e-mail: goroshkova69@gmail.com
Волков Владимир Петрович, д.т.н., профессор, академик Академии экономических наук Украины, профессор кафедры предпринимательства, менеджмента организаций и логистики Запорожского национального университета,
e-mail: volkovvp49@gmail.com
Карбивничий Иван Алексеевич, аспирант Запорожского национального университета,
e-mail: ivan.karbivnichi@gmail.com

INFORMATION ABOUT AUTHORS
Horoshkova Lidiia, D. Sc. in Economics, Professor of the Chair of entrepreneurship, management of organizations and logistics, Zaporizhzhya National University,
e-mail: goroshkova69@gmail.com
Volkov Vladimir, D. Sc. in Technical, Professor, Professor of the Chair of entrepreneurship, management of organizations and logistics, Zaporizhzhya National University,
e-mail: volkovvp49@gmail.com
Karbivnychyi Ivan, Postgraduate, Zaporizhzhya National University,
e-mail: ivan.karbivnichi@gmail.com

УДК 631.162:657 https://doi.org/10.31470/2306-546X-2018-38-47-53

ВПЛИВ АВТОМАТИЗАЦІЇ ОБЛІКУ ТА ФІНАНСОВОЇ ЗВІТНОСТІ НА БЕЗПЕКУ ПІДПРИЄМСТВ

Ігнатенко М.М.
Сарапіна О.А.

Предметом дослідження *виступають теоретичні, методичні та практичні аспекти автоматизації обліку та фінансової звітності на безпеку підприємств.*

Метою роботи *є виявлення проблем і встановлення тенденцій здійснення бухгалтерського обліку та фінансової звітності на засадах автоматизації та обґрунтування вирішення проблем комп'ютеризації облікових процесів, забезпечення інформаційної безпеки підприємств та управління нею на перспективу.*

Методологічною основою статті *стали загальнонаукові методи пізнання, узагальнення, метод порівняльного аналізу та інші методи дослідження.*

Результати роботи. *Визначено роль впровадження автоматизації, програмного забезпечення й комп'ютеризації облікових процесів та фінансової звітності на безпеку вітчизняних підприємств та організацій. Надана змістовна характеристика конкурентних переваг та властивостей найбільш використовуваних програм. Одночасно виявлено ризики й загрози інформаційній безпеці підприємств, їх джерела та прояви. Обґрунтовано комплекс заходів збереження та зміцнення інформаційної безпеки. Розроблено план і заходи їх впровадження. Надані пропозиції щодо здійснення подальших досліджень з метою посилення безпеки підприємств і вдосконалення управління нею.*

Галузь застосування результатів *полягає в тому, що викладені пропозиції з питань автоматизації обліку та фінансової звітності можуть бути використані керівниками та фахівцями підприємств з метою підвищення безпеки.*

Висновки. *Впровадження автоматизованих систем і програм здійснення бухгалтерського обліку й формування обліково-фінансової звітності є вагомим чинником підвищення ефективності функціонування вітчизняних підприємств. При цьому підвищується безпека функціонування підприємств на основі більшої точності й неупередженості використовуваної інформації, значного скорочення їх витрат на обліково-аналітичні процеси. Проте через специфіку автоматизації й комп'ютеризації (під'єднання до більш глобальних мереж, використання типових програм та показників обліку тощо) збільшується відкритість інформаційних систем, зростають загрози комерційній таємниці та ризики конкурентоспроможної діяльності загалом. Це актуалізує значимість забезпечення та подальшого удосконалення інформаційної безпеки підприємств і організацій на перспективу.*

Ключові слова: *підприємства, безпека, комп'ютерні мережі, автоматизація, бухгалтерський облік, фінансова звітність, програмні продукти.*

ВЛИЯНИЕ АВТОМАТИЗАЦИИ УЧЕТА И ФИНАНСОВОЙ ОТЧЕТНОСТИ НА БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ

Игнатенко М.М.
Сарапина О.А.

Предметом исследования *выступают теоретические, методические и практические аспекты автоматизации учета и финансовой отчетности на безопасность предприятий.*

Целью *работы является выявление проблем и установление тенденций осуществления бухгалтерского учета и финансовой отчетности на основе автоматизации и обоснования решения проблем компьютеризации учетных процессов, обеспечения информационной безопасности предприятий и управления ею на перспективу.*

Методологической основой статьи *стали общенаучные методы познания, обобщения, метод сравнительного анализа и другие методы исследования.*

Результаты работы. *Определена роль внедрения автоматизации, программного обеспечения и компьютеризации учетных процессов и финансовой отчетности на безопасность отечественных предприятий и организаций. Предоставленная содержательная характеристика конкурентных преимуществ и свойств наиболее используемых программ. Одновременно выявлено риски и угрозы информационной безопасности предприятий, их источники и проявления. Обоснован комплекс мероприятий сохранения и укрепления информационной безопасности. Разработан план и меры их внедрения. Представлены предложения по осуществлению дальнейших исследований с целью усиления безопасности предприятий и совершенствования управления ею.*

Область применения *заключается в том, что изложенные предложения по вопросам автоматизации учета и финансовой отчетности могут быть использованы руководителями и специалистами предприятий с целью повышения безопасности.*

Выводы. *Внедрение автоматизированных систем и программ осуществления бухгалтерского учета и формирования учетно-финансовой отчетности является весомым фактором повышения эффективности функционирования отечественных предприятий. При этом повышается безопасность функционирования предприятий на основе большей точности и беспристрастности используемой информации, значительного сокращения их расходов на учетно-аналитические процессы. Однако в силу специфики автоматизации и компьютеризации (подключение к более глобальным сетям, использование типовых программ и показателей учета и т.п.) увеличивается открытость информационных систем, растут угрозы коммерческой тайны и риски конкурентоспособной деятельности в целом. Это актуализирует значимость обеспечения и дальнейшего совершенствования информационной безопасности предприятий и организаций на перспективу.*

Ключевые слова: *предприятия, безопасность, компьютерные сети, автоматизация, бухгалтерский учет, финансовая отчетность, программные продукты.*

THE EFFECT OF AUTOMATION OF ACCOUNTING AND FINANCIAL STATEMENTS ON ENTERPRISES SAFETY

Ignatenko M.M.
Sarapina O.A.

The subject of the research *is theoretical, methodological and practical aspects of accounting automation and financial reporting on enterprise security.*

The purpose of the work *is to identify problems and establish trends in the implementation of accounting and financial reporting on the basis of automation and substantiation of the problem of computerization of accounting processes, information security of enterprises and management of the future.*

Methodological basis of the article *became general scientific methods of cognition, generalization, method of comparative analysis and other methods of research.*

Results of work. *The role of implementation of automation, software and computerization of accounting processes and financial reporting on the security of domestic enterprises and organizations has been determined. An informative characteristic of competitive advantages and properties of the most used programs is provided. At the same time, risks and threats to information security of enterprises, their sources and manifestations are revealed. The complex of measures for preservation and strengthening of information security is substantiated. A plan and measures for their implementation have been developed. Submitted suggestions for further research in order to strengthen the security of enterprises and improve its management.*

The field of application of the results *is that the stated proposals on automation of accounting and financial reporting can be used by managers and specialists of enterprises for the purpose of safety improvement.*

Conclusions*. The introduction of automated systems and programs for accounting and accounting and financial reporting is a significant factor in improving the efficiency of domestic enterprises. At the same time, the security of the operation of enterprises increases due to greater accuracy and impartiality of the information used, and a significant reduction of their costs on accounting and analytical processes. However, because of the specifics of automation and computerization (connecting to more global networks, using typical programs and metrics, etc.), the openness of information systems increases, the threats to commercial secrets and the risks of competitive business increase in general. It updates the importance of providing and further improving the information security of enterprises and organizations in the long run.*

Key words: *enterprises, security, computer networks, automation, accounting, financial reporting, software products.*

Постановка проблеми. У формуванні сучасних мереж бухгалтерського обліку та фінансової звітності на підприємствах всіх галузей і видів діяльності та господарювання провідне місце займає автоматизація. Використання відповідних програмних продуктів забезпечує можливість здійснення моніторингу і контролю за

відповідністю й точністю облікових даних і процесів. При цьому комп'ютерні мережі забезпечують надійність інформаційних зв'язків як всередині бухгалтерії, так і між бухгалтерією та іншими структурними підрозділами підприємства. Це є запорукою безпеки підприємств. Проте питання інформаційної безпеки особливо мають бути у полі зору працівників та власників. Зважаючи на це, перспективною є така організація роботи бухгалтерії при застосуванні персональних комп'ютерів (ПК) і програм, що складається з двох основних відділів: відділу інформаційної системи та відділу контролю.

Аналіз останніх досліджень та публікацій. Проблеми формування безпеки й інформаційної безпеки зокрема, автоматизації бухгалтерського обліку та фінансової звітності підприємств знаходяться в полі зору багатьох дослідників. Зокрема, йдеться про роботи О.С. Можаєва, І.А. Рябініна, Г.М. Черкесова та ін. Проте питання захисту інформації в умовах автоматизації обліку та облікових процесів, впровадження нових програмних продуктів з однієї сторони та зростання ризиків і загроз збереження їх цілісності через можливі кібератаки з іншої, - потребують подальших досліджень.

Метою статті є виявлення проблем і встановлення тенденцій здійснення бухгалтерського обліку та фінансової звітності на засадах автоматизації та обґрунтування вирішення проблем комп'ютеризації облікових процесів, забезпечення інформаційної безпеки підприємств та управління нею на перспективу.

Виклад основного матеріалу дослідження. Впровадження автоматизації та комп'ютеризації бухгалтерського обліку й фінансової звітності на підприємствах національного господарства України всіляко сприяє підвищенню їх конкурентоспроможності, удосконаленню діяльності та управління розвитком на засадах безпеки. Воно значно зменшує адміністративні витрати, підвищує ефективність роботи підрозділів бухгалтерії, контролінгу, фінансово-аналітичної служби. Так, найбільш відома та впроваджувана програма «1-С: Підприємство» значно спрощує реєстрацію та ведення господарських операцій підприємствами, які займаються виробничою діяльністю.

Програма «Бест-Звіт» призначена для автоматизації процесів підготовки, подання, прийняття, контролю, збереження, обробки та аналізу документів підприємствами, що звітують керівним державним органам, подання звітів їм або контролюючим державним установам. Її функціональні можливості, як і попередньої, справляють велике враження у контексті удосконалення складання фінансової звітності [1, с. 195]. Зокрема, програма охоплює бази основних документів, що постійно поповнюються. Вона дозволяє вести реєстр та комплект форм звітності як за типовими зразками, так і орієнтованими на підприємства різних видів діяльності із можливістю створювати й коригувати власні комплекти форм звітності; забезпечує перевірку коректності заповнення звітних документів, формування пакетів електронної звітності для передачі в автоматизоване робоче місце збору і обробки.

Також програма має можливості обробки й аналізу інформації, яку містять звітні документи за допомогою вбудованого генератора звітів і засобами Windows (Word, Excel). Наявний модуль «Бухгалтерський календар» з функціями планувальника автоматично співставляється з комплектом форм звітності та сплати податків. Підключення групи первинної документації означає, що бланки платіжного доручення, податкової накладної, посвідчення про відрядження тощо завжди наготові. Сервісні функції автоматизованої системи означають: наявність засобів адміністрування системи і розподілу доступу; авторизацію доступу за ім'ям та паролем користувача; наявність засобів управління резервними копіями баз даних; можливість прийняття пакетів звітності в електронному вигляді – файлів; можливість автоматичної підстановки значень реквізитів з підпорядкованих форм до головних у процесі введення та використання інформації.

Крім цього, автоматично відбувається перевірка пакетів звітності, реєстрація її форм при введенні або прийнятті пакетів в електронному вигляді. Отже, програма «Бест-Звіт» має дуже високі операційні переваги. У неї висока швидкість в роботі, введення інформації в первинний документ проводиться на робочій станції. Також відзначається висока технологічна надійність, стійкість відносно відмов і збоїв. Якщо такі випадки відбуваються, то це не супроводжується руйнуванням баз даних [2, с. 60]. Простота установки й експлуатації не передбачає необхідність наявності в штаті фахівця-адміністратора бази даних. Таким чином, автоматизована система формування звітної обліково-фінансової документації практично виключає можливість допущених помилок, береже робочий час, що позитивно відображається на безпеці суб'єктів господарювання.

Однак при наявності таких безсумнівних переваг перед підприємствами виникають нові проблеми власне інформаційної безпеки. Це питання захисту інформації від несанкціонованого втручання; юридичної доказовості електронних первинних документів і т.п. Також можливими є ризики втрати або псування інформації під час вимкнення електроенергії; небезпека проникнення комп'ютерних вірусів, зламу облікової інформації, кібератак тощо.

В сучасних умовах господарювання проблеми інформаційної безпеки підприємств за наявності автоматизованого бухгалтерського обліку й обліково-фінансової звітності розглядаються теоретиками та практиками кількох галузей знань: управлінцями, юристами, представниками служби безпеки, фахівцями інформаційних мереж, бухгалтерами, фінансистами. Надійний захист інформації в розроблюваних і функціонуючих системах обробки даних може бути ефективним, якщо він буде надійним на всіх об'єктах і в усіх елементах системи, які можуть бути піддані загрозам та ризикам.

У зв'язку з цим для створення засобів захисту важливо визначити природу загроз, форми і шляхи їх можливого прояву і здійснення, перелік об'єктів та елементів, які, з одного боку, можуть бути піддані (побічно або безпосередньо) загрозам з метою порушення захищеності інформації, а з іншого – можуть бути досить

чітко локалізовані для організації ефективного захисту інформації. При проведенні дослідних робіт в цьому напрямі необхідно розмежувати два класи ризиків: один – для автономних персональних комп'ютерів і автономних комп'ютерних мереж; інший – для систем, що мають вихід у великі мережі, включаючи Інтернет.

У спеціальній літературі під об'єктом інформаційної безпеки розуміється такий структурний компонент автоматизації обліку та звітності, в якому перебуває або може перебувати підлягаюча захисту інформація, а під елементом захисту – сукупність даних, яка може містити підлягаючі захисту відомості [3, с. 127]. Практика показує, що інформація в процесі введення, зберігання, обробки, виведення і передачі піддається різним випадковим впливам, в результаті яких на апаратному рівні відбуваються фізичні зміни в абстрактних формах її представлення. Якщо в якомусь чи в якихось розрядах цифрового коду, що несе інформацію, відбулося інвертування двійкового знаку (з 1 на 0 або навпаки) і воно не виявлено спеціальними апаратними засобами функціонального контролю, то при подальшій обробці інформації або буде отриманий невірний результат, або повідомлення попрямує за помилковою адресою, або відбудуться інші небажані події (руйнування, модифікація, витік інформації та ін.)

На програмному рівні в результаті випадкових впливів може відбутися зміна алгоритму обробки інформації на непередбачений і, як наслідок цього, – припинення або модифікація облікового процесу, в результаті якого знову ж можливі руйнування або витік інформації (при переплутуванні, наприклад, адресата). Причинами випадкових впливів при функціонуванні комп'ютерних систем можуть бути: відмови і збої апаратури в разі її неякісного виконання і фізичного старіння; перешкоди в каналах і на лініях зв'язку від впливу зовнішнього середовища; аварійні ситуації (пожежа, повінь, вихід з ладу електроживлення та ін.); помилки і прорахунки розробників і виробників ПК; алгоритмічні і програмні помилки, помилки людини при роботі з ПК.

Зловмисні чи навмисні загрози – результат впливу людини на об'єкти і процеси з найрізноманітніших причин (матеріальний інтерес, бажання нашкодити, небажання працювати, розвага із самоствердженням своїх здібностей й ін.). В якості об'єктів забезпечення інформаційної безпеки в системах обробки облікових та фінансових даних у таких випадках можна виділити наступні: термінали користувачів (персональні комп'ютери, робочі станції, мережі); термінал адміністратора мережі або груповий абонентський вузол; вузол зв'язку; засоби відображення інформації; засоби документування інформації; комп'ютерний зал і сховище носіїв інформації; зовнішні канали зв'язку та мережеве обладнання; накопичувачі та носії інформації.

У відповідності з наведеним вище визначенням в якості елементів захисту виступають блоки (порції, масиви, потоки та ін.) інформації в об'єктах захисту. Це дані і програми в основній пам'яті комп'ютера; дані і програми на зовнішньому носії або гнучкому і жорсткому дисках; дані, відображувані на екрані монітора; дані, що виводяться на принтер при автономному та мережевому використанні ПК; пакети даних, що передаються по каналах зв'язку; дані, що розмножуються (тиражовані) за допомогою копіювально-розмножувального устаткування; паролі й пріоритети зареєстрованим користувачам; службові інструкції по роботі з комплексами завдань; архіви даних і програмне забезпечення та ін.

Необхідно зазначити, що доступ до об'єктів та елементів захисту інформації теоретично і практично можливий для двох категорій осіб: законних користувачів і порушників [4, с. 62]. За відсутності на робочому місці законного користувача або при його недбалому ставленні до своїх посадових обов'язків, при недостатньому захисті інформації кваліфікований порушник може здійснити шляхом введення відповідних запитів (команд) несанкціонований доступ до інформації.

При досить вільному доступі в приміщеннях, де встановлені засоби, можна візуально спостерігати інформацію на засобах відображення і документування, а також викрасти носії з інформацією або зняти з них копію. При безконтрольною завантаженні в комп'ютер програми порушник може модифікувати облікові та звітні дані й алгоритми, ввести шкідливу програму типу «троянський кінь», за допомогою якої згодом він може реалізовувати потрібні для себе функції.

Особливо небезпечна ситуація, коли порушником є користувач комп'ютерної системи, що має, згідно своїм функціональним обов'язкам, законний доступ до однієї частини інформації, але звертається до іншої за межами своїх повноважень. Несанкціонований доступ до інформації може відбуватися під час технічного обслуговування (профілактики або ремонту) комп'ютерів за рахунок прочитання інформації на машинних та інших носіях, незважаючи на її видалення (стирання) користувачем звичайними методами. Інший спосіб – прочитання інформації з носія під час його транспортування без охорони всередині об'єкта або регіону.

Сучасні засоби обчислювальної техніки базуються на широкому застосуванні інтегральних схем. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, а це, в свою чергу, призводить до виникнення в ланцюгах живлення, в ефірі, в близько розташованої апаратурі і т.п. різних електромагнітних полів і наведень, які за допомогою спеціальних засобів можна трансформувати в оброблювану інформацію [5, с. 127]. Причому, із зменшенням відстані між приймачем порушника та апаратними засобами імовірність такого роду знімання і розшифровки інформації збільшується.

Несанкціоноване ознайомлення з інформацією підрозділяється на пасивне й активне. У першому випадку не відбувається порушення інформаційних ресурсів. Порушник лише отримує можливість розкривати зміст повідомлень, використовуючи це надалі в своїх корисливих цілях. У другому випадку порушник може вибірково змінити, знищити, переупорядкувати й перенаправити повідомлення, затримати і створити підроблені повідомлення та ін. Для забезпечення безпеки інформації в особистих комп'ютерах і, особливо, в офісних системах та комп'ютерних мережах проводяться різні заходи, що об'єднуються поняттям

інформаційна безпека. Інформаційна безпека – це сукупність організаційних (адміністративних) та технологічних заходів, програмно-технічних засобів, правових та морально-етичних норм, спрямованих на протидію загрозам порушників з метою зведення до мінімуму можливого збитку користувачам і власникам автоматичних систем обліку й фінансової звітності.

На практиці при формуванні інформаційної безпеки підприємств і організацій склалися два підходи: фрагментарний та комплексний. У першому випадку заходи щодо захисту спрямовуються на протидію цілком певним загрозам при суворо визначених умовах, наприклад, обов'язкова перевірка носіїв антивірусними програмами, застосування криптографічних систем шифрування і т.д. При комплексному підході різні заходи протидії загрозам об'єднуються, формуючи так звану архітектуру безпеки автоматизованих систем обліку й фінансової звітності [6, с. 108]. Вивчення й аналіз практики функціонування систем обробки даних і комп'ютерних мереж показали, що існує досить багато можливих напрямів витоку інформації та шляхів несанкціонованого доступу до неї в системах та мережах. Це перехоплення електронних випромінювань; примусове електромагнітне опромінення (підсвічування) ліній зв'язку; дистанційне фотографування; перехоплення акустичних хвильових випромінювань.

Також йдеться про розкрадання носіїв інформації і виробничих відходів систем обробки даних; зчитування інформації з масивів інших користувачів; копіювання носіїв інформації і файлів з подоланням заходів захисту. Може бути використана модифікація програмного забезпечення шляхом виключення або додавання нових функцій; здійснене використання недоліків операційних систем і прикладних програмних засобів; незаконне підключення до апаратури та ліній зв'язку, в тому числі в якості активного ретранслятора;зловмисний вивід з ладу механізмів захисту. Фіксуються випадки маскування під зареєстрованого користувача і присвоєння собі його повноважень; введення нових користувачів; впровадження комп'ютерних вірусів. Крім того, система захисту не повинна допускати, щоб зловмисник міг зняти з себе відповідальність за формування помилкової або руйнування облікової інформації.

Враховуючи важливість, масштабність і складність вирішення проблеми збереження та безпеки інформації, рекомендується розробляти архітектуру безпеки в декілька етапів: аналіз можливих загроз; розробка систем безпеки; реалізація систем; супровід систем. Необхідно зауважити, що на конкретному об'єкті і в конкретній системі обробки даних з усього різноманіття загроз і можливих ризиків слід, насамперед, вибрати найбільш ймовірні, а також ті, які можуть завдати найбільш суттєвий збиток. Алгоритм розробки систем інформаційної безпеки підприємств і організацій в умовах автоматизації бухгалтерського обліку й обліково-фінансової звітності передбачає використання різних заходів організаційно-адміністративного, технічного, програмного, технологічного, нормативно-правового, морально-етичного характеру та ін.

Організаційно-адміністративні засоби формування інформаційної безпеки зводяться до регламентації доступу до інформаційних й обчислювальних ресурсів, функціональних процесів і систем обробки даних, до регламентації діяльності персоналу та ін. Їх мета – найбільшою мірою ускладнити або виключити можливість реалізації загроз безпеці. Технічні засоби захисту покликані створити певне фізично замкнуте середовище навколо об'єкта й елементів захисту. У цьому випадку використовується установка засобів фізичної перешкоди захисного контуру приміщень, де ведеться обробка інформації - кодові замки; охоронна сигналізація – звукова, світлова, візуальна без запису і з записом на відеоплівку.

Програмні засоби і методи захисту активніше і ширше за інших застосовуються в системах інформаційної безпеки в персональних комп'ютерах та комп'ютерних мережах, реалізуючи такі функції захисту, як розмежування і контроль доступу до ресурсів; реєстрація та аналіз протікають процесів, подій, користувачів; запобігання можливих руйнівних впливів на ресурси; криптографічний захист інформації; ідентифікація і аутентифікація користувачів і процесів та ін.

В даний час найбільшу питому вагу в цій групі заходів у системах обробки обліково-звітної інформації складають спеціальні пакети програм або окремі програми, які включаються до складу програмного забезпечення з метою реалізації завдань щодо захисту інформації. Технологічні засоби інформаційної безпеки – це комплекс заходів, які органічно вбудовуються в технологічні процеси перетворення даних. Серед них найбільш поширеними є створення архівних копій носіїв; ручне або автоматичне збереження оброблюваних файлів у зовнішній пам'яті комп'ютера; реєстрація користувачів комп'ютерних засобів у журналах; автоматична реєстрація доступу користувачів до тих або інших ресурсів; розробка спеціальних інструкцій щодо виконання всіх технологічних процедур та ін. [7, с. 264].

До нормативно-правових і морально-етичних заходів забезпечення інформаційної безпеки підприємств відносяться діючі в країні закони, нормативні акти, що регламентують правила поводження з інформацією та відповідальність за їх порушення. Це етичні норми ділової поведінки, корпоративної культури, розробка й дотримання яких сприяє збереженню та зміцненню інформаційної безпеки. Тільки спільне застосування всього арсеналу засобів забезпечення алгоритмів автоматизації облікової й звітної діяльності, програмної, технічної, технологічної та інших складових безпеки підприємств дозволяє досягати високої якості й корисності автоматичних програм обліку й звітності, баз обліково-фінансових даних, потрібних для їх подальшого використання в системах управління й прийняття управлінських рішень.

Висновки. Впровадження автоматизованих систем і програм здійснення бухгалтерського обліку й формування обліково-фінансової звітності є вагомим чинником підвищення ефективності функціонування вітчизняних підприємств. При цьому підвищується безпека функціонування підприємств на основі більшої

точності й неупередженості використовуваної інформації, значного скорочення їх витрат на обліково-аналітичні процеси. Проте через специфіку автоматизації й комп'ютеризації (під'єднання до більш глобальних мереж, використання типових програм та показників обліку тощо) збільшується відкритість інформаційних систем, зростають загрози комерційній таємниці та ризики конкурентоспроможної діяльності загалом. Це актуалізує значимість забезпечення та подальшого удосконалення інформаційної безпеки підприємств і організацій на перспективу.

При цьому альтернатив подальшій дигіталізації або оцифровуванню всіх сторін підприємницької діяльності не існує. Отже, забезпечення й підвищення ефективності функціонування, конкурентоспроможності й безпеки підприємств на перспективу має здійснюватися на основі подальшого удосконалення програмних розробок з обліку і звітності та їх захисту від будь-яких видів несанкціонованого доступу.

Список використаних джерел

1. Євдокимов В. В. Особливості впровадження комп'ютерних систем бухгалтерського обліку на великих підприємствах // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2009. № 1(13). С. 193-202. URL : http://eztuir.ztu.edu.ua/1796/1/20.pdf

2. Ігнатенко М. М. Развитие системы бухгалтерского учёта и отчетности в бюджетных организациях в соответствие с международными стандартами // Економіка та держава: наук. жур. 2017. № 4. С. 21-23.

3. Безродна Т. М. Обліково-аналітичне забезпечення управління підприємством: визначення сутності поняття // Вісник Східноукраїнського національного університету ім. В. Даля. Луганськ, 2008. № 10, ч. 2. С. 58-62.

4. Житна І. П., Садовніков О. А. Сучасні технології удосконалення системи автоматизації обліку та управління виробництвом // Управлення розвитком. 2010. № 3. С. 126-128.

5. Мармуль Л. О., Коваль С. В., Круковська О. В. Перспективи розвитку національних стандартів бухгалтерського обліку та фінансової звітності // Вісник Бердянського університету менеджменту і бізнесу. Бердянськ: Видавець Ткачук О.В., 2017. № 4 (40). С. 89-92.

6. Гнилицька Л. В. Обліково-аналітична інформація як визначальний чинник забезпечення економічної безпеки суб'єктів господарювання // Вісник Східноукраїнського національного університету імені Володимира Даля. Луганськ: СНУ ім. В.Даля, 2011. № 3 (157). С. 57-65.

7. Боголіб Т. М. Дотації місцевим бюджетам як інструмент фінансового вирівнювання // Економічний вісник університету. 2016. Вип. 29/1. С. 282-287.

8. Клименко О. В. Інформаційні системи і технології в обліку: [навч. посіб.] Київ : Центр учбової літератури, 2008. 320 с.

9. Леваєва Л. Ю., Кучеренко С. Ю. Необхідність забезпечення прозорості бюджетного процесу // Економічний вісник університету. 2017. Вип. 33 (1). С. 350-354.

10. Домашенко С. В. Інформаційні технології в управлінні підприємством: електронний документообіг // Збірник наукових праць Таврійського державного агротехнологічного університету. Економічні науки. 2013. № 2 (3). С. 103-112.

11. Озеран А. В. Теорія та методологія формування фінансової звітності підприємств: [монографія]; ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана». Київ : КНЕУ, 2015. 471 с.

12. Євтушенко Н. М., Виноградня В. М. Управління акумуляцією та витратами бюджетних коштів // Економічний вісник університету. 2017. Вип. 33 (1). С. 314-327.

References

1. Yevdokymov, V. V. (2009). Osoblyvosti vprovadzhennya komp'yuternykh system bukhhalters'koho obliku na velykykh pidpryyemstvakh [Features of introduction of computer accounting systems at large enterprises]. Problemy teoriyi ta metodolohiyi bukhhalters'koho obliku, kontrolyu i analizu, 1(13), 193-202 URL : http://eztuir.ztu.edu.ua/1796/1/20.pdf (in Ukr.).

2. Ígnatenko, M. M. (2017). Razvitiye sistemy bukhgalterskogo uchota i otchetnosti v byudzhetnykh organizatsiyakh v sootvetstviye s mezhdunarodnymi standartami [Development of the system of accounting and reporting in budget organizations in accordance with international standards]. Ekonomika ta derzhava, 4, 21-23 (in Ukr.).

3. Bezrodna, T. M. (2008). Oblikovo-analitychne zabezpechennya upravlinnya pidpryyemstvom: vyznachennya sutnosti ponyattya [Accounting and analytical support for enterprise management: the definition of the essence of the concept]. Visnyk Skhidnoukrayins'koho natsional'noho universytetu im. V. Dalya, 10, 58-62 (in Ukr.).

4. Zhytna, I. P. & Sadovnikov, O. A. (2010). Suchasni tekhnolohiyi udoskonalennya systemy avtomatyzatsiyi obliku ta upravlinnya vyrobnytstvom [Modern technologies of improvement of the system of automation of accounting and production management]. Upravlennya rozvytkom, 3, 126-128 (in Ukr.).

5. Marmul', L. O., Koval', S. V. & Krukovs'ka O. V. (2017). Perspektyvy rozvytku natsional'nykh standartiv bukhhalters'koho obliku ta finansovoyi zvitnosti [Prospects for the development of national accounting and financial reporting standards]. Visnyk Berdyans'koho universytetu menedzhmentu i biznesu, 4 (40), 89-92 (in Ukr.).

6. Hnylyts'ka, L. V. (2011). Oblikovo-analitychna informatsiya yak vyznachal'nyy chynnyk zabezpechennya ekonomichnoyi bezpeky sub'yektiv hospodaryuvannya [Accounting and analytical information as a determinant of economic security of economic entities]. Visnyk Skhidnoukrayins'koho natsional'noho universytetu imeni Volodymyra Dalya, 3(157), 57-65 (in Ukr.).

7. Boholib, T. M. (2016). Dotatsiyi mistsevym byudzhetam yak instrument finansovoho vyrivnyuvannya [Grants to local budgets as a tool for financial equalization]. Ekonomichnyy visnyk universytetu, 29/1, 282-287 (in Ukr.).

8. Klymenko, O. V. (2008). Informatsiyni systemy i tekhnolohiyi v obliku [Information systems and technologies in accounting]. Kyyiv: Tsentr uchbovoyi literatury (in Ukr.).

9. Levayeva, L. Yu. & Kucherenko, S. Yu. (2017). Neobkhidnist' zabezpechennya prozorosti byudzhetnoho protsesu [The need to ensure the transparency of the budget process]. Ekonomichnyy visnyk universytetu, 33 (1), 350-354 (in Ukr.).

10. Domashenko, S. V. (2013). Informatsiyni tekhnolohiyi v upravlinni pidpryyemstvom: elektronnyy dokumentoobih [Information technology in enterprise management: electronic document flow]. Zbirnyk naukovykh prats' Tavriys'koho derzhavnoho ahrotekhnolohichnoho universytetu, 2(3), 103-112 (in Ukr.).

11. Ozeran, A. V. (2015). Teoriya ta metodolohiya formuvannya finansovoyi zvitnosti pidpryyemstv [Theory and methodology of formation of financial reporting of enterprises]. Kyyiv: KNEU (in Ukr.).

12. Yevtushenko, N. M. & Vynohradnya, V. M. (2017). Upravlinnya akumulyatsiyeyu ta vytratamy byudzhetnykh koshtiv [Accumulation management and budget expenditures]. Ekonomichnyy visnyk universytetu, 33 (1), 314-327 (in Ukr.).

ДАНІ ПРО АВТОРА

Ігнатенко Микола Миколайович, доктор економічних наук, доцент, завідувач кафедри економіки
ДВНЗ «Переяслав-Хмельницький ДПУ імені Григорія Сковороди»
e-mail: professorignatenko@ukr.net

Сарапіна Ольга Андріївна, доктор економічних наук, професор, завідувач кафедри обліку, аудиту і оподаткування
Херсонський національний технічний університет
e-mail: o_sarapina@ukr.net

ДАННЫЕ ОБ АВТОРЕ

Игнатенко Николай Николаевич, доктор экономических наук, доцент, заведующий кафедрой экономики
ГВУЗ «Переяслав-Хмельницкий ГПУ имени Григория Сковороды»
e-mail: professorignatenko@ukr.net

Сарапина Ольга Андреевна, доктор экономических наук, профессор, заведующий кафедрой учета, аудита и налогообложения
Херсонский национальный технический университет
e-mail: o_sarapina@ukr.net

DATA ABOUT THE AUTHOR

Ignatenko Nikolay Nikolaevich, Doctor of Economics, Associate Professor, Head of the Department of Economics
Pereiaslav-Khmelnytsky Hrygorii Skovoroda State Pedagogical University
e-mail: professorignatenko@ukr.net

Sarapina Olga Andreevna, Doctor of Economics, Professor, Head of the Department of Accounting, Audit and Taxation
Kherson National Technical University
e-mail: o_sarapina@ukr.net

УДК 005.21:005.7:658 https://doi.org/10.31470/2306-546X-2018-38-53-63

НАУКОВО-ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ СУТНОСТІ СТРАТЕГІЧНИХ ЗМІН НА ПІДПРИЄМСТВІ

Краснорyцький О.О.
Гринь Є.Л.
Власенко Т.А.

Актуальність теми дослідження. *Сучасне бізнес-середовище характеризується низкою властивостей, які обумовлюють характер діяльності суб'єктів господарювання. Вплив всіх цих характеристик є постійним і пролонгованим у часі, але прогнозування особливостей цього впливу залишається достатньо складним для управління завданням, що визначає актуальність дослідження сутності стратегічних змін та підприємстві та методології їх планування та реалізації.*

Постановка проблеми. *Визначення напрямів діяльності підприємства у довгостроковій перспективі традиційно відноситься до сфери стратегічного управління. А високий рівень динаміки зовнішнього та внутрішнього середовища вимагає розробки та впровадження сучасної концепції стратегічних змін. Незважаючи на важливість та нагальність вирішення даного завдання становлення*