управління: актуальні питання / О.М. Кондратюк // Актуальні проблеми економіки. – 2014. – № 7(157). – С. 441-448.
9. Кондратюк О.М. Бухгалтерський облік і психологія: міждисциплінарний зв'язок / О.М. Кондратюк // Бухгалтерський облік, економічний аналіз та контроль в умовах формування і розвитку сучасних концепцій управління : тези виступів XII Міжнар. наукової конференції ЖДТУ. – Житомир : ЖДТУ, 2013. – С. 24-26.
10. Кузнецова Л.Н. Применение процессного подхода в организации учета / Л.Н. Кузнецова // Проблемы современной экономики. – 2010. – № 2(34) [Електронний ресурс]. – Режим доступу : http://www.m-economy.ru/art.php?nArtId=3109.
11. Легенчук С.Ф. Бухгалтерське теоретичне знання: від теорії до метатеорії : [монографія] / С.Ф. Легенчук. – Житомир : ЖДТУ, 2012. – 336 с.
12. Лучко М.Р. Особистісна адаптованість бухгалтера як провідна характеристика його професіоналізму / М.Р. Лучко, І.С. Ревасевич // Незалежний АУДИТОР. – 2012. – № 1(III). – С. 10-19.
13. Малявко А.Б. Обеспечение качества учетных систем / А.Б. Малявко // Вестник НГУ. Серия: Социально-экономические науки. – 2009. – Том 9, Выпуск 1. – С. 60-70.
14. Мягмар М. Методы и методики оценки качества учетной информации / М. Мягмар // Вопросы экономики и права. – 2012. – № 3. – С. 273-276.
15. Пушкар М.С. Ідеальна система обліку: концепція, архітектура, інформація / М.С. Пушкар, М.Г. Чумаченко. – Тернопіль : Карт-бланш, 2011. – 336 с.
16. Развитие интегрированной системы учета и отчетности: методология и практика : монография. Под ред. Каморджановой Н.А. – М. : «Издательство «Проспект», 2015. – 172 с.
17. Рудановский А.П. Теория балансового учета. Оценка как цель балансового учета. – М. : МАКИЗ, 1928. – 174 с.
18. Садовська І.Б. Критерії оцінки якості управлінської звітності / І.Б. Садовська, К.Є. Нагірська // Глобальні та національні проблеми економіки. – 2015. – Випуск 3. – С. 899-904.
19. Соколов Я.В. Бухгалтерский учёт: от истоков до наших дней : учебн. пособие для вузов. – М. : Аудит, ЮНИТИ, 1996. – 638 с.
20. Соколова Е.Е. Методы оценки качества учётной информации / Е.Е. Соколова // Экономика, Статистика и Информатика. Вестник УМО. – 2011. – № 2. – С. 118-124.
21. Старовойтова Е.В. Развитие бухгалтерского учета и отчетности в россии на основе международных стандартов финансовой отчетности / Е.В. Старовойтова // Аудит и финансовый анализ. – 2007. – № 4. – С. 96-103.
22. Чайковская Л.А. Современные концепции бухгалтерского учета (теория и методология) : автореф автореф. дис. … на соискание уч. степени докт. экон. наук : спец. 08.00.12 «Бухгалтерский учет, статистика» / Л.А. Чайковская. – Москва, 2007. – 45 с.
23. Шеверя Я.В. Регулювання та якість фінансової звітності в Україні / Я.В. Шеверя // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. – 2014. – № 1(28). – С. 302-318.

УДК 657.454:004.424

Сахаров П.О.
кандидат економічних наук,
доцент кафедри бухгалтерського обліку
Харківського національного економічного університету
імені Семена Кузнеця

УДОСКОНАЛЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ РОЗРАХУНКІВ ЕЛЕКТРОННИМИ ГРОШИМА В АВТОМАТИЗОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА

Проаналізовано сутність контрольних процедур щодо внутрішнього контролю розрахунків електронними грошима. Досліджено теоретичні питання контролю розрахунків. Розроблено алгоритм перевірки достовірності розрахунків електронними грошима.
Ключові слова: електронні гроші, система внутрішнього контролю, фішинг.

Сахаров П.А. УСОВЕРШЕНСТВОВАНИЕ ВНУТРЕННЕГО КОНТРОЛЯ РАСЧЕТОВ ЭЛЕКТРОННЫМИ ДЕНЬГАМИ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ
Проанализирована сущность контрольных процедур относительно внутреннего контроля расчетов электронными деньгами. Исследованы теоретические вопросы контроля расчетов. Разработан алгоритм проверки достоверности расчетов электронными деньгами.
Ключевые слова: электронные деньги, система внутреннего контроля, фишинг.

Sakharov P.O. IMPROVING INTERNAL CONTROL ELECTRONIC MONEY SETTLEMENT IN AUTOMATED INFORMATION SYSTEM OF ENTERPRISE
The essence of control procedures regarding internal control electronic money payments. Theoretical calculations control issues. The algorithm validation calculations electronic money.
Keywords: electronic money, system of internal control, phishing.

Постановка проблеми. Якість проведення аналізу та своєчасне надходження інформації значною мірою залежать від своєчасного прийняття ефективних управлінських рішень щодо операцій з використанням електронних грошей, забезпечення безумовного та якісного їх виконання та використання сучасних форм звітності та методів контролю за їхнім виконанням. Побудова цілісної ефективної системи інформаційно-аналітичного забезпечення внутрішнього контролю з використанням новітніх інформаційних технологій – це єдина умова для вирішення цих проблем.

Аналіз останніх досліджень і публікацій. Процес управління та контролю розрахунків електронними грошима описують у своїх працях Ч. Хорнгер, Дж. Фостер, І.О. Бланк, А.М. Поддєрьогін, І.С. Несходовський, О.С. Височан, В.В. Варавка, В.В. Скоробогатова та інші науковці. Ч. Хорнгер та Дж. Фостер визначають внутрішній контроль як комплекс бухгалтерського управлінського контролю, який допомагає забезпечити відповідність рішень, прийнятих в організації, з реалізацією їх на практиці. На думку Ю.С. Рогозян та Н.О. Ковальової, «контроль грошових коштів – це контролююча сис-

тема, яка забезпечує концентрацію контрольних дій на найпріоритетніші напрями розвитку, своєчасне виявлення відхилень фактично досягнутих результатів їх формування від планових і прийняття оперативних управлінських рішень, що забезпечить їх безперервний рух».

Постановка завдання. Відповідно до поставленої мети визначено такі завдання дослідження:

- дослідити сучасний стан і перспективи використання електронних грошових засобів у національній економіці;
- запропонувати напрями удосконалення контролю розрахунків електронними грошима в інформаційній системі торговельно-виробничого підприємства.

Метою статті є обґрунтування теоретико-методичних засад та розробка практичних рекомендацій щодо удосконалення обліку і внутрішнього контролю розрахунків електронними грошима.

Виклад основного матеріалу дослідження. Система внутрішнього контролю розрахунків торговельно-виробничих підприємств відрізняється урахуванням специфіки проведення розрахунків з використанням електронних грошей, що дозволило рекомендувати організаційно-методичні підходи до перевірки функціонування системи захисту електронних грошей від фішингових атак.

За допомогою таких чинників обумовлена необхідність використання автоматизованих систем та інформаційних технологій для підвищення ефективності здійснення внутрішнього контролю за розрахунками з використанням електронних грошей на торговельно-виробничому підприємстві, а саме:

- трудомісткістю контрольних процедур, які вимагають здійснення великої кількості арифметичних розрахунків, різних видів аналізу. Автоматизація внутрішнього контролю підвищить ефективність прийняття рішення і надасть можливість проведення розрахунків різного ступеню складності, аналітичних процедур з використанням статистичних методів і методів моделювання;
- значними обсягами інформації торговельно-виробничого підприємства, які необхідно обробити, і на основі одержаних результатів розробити рекомендації щодо запобігання в майбутньому помилок, зловживань, невідповідностей діючому законодавству функціонування систем електронних грошей;
- вимогами до швидкості проведення обчислень, перевірок, забезпеченням їх високої якості;
- циклічністю технологічного процесу внутрішнього контролю. Господарська діяльність торговельно-виробничих підприємств здійснюється циклічно. Відповідно процеси, пов'язані з нею, відбуваються систематично. Процес контролю також не є винятком. Це дає змогу стандартизувати та уніфікувати методику його процедур і їх автоматизувати;
- необхідністю швидкого і повного виявлення помилок. При використанні засобів автоматизованої обробки даних зменшується вплив людського фактору на будь-який процес. Система навмисне не зможе зробити помилку, тому зменшується імовірність їх здійснення, полегшується процес їх виявлення [1, с. 90].

Конфіденційність, цілісність, аутентифікація, авторизація, гарантії та збереження таємниці – це одні з основних вимог, які враховуються до проведення комерційних операцій з використанням електронних грошей. Перші чотири вимоги забезпечуються технічними та програмними засобами, але виконання останніх двох – досягнення гарантій і збереження таємниці – однаково залежить як від програмно-технічних засобів та відповідальності окремих осіб та організацій, так і від дотримання законів, що захищають споживача систем електронних грошей від можливого шахрайства [2, с. 20].

Використання у практиці діяльності підприємств електронних грошей завжди супроводжується підвищеними, порівняно з традиційними розрахунками, ризиками [3, с. 172-175].

При проведенні внутрішнього контролю операцій з електронними грошима службі внутрішнього контролю (СВК) необхідно оцінювати такі види ризиків:

- дублювання технічного пристрою – носія електронної готівки;
- порушення цілісності відомостей або програм функціонування систем електронних грошей;
- перехоплення та зміни повідомлень між торговельно-виробничим підприємством та емітентом електронних грошей;
- крадіжки коштів з електронного пристрою;
- викрадення комп'ютерних даних,
- відмови від операцій з використанням електронних грошей;
- шахрайства, пов'язані з електронними переказами.

Ризик дублювання технічного пристрою є вірогідністю збитків у результаті створення шахраєм нового електронного гаманця, який приймав би електронні гроші як справжній, шляхом копіювання криптографічних ключів електронного гаманця та залишків по рахунку. Як альтернатива, шахраї можуть створити електронний гаманець, який функціонував би як справжній, але містив би залишки електронних грошей, створених шахрайським шляхом.

Іншим ризиком шахрайства може бути ризик зміни інформації, що зберігається в електронному гаманці. Якщо залишки грошових коштів, записані на карті, були збільшені шахрайським шляхом без видимих порушень (поломок) самої карти, то власник такої картки може виконувати операції з цієї карти, яка торговельному терміналу здаватиметься справжньою. Крім того, можуть бути змінені внутрішні функції електронного гаманця, наприклад процедури звітності (при запиті «Довідки про залишок електронних грошей» в ній може вказуватися сума електронних грошей, яка була на рахунку до здійснення незаконних операцій з електронними грішми). Шляхом фізичної дії безпосередньо на сам чіп електронного гаманця або завдяки слабкій безпеці операційної системи шахрай може змінити дані або функції електронного гаманця.

У результаті зміни даних або процесів технічного пристрою шляхом видалення, повтору виникає ризик зміни повідомлень, який може призвести до значних збитків. При цьому повідомлення між технічними пристроями можуть бути перехоплені шахраями у момент їх передачі по телекомунікаційних лініях, комп'ютерних мережах або при прямому контакті між технічними пристроями.

Також шахрай може викрасти технічний пристрій, або дані, що зберігаються на ньому, шляхом незаконного копіювання і незаконно використати залишки електронних грошей, записаних на ньому. Шахрай може перехопити повідомлення між законним власником електронних грошей та їх емітентом, а потім використовувати перехоплені дані при здійсненні будь-яких операцій, при цьому така крадіжка буде виявлена лише після того, як емітент отримає справжні електронні грошові знаки, які матимуть

аналогічні характеристики з незаконними грошима, а шахрай на той час вже отримає фінансову вигоду.

Шахрайство може бути здійснене також шляхом відмови від операцій, зроблених за допомогою електронних грошей. Наприклад, при дистанційних операціях, що здійснюються за допомогою телефону або комп'ютерних мереж, користувач може заявити, що не дозволяв проводити операцію. Це, у свою чергу, може призвести до фінансових втрат торговельно-виробничого підприємства або емітента електронних грошей [4].

Спеціальних систем автоматизації контрольних процедур для перевірки систем електронних грошей на ринку не існує. Тому службі внутрішнього контролю доцільно у процесі перевірки адаптовувати та використовувати системи автоматизації бухгалтерського обліку та окремі програмні модулі, які автоматизують товарно-грошові відносини з використанням електронних грошей в відкритих та закритих системах їх функціонування.

Серед найпоширеніших загроз, які можуть виникати у системах електронних грошей, можна виділити: фішинг, шахрайства, пов'язані з електронними переказами, викрадення комп'ютерних даних, віртуальний шантаж тощо. За принципом поширеності можна виділити такі типи шахрайств (табл. 1) [5].

Таблиця 1

Класифікація шахрайств за принципом поширеності

Типи шахрайств	Частка поширеності шахрайства (%)
1. Шахрайство з втраченими і викраденими пластиковими картками	72,2
2. Шахрайство з підробленими картками	20,5
3. Шахрайство з картками, не отриманими законним держателем	2,8
4. Шахрайство з використанням рахунку	1,4
5. Інші форми шахрайства	3,1

Зупинимося більш детально на найпоширенішому методі шахрайства у системах електронних грошей – фішингу. Більше 20% атак спрямовані на банки та інші фінансово-кредитні установи, збитки від фішингових атак вимірюються декількома мільярдами доларів США, при цьому, згідно із статистикою, кількість фішингових атак кожного року збільшується приблизно у півтора рази [199].

Існує декілька видів фішингу – поштовий, онлайновий та комбінований. Поштовий фішинг – це проведення масових розсилок електронних листів або повідомлень у соціальних мережах від імені відомих організацій, наприклад від імені банків користувачам електронних гаманців. Наприклад, бухгалтеру торговельно-виробничого підприємства надходить лист з банку або від контрагента з проханням надіслати конфіденційні дані про підприємство або про зміну правил користування електронним гаманцем (про необхідність перереєстрації електронного гаманця, погрозі блокування клієнтського рахунку тощо) та пропонують пройти по посиланню або ввести паролі до електронного гаманця (рис. 1).

Основними характерними ознаками фішингових листів є неперсоналізованість (в листі не наведено прізвище користувача електронного гаманця чи назву торговельно-виробничого підприємства), екстреність (прохання надіслати відповідь в певний проміжок часу окреслюючи ліміт часу), у листі обов'язково буде присутнє гіперпосилання на сайт і пропозиція туди перейти, у листі можлива наявність погроз (заблокувати рахунок, припинити співпрацю тощо) у разі відмови від виконання вимог.

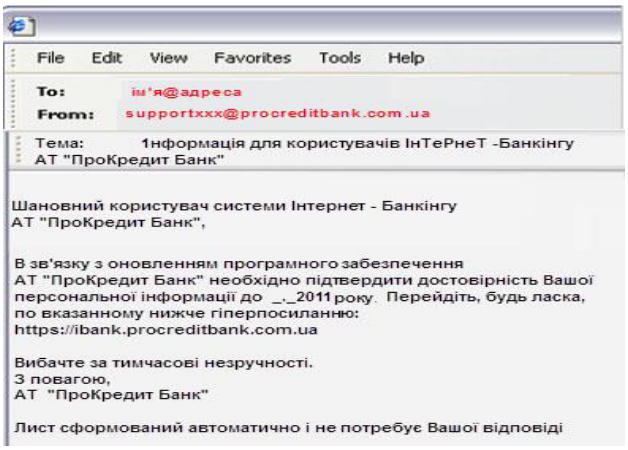

Рис. 1. Приклад фішингового листа

Онлайн-фішинг – це копіювання відомих сайтів (найчастіше інтернет-магазинів), на яких пропонується здійснити вигідні покупки товарів за привабливими цінами [7, с. 10-11]. Зовні сайти схожі на офіційні веб-адреси інтернет-магазинів і перенаправляють користувачів електронних гаманців на вебсайти, які імітують зовнішній вигляд легітимного сайту (рис. 2).

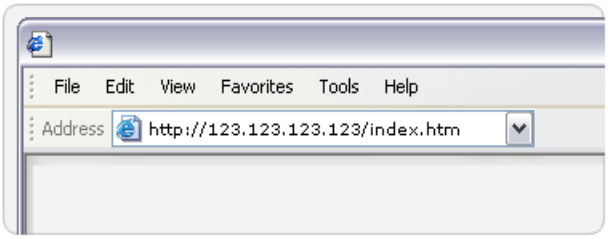

Рис. 2. Приклад адресного рядка фальшивого веб-сайту

Бухгалтер торговельно-виробничого підприємства може перевести електронні гроші на фальшивий рахунок, проте замовлений товар не отримати.

Існує також комбінований фішинг – це поєднання поштового та онлайн фішингу. Наприклад, бухгалтер торговельно-виробничого підприємства заходить на легітимний сайт, під час перегляду якого автоматично завантажуються віруси або шпіонські програми, які фіксують коди входу до електронного гаманця.

Для запобігання втрати електронних грошей при фішингових атаках службі внутрішнього контролю (СВК) торговельно-виробничого підприємства необхідно розробляти системи захисту електронних грошей від фішингу та рекомендації, щодо безпечного користування електронними гаманцями персоналу, що мають до них доступ. Найбільшу загрозу фішингові ресурси представляють у першу добу їх існування [8, с. 50-55.], тому СВК необхідно проводити безперервний моніторинг інтернет-ресурсів. На основі проведеного моніторингу необхідно створювати повноцінну систему захисту від фішингових атак та вносити її до інформаційної бази роботи СВК. Пропонуємо таку послідовність перевірки СВК функ-

ціонування системи захисту електронних грошей від фішингових атак:

1) генерація списку потенційно небезпечних інтернет-сайтів та внесення їх до «банку даних перевірок»;

2) формування списку зареєстрованих та доступних потенційно небезпечних інформаційних ресурсів;

3) визначення ступеня небезпечності кожного потенційно небезпечного інформаційного ресурсу;

4) поповнення антифішингових баз виявленими небезпечними інформаційними ресурсами.

При реєстрації електронного гаманця СВК необхідно перевірити налаштування програмного забезпечення, яке використовується для обслуговування електронних гаманців. Це можна зробити таким чином: в інформаційній системі необхідно налаштувати функцію безпечного перегляду, яка відповідає за виявлення фішингу і небезпечного програмного забезпечення та призначена для захисту комп'ютера і конфіденційності користувача електронного гаманця (рис. 3).

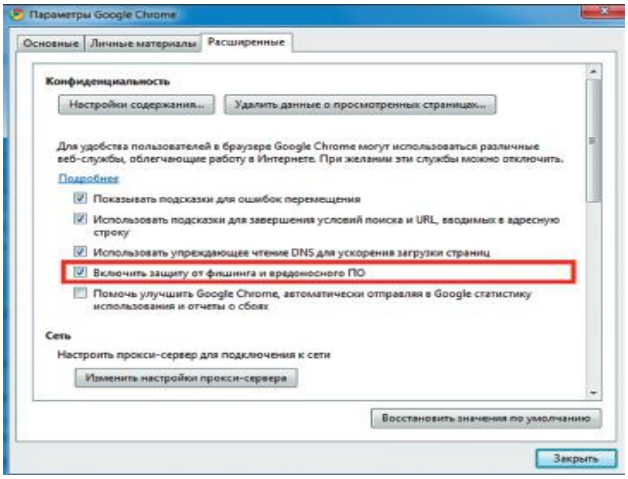

Рис. 3. Налаштування в інформаційній системі захисту від фішингу

Також при кожній операції з використанням електронних грошей СВК доцільно перевіряти автентичність сайту емітента електронних грошей, шляхом перевірки цифрового сертифікату безпеки шляхом натискання на символ безпечного з'єднання в інтернет-браузері, який використовується на торговельно-виробничому підприємстві (рис. 4).

При втраті електронних грошей внаслідок фішингу або інших протиправних дій службі внутрішнього контролю необхідно перевірити правильність відображення в обліку втрати електронних грошей. На основі відповідної заяви до правоохоронних органів про втрату електронних грошей з електронного гаманця в обліку необхідно відобразити: Дт 947 «Нестачі і втрати від псування цінностей» та Кт 321 «Електронні гроші на картковій основі» (у разі втрати електронних грошей з картки) або 322 «Електронні гроші на програмній основі» (у разі втрати електронних грошей, які функціонують на програмній основі), з одночасним віднесенням суми втрати електронних грошей у дебет позабалансового субрахунку 072 «Невідшкодовані нестачі і втрати від псування цінностей». Якщо електронні гроші будуть знайдені в обліку необхідно відобразити: Дт 375 «Розрахунки за відшкодуванням завданих збитків», Кт 751 «Відшкодування збитків від надзвичайних подій», Кт 072 «Невідшкодовані нестачі і втрати від псування цінностей». Повернення правопорушником електронних грошей у гаманець користувача відображається в обліку: Дт 321 «Електронні гроші на картковій основі» або 322 «Електронні гроші на програмній основі», Кт 375 «Розрахунки за відшкодуванням завданих збитків».

Контроль розрахунків електронними грошима з використанням інформаційних технологій забезпечує централізацію управління грошовими коштами торговельно-виробничого підприємства в режимі реального часу і в рамках єдиної інформаційної системи, виключає ризики несанкціонованого витрачання електронних грошей. Це стає можливим завдяки поєднанню в рамках контролю повного циклу фінансових процесів у короткостроковому періоді, починаючи з введення планових даних руху електронних грошей і до реєстрації факту витрачання електронних грошей на основі даних про виконання платежу з систем банк-клієнт.

Висновки з проведеного дослідження. Відповідно до поставленої мети можна зробити висновок, що: електронні гроші є різновидом грошових засобів, тому для розробки системи їх внутрішнього контр-

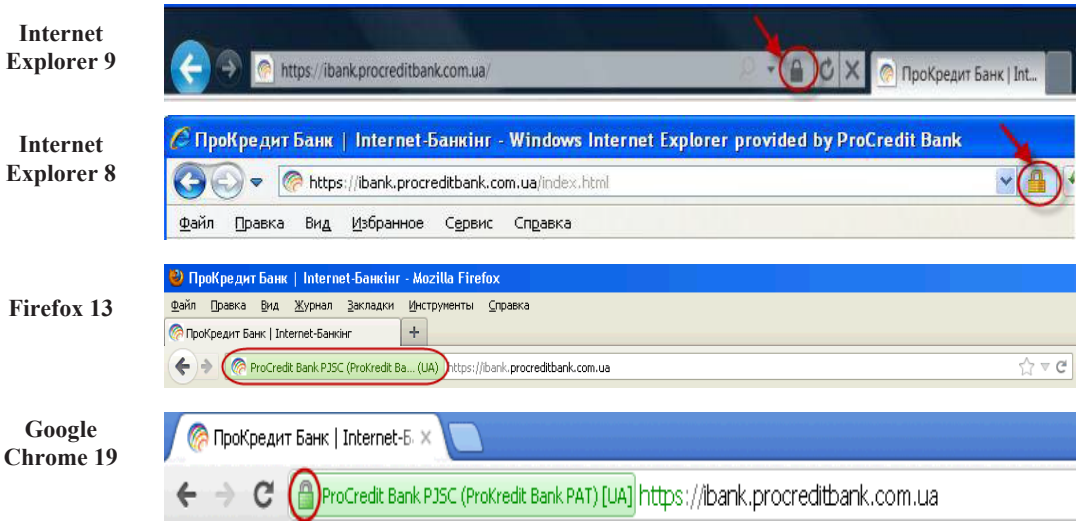

Рис. 4. Види символів безпечного з'єднання в інтернет-браузерах

олю на рівні торговельно-виробничих підприємств пропонується трактувати внутрішній контроль розрахунків електронними грошима як систему безперервного спостереження ініційовану керівництвом підприємства: за дотриманням порядку проведення розрахункових операцій, з використанням електронних грошей вимогам нормативно-правових актів та внутрішніх розпорядчих документів; повноти і своєчасності відображення електронних грошей в обліку та звітності господарюючого суб'єкта; виявлення і запобігання відхилень, що перешкоджають законному та ефективному використанню електронних грошей; усунення причин і умов, що призводять до їх втрати; розробки рекомендацій з усунення їх у майбутньому з метою підвищення ефективності управління підприємством. Визначено мету внутрішнього контролю використання електронних грошей на торговельно-виробничих підприємствах, яка полягає в отриманні доказів впевненості в ефективності здійснення товарно-грошових операцій, підтвердженні достовірності даних про наявність та рух електронних грошей у відповідності з організацією методики їх обліку, встановленні правильності оформлення господарських фактів відповідно до чинного законодавства та виявленні резервів і визначенні найбільш ефективних шляхів подальшого розвитку торговельного підприємства. Аналіз контрольних процедур розрахунків різними видами грошей (безготівкові, електронні, готівкові) свідчать про необхідність розробки окремого блоку контрольних процедур, які не притаманні готівковим та безготівковим розрахункам, але є актуальними для контролю розрахунків електронними грошима: перевірка Легітимності платіжної системи; контроль автентичності електронних цифрових підписів; Інвентаризація електронного гаманця; перевірка надійності технічного забезпечення функціонування електронного гаманця; Контроль правильності відображення електронних грошей у облікових регістрах та фінансовій звітності. За результатами перевірки розрахунків електронними грошима системою внутрішнього контролю пропонується складати пакет документів, форми яких розроблені у процесі дослідження.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Яровенко Г.М. Аспекти автоматизації фінансового контролю підприємств / Г.М. Яровенко // Вісник Української академії банківської справи. – 2004. – № 2(17). – С. 89-96.
2. Берко А.Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А.Ю. Берко, В.А. Висоцька, І.В. Рішняк // Вісник Національного університету «Львівська політехніка». – 2008. – № 610. – С. 20-33.
3. Абдеева З.Р. Проблемы безопасности электронной коммерции в сети Интернет / З.Р. Абдеева // Проблемы современной экономики. – 2012. – № 1(41). – С. 172-175.
4. Горюков Е.В. Электронные деньги: развитие, направления использования в современной банковской практике (окончание) / Е.В. Горюков, О.В. Котина [Электронный ресурс]. – Режим доступа : <http://bankir.ru/tehnologii/s/elektronnie-dengi-razvitie-napravleniya-ispolzovaniya-v-sovremennoi-bankovskoi-praktike-okonchanie-1373402/>.
5. Петрущак В. Пластикові небезпеки / В. Петрущак [Електронний ресурс]. – Режим доступу : <http://www.gazeta.lviv.ua/articles/2007/08/21/25702/>.
6. Phishing Activity Trends Report [Electronic resource]. – Access mode : <www.apwg.org>.
7. Валентинова Т. Осторожно – фишинг! Как могут «выудить» деньги из вашего електронного кошелика / Т. Валентинова // Все о бухгалтерском учете. – 2012. – № 42. – С. 10-11.
8. Милошенко А.В. Разработка комплексной обучаемой системы защиты информационных ресурсов от фишинговых атак / А.В. Милошенко, Т.М. Соловьёв, Р.И. Черняк, М. В. Шумская // Прикладная дискретная математика. – 2011. – № 4. – С. 50-55.