шифрування даних (захист при зберіганні, обробці та передачі); - цифровий підпис і сертифікація	Забезпечення конфіденційності, цілісності даних і підтвердження авторства документів.
Розробка політик безпеки і внутрішнього аудиту	- моніторинг і логування дій користувачів; - регулярні аудити безпеки; - навчання персоналу	Виявлення і запобігання інцидентам безпеки, підвищення обізнаності персоналу щодо захисту інформації.
Резервування і відновлення даних	- автоматичне резервне копіювання баз даних; - системи швидкого відновлення після збоїв або атак	Гарантування збереження інформації та відновлення доступу в найкоротші терміни.
Використання антивірусних систем та антишпигунського програмного забезпечення	- постійне оновлення баз сигнатур; - сканування отриманих файлів і програм	Захист від шкідливого програмного забезпечення і новітніх загроз.
Захист інфраструктури систем	- розподілена архітектура для зменшення залежності від одного сервера; - джерела безперебійного живлення; - стабільна мережа з захистом від атак DDoS	Забезпечення стійкості системи до збоїв і атак.
Інтеграція із хмарними технологіями	- модель SaaS з сертифікацією безпеки; - розмежування даних між користувачами	Забезпечення доступності та захисту даних через сучасні хмарні технології.
Розробка кастомізованих рішень	- врахування специфіки підприємства; - модульна архітектура для адаптації без зупинки процесів	Надання індивідуальних рішень для конкретних потреб компанії.

Джерело: узагальнено автором на основі [1; 3; 5; 15]

В умовах цифровізації бухгалтерський облік вимагає особливої уваги до питань захисту інформації. Одним із найбільш ефективних підходів до забезпечення конфіденційності та цілісності даних є впровадження багаторівневого захисту доступу до бухгалтерського програмного забезпечення.

Багаторівневий захист передбачає організацію декількох рівнів перевірки користувача перед наданням йому доступу до системи. До основних компонентів такого підходу належать:

Для забезпечення надійного захисту бухгалтерського програмного забезпечення використовуються сучасні методи безпеки, що включають кілька ключових елементів. По-перше, аутентифікація користувачів передбачає перевірку їхньої особи шляхом введення логіна та пароля, а також застосування багатофакторної аутентифікації, прикладом додаткової безпеки можуть бути використовувати SMS-коди або спеціальні додатки-генератори паролів. По-друге, реалізується розмежування прав доступу, щоб кожен співробітник мав доступ лише до тих функцій, які потрібні для виконання його обов'язків (касир може вводити дані про платежі, але не має права змінювати налаштування системи). Третім важливим аспектом є фіксування дій користувачів.

Крім того, захист даних забезпечується на рівні мережі, що досягається шляхом обмеження доступу до програмного забезпечення через конкретні IP-адреси або використанням віртуальних приватних мереж (VPN), які створюють безпечний канал для передачі інформації.

Нарешті, особливу увагу приділяють шифруванню даних, через що, інформація залишається захищеною як під час зберігання, так і під час передачі.

Усі ці заходи разом формують багаторівневу систему захисту, яка гарантує конфіденційність і цілісність бухгалтерської інформації.

Впровадження багаторівневого захисту у бухгалтерському програмному забезпеченні має низку важливих переваг, які підвищують ефективність та надійність управління даними.

Однією з таких переваг є підвищення безпеки даних, завдяки використанню сучасних методів захисту значно знижується ризик несанкціонованого доступу до конфіденційної інформації, що особливо важливо для фінансової документації.

Іншою перевагою є зменшення ризиків внутрішнього шахрайства. Розмежування прав доступу гарантує, що кожен співробітник має доступ лише до тієї інформації та функцій, які необхідні для виконання його обов'язків, що мінімізує можливість зловживань або недобросовісних дій з боку персоналу.

Крім того, багаторівневий захист забезпечує відповідність законодавчим вимогам. У багатьох країнах існують стандарти

кібербезпеки, які зобов'язують підприємства дотримуватися високого рівня захисту фінансових даних. Окремо варто виділити контроль дій користувачів, що дає можливість адміністраторам системи аналізувати дії користувачів, виявляти підозрілі активності та оперативно запобігати потенційним загрозам.

Загалом багаторівневий захист є ефективним інструментом забезпечення безпеки, прозорості та відповідності сучасним вимогам у сфері обліку та управління даними. Впровадження багаторівневого захисту доступу не лише забезпечує збереження бухгалтерської інформації, а й підвищує довіру клієнтів і партнерів до організації. Це також сприяє більш ефективному управлінню ризиками, адже кожен етап доступу та виконання операцій підлягає контролю.

Таким чином, багаторівневий захист є необхідною умовою для безпечного функціонування сучасних бухгалтерських систем в умовах стрімкого розвитку інформаційних технологій.

Одним із найбільш ефективних підходів є впровадження повного шифрування даних. Такий підхід забезпечує захист інформації на всіх етапах її обробки: під час зберігання, обробки, а також передачі через відкриті мережі між серверами та клієнтами, що дозволяє мінімізувати ризики перехоплення або несанкціонованого доступу до конфіденційної інформації, яка може включати фінансові звіти, відомості про транзакції та персональні дані.

Ще одним важливим аспектом є використання цифрового підпису та сертифікації. Приведена технологія забезпечує цілісність електронних документів і підтверджує їх авторство, завдяки цьому знижуються ризики підробки документів або внесення до них несанкціонованих змін. Використання сертифікатів автентичності також додає рівень довіри між сторонами, які взаємодіють у системі.

Загалом, інтеграція таких технологій у бухгалтерське програмне забезпечення забезпечує не лише технічний захист даних, але й підвищує довіру користувачів до системи, вона відповідає сучасним вимогам інформаційної безпеки та дозволяє організаціям відповідати нормативним стандартам у сфері обліку й звітності.

Розробка політик безпеки та внутрішнього аудиту є важливим елементом забезпечення захисту бухгалтерського програмного забезпечення. Один із ключових аспектів – моніторинг і логування дій користувачів, що дозволяє автоматично фіксувати всі операції в системі, що сприяє виявленню підозрілих активностей та їхньому подальшому аналізу, що підвищує прозорість і контроль за процесами. Проведення регулярних аудитів безпеки дає змогу оцінити відповідність системи актуальним стандартам і виявити потенційні вразливості та забезпечує

своєчасне впровадження змін, що знижує ризики, пов'язані з кіберзагрозами.

Не менш важливим є навчання персоналу. Проведення тренінгів дає змогу підвищити обізнаність співробітників щодо безпечного поводження з інформацією та дозволяє запобігти витоку конфіденційних даних через людську недбалість або незнання правил кібербезпеки. Такий підхід забезпечує комплексний захист інформації та підвищує загальну безпеку підприємства.

Резервування і відновлення даних є важливими складовими забезпечення безперебійної роботи бухгалтерського програмного забезпечення. Автоматичне створення резервних копій баз даних із зберіганням у захищених місцях дозволяє уникнути втрати інформації у разі технічних несправностей або кібератак. Впровадження систем швидкого відновлення забезпечує оперативне відновлення роботи у разі збоїв, що мінімізує простої та втрати для підприємства.

Використання антивірусних систем та антишпигунського програмного забезпечення є ключовим елементом захисту бухгалтерських систем від зовнішніх загроз. Постійне оновлення баз сигнатур дозволяє ефективно протидіяти новітнім видам шкідливого програмного забезпечення, що швидко з'являється у цифровому середовищі. Автоматичне сканування файлів і програм на наявність загроз забезпечує своєчасне виявлення потенційно небезпечного коду, зменшуючи ризик пошкодження чи компрометації даних.

Захист інфраструктури систем є важливим компонентом забезпечення їх надійності та безперебійного функціонування. Використання розподіленої архітектури дозволяє зменшити залежність від одного сервера або бази даних, що мінімізує ризик повного збою системи. Джерела безперебійного живлення забезпечують збереження даних навіть у разі раптового відключення електроенергії. Стабільна мережа, яка характеризується високою пропускною здатністю та захистом від атак типу DDoS, гарантує безперервний доступ до системи та безпеку її використання.

Інтеграція із хмарними технологіями відкриває нові можливості для підвищення безпеки та ефективності використання бухгалтерського програмного забезпечення. Використання моделі SaaS (програмне забезпечення як послуга) забезпечує збереження даних у сертифікованих хмарних дата-центрах, які відповідають сучасним стандартам безпеки, таким як GDPR. Це гарантує захист інформації як від зовнішніх загроз, так і від технічних збоїв. Додатково розмежування даних між користувачами хмари унеможливлює несанкціонований доступ до інформації, забезпечуючи її конфіденційність та інтегритет.

Розробка кастомізованих рішень дозволяє адаптувати бухгалтерське програмне забезпечення до унікальних потреб конкретного підприємства. Враховуючи специфіку діяльності організації, створюються індивідуальні рішення з унікальними параметрами безпеки, що забезпечує ефективність та відповідність вимогам, наприклад, у таких системах, як «BAS Бухгалтерія» чи ISpro. Використання модульної архітектури дозволяє впроваджувати зміни та оновлення без перерви основних робочих процесів, забезпечуючи стабільну роботу системи навіть у разі масштабування чи внесення нових функцій.

Технічний захист інформації має низку переваг, зокрема підвищення довіри та репутації підприємства серед клієнтів, партнерів і співробітників, а також забезпечення відповідності вимогам законодавства та стандартів, що сприяє уникненню штрафів та підвищує конкурентоспроможність. Крім того, такий захист знижує ризики та втрати, пов'язані з загрозами безпеці інформації, такими як витік, крадіжка чи знищення даних, і дозволяє ефективно відновлювати інформацію після інцидентів. Завдяки цьому поліпшується ефективність і якість роботи з інформацією, що забезпечує її актуальність, достовірність та цілісність, а також оптимізує витрати на обробку та зберігання.

Сфера бухгалтерського обліку стає все більш залежною від цифрових технологій. Забезпечення кібербезпеки в цій галузі є необхідним для захисту конфіденційності та надійності даних. Дотримання сучасних стандартів інформаційної безпеки та постійне оновлення заходів захисту допоможуть запобігти загрозам і забезпечити ефективну роботу цих систем для бізнесу.

Висновки

Автоматизовані системи бухгалтерського обліку потребують впровадження сучасних і багаторівневих підходів до захисту інформації, що стає критично важливим в умовах цифровізації. Розглянуті напрями, зокрема багаторівневий захист доступу, використання сучасних технологій шифрування, розробка політик безпеки, систем внутрішнього аудиту та впровадження резервного копіювання, забезпечують комплексне вирішення питань конфіденційності, цілісності та доступності даних.

Поєднання цих заходів дозволяє мінімізувати ризики несанкціонованого доступу, втрати інформації та внутрішніх зловживань. Багаторівневий захист забезпечує контроль доступу до системи, запобігаючи загрозам як зовнішнього, так і внутрішнього характеру. Сучасні технології шифрування гарантують безпеку обробки даних на

всіх етапах, а цифрові підписи сприяють прозорості й довірі між сторонами.

Завдяки інтеграції цих рішень підприємства можуть ефективно реагувати на новітні виклики кіберзлочинності, відповідати нормативним вимогам та зберігати конкурентоспроможність на ринку. Захист бухгалтерської інформації стає не лише технічною необхідністю, а й важливим елементом стратегії управління ризиками, що сприяє підвищенню довіри клієнтів і партнерів до організації. Ефективна організація інформаційної безпеки є невід'ємною частиною цифрової трансформації бухгалтерського обліку, сприяючи мінімізації ризиків та підвищенню конкурентоспроможності організацій.

Отже, впровадження перспективних заходів безпеки є основою для стабільної та безпечної роботи автоматизованих систем бухгалтерського обліку, що дозволяє підприємствам ефективно функціонувати в умовах динамічного розвитку інформаційних технологій.

Список використаних джерел:

1. Безпека Облік SaaS. *Облік SaaS*. URL: https://oblik.ua/uk/documentation/bezopasnost_oblik_saas (дата звернення: 11.11.2024)
2. Засадний Б.А. Ризики системи бухгалтерського обліку в умовах застосування МСФЗ. *Науковий вісник Ужгородського національного університету.* 2017. Випуск 14. С. 111–115. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/699587.pdf (дата звернення: 19.11.2024)
3. Захист комплексу. *ISpro*. URL: https://doc.ispro.ua/ru/init/zaxist.html (дата звернення: 18.11.2024)
4. Кулиняк І.Я., Жигало І.І., Горбенко Т.М. Кризові ситуації на підприємствах: сутність, класифікація, загрози виникнення та заходи реагування. *Інфраструктура ринку.* 2021. Випуск 51. С. 175–183. DOI: https://doi.org/10.32843/infrastruct51-27.
5. «M.E.Doc IS». Захист інформації. *Восток-Дніпро*. URL: https://www.vostok.dp.ua/ukr/infa1/program/medoc_is/ (дата звернення: 11.11.2024)
6. Положення про документальне забезпечення записів у бухгалтерському обліку: Наказ Міністерства фінансів України від 24.05.1995 р № 88. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0168-95#Text (дата звернення: 19.11.2024)
7. Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 19.11.2024)
8. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 19.11.2024)
9. Про електронну комерцію: Закон України від 03.09.2015 р. № 675-VIII. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 19.11.2024)
10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Законодавство України / Верховна Рада

України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 19.11.2024)

11. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 19.11.2024)

12. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Законодавство України / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 19.11.2024)

13. Про платіжні послуги: Закон України від 30.06.2021 р. № 1591-IX. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 19.11.2024)

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 19.11.2024)

15. Як убезпечити базу даних BAS. *Inteltech*. URL: https://inteltech.com.ua/uk/blogs/yak-ubezpechyty-bazu-danyh-BAS (дата звернення: 11.11.2024)

References:

1. Bezpeka Oblik SaaS. [Security SaaS Accounting]. *Oblik SaaS – SaaS Accounting*. Available at: https://oblik.ua/uk/documentation/bezopasnost_oblik_saas (accessed November 11, 2024)

2. Zasadnyi B.A. (2017) Ryzyky systemy bukhhalterskoho obliku v umovakh zastosuvannia MSFZ [Risks of the accounting system in the context of applying IFRS]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu – Scientific Bulletin of Uzhhorod National University,* vol. 14. pp. 111–115. Available at: https://journals.indexcopernicus.com/api/file/viewByFileId/699587.pdf (accessed November 19, 2024)

3. Zakhyst kompleksu [Complex protection]. *ISpro – ISpro*. Available at: https://doc.ispro.ua/ru/init/zaxist.html (accessed November 18, 2024)

4. Kulyniak I.Ia., Zhyhalo I.I., Horbenko T.M. (2021) Kryzovi sytuatsii na pidpryiemstvakh: sutnist, klasyfikatsiia, zahrozy vynyknennia ta zakhody reahuvannia [Crisis situations at enterprises: essence, classification, threats of occurrence and response measures]. *Infrastruktura rynku – Market infrastructure.* vol. 51. pp. 175–183. DOI: https://doi.org/10.32843/infrastruct51-27.

5. «M.E.Doc IS». Zakhyst informatsii [«M.E.Doc IS». Information protection]. *Vostok-Dnipro – Vostok-Dnipro*. Available at: https://www.vostok.dp.ua/ukr/infa1/program/medoc_is/ (accessed November 11, 2024)

6. Polozhennia pro dokumentalne zabezpechennia zapysiv u bukhhalterskomu obliku: Nakaz Ministerstva finansiv Ukrainy vid 24.05.1995 r № 88 [Regulations on documentary support of accounting records: Order of the Ministry of Finance of Ukraine № 88 (May 24, 1995)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/z0168-95#Text (accessed November 19, 2024)

7. Polozhennia pro tekhnichnyi zakhyst informatsii v Ukraini: Ukaz Prezydenta Ukrainy vid 27.09.1999 r. № 1229/99 [Regulations on technical protection of information in Ukraine: Decree of the President of Ukraine № 1229/99 (September 27, 1999)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/1229/99#Text (accessed November 19, 2024)

8. Pro elektronni dokumenty ta elektronnyi dokumentoobih: Zakon Ukrainy vid 22.05.2003 r. № 851-IV [About electronic documents and electronic document management: Law of Ukraine № 851-IV (May 22, 2003)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/851-15#Text (accessed November 19, 2024)

9. Pro elektronnu komertsiiu: Zakon Ukrainy vid 03.09.2015 r. № 675-VIII [About e-commerce: Law of Ukraine №. 675-VIII (September 3, 2015)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/675-19#Text (accessed November 19, 2024)

10. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh : Zakon Ukrainy vid 05.07.1994 r. № 80/94-VR [On information protection in information and telecommunication systems: Law of Ukraine № 80/94-VR (July 5, 1994)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (accessed November 19, 2024)

11. Pro zakhyst personalnykh danykh : Zakon Ukrainy vid 01.06.2010 r. № 2297-VI [About personal data protection: Law of Ukraine № 2297-VI (June 1, 2010)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (accessed November 19, 2024)

12. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII [About information: Law of Ukraine № 2657-XII (October 2, 1992)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (accessed November 19, 2024)

13. Pro platizhni posluhy: Zakon Ukrainy vid 30.06.2021 r. № 1591-IKh [On payment services: Law of Ukraine № 1591-IX (June 30, 2021)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/1591-20#Text (accessed November 19, 2024)

14. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 roku № 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine»: Decree of the President of Ukraine № 447/2021 (August 26, 2021)]. Zakonodavstvo Ukrainy / Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (accessed November 19, 2024)

15. Iak ubezpechyty bazu danykh BAS [How to secure a BAS database]. *Inteltech*. Available at: https://inteltech.com.ua/uk/blogs/yak-ubezpechyty-bazu-danyh-BAS (accessed November 11, 2024)