DOI: https://doi.org/10.32782/2524-0072/2021-33-34

УДК 657:004.056

ЗАХИСТ ІНФОРМАЦІЇ ТА ПОПЕРЕДЖЕННЯ ШАХРАЙСТВА У СФЕРІ ОБЛІКОВОГО ЗАБЕЗПЕЧЕННЯ

PROTECTION OF INFORMATION AND FRAUD PREVENTION IN THE FIELD OF ACCOUNTING SUPPORT

Гаркуша Сергій Анатолійович
кандидат економічних наук, доцент,
Сумський національний аграрний університет
ORCID: https://orcid.org/0000-0002-2043-1217

Harkusha Serhii
Sumy National Agrarian University

Стаття присвячена дослідженню захисту інформації та попередження шахрайства у сфері облікового забезпечення. Для забезпечення інформаційної безпеки підприємства повинні бути створені такі умови, за яких використання, втрата або спотворення будь-якої інформації працівниками або зовнішніми особами не призведуть до виникнення загроз переривання діяльності. Досліджено питання доступу до інформації в програмі «BAS: Бухгалтерія» та визначення профілів груп доступу. Виділено класифікації існуючих загроз бухгалтерської інформації: штучні і природні; потенційні. Запропоновано для захисту бази даних застосувати наступні методи: не бажано встановлювати оновлення програми самостійно, завантажувати їх із підозрілих сайтів; рекомендується не тримати бухгалтерську програму на власному комп'ютері, для цього краще використовувати онлайн-сервіс, який забезпечує захист даних та містить усі необхідні оновлення.

Ключові слова: інформація, шахрайство, облікове забезпечення, кібербезпека.

Статья посвящена исследованию защиты информации и предупреждению мошенничества в области учетного обеспечения. Для обеспечения информационной безопасности предприятия должны быть созданы условия, при которых использование, утрата или искажение какой-либо информации работниками или внешними лицами не приведут к возникновению угроз прерывания деятельности. Исследованы вопросы доступа к информации в программе «BAS: Бухгалтерия» и определения профилей групп доступа. Выделены классификации существующих угроз бухгалтерской информации: искусственные и естественные; потенциальные. Предложено для защиты базы данных применить следующие методы: не желательно устанавливать обновление программы самостоятельно, загружать их с подозрительных сайтов; рекомендуется не держать бухгалтерскую программу на собственном компьютере, для этого лучше использовать онлайн-сервис, обеспечивающий защиту данных и содержащий все необходимые обновления.

Ключевые слова: информация, мошенничество, учетное обеспечение, кибербезопасность.

The article is devoted to the study of information security and fraud prevention in the field of accounting. To ensure information security of the enterprise, conditions must be created in which the use, loss or distortion of any information by employees or external persons will not lead to threats of business interruption. The issues of access to information in «BAS: Accounting» and definition of access group profiles have been studied. The classification of existing threats to accounting information is highlighted: artificial and natural; potential threats. It is suggested to use the following methods to protect databases: it is not desirable to install updates of the program on your own, download them from suspicious sites; it is recommended not to keep the accounting program on your own computer, it is better to use an online service that provides data protection and contains all the necessary updates. It is concluded that you should provide means to protect the accounting data on removable media: after removing the device (SSD or hard drive), you must lock it in a cabinet or better in a safe; external media – memory cards, flash drives, removable disks – must also be kept locked up; if you carry removable media, you should choose one in which the information is protected by a PIN or password; you can not leave electronic digital signature (EDS) in the card reader for a long time unattended. To avoid the risk of theft or failure of office equipment, it is recommended to use cloud services. They allow you to work with the program via the Internet, and besides there is no need to buy the program, it simply needs to be rented and connected via an encrypted channel. The basic rule of information protection is to limit the rights and opportunities of users, as well as control over them when using information systems, the less rights the user has when working

with information system, the less chance of leakage or damage information by malice or negligence. Regarding the limitations of the study, it should be recognized that the study focused solely on information protection and the prevention of accounting fraud.

Keywords: information, fraud, accounting, cybersecurity.

Постановка проблеми. Будь-яке підприємство має використовувати сучасні інформаційні досягнення, у тому числі стосовно ведення бухгалтерського обліку. Інформаційну безпеку підприємства розглядають як комплексне рішення, адже треба враховувати усі можливі небезпеки. Основні загрози, з якими регулярно стикається суб'єкт господарювання, це поширення вірусів, злом, порушення цілісності бази даних та крадіжка або знищення конфіденційних відомостей. Подібні махінації можуть проводити як випадкові кібер-злочинці, так і конкуренти. Також небезпека походить від непередбачених ситуацій – наприклад, проблеми з електроживленням, за таких умов вдаються до резервування важливої інформації.

Для забезпечення інформаційної безпеки підприємства повинні бути створені такі умови, за яких використання, втрата або спотворення будь-якої інформації, у тому числі бухгалтерської та фінансової, працівниками або зовнішніми особами не призведуть до виникнення загроз переривання діяльності.

Аналіз останніх досліджень і публікацій. Значний внесок у розвиток теоретичних, методичних, методологічних та прикладних аспектів захисту інформації та попередження шахрайства у сфері облікового забезпечення зробили Вітер С.А., Григоревська О.О., Ілляшенко К.В., Попівка Ю.М., Світлишин І.І., Скрипник М.І. та ін.

Проблем теорії та методології захисту інформації та попередження шахрайства у сфері облікового забезпечення приділяється достатня увага в роботах зарубіжних і українських вчених. Однак більшість вітчизняних розробок щодо вдосконалення захисту інформації та попередження шахрайства у сфері облікового забезпечення, на практиці України слабо впроваджуються, що пов'язано з відсутністю економічної культури і кваліфікації власника підприємства, керівного персоналу і бухгалтерської служби.

Швидке вдосконалювання інформатизації, її проникнення в усі сфери суспільства та держави викликали, крім безсумнівних переваг, і появу низки суттєвих проблем. Однією з них стала необхідність захисту підприємства від імовірних інформаційних небезпек [1, с. 179].

Останніми роками в Україні почастішали кібератаки, які, серед іншого, зумовлені національними особливостями господарювання, такими як брак належної законодавчої бази, велика питома вага підприємств, що використовують неліцензійні бухгалтерські програмні продукти, нехтування правилами захисту автоматизованих робочих місць, брак у спеціалістів з бухгалтерського обліку знань з основ кібербезпеки тощо [2, с. 155].

Кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями і це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства. Зрозуміло, що неможливо досягти стовідсоткової безпеки захисту облікових даних, проте індивідуальна відповідальність кожного працівника бухгалтерської служби є найпершим і найпростішим фактором, який сприяє захисту цінної облікової інформації [3, с. 502].

Контроль несанкціонованого доступу до бухгалтерських записів є важливим компонентом внутрішнього контролю. Політика доступу і паролів, шифрування, цифрові підписи, блокування дисків, міжмережеві екрани і цифрові сертифікати є прикладами заходів контролю, які повинні бути ідентифіковані, задокументовані, повідомлені і піддані перевірці при оцінці ефективності контролю [4, с. 101].

Виділення невирішених раніше частин загальної проблеми. Проблема захисту є багатоплановою і комплексною і охоплює низку важливих завдань. Проблеми інформаційної безпеки постійно посилюються процесами проникнення в усі сфери суспільства технічних засобів обробки та передачі даних, особливо гостро ця проблема стоїть у галузі фінансових облікових систем. Тому питання захисту інформації та попередження шахрайства у сфері облікового забезпечення потребують додаткового вивчення і дослідження.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження теоретичних засад формування захисту інформації та попередження шахрайства у сфері облікового забезпечення підприємств.

Для вивчення стану та проблем захисту інформації та попередження шахрайства у сфері облікового забезпечення на практиці підприємств використано аналітичний, порівняльний методи дослідження, а також абстрактно-логічні підходи до пошуку та обґрунтування шляхів подолання окреслених проблем.

Виклад основного матеріалу дослідження. Розвиток інформаційних технологій у рази спрощує бухгалтерську роботу, але водночас збільшує ризик втрати конфіденційної інформації або зіткнутися з діями зловмисників. Тому захист даних та підвищення рівня знань бухгалтерів у сфері ІТ є найважливішим завданням.

В основних профілях користувачів важливо передбачити такий набір ролей, який з одного боку, не буде давати надлишкового (небажаного) доступу до функцій і даних програми, а з іншого – буде достатнім для роботи користувачів в межах кола їх задач та обов'язків. Зокрема, в основному профілі слід передбачити ряд допоміжних ролей, які безпосередньо не пов'язані з основною діяльністю користувачів, але, тим не менш, необхідні для неї, а саме: для бухгалтера можливий додатковий доступ до складських операцій, операцій з роздрібної торгівлі в структурних підрозділах та ін.

Контроль за створенням, зміною та видаленням даних у програмі виконується в «Журналі реєстрації». Контролю можуть підлягати наступні події: вхід у програму; вихід із програми; аутентифікація; відмова від аутентифікації.

BAS дозволяє коригувати події доступу до інформації в програмі зі спеціального налаштування «Настройка користувачів і прав».

У «Настройці користувачів і прав» доступна команда «Користувачі», де є можливість ведення списку користувачів, які працюють з програмою та налаштування входу в програму (рис. 1).

«Настройки входу» – призначені для налаштування параметрів входу в програму для користувачів (вимоги до паролю) (рис. 2).

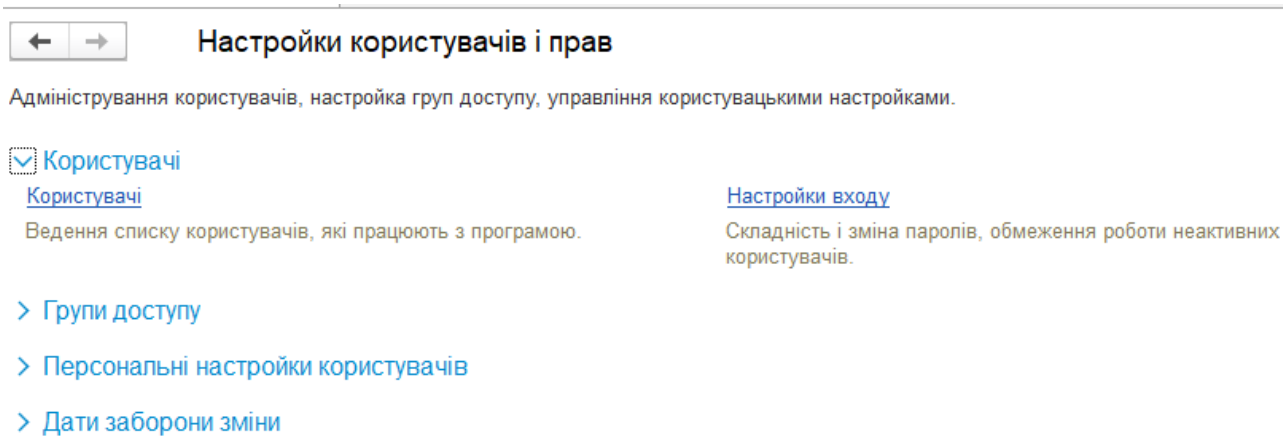

Рис. 1. Розміщення команди «Користувачі», де є можливість ведення списку користувачів, які працюють з програмою та налаштування входу в програму

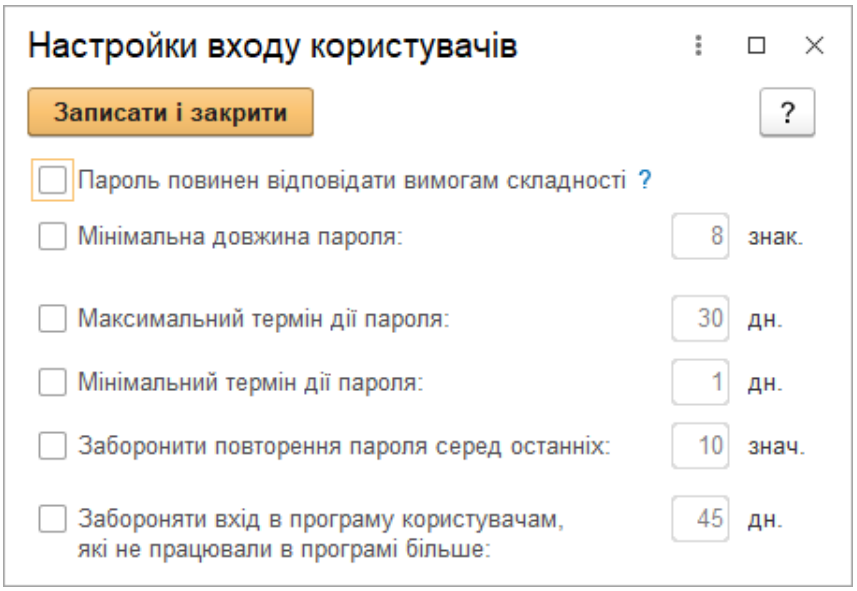

Рис. 2. Екранна форма для налаштування параметрів входу в програму для користувачів

Для захисту від несанкціонованого доступу до програми вимоги до паролю вказують за допомогою відміток:

– «Пароль повинен відповідати вимогам складності» – настройка та контроль складності пароля. Відмітку потрібно робити для того, щоб перевіряти, чи новий пароль має не менше 7 символів, містить будь-які 3 з 4-х типів символів: великі літери, малі літери, цифри, спеціальні символи, не збігається з ім'ям (для входу);

– «Мінімальна довжина пароля» – за замовчуванням 8 знаків;

– «Максимальний термін дії пароля» – термін після першого входу з новим паролем, після якого користувачу потрібно змінити пароль (за замовчуванням – 30 днів);

– «Мінімальний термін дії пароля» – термін після першого входу з новим паролем, протягом якого користувач не може змінити пароль (за замовчуванням – 1 день.

– «Заборонити повторення пароля серед останніх» – за замовчуванням – 10 значень (таким чином, забезпечується контроль повторення паролів);

– «Забороняти вхід в програму користувачам, які не працювали в програмі більше» – строк щодо останньої активності користувача, після якого вхід в програму буде заборонений (за замовчуванням – 45 днів).

Команду «Групи доступу», де є можливість налаштовувати права доступу та шаблони прав доступу, наведено на рисунку 3.

Профілів груп доступу може бути багато і з схожим призначенням, тому передбачена можливість створювати папки для спрощення пошуку потрібного профілю і розуміння принципів їх формування (рис. 4).

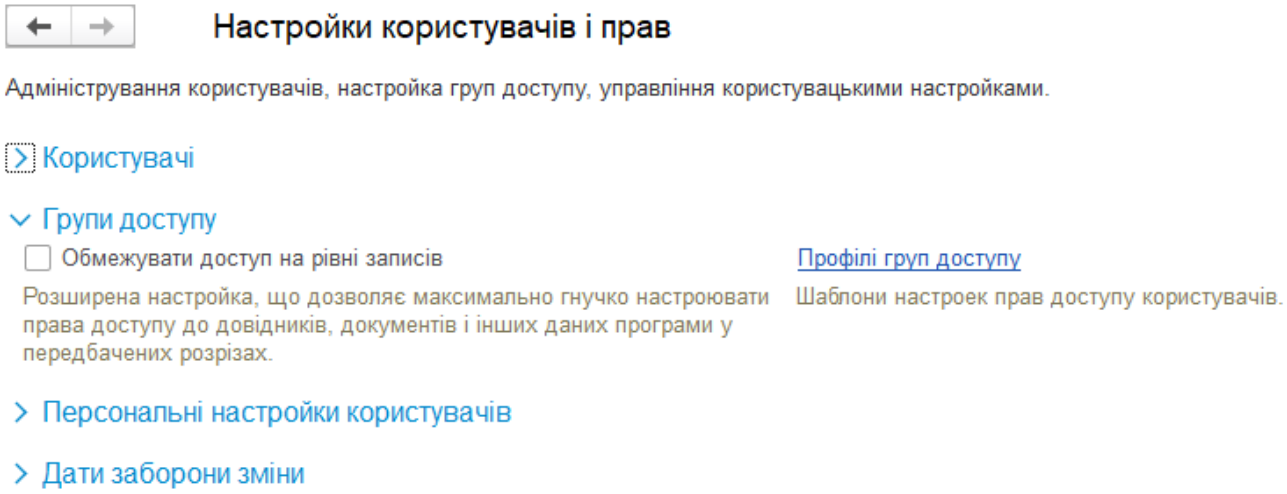

Рис. 3. Команда «Групи доступу», де є можливість налаштовувати права доступу та шаблони прав доступу

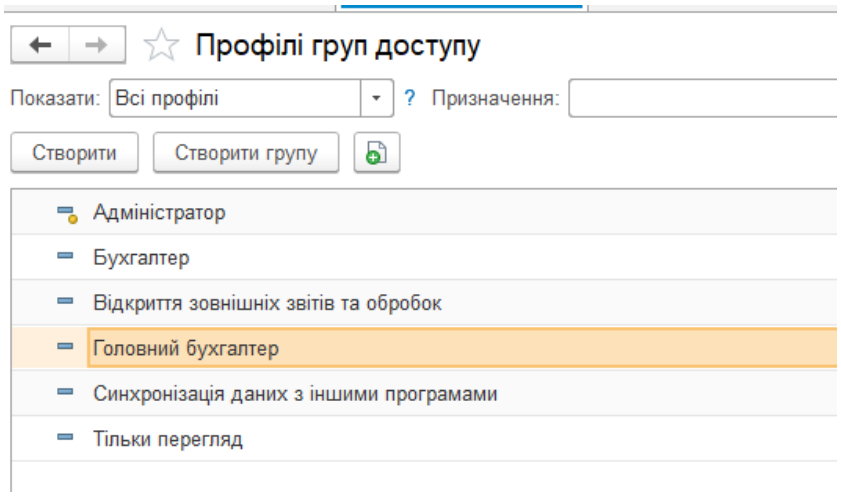

Рис. 4. Зображення профілів груп доступу

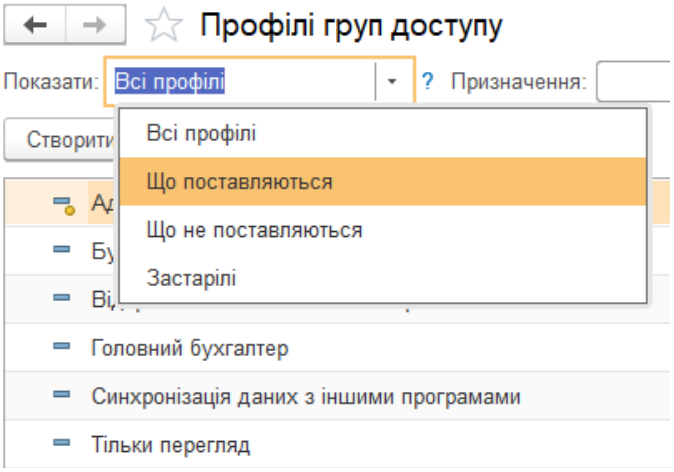

Рис. 5. Варіанти показу профілів груп доступу

За допомогою поля «Показати» можна вивести їх на перегляд (рис. 5).

– «Всі профілі» (за замовчуванням);

– «Що поставляються» – профілі, що входять в поставку програми;

– «Що не поставляються» – профілі, які не входять в поставку програми;

– «Застарілі» – застарілі.

За допомогою поля «Призначення» можна відібрати профілі груп доступу за видами користувачів, для кого вони призначені (рис. 6).

Вказується за допомогою відміток, для кого призначені профілі груп доступу, наприклад, «Користувачі».

Розрізняють основні і додаткові профілі груп доступу (рис. 7).

– основний профіль описує деяку сукупність прав доступу, достатню для виконання в програмі певної ділянки робіт;

– за допомогою додаткових профілів користувачам можуть бути видані будь-які допоміжні права додатково до основного профілю.

Щодо можливих фінансових втрат у системі обліку питання недостатнього захисту інформації стоїть особливо гостро. Неправильне використання бази даних, відсутність необхідної мережевої безпеки – здатне призвести до витоку фінансових відомостей з облікової системи.

Якщо досліджувати кібербезпеку в масштабах держави, то викликами для України у цій сфері, відповідно до «Стратегії кібербезпеки України» затвердженої указом Президента України від 26 серпня 2021 року № 447/2021 [5], є:

– активне використання кіберзасобів у міжнародній конкуренції;

– змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;

– мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано

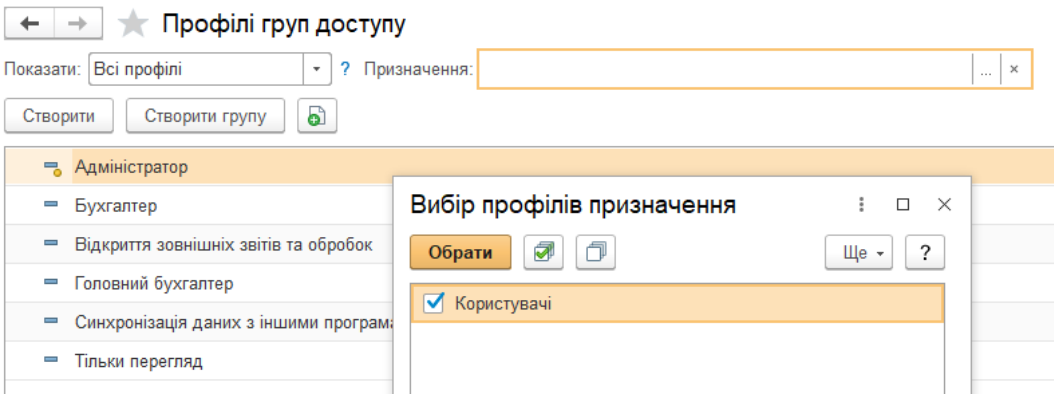

Рис. 6. Обрання профілів призначення

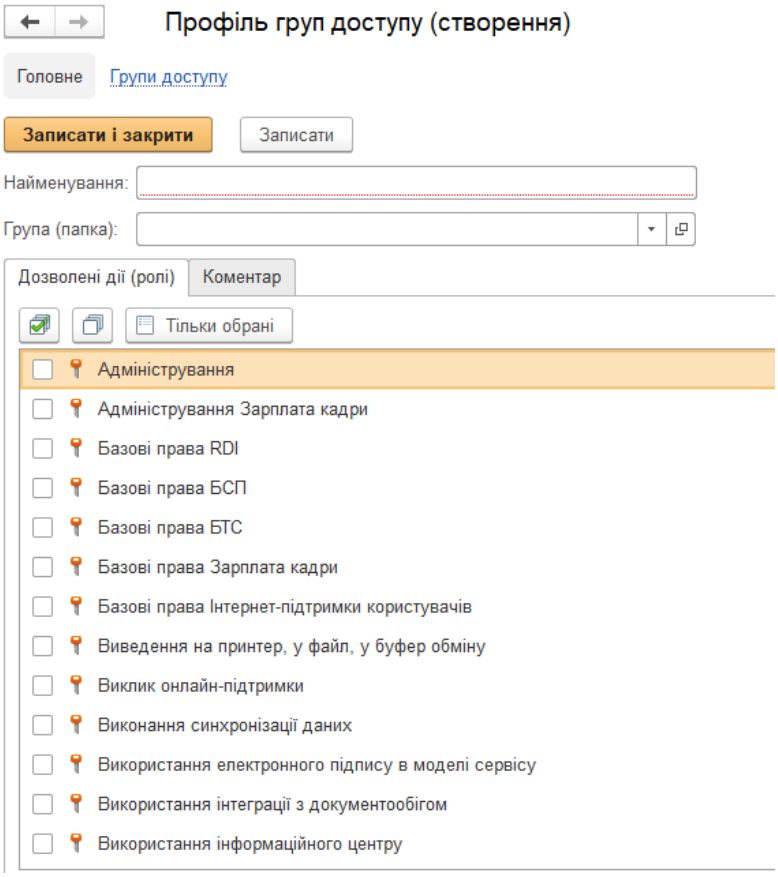

Рис. 7. Створення профілю груп доступу

проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

– вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

– упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Можна виділити такі класифікації існуючих загроз бухгалтерської інформації. Класифікація за ознакою їх виникнення: штучні чи природні.

Природні, чи об'єктивні загрози, тобто незалежні від людини – форс-мажорні обставини, стихійні лиха, повені, і пожежа.

Штучні, чи суб'єктивні загрози, викликані діями чи бездіяльністю співробітників підприємства. Серед них виділяють:

– випадкові загрози – помилки програмного забезпечення, збої в роботі, відмови або повільна робота комп'ютера та систем інформаційних технологій в цілому;

– умисні загрози – неправомірний доступ до інформації, поширення вірусних програм тощо.

Потенційних загроз існує ще більше, варто розібратися, що вони представляють собою, і як можна надійно захистити базу даних.

До файлових баз найпростіше отримати фізичний доступ. Це зумовлено особливостями цього виду баз: необхідно надавати у відкритому доступі файли та конфігурації для всіх користувачів. Теоретично будь-який з користувачів з правом доступу до програми здатний видалити або скопіювати всю інформацію для передачі стороннім особам.

У випадку, якщо сховищем даних виступає СУБД (SQL, PosgreSQL, MS), сервер бухгалтерської програми є сполучною ланкою між СУБД і базою даних. Багато підприємств допрацьовують конфігурацію під свої потреби, в ході якої, нерідко забувають про умови інтернет-безпеки. В результаті особи, у яких є прямий або тимчасовий доступ до системної бази, легко здатні скопіювати інформацію та розпоряджатися нею на свій розсуд.

Загрозу безпеці даних також становлять декілька аспектів, що сприяють несанкціонованому доступу до інформації при її обробці. Іноді такий доступ буває випадковим, але в результаті цінні відомості можуть бути заблоковані, змінені, скопійовані, передані третім особам

Якщо є незаконний доступ до серверного обладнання, то будь-який співробітник підприємства або стороння особа зможе вкрасти або зіпсувати інформацію. Особливо можливості зловмисника зростають, якщо у нього буде прямий доступ до консолі та серверу.

Мережевий обмін інформацією (з корпоративними порталами, банками, іншими програмами) представляє загрозу для даних. У цій сфері не приділяється увага стандартам безпеки, тому зникнення, перехоплення відомостей можливі за короткий час їхньої передачі.

Якщо система інформації підприємства сформована з порушеннями, не відповідає вимогам безпеки, а також не має повноцінної IT-підтримки, це може призвести до занесення в програму шкідливих вірусів, шпигунського програмного забезпечення, численних несанкціонованих доступів до закритої мережі. Все це сприяє тому, що зловмисник без проблем проникає до комерційно цінних відомостей та застосовує їх у корисливих цілях.

Комп'ютер із встановленою бухгалтерською програмою має бути захищений якісним антивірусом. Також рекомендується використовувати мережевий екран – це модуль антивірусу, що аналізує обмін даними між мережею та комп'ютерною технікою.

Зловмисники для виманювання корпоративної інформації найчастіше посилають файли із шкідливими посиланнями. Зазвичай вірусна програма маскується під оновлення, дія її полягає в завантаженні того, що відбувається на комп'ютері, та трансляції на сервер. Таким чином, вся інформація з бази буде у розпорядженні інших осіб, що може спричинити вкрай негативні наслідки для підприємства. Щоб захистити від зловмисників базу даних, можна застосувати наступні методи:

– не бажано встановлювати оновлення програми самостійно, завантажувати їх із підозрілих сайтів;

– рекомендується не тримати бухгалтерську програму на власному комп'ютері, для цього розумніше використовувати онлайн-сервіс, який забезпечує захист даних та містить усі необхідні оновлення.

Для обмеження доступу сторонніх осіб до таємної інформації на бухгалтерському комп'ютері потрібен пароль. У ньому має бути щонайменше 8 знаків, серед яких великі та маленькі латинські літери, а також символи.

Небезпека для даних існує не тільки від світової мережі. З цієї причини варто передбачити засоби захисту бухгалтерських даних на знімних носіях:

– після виймання пристрою (SSD або жорсткого диска), потрібно замикати його в шафі, а краще в сейф;

– носії зовнішні – карти-пам'яті, флешки, знімні диски – також потрібно тримати під замком;

– якщо носити знімний носій із собою, слід вибирати такий, у якому інформація захищена PIN чи паролем;

– не можна залишати ЕЦП у картридері тривалий час без нагляду.

Щоб уникнути ризику злодійства або виходу з ладу оргтехніки, рекомендується використовувати хмарні сервіси. Вони дозволяють вести роботу з програмою через інтернет. До того ж, немає необхідності купувати програму, її просто потрібно орендувати та здійснювати підключення зашифрованим каналом.

Це найефективніший спосіб захистити бухгалтерську базу даних від зовнішніх зазіхань та форс-мажорних обставин. База з інформацією зберігається не на комп'ютері бухгалтера, а на віддалених серверах у приміщеннях без права доступу сторонніх осіб і щоб не трапилося з технікою (поломка, вилучення, крадіжка тощо), цінні відомості будуть надійно захищені та збережені.

Захист конфіденційних даних – це комплексний захід, що вимагає докладного і ретельного підходу. При дотриманні вищезазначених заходів безпеки можна звести до мінімуму ризик загроз та виникнення неприємних інцидентів, пов'язаних із втратою, викривленням або розкраданням інформації.

Висновки. Основним правилом при захисті інформації є обмеження прав та можливостей користувачів, а також контроль над ними під час використання інформаційних систем. Чим менше користувач має прав при роботі з інформаційною системою, тим менший шанс витоку або псування інформації за злим наміром або необережністю.

Що стосується обмежень дослідження, слід визнати, що дослідження було зосереджено виключно на захисті інформації та попередження шахрайства у сфері облікового забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ілляшенко К.В. Інформаційна безпека сучасного бухгалтерського обліку. *Науковий вісник Міжнародного гуманітарного університету.* 2019. Випуск 40. С. 179–183. URL: http://vestnik-econom.mgu.od.ua/journal/2019/40-2019/25.pdf

2. Попівняк Ю.М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *Бізнес Інформ.* 2019. № 8. С. 150–157. URL: https://www.business-inform.net/export_pdf/business-inform-2019-8_0-pages-150_157.pdf

3. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Випуск 11. С. 497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf

4. Скрипник М.І., Григоревська О.О. Організація захисту облікової інформації в умовах забезпечення кібербезпеки. *Наукові записки Національного університету «Острозька академія». Серія «Економіка».* 2020. № 19(47). С. 95–102. DOI: https://doi.org/10.25264/2311-5149-2020-19(47)-95-102

5. 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

REFERENCES:

1. Illiashenko K.V. (2019) Informatsiina bezpeka suchasnoho bukhhalterskoho obliku [Information security of modern accounting]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu – Scientific Bulletin of the International Humanities University*, 40, 179–183. Retrieved from: http://vestnik-econom.mgu.od.ua/journal/2019/40-2019/25.pdf (in Ukrainian)

2. Popivniak Yu.M. (2019) Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii [Cybersecurity and Protection of Accounting Data under Conditions of Modern Information Technology]. *Biznes Inform – Business Inform*, 8, 150–157. Retrieved from: https://www.business-inform.net/export_pdf/business-inform-2019-8_0-pages-150_157.pdf (in Ukrainian)

3. Viter S.A., Svitlyshyn I.I. (2017) Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cyber security of the enterprise]. *Ekonomika i suspilstvo – Economy and society,* 11, 497–502. Retrieved from: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (in Ukrainian)

4. Skrypnyk M.I., Hryhorevska O.O. (2020) Orhanizatsiia zakhystu oblikovoi informatsii v umovakh zabezpechennia kiberbezpeky [Organization of accounting information protection in terms of cyber security]. *Naukovi zapysky Natsionalnoho universytetu «Ostrozka akademiia – Scientific notes of the National University «Ostroh Academy»*, 19(47), 95–102. DOI: https://doi.org/10.25264/2311-5149-2020-19(47)-95-102 (in Ukrainian)

5. Prezydent Ukrainy (2021) Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 «On the Cyber Security Strategy of Ukraine»], 447/2021, August 26. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#Text (in Ukrainian)