Тематична рубрика: **БУХГАЛТЕРСЬКИЙ ОБЛІК, АНАЛІЗ ТА АУДИТ (ЗА ВИДАМИ ДІЯЛЬНОСТІ)**

УДК 657

Гаркуша С.А.

к.е.н., доцент

доцент кафедри бухгалтерського обліку

Сумський національний аграрний університет

ОСОБЛИВОСТІ ЗБЕРІГАННЯ, АРХІВУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ В ПРОЦЕСІ ОРГАНІЗАЦІЇ БУХГАЛТЕРСЬКОГО ОБЛІКУ

FEATURES OF STORAGE, ARCHIVING AND PROTECTION OF INFORMATION AT THE ACCOUNTING ORGANIZATION

У статті розглянуто особливості зберігання, архівування та захисту інформації в процесі організації бухгалтерського обліку. Зроблено групування документів відносно термінів зберігання. Зроблено висновок, що строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. Встановлено вимоги при зберіганні електронних документів. Узагальнено архітектуру архівації документів програмних продуктів. Визначено типи загроз кібербезпеки. Особлива увага повинна бути приділена захисту даних, що містяться в обліковій системі. Специфіка даних в тому, що вони нематеріальні й не існують окремо, тому в будь-якому випадку для їх збереження потрібно робити спеціальні зусилля, щоб вони не зникли разом з носієм. Забезпечення безпеки облікової інформації – досить затратна справа, і не тільки через витрати на закупівлю або установку засобів захисту, але й через те, що важко кваліфіковано визначити межі належної безпеки та забезпечити відповідну безпеку

інформаційної системи. Внутрішньої системи захисту даних недостатньо для запобігання всіх ризиків із витоку конфіденційної інформації.

Ключові слова: *архівування, захист інформації, зберігання інформації, кібербезпека, документ, документообіг, електронний документ.*

В статье рассмотрены особенности хранения, архивирования и защиты информации в процессе организации бухгалтерского учета. Сделано группировки документов относительно сроков хранения. Сделан вывод, что срок хранения электронных документов на электронных носителях информации должен быть не меньше срока, установленного законодательством для соответствующих документов на бумаге. Установлены требования при хранении электронных документов. Обобщена архитектура архивации документов программных продуктов. Определены типы угроз кибербезопасности. Сделан вывод, что особое внимание должно быть уделено защите данных, содержащихся в учетной системе. Специфика данных в том, что они нематериальные и не существуют отдельно, поэтому в любом случае для их сохранения нужно делать специальные усилия, чтобы они не исчезли вместе с носителем. Обеспечение безопасности учетной информации - достаточно затратное дело, и не только из-за расходов на закупку или установку средств защиты, но и потому, что трудно квалифицированно определить границы надлежащей безопасности и обеспечить безопасность информационной системы. Внутренней системы защиты данных недостаточно для предотвращения всех рисков с утечки конфиденциальной информации.

Ключевые слова: *архивирование, защита информации, хранение информации, кибербезопасность, документ, документооборот, электронный документ.*

The ability to protect your information from the third parties and prevent its accidental loss play an important role. Saving of information is very important both for the simple user and for the enterprises. Various devices are used to store electronically dates, some of which are highly reliable. Storing of information is an

essential guarantee of the development of human society, taking knowledge and moving forward. The article discusses the features of storage, archiving and protection of information at the accounting organization. Made a grouping of documents regarding the shelf life. It was concluded that the storage period of electronic documents on electronic media should be no less than the period established by law for the relevant documents on paper. Established requirements for the storage of electronic documents. The architecture of document archiving of software products is summarized. Types of cybersecurity threats identified. It is concluded that special attention should be paid to the protection of the data contained in the accounting system. Particular attention should be paid to the protection of data contained in the accounting system. Unfortunately, the internal data protection system is not enough to prevent all risks of leakage of confidential information. This is data copying, and theft or unauthorized removal of server equipment, seizure of property, actions of competitors, aimed at stopping the work of the enterprise, raider capture, etc. The specifics of the data are that they are intangible and do not exist separately, so in any case, special efforts must be made to preserve them so that they do not disappear along with the carrier. Ensuring the security of accounting information is a rather costly thing, and not only because of the cost of purchasing or installing remedies, but also because it is difficult to determine qualitatively the limits of proper security and ensure the appropriate security of the information system.

Keywords: *archiving, information protection, information storage, cybersecurity, document, document flow, electronic document.*

Постановка проблеми. Здатність захистити свою інформацію від сторонніх осіб і запобігти її випадкову втрату відіграють важливу роль. Збереження інформації дуже важлива як для простого користувача, так і для підприємств. Для зберігання даних в електронному вигляді використовуються різноманітні пристрої, деякі з яких відрізняються високою надійністю. Зберігання інформації – найважливіша запорука розвитку

людського суспільства, переймання знань й руху вперед. Це помітно як на глобальному рівні, так і на рівні конкретної людини або підприємства. Кожному сьогодні доводиться якось по-своєму вирішувати питання, пов'язані зі збереженням цифрових файлів. На щастя, для цього є чимало спеціальних пристроїв і накопичувачів. Але чи всі рішення, девайси і носії можуть бути визнані по-справжньому надійними? Як не прикро констатувати цей факт, – далеко не всі способи зберігання даних гарантують повну безпеку і, тим більше, зручність.

Аналіз останніх досліджень і публікацій. Значний внесок у розвиток теоретичних, методичних, методологічних та прикладних аспектів зберігання, архівування та захисту інформації в процесі організації бухгалтерського обліку зробили вітчизняні вчені, як А.П. Дикий, В.М. Гужва, В.П. Завгородний, С.В. Івахненков, Р.В. Скалюк, Я.С Ткаль та ін.

Постановка завдання. Метою дослідження є визначення особливостей зберігання, архівування та захисту інформації в процесі організації бухгалтерського обліку.

Виклад основного матеріалу дослідження. Скалюк Р.В. [1, с. 101] наголошує на тому, що забезпечення раціонального вибору адекватного для конкретного підприємства програмного продукту для автоматизації процедур бухгалтерського обліку та ефективне його використання у процесі обробки облікових даних дозволяє забезпечити підприємству: оперативне введення; обробку та формування вихідного інформаційного масиву даних бухгалтерського обліку; забезпечення внутрішнього контролю інформації; зменшення ручної праці; підвищення якості та ефективності роботи бухгалтерів; вдосконалення процесу організації бухгалтерського обліку та формування фінансової звітності підприємства, що у сукупності сприяє удосконаленню системи менеджменту, підвищенню рентабельності та економічному зростанню підприємства.

Дикий А.П. [2, с. 213] зазначає, що комп’ютеризація бухгалтерського обліку та використання автоматизованих робочих місць бухгалтерів дає

змогу забезпечити своєчасне надходження повної та достовірної інформації про господарську діяльність та майновий стан підприємства як до головного бухгалтера так і до керівництва підприємства при цьому не втрачаючи її. Крім того, автор вказує, що використання комп'ютерів призводить до зниження загальної трудомісткості облікових робіт та зміни самого характеру облікової праці. Діяльність бухгалтера перетворюється на творчу, оскільки шаблонні види робіт виконуються комп'ютером, а за працівником залишаються творчі дії по змістовній оцінці отриманих облікових даних.

Стаття 9 Закону України «Про бухгалтерський облік та фінансову звітність в Україні» від 16.07.1999 р. № 996-XIV [3], а також пункт 2.4 Положення про документальне забезпечення записів у бухгалтерському обліку, затвердженого наказом Мінфіну від 24.05.1995 р. № 88 [4], дозволяють складати первинні документи в електронній формі. Але – за умови дотримання вимог законодавства про електронні документи й електронний документообіг. Основним нормативом щодо цього є Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851-IV [5]. Тож, згідно із цим Законом, під електронним документом мають на увазі документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Збереження даних є одним з основних завдань при роботі з комп'ютерними програмами. На сьогодні є значна кількість спеціальних програм, які допомагають в практичному аспекті забезпечити збереження і захист даних (антивірусні програми, які справляються з віртуальними загрозами, програми для діагностики та відновлення жорстких дисків).

Усі юридичні особи, незалежно від форм власності, повинні застосовувати спеціальний Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затверджений наказом Мін'юсту від 11.11.2014 р. № 1886 [6]. На цей документ слід особливо звернути увагу, адже він містить різноманітні вимоги, зокрема щодо:

- найменування файлів електронних документів;
- найменування файлів електронних облікових документів;
- найменування файлів архівних електронних документів.

Серед іншого установи зобов’язані створювати документи постійного та тривалого (понад 10 років) зберігання у двох формах – паперовій та електронній.

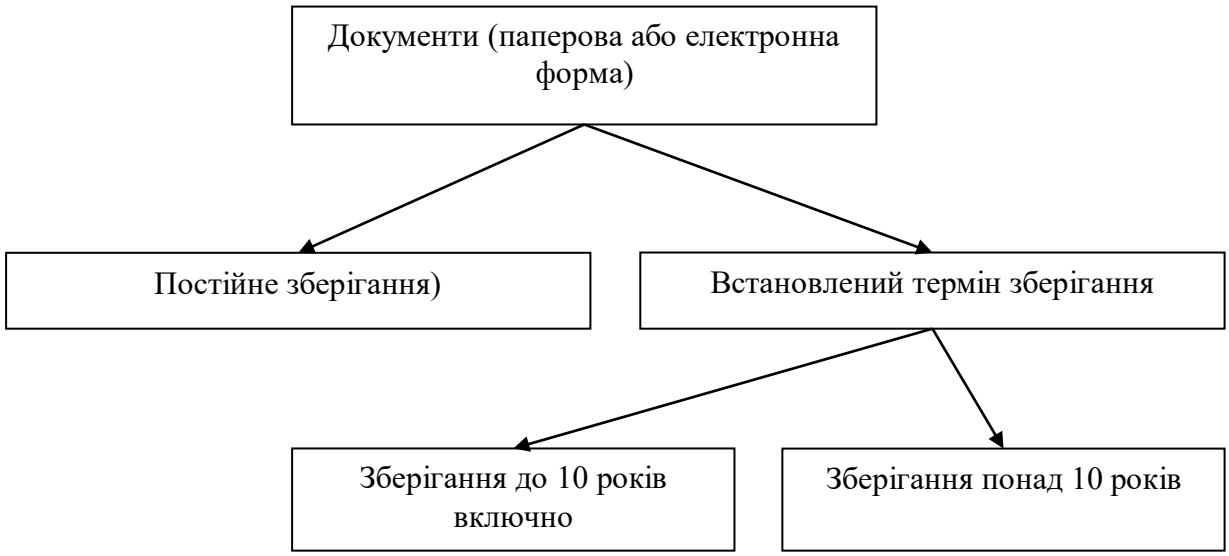

Рис. 1. Групування документів відносно термінів зберігання

Звісно, на підприємстві дозволено розробити й затвердити окремі регламенти роботи з електронними документами, але з обов’язковим урахуванням вимог Порядку № 1886 [6], специфіки організації діяльності установи, характеристик технічних і програмних засобів, що функціонують в установі.

За загальними правилами, строк зберігання електронних документів, зокрема щодо податкової звітності, не може бути меншим від строку, встановленого для відповідних паперових документів: не менш як 1095 днів від дня подання податкової звітності.

Суб’єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері (табл. 1).

Таблиця 1

Строки зберігання первинних документів

№ з/п	Вид документу
3 роки	
1	Розрахункові відомості сплати внесків до різних фондів
2	Договори кредитні, поруки, застави, гарантії, переведення боргу (після закінчення строку дії договору)
3	Відомості на виплату грошей (за відсутності розрахунково-платіжних відомостей – 75 років)
4	Довіреності (у т. ч. анульовані) на одержання грошових сум і товарно-матеріальних цінностей; на одержання зарплати та інших виплат
5	Документи (копії звітів, витяги з протоколів, висновки, заяви, довідки, списки працівників) про виплату допомоги, пенсій, оплату листків непрацездатності з фонду соціального страхування
6	Документи (заяви, рішення, довідки, листи) про оплату відпусток у зв'язку з навчанням, одержання пільг із податків тощо
7	Документи (акти, відомості, листи) про взаєморозрахунки між організаціями
8	Протоколи взаємозаліків
9	Документи (акти, процентовки, довідки, рахунки) про приймання виконаних робіт
10	Первинні документи та додатки до них, що фіксують факт виконання господарських операцій і стали підставою для записів у регістрах бухобліку та податкових документах (касові, банківські документи, ордери, повідомлення банків і переказні вимоги, виписки банків, корінці квитанцій, банківських чекових книжок, наряди на роботу, акти про приймання, здавання і списання майна й матеріалів, квитанції і накладні з обліку ТМЦ, рахунки-фактури, авансові звіти тощо)
11	Податкові накладні
12	Документи (плани, звіти, протоколи, акти, довідки, доповідні записки) документальних ревізій, перевірок та аудиту фінансово-господарської діяльності, контрольно-ревізійної роботи, у т.ч. перевірок каси, правильності стягнення податків тощо
13.	Документи (довідки, акти, зобов'язання, листи) щодо розтрат, недостач, розкрадань
14.	Документи (протоколи засідань інвентаризаційних комісій, акти інвентаризації, інвентаризаційні описи, порівняльні відомості) про інвентаризацію основних засобів, нематеріальних активів, грошових коштів, матеріальних цінностей тощо
10 років	
15.	Аналітичні документи (таблиці, доповіді, доповідні записки тощо) до річних звітів і балансів
75 років	
16.	Розрахунково-платіжні відомості (особові рахунки) працівників, аспірантів, студентів
До ліквідації підприємства	

17.	Звіти (відомості) про нарахування та перерахування страхових внесків на державне та недержавне соціальне страхування (пенсійне, на випадок безробіття, у зв'язку з тимчасовою непрацездатністю тощо: - зведені річні й з більшою періодичністю; - річні й з більшою періодичністю
18.	Документи (протоколи, акти, звіти, відомості переоцінки й визначення зношеності основних засобів про переоцінку основних фондів, нематеріальних активів, незавершеного будівництва

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така

установа додержується вимог цієї статті. Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

Зберігання файлів відбувається в базі даних або в томах на диску, а при першій необхідності роботи з тим чи іншим файлом, він копіюється на комп'ютер користувача.

Зберігання файлів в інформаційній базі здійснюється за допомогою розподілу по папках. При необхідності є можливість розмежувати доступ того чи іншого користувача до папок з певною інформацією.

Структура папок може формуватися різними способами:

- за організаційною структурою підприємства (наприклад, бухгалтерія, відділ збуту та ін.);
- за тематикою даних (плани, калькуляції, розробки та ін.);
- за правами доступу (загальні, конфіденційні та ін.)

У процесі роботи щодня в інформаційну базу вводяться первинні дані, які створюють нові документи, елементи довідників та ін. Розмір інформаційної бази при цьому поступово збільшується.

В процесі організації бухгалтерського обліку в практичному аспекті можуть мати місце ситуації, які призводять до збою обладнання (на жорстких дисках з'являються помилки внаслідок різних збоїв або перепадів напруги в електромережі; пошкодження жорсткого диску без можливості відновлення даних; втрата робочої бази).

Наслідки повної втрати даних (при відсутності резервних копій на інших комп'ютерах / компакт-дисках та інших носіях) дуже складно переоцінити.

З метою забезпечення збереження інформаційної бази потрібно створити надійну систему захисту інформації. Якщо на підприємстві працює системний адміністратор, то він може забезпечити щоденне (або навіть

кілька разів за день) автоматичне зберігання інформації на інший комп’ютер або інший носій.

У випадку, якщо на підприємстві у штатному розписі не передбачено посаду штатного системного адміністратора, то з метою збереження інформації, яка акумулюється в бланках електронних документів, потрібно постійно виконувати архівування облікової інформації на інший комп’ютер (ймовірність того, що з ладу одночасно вийдуть два комп’ютери значно низька).

Архівування також доцільно виконувати перед кожним сеансом сервісного обслуговування (розрахунку підсумків, перепроведення документів, тестування даних та ін.) (рис. 2).

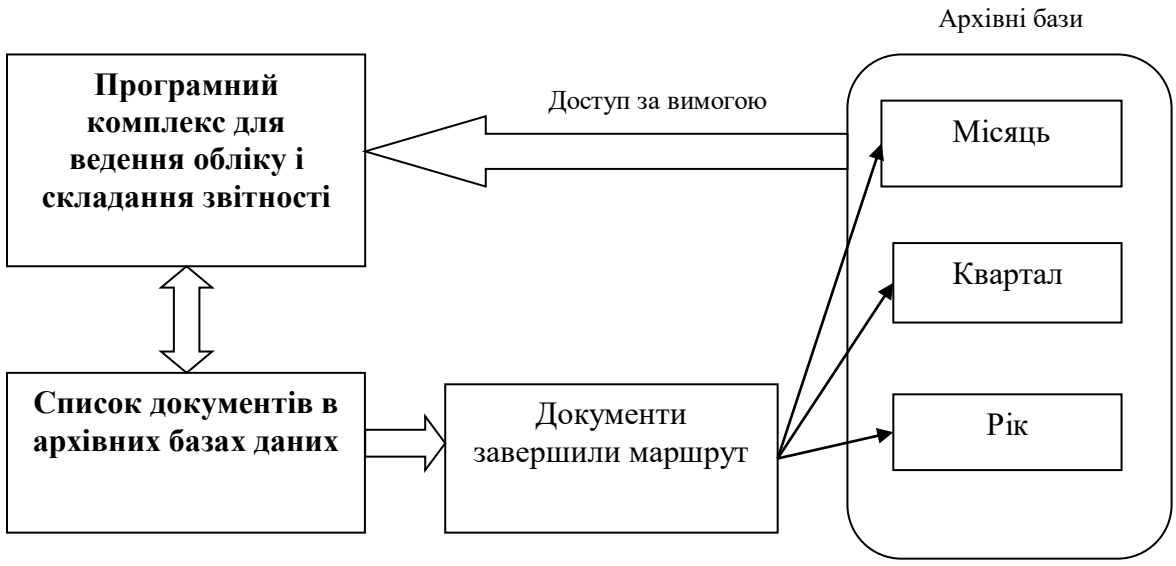

Рис. 2. Загальна архітектура архівації документів програмних продуктів

На сьогодні пристрої для зберігання цифрової інформації мають великий об’єм пам’яті. Flash-карти пам’яті, жорсткі диски та спеціалізовані сховища даних надають десятки та сотні терабайт пам’яті під різні потреби.

Саме це і досягається завдяки використанню процесу архівування даних. Збереження інформації підвищується завдяки створенню та

використанню резервних копій даних. Передача інформації меншого обсягу економить час і доступні потужності мережі передачі даних.

Процес стиснення або архівування даних – це перетворення вихідної інформації, засноване на спеціальних алгоритмах, що проводиться з метою зменшення її обсягу.

Майже всі сучасні програми-архіватори для Windows дозволяють працювати з архівами різних форматів. Принципи управління даними програмами практично ідентичні.

Програма-архіватор призначена для виконання двох основних функцій:

- створення архівів;
- вилучення файлів з архівів.

Головним недоліком архівації є те, що файл, який знаходиться в архіві, не можна відкрити і використовувати відразу. Перед кожним доступом до такого файлу його необхідно попередньо вилучити з архіву. Процес вилучення не складний, але якщо архів великий, це може зайняти досить багато часу. Тому файли, які часто використовуються, зберігати в заархівованому вигляді не дуже зручно.

Даний недолік значною мірою перекреслює переваги архівування. У той же час, в разі зберігання файлів, що рідко використовуються, а також пересилання файлів через Інтернет, архівація повністю себе виправдовує.

Зберігання інформації в процесі організації електронного бухгалтерського обліку здійснюється за допомогою централізованого сховища робочої документації.

Централізоване сховище робочої інформації – це каталогізований загальний мережевий ресурс, який може мати обмеження прав доступу в зазначені каталоги.

Централізоване сховище робочої інформації забезпечує вирішення наступних завдань:

- оптимізацію пошуку робочої інформації в разі потреби;
- забезпечення системи збереження документації;

- мінімізацію ймовірності втрати робочої інформації;
- захист інформації від несанкціонованого доступу з боку співробітників підприємства;
- створення і зберігання повних комплектів робочої документації за межами сховища та за межами підприємства;
- мінімізацію впливу людського фактору в плані випадкових і некваліфікованих дій співробітників з документами.

Централізація зберігання робочої документації є першим та обов'язковим завданням перед впровадженням систем збереження інформації, систем гарантованого і розподіленого збереження інформації.

При електронному бухгалтерському обліку здійснюється автоматизована робота зі звичайними файлами, що створюються як в процесі функціонування підприємства, так і в робочому порядку (чернетками, проектами, результатами переговорів і т.п.). Також користувач може працювати і з іншими типами файлів – офісними документами, зображеннями, текстами, файлами в аудіо - та відео форматі, архівами, додатками та ін.

Обробка різних типів файлів реалізується за допомогою встановлених на комп'ютері програм, призначених для роботи з тим чи іншим типом файлів.

Реалізація заходів ефективної кібербезпеки в даний час є досить складним завданням, оскільки сьогодні існує набагато більше пристроїв, ніж людей, а зловмисники стають все більш винахідливими.

Кібербезпека – це реалізація заходів щодо захисту систем, мереж і програмних додатків від цифрових атак. Такі атаки зазвичай спрямовані на отримання доступу до конфіденційної інформації, її зміни і знищення, на вимагання у користувачів грошових коштів або на порушення нормальної роботи підприємств.

Успішний підхід в сфері кібербезпеки виражається у вигляді багаторівневого захисту, що охоплює комп'ютери, мережі, програми або

дані, які необхідно убезпечити. Співробітники, робочі процеси і технології повинні доповнювати один одного, щоб забезпечити ефективний захист від кібератак.

Користувачі мають розуміти і дотримуватися основних принципів інформаційної безпеки, такі як вибір надійних паролів, уважне ставлення до вкладень в електронних листах і резервне копіювання даних.

На підприємстві повинен бути розроблений набір базових заходів з протидії атакам. Можна керуватися одним надійним набором заходів, який пояснюватиме, як визначати атаки, захищати системи, виявляти загрози та протидіяти їм, а також відновлювати працездатність після здійснених атак.

Технології є найважливішим елементом, що надає підприємствам і окремим користувачам інструменти, необхідні для захисту від кібератак. Основними компонентами, які необхідно захистити, є кінцеві пристрої, наприклад, комп'ютери, інтелектуальні пристрої та маршрутизатори; мережі і хмарне середовище. До найбільш поширених технологій, що використовуються для захисту перерахованих компонентів, відносяться міжмережеві екрани нового покоління, фільтрація DNS, захист від шкідливого програмного забезпечення, антивірусне програмне забезпечення та рішення для захисту електронної пошти (табл. 2).

Таблиця 2

Типи загроз кібербезпеки

Загрози кібербезпеки	**Характеристика загроз**
Програми-вимагачі	Це різновид шкідливого програмного забезпечення. Вони призначені для вимагання грошей за допомогою блокування доступу до файлів комп'ютерної системи до надходження викупу. Перерахування викупу не гарантує відновлення файлів або працездатності системи.
Шкідливе програмне забезпечення	Шкідливе програмне забезпечення призначене для отримання несанкціонованого доступу або пошкодження комп'ютерної системи.
Соціальна інженерія	Це тактика, яку використовують зловмисники, щоб схилити користувача до розкриття конфіденційної інформації. Вони можуть звернутися з проханням про грошові платежі або про отримання доступу до конфіденційних даних. Способи соціальної інженерії можуть застосовуватися разом з погрозами будь-якого з перерахованих вище типів, щоб з більшою ймовірністю змусити

	користувача натиснути на посилання, завантажити шкідливі програми та повірити зловмисному джерелу.
Фішинг	Це розсилка підробленої електронної кореспонденції, яка виглядає як повідомлення від надійних джерел. Метою є крадіжка конфіденційних даних, таких як номери кредитних карт і інформація про облікові записи. Це найпоширеніший тип кібератак. Забезпечити захист можна за допомогою вивчення необхідної інформації або установки технологічний рішень, які можуть відфільтрувати шкідливі електронні листи.

У сучасному світі програми розширеного кіберзахисту служать на благо кожного користувача. На індивідуальному рівні атака зі зломом кіберзахисту може привести до різноманітних наслідків, починаючи з крадіжки особистої інформації і закінчуючи вимаганням грошей або втратою цінних даних.

Варто застосовувати концепцію захисту даних, побудовану на використанні апаратно-програмного комплексу, яка забезпечує реалізацію наступних можливостей:

- обмеження доступу до конфіденційної інформації шляхом надійного шифрування даних;
- високу швидкодію завдяки використанню алгоритмів шифрування, вбудованих в центральний процесор;
- надання доступу до захищених даних тільки після двофакторної аутентифікації;
- виключення ризику несанкціонованого копіювання баз даних (навіть користувачами з правами адміністратора);
- миттєву повну заборону доступу до захищених даних у випадку надзвичайних ситуацій.

Інший спосіб захисту даних – захист комп’ютерів та програм від несанкціонованого доступу третіх осіб.

Даний спосіб захисту облікової інформації передбачає:

- встановлення паролів, починаючи від входу в Windows і закінчуючи запуском бази (краще, якщо пароль є послідовністю нічого не значущих символів, бажано довжиною не менше 8 символів);

- завершення роботи програми по закінченню робочого дня;
- застосування засобів розмежування доступу. Наприклад, можна заборонити користувачам переглядати певні документи, журнали документів, довідники або звіти, користуватися певними обробками, знову ж для безпеки даних, тобто користувач повинен мати доступ тільки до тієї інформації, яка йому необхідна для роботи;
- мінімізацію роботи з непов'язаними для роботи сайтами в мережі Internet з метою уникнення ризику атаки вірусних програм, які можуть призвести до збою інформаційної системи та втрати даних бухгалтерського обліку.

Висновки з проведеного дослідження. Специфіка даних в тому, що вони нематеріальні й не існують окремо, тому в будь-якому випадку для їх збереження потрібно робити спеціальні зусилля, щоб вони не зникли разом з носієм. Забезпечення безпеки облікової інформації – досить затратна справа, і не тільки через витрати на закупівлю або установку засобів захисту, але й через те, що важко кваліфіковано визначити межі належної безпеки та забезпечити відповідну безпеку інформаційної системи.

Проблема захисту інформації при використанні мережевих продуктів бухгалтерського обліку, якими користуються велика кількість користувачів, постає надзвичайно гостро. Сформовані в системі бази даних, при відсутності адекватних застережних заходів, можуть бути видалені з необережності, зламані або передані зацікавленим особам.

Особлива увага повинна бути приділена захисту даних, що містяться в обліковій системі. На жаль, внутрішньої системи захисту даних недостатньо для запобігання всіх ризиків із витоку конфіденційної інформації. Це й копіювання даних, й крадіжка або несанкціоноване вилучення серверного обладнання, арешт майна, дії конкурентів, спрямовані на зупинку роботи підприємства, рейдерське захоплення та ін.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Скалюк Р.В. Концептуальні основи ефективної автоматизації процедур бухгалтерського обліку на вітчизняних підприємствах. *Вісник Хмельницького національного університету*. 2015. № 3 (1). С. 95-102.

2. Дикий А.П. Порядок забезпечення безпеки бухгалтерської інформації в умовах застосування сучасних комп'ютерних технологій. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2008. № 3 (12). С. 208-214.

3. Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16.07.1999 р. № 996-XIV / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/996-14 (дата звернення: 24.03.2019).

4. Положення про документальне забезпечення записів у бухгалтерському обліку : Наказ міністерства фінансів України від 24.05.1995 р. № 88. / *База даних «Законодавство України».* URL : https://zakon.rada.gov.ua/laws/show/z0168-95 (дата звернення: 24.03.2019)

5. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 24.03.2019)

6. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання : Наказ Міністерства юстиції України від 11.11.2014 р. № 1886 / *База даних «Законодавство України».* URL : https://zakon2.rada.gov.ua/laws/show/z1421-14 (дата звернення: 24.03.2019)

REFERENCES:

1. Skalyuk R. V. (2015). Kontseptual'ni osnovy efektyvnoyi avtomatyzatsiyi protsedur bukhhalters'koho obliku na vitchyznyanykh pidpryyemstvakh [Conceptual bases of effective automation of accounting procedures at domestic enterprises]. *Visnyk Khmel'nyts'koho natsional'noho universytetu* [Bulletin of Khmelnytsky National University], (3 (t.1), 95-102.

2. Dykyy A. P. (2008). Poryadok zabezpechennya bezpeky bukhhalters'koyi informatsiyi v umovakh zastosuvannya suchasnykh komp"yuternykh tekhnolohiy [Procedure security of accounting information in terms of the use of modern computer technology]. *Problemy teoriyi ta metodolohiyi bukhhalters'koho obliku, kontrolyu i analizu* [Problems of the theory and methodology of accounting, control and analysis], (3 (12)), 208-214.

3. Pro bukhhalters'kyy oblik ta finansovu zvitnist' v Ukrayini : Zakon Ukrayiny vid 16.07.1999 r. № 996-XIV. URL : https://zakon.rada.gov.ua/laws/show/996-14 (accessed 24 March 2019).

4. Polozhennya pro dokumental'ne zabezpechennya zapysiv u bukhhalters'komu obliku : Nakaz ministerstva finansiv Ukrayiny vid 24.05.1995 r. № 88. URL : https://zakon.rada.gov.ua/laws/show/z0168-95 (accessed 24 March 2019).

5. Pro elektronni dokumenty ta elektronnyy dokumentoobih : Zakon Ukrayiny vid 22.05.2003 r. № 851-IV. URL : https://zakon.rada.gov.ua/laws/show/851-15 (accessed 24 March 2019).

6. Poryadok roboty z elektronnymy dokumentamy u dilovodstvi ta yikh pidhotovky do peredavannya na arkhivne zberihannya : Nakaz Ministerstva yustytsiyi Ukrayiny vid 11.11.2014 r. № 1886. URL : https://zakon2.rada.gov.ua/laws/show/z1421-14 (accessed 24 March 2019).

Harkusha Serhii

Candidate of Economic Sciences, Associate Professor

Associate Professor of the Department of Accounting

Sumy National Agrarian University

FEATURES OF STORAGE, ARCHIVING AND PROTECTION OF INFORMATION AT THE ACCOUNTING ORGANIZATION

The purpose of the article. The ability to protect your information from the third parties and prevent its accidental loss play an important role. Saving of information is very important both for the simple user and for the enterprises. Various devices are used to store electronically dates, some of which are highly reliable. Storing of information is an essential guarantee of the development of human society, taking knowledge and moving forward. This is noticeable both at the global level and at the level of a particular person or enterprise.

Methodology. A review of the regulatory framework for the storage of accounting information has been made and generalizations have been made regarding the research problem.

Results. Enterprises are obliged to create documents of permanent and long (more than 10 years) storage in two forms – paper and electronic.

According to the general rules, the period of storage of electronic documents, in particular regarding tax reporting, can not be shorter than the time period established for the relevant paper documents: not less than 1095 days from the date of submission of tax returns.

In case of the impossibility of storing of electronic documents on electronic media within the time period prescribed by the legislation for the corresponding documents on paper, subjects of electronic document circulation should take measures to duplicate documents on several electronic media of information and to make them periodically copied in accordance with the procedure of recording and copying documents, established by law. If it is not possible to meet the specified requirements, electronic documents should be kept as a copy of the document on paper (in case of absence of the original of this document on paper).

In order to ensure the maintenance of the information base, it is necessary to create a reliable information security system. If the company has a system administrator, then it can provide a daily (or even multiple times per day) automatic storage of information to another computer or other carrier.

It is also advisable to perform archiving before each session of service (calculation of results, overwriting of documents, data testing, etc.).

The main disadvantage of archiving is that the file in the archive can not be opened and used immediately. It must be removed from the archive beforehand before each access to such a file. The process of extracting is not complicated, but if the archive is large, it can take a lot of time. Therefore, files that are often used are archived in a non-convenient way.

The implementation of effective cybersecurity is currently a rather difficult task, since today there are many more devices than people, and attackers are becoming more inventive.

A set of basic anti-attack measures should be developed at the enterprise. You can be guided by one reliable set of measures that will explain how to identify attacks, protect systems, detect threats and counteract them, and restore performance after attacks.

Practical implications. Particular attention should be paid to the protection of data contained in the accounting system. Unfortunately, the internal data protection system is not enough to prevent all risks of leakage of confidential information. This is data copying, and theft or unauthorized removal of server equipment, seizure of property, actions of competitors, aimed at stopping the work of the enterprise, raider capture, etc.

Value/originality. The specifics of the data are that they are intangible and do not exist separately, so in any case, special efforts must be made to preserve them so that they do not disappear along with the carrier. Ensuring the security of accounting information is a rather costly thing, and not only because of the cost of purchasing or installing remedies, but also because it is difficult to determine qualitatively the limits of proper security and ensure the appropriate security of the information system.