УДК 657 **DOI 10.33042/2522-1809-2019-2-148-111-117**

Н.О. Чех, О.О. Конопліна, Д.С. Шахвердян

Харківський національний університет міського господарства імені О.М. Бекетова, Україна

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БУХГАЛТЕРСЬКОГО ОБЛІКУ ПІДПРИЄМСТВА

В даній статті проаналізовано теоретичні основи інформаційної безпеки бухгалтерського обліку підприємства. Проаналізовано основні види потенційних загроз інформаційній безпеці та джерела цих загроз. Сформовано рекомендації щодо заходів підвищення рівня інформаційної безпеки та забезпечення захисту бухгалтерської інформації.

***Ключові слова**: інформація, інформаційна безпека, загрози, витік інформації, бухгалтерські дані.*

Постановка проблеми

У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту. Проблема інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем.

У зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні цієї проблеми.

Тому питання захисту інформаційного простору та інформації, що передається, приймається та зберігається у ньому, є надзвичайно актуальними. З урахуванням рівня втілення інформаційних технологій сучасності, розглядаючи інформацію як об'єкт діяльності, треба відзначити, що залежно від її важливості та значення для користування нею витрачаються відповідні ресурси.

Системи бухгалтерського обліку містять конфіденційну інформацію, безпека якої повинна забезпечуватись постійно. Наслідки несанкціонованого доступу до бухгалтерської інформації можуть бути руйнівними - від проблеми крадіжки особистості до втрати даних, що неможливо відновити чи замінити. Коли дані обліку змінюють або видаляють навмисно або випадково, створюється хаос у бухгалтерії, ставлячи під сумнів достовірність або точність всіх даних.

Аналіз останніх досліджень і публікацій

Дослідженням проблем забезпечення інформаційної безпеки підприємств присвячені роботи таких вчених як: О.В. Арефєвої, В.В. Буряковського, М.І. Камлика, В.Л. Ортинського, С.М. Шкарлета та інших. Однак, враховуючи наявні теоретичні розробки, проблеми удосконалення в розрізі інформаційної безпеки даних обліку та оподаткування потребують додаткового розгляду.

Метою статті є дослідження теоретичних основ управління інформацією бухгалтерського обліку організації в системі фінансово-економічної безпеки підприємства, та розроблення напрямків підвищення інформаційної безпеки підприємства.

Виклад основного матеріалу

Основна задача організації полягає у ефективному і раціональному використанні інформації. Для вирішення цієї задачі керівництву організації необхідна оперативна і достовірна інформація з метою прийняття управлінських рішень.

Для отримання додаткових переваг у діяльності підприємства необхідно забезпечити активне використання інформаційного ресурсу у системі управління організації. Переробка інформації формує знання про поточний стан виробництва, завдяки яким здійснюється вплив на виробничі, фінансові і адміністративногосподарські процеси. Дослідження інформації допомагає знайти не тільки шляхи до розробки нового товару або послуги, але й забезпечити виправданий ризик вибору нового напряму у виробництві, формування нового ринку.

Процес управління який базується на результатах обробленої інформації, передбачає вибір та застосування менеджерам таких дій, які дозволять управляти відповідними підрозділами організації. Результатом такого управління є підтримання

заданої ефективності виробничого процесу і реалізація відповідної бізнес-функції організації.

Усі економічно розвинуті країни світу використовують переваги інформаційних технологій у виробничій, комерційній та банківських сферах. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси економічної діяльності підприємства. Швидше за все розвиваються технології, по'вязані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд та ін. [4].

Систему бухгалтерського обліку можна визначити як організаційний компонент, який накопичує, класифікує, обробляє, аналізує та передає відповідну (перважно фінансову) інформацію необхідну для прийняття рішення внутрішнім та за необхідності зовнішнім користувачам організації.

Саме бухгалтерія є основним «виробником» та «поширювачем» інформації різних напрямків та для різних груп користувачів, які включають клієнтів, інвесторів, постачальників, урядові організації та інших сторін, що не є бухгалтерами.

В цілому можна стверджувати, що сьогодні бухгалтерський облік включає пять основних компонентів. До них належать:

- люди;
- операції;
- дані;
- програмне забезпечення;
- інфраструктура інформаційних технологій.

Разом ці пять компонентів дають можливість реалізовувати три основні функції в будь-якій організації:

- збір та зберігання даних щодо діяльності організації;
- опрацювання даних та перетворення їх у інформацію корисну для прийняття рішень;
- належний контроль для захисту активів, в тому числі даних, та забезпечення наявності достовірної та адекватної інформації.

Комп'ютеризовані системи бухгалтерського обліку в інформаційній ері виконують багато завдань, що раніше виконувались традиційними ручними методами, наприклад, збір, обробка, зберігання, трансформація і розповсюдження як фінансової, так і нефінансової інформації для планування, прийняття рішень і контролю досягнення цілей.

Отже, використання розвинутих інформаційних технологій позитивно впливає на бізнес. Однак, як і у випадку з усіма нововведеннями, існують і негативні сторони, повязані з їх запровадженням. Організації, як великі, так і малі, стали в значній мірі покладатися на інформаційні технології, щоб забезпечити своєчасність інформації, яка використовується для прийняття критично важливих бізнес-рішень. Таким чином, зростає залежність від інформаційних технологій, а також ризики, з якими стикаються організації. До них можна віднести ризик різного роду махінацій та кібератак.

Можна виділити найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо [5].

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз [2].

Не існує універсального заходу безпеки, який би захистив бізнес від всіх видів загроз та ризиків інформаційній безпеці бухгалтерського обліку. Різноманітність атак та швидкість, з якою зловмисники пристосовують свої методи, підкреслюють необхідність реалізації декількох методів для підтримання надійного плану інформаційного захисту.

Уважність та старанність з боку працівників є обов'язковою. Опиратись лише на технології, щоб захистити свій бізнес – це, можливо, найбільша помилка компаній при розробці плану безпеки. Хоча технологічні рішення такі як антивірусне програмне забезпечення, щоденне резервне копіювання даних, брандмауер, методи шифрування, потужні паролі та протоколи веб-браузера дуже важливі, вони є лише складовими системи інформаційного захисту і їх використання може навіть створити помилкове відчуття безпеки. Навчання ваших співробітників має першорядне значення для будь-якого успішного плану захисту організації, оскільки часто працівники ненавмисно стають точкою доступу для злочинців через електронні атаки електронною поштою чи

соціальну інженерію. Наприклад, користувач, який перевіряє електронну пошту, натиснувши шкідливе посилання або вкладення, заражає всю офісну мережу.

Ось чому тренінг з інформування про безпеку для співробітників є дуже важливим. Організація може використовувати найсучасніші програмні та технологічні засоби стримування, але насправді, ви завжди на відстані одного кліку від втрати даних.

Технології захисту даних грунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз.

Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов’язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила.

Коли використовуються способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісним міркувань, то йдеться про спонукання [7].

Способи захисту інформації передбачають використання певного набору засобів. Для запобігання втрати та витоку таємних даних використовуються засоби:

– фізичні;

– апаратні;

– програмні;

– апаратно-програмні;

– законодавчі;

– криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об’єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв’язку тощо.

Програмні засоби захисту, які вмонтовані в програмне забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.

Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [16].

Розглянемо основні джерела загроз інформаційній безпеці бухгалтерського обліку підприємства та заходи їх мінімізації:

- низький рівень фізичної безпеки інформації;

Підприємства повинні захищати свою бухгалтерську інформацію та комп'ютерні системи від втрат і крадіжок. Особливо важливі документи повинні зберігатись в сейфах та в приміщеннням з обмеженим доступом. Бухгалтерське обладнання та сервери також повинні зберігатись в офісах, де двері блокуються (закриваються), що обмежує несанкціонований доступ. Кабелі, що підключаються до облікового обладнання, повинні бути на безпечній відстані від людей, гризунів, води та інших чинників, що можуть знищити їх.

Якщо використовується бездротове з'єднання для доступу до мережі або Інтернету, необхідно дотримуватись протоколів безпеки. Відносно легко зламати бездротові системи.

Якщо використовуються портативні комп'ютери (ноутбуки), доцільно розглянути можливість придбання програмного забезпечення, що відстежує місцезнаходження комп'ютера.

- електронна пошта;

Електронна пошта є найбільшою загрозою безпеці для більшості компаній. За даними Digital Guardian, 91% кібератак починаються з фішингової електронної пошти, що робить її загрозою номер один для вашого бізнесу. Фішинг – це надсилання

електронного листа, який не виглядає підозріло, і наче б то надходить від контакту, і запитує інформацію. Більшість людей відкриє електронний лист від знайомої їм особи, неперевіряючи фактичну адресу електронної пошти. Електронну пошту потрібно захистити від несанкціонованого доступу. Один із способів зробити це - включити двокрокову аутентифікацію, яку пропонують основні служби електронної пошти, такі як Gmail, Microsoft Office 365, AOL і Yahoo.

Двокрокова автентифікація або двоетапне підтвердження вимагає від користувача ввести своє звичайне ім'я користувача та пароль, а потім ввести спеціальний код. Цей код кожного разу надсилається на мобільний телефон (або, що більш безпечно, генерується програмою аутентифікації на телефоні, такою як Google Authenticator або Microsoft Authenticator). Це перший важливий крок у запобіганні несанкціонованому доступу до вашої інформації та відмінною відправною точкою для запобігання кіберзлочинності. Надзвичайно важливо, щоб люди усвідомлювали збиток, який може завдати доступ до електронної пошти. Зловмисник може скинути ваші паролі та використати електронну пошту для доступу до облікових записів через Інтернет, в тому числі інтернет-банкінгу.

Іншою поширеною загрозою є викрадення особистих даних, таких як ім'я, адреса, індентифікаційний податковий номер та будь-яких інших реквізитів. Щоб запобігти отриманню хакерами цієї інформації, потрібно надсилати електронні листи з шифруванням. Microsoft Office 365 пропонує шифрування електронної пошти за номінальну щомісячну плату. НЕ слід вважати, що PDF-файл з паролем є захищеним. Є доступні утиліти (як безкоштовні, так і за плату), які зламують ці паролі. Повне шифрування електронної пошти – це єдиний варіант.

- ризики, повязані з роботою в інтернеті

Завантаження з веб-браузерів є ще однією з основних загроз інформаційній безпеці підприємства. Пошук в Інтернеті може призвести до скомпрометованих веб-сайтів, які можуть заразити мережу вірусами та шкідливими програмами. Щоб запобігти цьому типу атаки, необхідно встановити всі останні оновлення безпеки на комп'ютери та сервери організації. Встановіть маршрутизатор брандмауера з антивірусним шлюзом, шлюзом антивірусного захисту та захистом від вторгнення, щоб зупинити вірус, перш ніж він потрапить у мережу. Маршрутизатори, надані Інтернет-провайдерами, не мають такого типу захисту. Це може бути достатнім для домашніх умов, але не для бізнесу.

Найбільш поширеною кібератакою є спливаюче вікно браузера, яке стверджує, що це попередження законної компанії (наприклад, Microsoft) про те, що комп'ютер інфікований, і необхідно зателефонувати за вказаним номером. Ці сповіщення підштовхують користувача до дзвінка, а потім хакери з дозволу користувача отримують доступ до комп'ютера наче б то для його очищення. Замість цього вони справді заражають його та отримують доступ до інформації.

Доступним заходом безпеки є підписка на хорошу антивірусну програму, яка надає веб-переглядачу плагін, який кваліфікує веб-сайт як безпечний, що не дозволяє користувачу перейти на сайти, які раніше заражали інших користувачів.

Ще одним заходом захисту є програма «пісочниця» (sandbox), яка дозволяє веб-браузеру доступ до Інтернету, але запобігає будь-яким постійним змінам на комп'ютері або в мережі. Наприклад, якщо випадково було завантажене шкідливе програмне забезпечення, будь-які зміни, які воно намагатиметься зробити, будуть міститися у віртуальній пісочниці, яку легко очистити.

- віддалений доступ

Віддалений доступ до комп'ютерів має здійснюватися за допомогою захищеної віртуальної приватної мережі або VPN-з'єднання. Ніколи не використовуйте Microsoft Remote Desktop без VPN. Це майже гарантує хакерам доступ до ваших даних. Якщо не доцільно налаштувати VPN, скористайтеся однією з програм віддаленого доступу, які пропонують двофакторну аутентифікацію.

- передача даних;

Передача даних за допомогою USB-накопичувача не є безпечною. USB-накопичувач повинен бути з вбудованим шифруванням, та вимагати пароль для доступу. Якщо пароль введено неправильно занадто багато разів доцільно передбачити автоматичне знищення інформації.

Ноутбуки - ще одна проблема безпеки. Жорсткі диски ноутбуків повинні бути зашифровані. Для цього Microsoft має вбудовану утиліту шифрування BitLocker, яка входить в професійну версію Windows 10.

Утилізацію комп'ютерного обладнання також необхідно здійснювати належним чином. Обладнання, яке використовувалось в бухгалтерії, продається або віддається третій стороні, все ще може містити конфіценційну інформацію на жорсткому диску. Видалення та знищення жорстких дисків або їх очищення фахівцями - це хороший спосіб запобігти несанкціонованому доступу до даних. Також потрібно уважно відбирати тих, хто буде проводити будь-які ремонтні роботи з технікою організації, оскільки вони отримують доступ до конфіденційної інформації.

- бездротовий доступ до інтернету

Необхідно захистити бездротовий доступ до мережі. Само собою необхідні паролі. Крім того, для відвідувачів офісу, які потребують доступу до Інтернету, повинна бути налаштована гостьова мережа. Це запобігає доступу будь-якого гостя до комп'ютерів і ресурсів мережі. Це особливо необхідно у випадку, якщо один з ноутбуків або пристроїв, що використовуються гостем, заражений.

Крім цього, обовязковими елементами інформаційної безпеки повинні бути:

- аутентифікація

Всі системи організації повинні мати ідентифікатори входу (логіни) та паролі, які автентифікують користувача, підтверджуючи, що він має право використовувати комп'ютер. Паролі не повинні розголошуватись та доцільно їх періодично змінювати. Багато систем можна налаштувати для автоматичного запиту зміни пароля, наприклад, через 90 днів.

Процес аутентифікації зазвичай передбачає надання прав користувачам. Не всі користувачі повинні мати доступ до всієї інформації. Профілі можна налаштувати, надаючи певним користувачам доступ лише, наприклад, до кредиторської заборгованості, тоді як інші можуть мати доступ лише до звітів, що обмежує ризик неправильного використання даних.

- захист від вірусів

Комп'ютери – вразливий обєкт атак вірусів і шкідливих програм, які впливають на їх роботу. Деякі віруси дозволяють вторгнення в систему - хакер може потрапити всередину системи і створити проблеми. З використанням Інтернету загроза вірусів і шкідливих програм є реальною, тому використання антивірусних програм, брандмауерів та інших заходів безпеки є обов'язковими. Вірусна атака може звести всю систему обліку, зробивши її непридатною і неефективною.

- резервне копіювання

Стандартною процедурою безпеки систем обліку є резервне копіювання даних і збереження резервної копії в безпечному місці за межами приміщення. Справа в тому, що якщо щось трапиться з системою, наприклад, пожежі, повені або інші втрати, дані в безпеці і можуть бути відновлені. Хорошою мірою безпеки є виконання нічних резервних копій, а також періодичне відновлення резервних копій, щоб переконатися, що дані безпечні та корисні.

На сьогоднішній день, найкраща система віддаленого резервного копіювання включає в себе віртуалізацію комп'ютера або сервера. Віртуалізація комп'ютера або сервера робить фотокопію віртуального програмного забезпечення вашої системи, яку потім можна досить швидко активувати з віртуального хостинг середовища. Резервне копіювання – це найкраще рішенням для безперервності бізнесу та мінімізації простою системи.

Отже, у сучасних умовах головною метою будь-якої системи інформаційної безпеки підприємства є забезпечення стійкого функціонування підприємства, запобігання загрозам його безпеці, захист законних інтересів від протиправних посягань, недопущення розкрадання фінансових коштів, розголошування, втрати, спотворення і знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об’єкту.

Отже забезпечення інформаційної безпеки безпеки бухгалтерського обліку організаціям необхідно адаптувати три типи заходів контролю: фізичний контроль, який передбачає запобігання доступу несанкціонованих осіб до об'єктів організації; контроль доступу, що передбачає обмеження використання неавторизованими особами інформаційних ресурсів; контроль засобів зв'язку, що передбачає забезпечення безпеки руху даних в мережі.

Забезпечення інформаційної безпеки підприємства повинне бути комплексним та системним.

Необхідність у політиці безпеки на сьогоднішній день є очевидним фактом для будь-якого навіть достатньо невеликого підприємства. Політика безпеки в цілому — це сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, які чітко регламентують усі аспекти діяльності підприємства, включаючи інформаційну систему, та забезпечують їх безпеку.

Політику з інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки організації, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації із урахуванням цінності інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Під час розробки політики безпеки повинні бути враховані технологія зберігання, оброблення та передавання інформації, моделі порушників і загроз, особливості апаратно-програмних засобів, фізичного середовища та інші чинники. У організації може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки у організації мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації. Політика безпеки повинна

стосуватись: інформації (рівня критичності ресурсів організації), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів організації політика безпеки стосується, а яких — ні).

Висновки

У сучасних умовах світового соціально-економічного розвитку, особливо важливою областю стало інформаційне забезпечення процесу управління, що складається в зборі і обробці інформації, необхідної для прийняття обґрунтованих управлінських рішень.

Сьогодні більшість суб'єктів господарювання використовують комп'ютеризовану форму ведення бухгалтерського обліку, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо.

Для захисту своїх інформаційних ресурсів організаціям необхідно впроваджувати засоби контролю або захисні механізми, призначені для захисту всіх компонентів інформаційної системи, включаючи дані, програмне забезпечення, апаратні засоби та мережі. Заходи контролю призначені для виявлення проблем запобігання випадковим загрозам та навмисним діям, відновлення пошкоджень та усунення проблем.

Безперервність бізнесу означає, що дані та програми організації продовжуватимуть діяти навіть в умовах порушення, знищення або катастрофи. Для її забезпечення необхідними складовими є розробка елементів управління, які запобігатимуть негативному впливу подій на організацію, а також план відновлення після аварії, який дозволить організації відновити ситуацію в разі порушення.

Вторгнення в систему - це вид проблеми безпеки, повинен який повинен отримувати найбільшу увагу. Є чотири типи зловмисників, які можуть намагаютатись отримати несанкціонований доступ до комп'ютерних мереж. Першими є випадкові зловмисники, які мають лише обмежені знання з комп'ютерної безпеки. Другий тип зловмисників - це фахівці з безпеки, але їх мотивація - гострі відчуття. Їх називають хакерами і вони часто мають сильну філософію щодо вільного доступу до інформації. Третій тип зловмисників, найнебезпечніший, - це професійні хакери, які проникають в корпоративні чи урядові комп'ютери з певною метою, наприклад, шпигунство, шахрайство, або навмисне знищення. Четвертий тип порушників - це співробітники організацій, які мають законний доступ до мережі, але отримали доступ до інформації, яку вони не мають права використовувати.

Ключовим принципом у запобіганні вторгненням є активність. Це означає постійне тестування систем безпеки перед тим, як зловмисник зробить це. Для запобігання втручанню та несанкціонованому доступу до організаційних даних і мереж можна вжити багато заходів, але жодна мережа не є повністю безпечною. В сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

Література

1. Вітер, С. А. Захист облікової інформації та кібербезпека підприємства [Текст] / С. А. Вітер, І. І. Світлишин // Економіка і суспільство. – 2017. - №11. – С. 497-502.

2. Гордієнко, С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії [Текст] / С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. — 2013. — № 1. — С. 104—107.

3. Захаркін, О. О. Інформаційні системи та технології у фінансових установах : конспект лекцій [Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. — Суми : Вид-во СумДУ, 2007. — 80 с. — Режим доступу : http://elkniga.info/book_188.html

4. Марущак, А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки [Текст] / А. І. Марущак // Державна безпека України. — 2011. — № 21. — С. 92—95.

5. Северина, С. В. Інформаційна безпека та методи захисту інформації [Текст] / С. В. Северина // Вісник Запорізького національного університету. – 2016. - №1 (29). – С. 155-161.

6. Цаль-Цалко, Ю.С. Облікова політика підприємства та її кібербезпека [Текст] / Ю.С. Цаль-Цалко, Ю.Ю. Мороз // Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць, том IV, частина І, Житомир: ПП «Рута», 2017 – С. 8-11.

7. Ясенев, В. Н. Информационная безопасность в экономических системах : учеб. пособ. [Электронный ресурс] / В. Н. Ясенев. — Н. Новгород: Изд-во ННГУ, 2006. — Режим доступа : http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html

References

1. Viter, S. A., Svetlyshyn, I. I. (2017). Protection of Accounting Information and Cyber Security of the Enterprise. *Economy and Society*, *11*, 497-502.

2. Gordienko, S. B. (2013). Methods and Recommendations for Providing Information Security to a Consulting Company. *Bulletin of the DUIKT*, *1*, 104-107.

3. Zakharkin, O. O. (2007). Information systems and technologies in financial institutions: abstract of lectures. Sumy: View of the SSU, 80. Retrieved from http://elkniga.info/book_188.html

4. Maruschak, A. I. (2011) Information and Legal Directions of Research of Information Security Problems. *State Security of Ukraine,21,* 92-95.
5. Severina, S. V. (2016) Information security and thods of information protection. *Bulletin of the Zaporizhzhya National University, 1(29),* 155-161.
6. Tsal-Tsalko, Ju. S. (2017). Accounting policy of the enterprise and its cyber security. Accounting, analysis and control in the conditions of modern concepts of management of the economic potential and market value of the enterprise: a collection of scientific works, volume IV, part I, Zhytomyr: PE "Ruta", P. 8-11.
7. Yasenev, V. N. (2006) Information security in economic systems: study. way. Publishing house of NNUU. Retrieved from: http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html

Рецензент: д.е.н., професор, завідувач кафедри фінансово-економічної безпеки, обліку і аудиту Т. В. Момот, Харківський національний університет міського господарства імені О.М. Бекетова, Україна

Автор: ЧЕХ Наталія Олександрівна
к.е.н., старший викладач кафедри фінансово-економічної безпеки, обліку і аудиту
Харківський національний університет міського господарства імені О.М. Бекетова
E-mail - natariathebest@gmail.com

Автор: КОНОПЛІНА Олена Олександрівна
асистент кафедри фінансово-економічної безпеки, обліку і аудиту
Харківський національний університет міського господарства імені О.М. Бекетова
E-mail - Konoplina.olena@gmail.com

Автор: ШАХВЕРДЯН Давид Сейранович
аспірант кафедри фінансово-економічної безпеки, обліку і аудиту
Харківський національний університет міського господарства імені О.М. Бекетова
E-mail - natariathebest@gmail.com

INFORMATION SECURITY PROVISION OF ACCOUNTING OF THE ENTERPRISE

N. Chekh, O. Konoplina, D. Shahverdyan
O. M. Beketov National University of Urban Economy in Kharkiv, Ukraine

In this article the theoretical bases of information security of accounting of enterprise are analyzed. The main types of potential threats to information security and sources of these threats are explored.

It is accounting that is the main "producer" and "distributor" of information in different areas and for different groups of users, which include clients, investors, suppliers, government organizations and other parties that are not accountants. As a whole, it can be argued that accounting today includes five main components. These include: people, operations, data, software, information technology infrastructure. Together, these five components make it possible to implement three main functions in any organization:

- *collection and storage of data on the activities of the organization;*
- *processing data and turning it into useful information for decision making;*
- *proper control for the protection of assets, including data, and ensuring that reliable and adequate information is available.*

The recommendations for measures to increase the level of information security and ensure the protection of accounting information have been formed. The task of providing information security must be solved systematically. This means that information security means must be applied simultaneously and under centralized control.

To protect their information resources, organizations need to implement controls oa security mechanisms designed to protect all components of the information system, including data, software, hardware and networks. Data protection technologies are based on the use of modern methods that prevent information leakage and its loss.

Today, six main methods of protection are used: obstruction, masking, regulation, management, coercion, induction. All of these techniques are aimed at building an effective technology of information security, which eliminates costs due to negligence and successfully displays various types of threats.Control measures are designed to identify problems of preventing accidental threats and intentional actions, repairing damages and troubleshooting.

Keywords: *information, information security, threats, information leakage, accounting data.*