УДК 657.15:[351.746:007

Фатенок-Ткачук Алла,
кандидат економічних наук, доцент,
Волинський національний університет ім. Лесі Українки,
кафедра обліку і оподаткування,
м. Луцьк; ORCID ID: 0000-0001-6200-4873
Fatenok-Tkachuk.Alla@vnu.edu.ua

https://doi.org/10.29038/2786-4618-2024-04-72-81

ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ У ФІНАНОВОМУ ОБЛІКУ

Анотація. Вступ. В умовах постійних загроз втручання в інформаційні системи суб'єкта господарювання, виникає потреба захисту та збереження цифрової інформації як первинних так і систематизованих облікових даних.

Метою даної роботи є систематизування теоретичних положень та обґрунтування практичних рекомендацій щодо організації захисту цифрових даних фінансового обліку.

Методи. У процесі досліджень використовувалися метод індукції на етапі збору, обробки та систематизації одержаної інформації, метод аналізу та синтезу – для поєднання складових елементів економічних явищ в єдиному процесі.

Результати. Виявлено сутнісні характеристики понять інформаційна безпека, цифрова безпека та кібер-безпека даних у контексті економічної безпеки підприємства. Ідентифіковано сукупність заходів у системі організування цифрової безпеки даних фінансового обліку. Визначено основні напрямки державної політики у сфері інформаційної безпеки. Визначено основні заходи забезпечення кібер-безпеки для підприємств критичної інфраструктури. Виокремили основні проблеми захисту цифрової інформації в обліку. Узагальнено основні способи запобігання кіберзагрозам. Практичне значення мають сформовано рекомендації щодо організації системи забезпечення безпеки цифрових даних у фінансовому обліку. Виокремлено дії облікового персоналу підприємства або підприємства партнера, що можуть створити загрозу витоку інформації. Ідентифіковано сукупність інформаційних джерел, що потребують захисту.

Висновки. Система захисту цифрової інформації має стати елементом облікової політики підприємства, а її впровадження сприятиме економічної безпеки суб'єкта господарювання.

Ключові слова. Організація інформаційної безпеки, цифрові дані фінансового обліку, кібер-безпека.

Fatenok-Tkachuk Alla,
Ph.D., Associate Professor,
Lesya Ukrayinka Volyn National University,
Lutsk,

ORGANIZATION OF THE DIGITAL INFORMATION PROTECTION SYSTEM IN FINANCIAL ACCOUNTING

Abstract. Introduction. The constant development of technologies, changing forms of threats and the need to adapt to new conditions will require organizations to constantly improve their security systems.

The purpose of this work is to systematize theoretical provisions and substantiate practical recommendations regarding the organization of protection of digital financial accounting data.

Methods. In the process of research, the method of induction was used at the stage of collecting, processing and systematization of the received information, the method of analysis and synthesis - to combine the constituent elements of economic phenomena in a single process.

Results. The essential characteristics of the concepts of information security, digital security and data cyber security in the context of economic security of the enterprise are revealed. A set of measures in the system of organizing digital security of financial accounting data has been identified. National and international legal acts, standards and recommendations define mandatory requirements for data storage, processing and transmission, thus providing a legal basis for the implementation of information security policies. The main directions of state policy in the field of information security have been determined. The state in which business entities currently work is accompanied by constant cyber-attacks both on the enterprises themselves and on the totality of their digital data in the

field of accounting and taxation. The main measures to ensure cyber security for critical infrastructure enterprises have been determined. They singled out the main problems of digital information protection in accounting, namely: data leakage; software attacks; phishing and social engineering; malware. The main methods of preventing cyber threats are summarized. Recommendations on the organization of the system for ensuring the security of digital data in financial accounting have been formed. The actions of the accounting staff of the enterprise or the enterprise of the partner, which may create a threat of information leakage, are singled out. A set of information sources in need of protection has been identified.

Conclusions. The digital information protection system should become an element of the company's accounting policy, and its implementation will contribute to the economic security of the business entity.

Key words. Organization of information security, digital data of financial accounting, cyber security.

Постановка проблеми та її значення. Безпека цифрової інформації на сьогодні – це безпека бізнесу в цілому. У час, коли всі платіжні інструкції, розрахунки, подача фінансової та податкової звітності є за допомогою інформаційних технологій; коли існуючі бухгалтерські програми не оновлюються і є ризик втручання зі сторони – захист є особливо важливим завданням. Доцільність обробки значного масиву даних спричиняє додаткові загрози виникнення витрат у випадку кібератаки чи збою системи. Значна кількість ресурсу на сьогодні витрачається на збереження обліково-аналітичної інформації суб’єкта господарювання.

Забезпечення безпеки обліково-аналітичних даних включає в себе комплекс заходів, спрямованих на запобігання несанкціонованому доступу, змінам, втратам або розголошенню інформації. Урахування сучасних технологій і зростаючих загроз, таких як кіберзлочинність, кібератаки, витоки даних, маніпуляції з інформацією, змушує організації розробляти спеціалізовані стратегії та інструменти для забезпечення захисту даних. Відсутність належного рівня безпеки може призвести до значних фінансових втрат, репутаційних збитків і навіть до втрати конкурентних переваг.

Проте навіть при застосуванні найсучасніших засобів захисту, питання забезпечення безпеки обліково-аналітичних даних залишається складним і багатогранним. Постійний розвиток технологій, зміна форм загроз і необхідність адаптації до нових умов вимагатимуть від організацій постійного вдосконалення систем безпеки. У зв'язку з цим, інтерес до інструментів і методів забезпечення безпеки цих даних є надзвичайно актуальним у сучасному інформаційному середовищі.

Аналіз останніх досліджень і публікацій. Проблеми обліково-аналітичного захисту обліково-аналітичної інформації, у системі управління підприємством знайшли відображення в працях вітчизняних та іноземних вчених, а саме: О. А. Баранова, К. П. Боримської, С. І. Василішина, С. М. Деньги, З.-М. Задорожного, З. Б. Живко. Незважаючи на ґрунтовний доробок, потребують уточнення методичні аспекти захисту обліково-аналітичної інформації та їх відображення в обліковій політиці підприємства.

Багато науковців вважають, що до сьогоднішнього дня питання однозначного розуміння сутності та основне методики забезпечення безпеки цифрових даних фінансового обліку не існує через відсутність нормативного забезпечення, тому все ще залишаються відкритими та потребують вирішення окремі питання.

Мета і завдання статті. Метою даної роботи є систематизування теоретичних положень та обґрунтування практичних рекомендацій щодо організації захисту цифрових даних фінансового обліку.

Викладення основного матеріалу та обґрунтування отриманих результатів дослідження. Однією з основних задач забезпечення безпеки обліково-аналітичних даних є створення багаторівневої системи захисту, яка включає як технічні, так і організаційні заходи. На технічному рівні використовуються різноманітні інструменти шифрування, засоби аутентифікації та управління доступом, системи моніторингу і виявлення загроз. Організаційні заходи включають розробку політик безпеки, регулярне навчання персоналу та створення системи реагування на інциденти.

Правове регулювання безпеки даних має величезне значення в забезпеченні належного рівня захисту обліково-аналітичної інформації. Національні та міжнародні нормативно-правові акти, стандарти та рекомендації визначають обов'язкові вимоги щодо зберігання, обробки та передачі

даних, забезпечуючи тим самим правову основу для реалізації політик інформаційної безпеки. Невиконання цих вимог може призвести до юридичних санкцій і серйозних економічних наслідків для організацій.

Інформаційна безпека – це безпека будь-якої інформації, включаючи паперові документи, голосову інформацію тощо. До неї часто відносять питання державної безпеки, пропаганди, цензури, соціальних маніпуляцій тощо. Крім того до інформаційної безпеки (ІБ) часто відносять фізичну безпеку, безпеку персоналу, безпеку відносин із третіми сторонами, безперервність бізнесу тощо. Прикладом такого бачення є міжнародний стандарт із управління безпекою організацій ISO 27001 [20].

Інформаційна безпека є основою економічної безпеки підприємства. Сьогодні термін «безпека» розглядається як одна з ключових проблем, яка зачіпає кожного індивіда, підприємства, регіони, держави та світову спільноту в цілому. Це поняття постійно еволюціонує, його зміст ускладнюється та набуває нових відтінків.

У Західній Європі термін «безпека» почав використовуватись ще в XII столітті, проте значного поширення набув лише у XVII–XVIII століттях, коли основним завданням держави вважалося забезпечення добробуту та захисту від загроз. У ті часи безпеку визначали як стан, в якому небезпеки усунуто або нейтралізовано, а соціальні інститути забезпечують стабільність.

Безпека розглядається як стан, що дозволяє ефективно запобігати зовнішнім та внутрішнім загрозам, забезпечувати стабільний розвиток об'єкта та його гармонійне існування. Це поняття багатогранне й застосовується на різних рівнях: від глобального та міжнародного до індивідуального.

На міжнародному рівні безпека передбачає гарантії для окремих держав і їхніх суб'єктів. Розширення інтеграційних зв'язків між країнами формує умови для економічного співробітництва, водночас впливаючи на внутрішні політики окремих держав.

На національному рівні безпека охоплює економічну стабільність та захист інтересів країни, що можливе завдяки участі в міжнародному поділі праці, сталому соціально-економічному розвитку та ефективній співпраці на світовій арені. Основним документом, який регулює державну політику в цій сфері, є Закон України «Про національну безпеку», ухвалений 21 червня 2018 року [11]. Координацію питань безпеки здійснює Рада національної безпеки і оборони України.

Поняття «економічна безпека» вперше ввів у вжиток Ф. Рузвельт близько 90 років тому, а офіційно його закріплено в 1985 році в резолюції Генеральної Асамблеї ООН «Міжнародна економічна безпека». Економічна безпека має особливе значення, оскільки всі інші види безпеки безпосередньо залежать від економічного забезпечення. Стабільна система економічної безпеки є фундаментом для захисту національних інтересів та забезпечення незалежності держави [4].

Державна політика у сфері інформаційної безпеки повинна зосереджуватись на: створенні та забезпеченні функціонування цілісної системи інформаційної безпеки в Україні; розробці та впровадженні новітніх інформаційних технологій для захисту інформаційної інфраструктури; вдосконаленні нормативно-правової бази в галузі інформаційної безпеки.

Таким чином, ефективне забезпечення інформаційної безпеки потребує комплексного підходу, що включає стратегічне планування, правову та організаційну підтримку, а також технологічні заходи для захисту національних інтересів у цифровому середовищі.

Основними принципами ІБ є – цілісність, доступність і конфіденційність. Ці вимоги застосовні не тільки до електронної інформації, але й до «паперової», усної тощо.

Безпека ІТ (комп'ютерна безпека, цифрова безпека, ІТ-безпека) це – захист від хакерів, вірусів, спаму, фішингу та безлічі інших загроз, що виникають, головним чином, з Інтернету. Цей захист найчастіше реалізується зниженням тих чи інших організаційних або технічних вразливостей безпеки [2].

Безпека ІТ – це забезпечення цілісності, доступності, конфіденційності та інших вимог безпеки, що пред'являються до обчислювальної та комунікаційної техніки та інформації, яку вона зберігає, обробляє та передає. До завдань безпеки ІТ відносять також захист від соціальної інженерії, управління ефективністю безпеки, надання гарантій безпеки, відповідності нормативним вимогам безпеки, страхування інформаційних ризиків, забезпечення безперервності бізнесу.

Поняття кібер-безпеки започатковане від теміну “кібернетика”. Він був придуманий Андре-Марі Ампером у 1834 році та розвинений Норбертом Вінером у 1948 році. Кібернетика в сучасному розумінні – це дисципліна про інформацію в складних керуючих системах. Наприклад, у комп’ютері, людині чи суспільстві.

У сучасному контексті приставка «кібер-» набула широкого поширення та переосмислення завдяки канадсько-американському письменнику-фантасту Вільяму Гібсону. У 1984 році у своєму романі «Нейромант» він запровадив та популяризував термін «кіберпростір» (cyberspace) для опису віртуальної реальності та глобальних комунікаційних мереж. Його роботи вплинули на масову культуру і сформували сучасне розуміння цифрового світу.

За визначенням Міжнародного союзу електрозв'язку (МСЕ), кібербезпека – це набір інструментів, стратегій, принципів безпеки, гарантій, керівних принципів, підходів до управління ризиками, поведінки, навчання, практичного досвіду, страхування та технологій, які можуть бути використані для захисту кіберсередовища, організаційних ресурсів та користувачів [3].

Враховуючи сутність поняття «захист інформації», що трактується міжнародним стандартом ISO/IEC 27001 [20] як забезпечення конфіденційності, цілісності та доступності інформації, під кібернетичною безпекою облікової інформації розуміється як стан захищеності, за якого забезпечується своєчасне виявлення, запобігання та зведення нанівець несанкціонованого використання, порушення конфіденційності, цілісності або знищення облікової інформації електронними засобами.

На сьогодні багато вітчизняних підприємств відносяться до об’єктів критичної інфраструктури. Фінансова інформація таких підприємств, що є результатом фінансового обліку потребує особливого захисту.

Стан у якому на сьогодні працюють суб’єкти господарювання супроводжується постійними кібератаками як на самі підприємства так і сукупність їх цифрових даних в сфері обліку та оподаткування. Визнання підприємства частиною критичної інфраструктури спрощує військовий облік та сприяє безперервному випуску продукції важливої для існування громадян України. У зв’язку з виникненням нового формату підприємств виникла необхідність нормативного забезпечення їх діяльності та обліку. Так у 2019 році Кабміном було прийнято постанову про затвердження «Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [9]. Саме вони є основою організації захисту обліково-аналітичної інформації на сьогодні.

Система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються), запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об’єкта критичної інформаційної, порушенню функціонування компонентів об’єкта; забезпечення спостережності за діями користувачів та функціонуванням засобів захисту об’єкта критичної інформаційної інфраструктури.

На таких об’єктах має діяти політика інформаційної безпеки. Політика інформаційної безпеки – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні забезпечувати: формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки; управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит; мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної

інфраструктури; доступність та відмовостійкість компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури; визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Формування додаткових заходів із забезпечення кіберзахисту розробник комплексної системи захисту інформації здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

Об'єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на підприємстві та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки. Крім того мають бути визначені права та обов'язки всіх категорій користувачів та адміністраторів інформаційної інфраструктури, обов'язки адміністраторів з обслуговування компонентів та забезпечення її інформаційної безпеки, які оформлюються окремим рішенням.

Рекомендовано для підприємств мати визначений перелік інформаційних, програмних та апаратних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта, рівень їх критичності та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушення функціонування компонентів об'єкта.

На об'єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення.

Бухгалтерські системи можуть бути вразливими до різноманітних кіберзагроз. Ми виокремили основні проблеми захисту цифрової інформації в обліку:

1. Витік даних. Один із найбільших ризиків, пов'язаний із бухгалтерськими системами, полягає в тому, що зловмисники можуть отримати доступ до фінансової інформації, такої як баланси, звіти, інформація про операції. Це може статися через слабкі місця в системах безпеки або через несанкціонований доступ до баз даних.

2. Атаки на програмне забезпечення. Зловмисники можуть скористатися уразливими місцями в програмному забезпеченні бухгалтерської системи (наприклад, уразливості в протоколах обміну даними або в алгоритмах шифрування) для того, щоб здійснити атаку. Атаки можуть включати злочинний доступ до даних або їх пошкодження.

3. Фішинг та соціальна інженерія. Зловмисники можуть використовувати методи соціальної інженерії для того, щоб отримати доступ до облікових даних працівників підприємства, шляхом обману. Наприклад, фішинг-атаки, коли зловмисники створюють фальшиві електронні листи або вебсайти, які імітують справжні, щоб отримати логіни, паролі чи іншу конфіденційну інформацію.

4. Шкідливе програмне забезпечення. Включаючи віруси, трояни, руткіти та програмне забезпечення для викрадення даних. Шкідливі програми можуть проникати в бухгалтерські системи через заражені файли, посилання чи електронні листи, а потім виводити або змінювати інформацію в облікових базах даних.

Завданням кіберзахисту та безпеки даних в бухгалтерському обліку є забезпечення комплексу організаційно-технічних заходів та кадрових завдань, спрямованих на захист комерційної таємниці. Заходи безпеки реалізуються у вигляді програм або програмних пакетів, які розширюють функціональність стандартних операційних систем або систем управління базами даних. Ми виокремили три групи заходів кіберзахисту облікової інформації, а саме організаційні, технічні та кадрові.

Організаційні полягають в обмеженні несанкціонованого доступу до обліково-аналітичної інформації. Технічні, у свою чергу, це попередження навмисного пошкодження облікових систем за допомогою спеціально спровокованих порушень роботи технічних засобів або інформаційних

технологій. Підвищення компетенцій працівників та їх відповідальності у процесі використання інформаційних технологій є основою кадрових заходів.

На технічному рівні заходи кібербезпеки включають контроль доступу до облікових даних, управління авторизацією та захист облікової інформації. Основним способом запобігання кіберзагрозам є впровадження заходів контролю доступу до веб-сайтів, систем та файлів на послідовному рівні [3].

Деякі функції безпеки передбачені в бухгалтерському програмному забезпеченні, наприклад наявність паролю для входу, фіксація того хто створює документи, ведення журналу роботи та керування документами. Крім вбудованих функцій контролю доречно регулярно здійснювати перевірку на наявність пристроїв призначених для прослуховування.

Основним способом запобігання кіберзагрозам є впровадження заходів контролю доступу до веб-сайтів, систем та файлів на послідовному рівні. Основним способом запобігання кіберзагрозам є запровадження послідовних заходів контролю доступу до веб-сайтів, систем і файлів.

Створення механізмів підзвітності дозволить визначити, хто працює над системою і що він робить у певний момент часу, а також реєструвати події, які відбуваються в комп'ютеризованих інформаційних системах бухгалтерського обліку.

Кіберзахист бухгалтерських систем є важливою складовою інформаційної безпеки підприємства. Використання багатошарових методів захисту, таких як шифрування, аутентифікація, моніторинг систем, антивірусні рішення та регулярне оновлення програмного забезпечення, дозволяє захистити чутливі фінансові дані від загроз, зберігаючи їх цілісність, конфіденційність і доступність. В умовах постійного зростання кіберзагроз підприємствам необхідно постійно вдосконалювати свою стратегію кіберзахисту для збереження своїх даних.

Шифрування є одним з найефективніших способів захисту даних від несанкціонованого доступу. Всі чутливі фінансові дані, що передаються по мережі або зберігаються на сервері, повинні бути зашифровані за допомогою стандартів шифрування, таких як AES (Advanced Encryption Standard) або RSA. Це забезпечує, що навіть якщо хакер отримає доступ до даних, він не зможе їх прочитати без відповідного ключа.

Всі користувачі бухгалтерських систем повинні мати чітко визначені ролі та доступ до конкретної інформації залежно від їхніх прав. Один із найважливіших методів захисту – це двофакторна аутентифікація (2FA), що додає додатковий рівень захисту при вході в систему. Крім традиційного пароля, користувачеві потрібно ввести код, що надсилається на його мобільний телефон або генерується спеціальним додатком.

Застосування систем, які потребують введення одноразового пароля (OTP) разом із звичайним паролем при вході в бухгалтерську систему. Це значно ускладнює злом пароля за допомогою крадіжки даних або методів соціальної інженерії.

Крім цього доречно здійснювати постійний моніторинг і виявлення вторгнень і системи, де здійснюється фінансовий облік. Системи для виявлення вторгнень (IDS) є важливою частиною кіберзахисту бухгалтерських систем. Ці системи постійно відстежують трафік і поведінку користувачів, виявляючи аномальні дії або спроби несанкціонованого доступу. Коли відбувається спроба атаки, система має змогу швидко сповістити адміністраторів для вжиття відповідних заходів. Спеціалісти ІТ пропонують також використання таких рішень, як Snort або Suricata, для виявлення та попередження атак на бухгалтерські системи. Вони можуть бути інтегровані з іншими компонентами системи безпеки для автоматичного блокування загроз. Splunk / SolarWinds / Nagios – системи моніторингу та аналізу логів для відстеження дій користувачів, включаючи спроби несанкціонованого доступу та аномальну активність.

Є відкриті інструменти для аудиту, а саме OSSEC – відкрита система для моніторингу та аналізу безпеки [22].

Спеціальні системи фільтрації трафіку можуть допомогти виявляти шкідливі програми та блокувати їх ще до того, як вони потраплять до системи. Програми типу Kaspersky, McAfee, або Bitdefender можуть бути інтегровані з бухгалтерським програмним забезпеченням для автоматичного сканування файлів і електронних листів на наявність шкідливих компонентів.

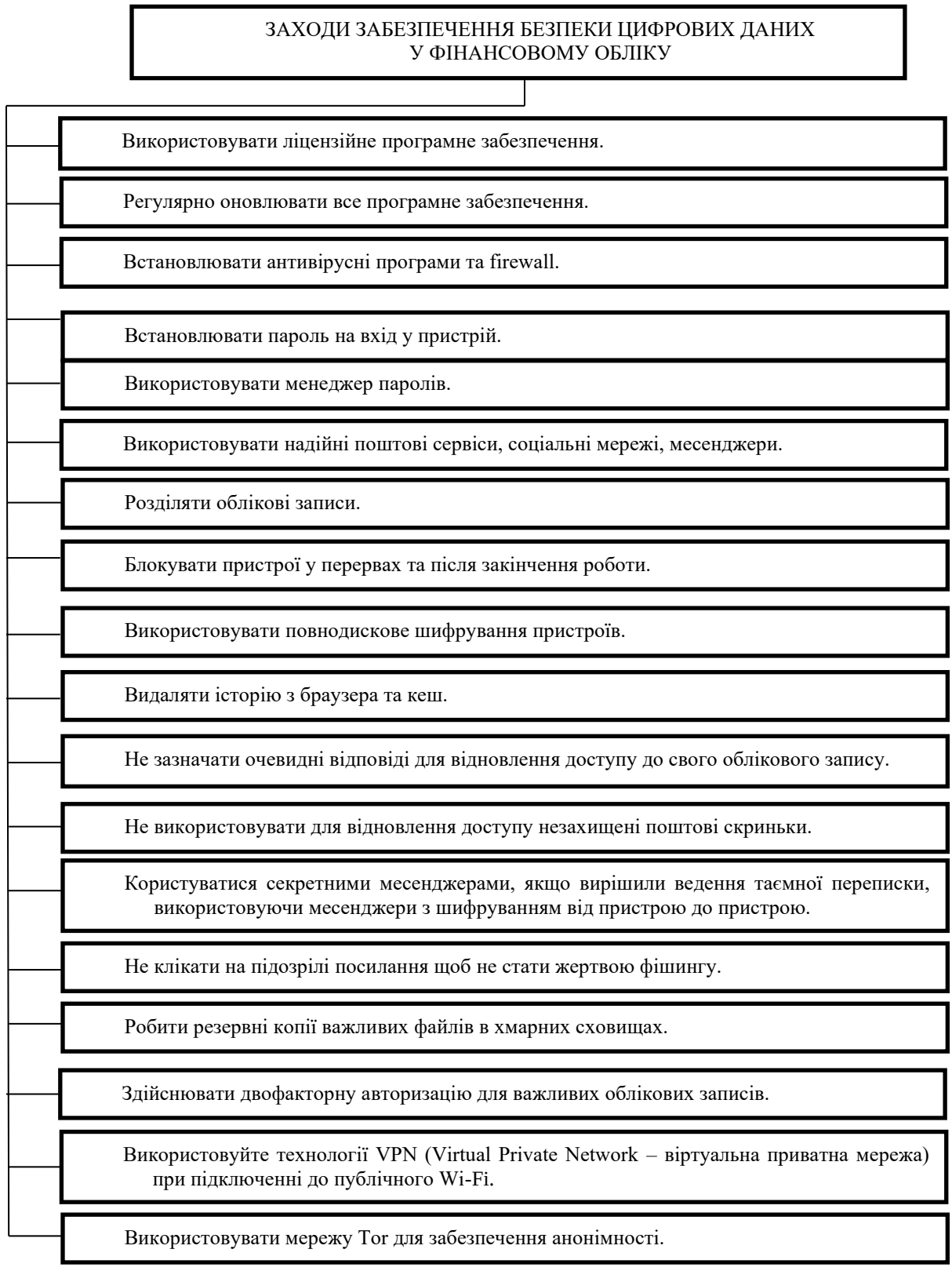

Рис. 1. *Заходи забезпечення безпеки цифрових даних у фінансовому обліку*
Примітка: сформовано автором на основі джерела [8]

Splunk / SolarWinds / Nagios – системи моніторингу та аналізу логів для відстеження дій користувачів, включаючи спроби несанкціонованого доступу та аномальну активність.

Регулярні оновлення програмного забезпечення є ключовим моментом для збереження безпеки бухгалтерських систем. Розробники постійно випускають патчі для усунення уразливостей, які можуть бути використані хакерами. Необхідно, щоб програмне забезпечення та операційні системи бухгалтерських систем завжди були актуальними та відповідали останнім стандартам безпеки. Системи оновлення, такі як Windows Update або patch management в програмному забезпеченні для бухгалтерії, можуть забезпечити своєчасне оновлення та виправлення пошкоджень, зокрема тих, що стосуються захисту від кіберзагроз.

Постачальників та підрядників слід заохочувати до дотримання принципів захисту інформації для компаній, які замовляють продукцію, товари, роботи та послуги. Загрозу витоку інформації становлять такі дії: відкриття файлів на комп'ютері від невідомих осіб, надісланих електронною поштою або через програми обміну миттєвими повідомленнями;

- встановлення неліцензійного програмного забезпечення, яке не потрібне працівнику для виконання своїх обов'язків;
- використання паролів «за замовчуванням», створення простих паролів, не намагання змінювати паролі протягом тривалого періоду часу, особливо у вікні введення даних на комп'ютері.

Ми виокремили основні рекомендації щодо організації системи забезпечення безпеки цифрових даних у фінансовому обліку (див. рис. 1).

Виникає питання, яку саме інформація потребує захисту. Фахівці сходяться на думці, що кожен суб’єкт господарювання повинен мати перелік конфіденційної комерційної інформації. Предметом комерційної таємниці є відомості бухгалтерського обліку, пов’язані з господарською діяльністю підприємства, до яких можна віднести виробничу та технологічну інформацію, інформацію про управління, фінанси й іншу діяльність. Також до предмета комерційної таємниці підприємства можуть бути віднесені документи про переговори підприємства з потенційними контрагентами та методи ціноутворення; документи, пов’язані з маркетинговими дослідженнями ринку; відомості про організацію праці і підбір працівників; інформація про умови зберігання документів, тобто відомості, що містять комерційну цінність.

Виконання переліку обов’язкових правил кібербезпеки сприятимуть захисту цифрових даних, що містяться у фінансовому обліку підприємства.

Висновки і перспективи подальших досліджень. Вітчизняний бізнес є інвестором у майбутню перемогу. Інформаційні системи, безперервність роботи яких, потребують постійної уваги та захисту від кібер-загроз. Методичні рекомендаціях щодо організування захисту облікових даних, мають стати основою облікових політики задля розуміння комплексу заходів кожним представником обліково-аналітичних служб. Нормативно-правове забезпечення цього процесу дасть змогу ефективно та правомірно здійснювати роботу у цифровому просторі, здійснюючи фінансовий облік.

Джерела та література

1. Боримська К. П. Захист бухгалтерської інформації в обліковій політиці з метою оподаткування: організаційні аспекти. *Збірник наукових праць Національного університету державної податкової служби України*. 2013. № 2. С. 14-21. URL: http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4 (дата звернення: 15.12.2024).

2. Булдижов В. Кібербезпека, ІБ, безпека ІТ – у чому різниця? URL: https://www.h-x.technology/ua/blog-ua/infosec-itsec-cybersecurity-defference-ua (дата звернення 20.10.2024).

3. Василішин С. І. Обліково-аналітичне забезпечення в системі ризиків та загроз економічної безпеки аграрних підприємств України: монографія. Харків: Друкарня Мадрид, 2020. 419 с.

4. Гнилицька Л. В. Обліково-аналітичне забезпечення економічної безпеки підприємства : монографія. Київ : КНЕУ, 2022. 305 с.

5. Деньга С. М. Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку. Бухгалтерський облік і аудит. 2004. № 5. С. 59-65.

6. Живко З. Б. Захист інформаційних ресурсів в управлінні системами економічної безпеки підприємства. Економічний простір. 2018. № 17. С. 166-173.

7. Кулинич М. Б., Фатенок-Ткачук А. О., Мельник К. П. Облік, аналіз, аудит і оподаткування в управлінні розвитком суб’єктів господарювання через призму цифровізації : монографія. Луцьк : Вежа-Друк,

2021. 170 с.

8. Настанови з кібербезпеки від експертів. URL: surl.li/lfoaiz (дата звернення: 15.12.2024).
9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова КМ від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення 15.12.2024 р.).
10. Про основні засади забезпечення кібербезпеки України: Закон України документ 2163-VIII від 05.10.2017 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.12.2024).
11. Про Раду національної безпеки і оборони України : Закон України. Відомості Верховної Ради України (ВВР), 1998, № 35, ст.237, редакція від 13.07.2023 документ 3223-IX. URL: https://zakon.rada.gov.ua/laws/show/3223-20#n59 (дата звернення 07.12.2024)
12. Фатенок-Ткачук А. О. Обліково-аналітичне забезпечення бізнес-процесів підприємства : монографія. Луцьк : Вежа-Друк, 2018. 200 с.
13. Фатенок-Ткачук, А., Скорук О., Януш, Р., & Захарчук І. (2024). Використання штучного інтелекту в обліково-аналітичних процесах. *Економічний часопис ВНУ ім. Лесі Українки*. 2024. № 2. С.21–29. https://doi.org/10.29038/2786-4618-2024-02-21-29.
14. BILL Spend & Expense (Formerly Divvy). BILL | Financial Operations Platform for Businesses & Firms. URL: https://www.bill.com/product/spend-and-expense (дата звернення: 08.12.2024).
15. Botkeeper | Bookkeeping for Accounting Firms. *Botkeeper | Bookkeeping for Accounting Firms*. URL: https://www.botkeeper.com/ (дата звернення: 07.12.2024).
16. Ehioghiren E. E., Ojeaga J. O. Cloud-based Accounting Technologies: Preparing Future-Ready Professional Accountants. International Journal of Innovative Science and Research Technology. 2022. Vol. 7, no. 2. URL: https://ijisrt.com/assets/upload/files/IJISRT22FEB658.pdf
17. Fahmi M., Muda I., Kesuma S. A. Digitization Technologies and Contributions to Companies towards Accounting and Auditing Practices. International Journal of Social Service and Research. 2023. Vol. 3, no. 3. URL: https://doi.org/10.46799/ijssr.v3i3.298
18. Financial Operations: Bookkeeping For Modern Startups. Financial Operations: Bookkeeping For Modern Startups. URL: https://www.zeni.ai/ (дата звернення: 08.12.2024).
19. Gridlex Sky Accounting, Expenses & ERP Software. Gridlex - CRM, Help Desk, HRMS, Expenses, Accounting &ERP. URL: http://surl.li/nordxy (дата звернення: 08.12.2024).
20. ISO/IEC 27001:2022. Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги. URL: https://www.iso.org/standard/27001 (дата звернення: 05.12.2024).
21. Zadorozhnyi Z. -M., Desyatnyuk O., Muravskyi V., Shevchuk O. Combination of Digital Twin Technology and FinOps in Management Accounting Modeling 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 352-356, doi: 10.1109/ACIT58437.2023.10275621.
22. Kaspersky Endpoint Security / Bitdefender / Symantec Endpoint Protection. URL: http://surl.li/cphfqw (дата звернення: 05.12.2024).
23. Splunk / SolarWinds / Nagios. URL: http://surl.li/feudxm (дата звернення: 12.12.2024).
24. Veeam Backup & Replication / Acronis Backup / Commvault. URL: http://surl.li/yedkva (дата звернення: 05.12.2024).
25. VeraCrypt / BitLocker / PGP (Pretty Good Privacy). URL: https://en.wikipedia.org/wiki/Pretty_Good_Privacy (дата звернення: 15.12.2024).

References

1. Boryms′ka, K. P. (2013). Zakhyst bukhhalters′koyi informatsiyi v oblikoviy politytsi z metoyu opodatkuvannya: orhanizatsiyni aspekty [Protection of accounting information in the accounting policy for taxation purposes: organizational aspects]. Zbirnyk naukovykh prats′ Natsional′noho universytetu derzhavnoyi podatkovoyi sluzhby Ukrayiny – Collection of scientific works of the National University of the State Tax Service of Ukraine. 2. 14-21. Retrieved from http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4 [in Ukrainian].
2. Buldyzhov, V. Kiberbezpeka, IB, bezpeka IT – u chomu riznytsya? [Cyber security, IS, IT security - what's the difference?]. Retrieved from https://www.h-x.technology/ua/blog-ua/infosec-itsec-cybersecurity-defference-ua [in Ukrainian].
3. Vasylishyn, S. I. (2020). Oblikovo-analitychne zabezpechennya v systemi ryzykiv ta zahroz ekonomichnoyi bezpeky ahrarnykh pidpryyemstv Ukrayiny [Accounting and analytical support in the system of risks and threats to the economic security of agricultural enterprises of Ukraine]. Kharkiv: Madrid Printing House. 419 p. [in Ukrainian].
4. Hnylyts′ka, L. V. (2022). Oblikovo-analitychne zabezpechennya ekonomichnoyi bezpeky pidpryyemstva [Accounting and analytical provision of economic security of the enterprise]. Kyiv: KNEU. 305 p. [in Ukrainian].

5. Den′ha, S. M. (2004). Zakhyst informatsiyi v komp`yuternykh informatsiynykh systemakh bukhhalters′koho obliku [Protection of information in computer accounting information systems]. Bukhhalters′kyy oblik i audyt – Accounting and auditing. 5. 59-65. [in Ukrainian].

6. Zhyvko, Z. B. (2018). Zakhyst informatsiynykh resursiv v upravlinni systemamy ekonomichnoyi bezpeky pidpryyemstva [Protection of information resources in the management of enterprise economic security systems]. Ekonomichnyy prostir – Economic space. 17. 166-173. [in Ukrainian].

7. Kulynych, M. B., Fatenok-Tkachuk, A. O. & Mel′nyk, K. P. (2021). Oblik, analiz, audyt i opodatkuvannya v upravlinni rozvytkom sub″yektiv hospodaryuvannya cherez pryzmu tsyfrovizatsiyi [Accounting, analysis, audit and taxation in the management of the development of economic entities through the prism of digitalization]. Lutsk: Vezha-Druk. 170 p. [in Ukrainian].

8. Nastanovy z kiberbezpeky vid ekspertiv [Guidelines on cyber security from experts] . Retrieved from surl.li/lfoaiz [in Ukrainian].

9. Resolution of the Cabinet of Ministers "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" № 518 (19.06.2019). Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [in Ukrainian].

10. Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine". Document 2163-VIII. (05.10.2017). Retrieved from http://zakon.rada.gov.ua/laws/show/2163-19. [in Ukrainian].

11. Law of Ukraine "On the National Security and Defense Council of Ukraine". Information of the Verkhovna Rada of Ukraine (VVR), 1998, No. 35, Article 237. (13.07.2023) document 3223-IX. . Retrieved from https://zakon.rada.gov.ua/laws/show/3223-20#n59 [in Ukrainian].

12. Fatenok-Tkachuk, A. O. (2018). Oblikovo-analitychne zabezpechennya biznes-protsesiv pidpryyemstva [Accounting and analytical support of business processes of the enterprise]. Луцьк : Вежа-Друк. 200 p. [in Ukrainian].

13. Fatenok-Tkachuk, A., Skoruk O., Yanush, R., & Zakharchuk I. (2024). Vykorystannya shtuchnoho intelektu v oblikovo-analitychnykh protsesakh [Use of artificial intelligence in accounting and analytical processes]. Ekonomichnyy chasopys VNU im. Lesi Ukrayinky – Economic Journal of Lesya Ukrainka Volyn National University. 2. 21–29. . Retrieved from https://doi.org/10.29038/2786-4618-2024-02-21-29. [in Ukrainian].

14. BILL Spend & Expense (Formerly Divvy). BILL | Financial Operations Platform for Businesses & Firms. Retrieved from https://www.bill.com/product/spend-and-expense [in English].

15. Botkeeper | Bookkeeping for Accounting Firms. Botkeeper | Bookkeeping for Accounting Firms. Retrieved from https://www.botkeeper.com/ [in English].

16. Ehioghiren, E. E., Ojeaga J. O. (2022)/ Cloud-based Accounting Technologies: Preparing Future-Ready Professional Accountants. International Journal of Innovative Science and Research Technology. 7, 2. Retrieved from https://ijisrt.com/assets/upload/files/IJISRT22FEB658.pdf [in English]/

17. Fahmi, M., Muda, I. & Kesuma S. A.(2023)/ Digitization Technologies and Contributions to Companies towards Accounting and Auditing Practices. International Journal of Social Service and Research. 3. 3. Retrieved from https://doi.org/10.46799/ijssr.v3i3.298 [in English].

18. Financial Operations: Bookkeeping For Modern Startups. Financial Operations: Bookkeeping For Modern Startups. Retrieved from https://www.zeni.ai/ [in English].

19. Gridlex Sky Accounting, Expenses & ERP Software. Gridlex - CRM, Help Desk, HRMS, Expenses, Accounting &ERP. Retrieved from http://surl.li/nordxy [in English].

20. ISO/IEC 27001:2022. Information security, cyber security and privacy protection - Information security management systems - Requirements. Retrieved from https://www.iso.org/standard/27001 [in Ukrainian].

21. Zadorozhnyi, Z. -M., Desyatnyuk, O., Muravskyi, V.& Shevchuk, O. (2023).Combination of Digital Twin Technology and FinOps in Management Accounting Modeling 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland. pp. 352-356. Retrieved from doi: 10.1109/ACIT58437.2023.10275621 [in English].

22. Kaspersky Endpoint Security / Bitdefender / Symantec Endpoint Protection. Retrieved from http://surl.li/cphfqw [in English].

23. Splunk / SolarWinds / Nagios Retrieved from http://surl.li/feudxm [in English].

24. Veeam Backup & Replication / Acronis Backup / Commvault. . Retrieved from http://surl.li/yedkva [in English].

25. VeraCrypt / BitLocker / PGP (Pretty Good Privacy). Retrieved from https://en.wikipedia.org/wiki/Pretty_Good_Privacy[in English].

Стаття надійшла до редакції 18.12.2024 р.