УДК 657.1.011.56

ЗАХИСТ ОБЛІКОВОЇ ІНФОРМАЦІЇ В УМОВАХ АУТСОРСИНГУ ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

©2017 **ЛЯХОВИЧ Г. І.**

УДК 657.1.011.56

Ляхович Г. І. Захист облікової інформації в умовах аутсорсингу із використанням інформаційно-комп'ютерних технологій

Метою статті є розкриття заходів захисту облікової інформації в умовах аутсорсингу, що здійснюється з використанням сучасних інформаційно-комп'ютерних технологій. На основі опрацювання наукових праць узагальнено підходи до розробки системи захисту облікової інформації, згруповано заходи із захисту за користувачами даних з визначенням суб'єктів забезпечення в умовах аутсорсингу. Особливу увагу приділено характеристиці та змістовному наповненню внутрішніх організаційних заходів із захисту облікової інформації (нормативним, кадровим, структурним). Визначено комплекс заходів щодо захисту інформації бухгалтерського обліку для великих і малих підприємств. Перспективами подальших досліджень є питання управління інформаційними ризиками при бухгалтерському аутсорсингу.

Ключові слова: *аутсорсинг, інформаційно-комп'ютерні технології, економічна безпека, захист інформації.*

Рис.: *1.* ***Табл.:*** *1.* ***Бібл.:*** *8.*

Ляхович Галина Іванівна *– кандидат наук з державного управління, доцент, директор Івано-Франківського навчально-наукового інституту менеджменту Тернопільського національного економічного університету (вул. Галицька, 7, Івано-Франківськ, 76000, Україна)*

E-mail: *kaffinance@ukr.net*

УДК 657.1.011.56

Ляхович Г. И. Защита учетной информации в условиях аутсорсинга с использованием информационно-компьютерных технологий

Целью статьи является раскрытие мер защиты учетной информации в условиях аутсорсинга с использованием современных информационно-компьютерных технологий. На основе обработки научных работ обобщены подходы к разработке системы защиты учетной информации, сгруппированы меры защиты по пользователям данных с определением субъектов обеспечения в условиях аутсорсинга. Особое внимание уделено характеристике и содержательному наполнению внутренних организационных мер защиты учетной информации (нормативным, кадровым, структурным). Определен комплекс мероприятий по защите информации бухгалтерского учета для крупных и малых предприятий. Перспективами дальнейших исследований является вопрос управления информационными рисками при бухгалтерском аутсорсинге.

Ключевые слова: *аутсорсинг, информационно-компьютерные технологии, экономическая безопасность, защита информации.*

Рис.: *1.* ***Табл.:*** *1.* ***Библ.:*** *8.*

Ляхович Галина Ивановна *– кандидат наук по государственному управлению, доцент, директор Ивано-Франковского учебно-научного института менеджмента Тернопольского национального экономического университета (ул. Галицкая, 7, Ивано-Франковск, 76000, Украина)*

E-mail: *kaffinance@ukr.net*

UDC 657.1.011.56

Liakhovych H. I. Protecting the Accounting Information in the Conditions of Outsourcing with Use of the Information-Computer Technologies

The article is aimed at disclosing measures of protection of accounting information in the conditions of outsourcing, using modern information-computer technologies. On the basis of processing of scientific works, the approaches to development of system of protection of the accounting information were generalized, measures of protection were grouped by users of data with definition of subjects of provision in the conditions of outsourcing. Special attention is paid to the characterization and content of internal organizational measures of protection of accounting information (normative, personnel, structural). The complex of measures on protection of the information of accountance for large and small-size enterprises has been defined. The prospect of further research is the issue of information risk management in accounting outsourcing.

Keywords: *outsourcing, information-computer technologies, economic security, information protection.*

Fig.: *1.* ***Tbl.:*** *1.* ***Bibl.:*** *8.*

Liakhovych Halyna I. *– PhD (State Administration), Associate Professor, Director of the Ivano-Frankivsk Educational and Scientific Management Institute of Ternopil National Economic University (7 Halytska Str., Ivano-Frankivsk, 76000, Ukraine)*

E-mail: *kaffinance@ukr.net*

Використання інформаційно-комп'ютерних технологій у бухгалтерському обліку пов'язане із необхідністю обробки значних обсягів інформації щодо діяльності підприємства, технології виробництва, даних працівників тощо. Як справедливо зазначає Б. Цибуляк: «Більшість інформації зосереджена в електронній формі, що дозволяє легко її скопіювати, змінити чи знищити за відсутності добре налагодженої системи інформаційної безпеки підприємства» [6, с. 246]. Дане твердження набуває особливої актуальності, коли до облікової інформації допускаються сторонні відносно підприємства суб'єкти, як це відбувається, наприклад, при залученні аутсорсингових компаній до ведення обліку. Крім того, сам процес передачі даних між аутсорсером і замовником, як правило, здійснюється з використанням інформаційно-комп'ютерних технологій, що в собі приховує загрози витоку інформації, кібератак. Так, згідно з проведеними дослідженнями [7], кількість зафіксованих кібератак на початок 2017 р. зросла порівняно з аналогічним періодом 2016 р. на 60%. Вищенаведене підтверджує необхідність дослідження питань розробки заходів із захисту облікової інформації в умовах аутсорсингу, який здійснюється з використанням інформаційно-комп'ютерних технологій.

Питанням безпеки та захисту облікової інформації займаються багато вчених, серед яких Дикий А. П., Євдокимов В. В., Семенчук М. В., Рожелюк В. М., Боримська К. П., Шишкова Н. Л., Вітер С. А., Світлишин І. І., Шпак В. А. та інші. Всі вони так чи інакше розглядають питання забезпечення економічної безпеки підприємства, що безпосередньо пов'язане із безпекою облікової інформації.

Під економічною безпекою підприємства слід розуміти такий його стан і характеристику, за якого за-

безпечується захист економічної та іншої інформації від реалізації загроз внутрішнього та зовнішнього характеру, що можуть призвести до різних маніпуляцій із даними та негативно вплинути на діяльність суб'єкта господарювання. До економічної безпеки підприємства належить і захист облікової інформації. Оскільки облікові дані переважно містять комерційну таємницю, організація захисту має свою специфіку в умовах ведення бухгалтерського обліку зовнішніми суб'єктами – аутсорсинговими компаніями.

Відповідно до ст. 505 Цивільного кодексу України комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Водночас Постановою КМУ від 09.08.1993 р. № 611 «Про перелік відомостей, що не становлять комерційної таємниці» встановлено перелік тих даних, що не можуть бути визнаними як комерційна таємниця, і до них належать:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що, відповідно до чинного законодавства, підлягають оголошенню.

Однак відкритість такої інформації, що не належить до комерційної таємниці, обмежується тим, як саме вона була отримана, оскільки відповідно до Постанови КМУ від 09.08.1993 р. № 611 «Про перелік відомостей, що не становлять комерційної таємниці» також встановлено, що підприємства зобов'язані подавати такі відкриті дані до контролюючих органів та інших органів відповідно до чинного законодавства та за їх вимогою.

Колобов Л. і Колеснікова І. [5] у своїх дослідженнях визначають дві групи інформації, що належить до комерційної таємниці:

- *перша група* – технічна інформація (включає всі розробки підприємства, незапатентовані розробки, «ноу-хау» тощо);
- *друга група* – комерційна інформація (інформація про покупців, постачальників, дані про переговори, розміри знижок тощо).

Комерційна таємниця передбачає її захист на підприємстві, що може здійснюватися такими заходами, як:

1) внутрішнє нормативне закріплення правил віднесення інформації до комерційної таємниці;

2) закріплення правил обліку документів, що містять комерційну таємницю;

3) визначення кола осіб, які можуть володіти нею;

4) встановлення кола осіб, яким може бути відкритий доступ до частини або повного складу комерційної таємниці;

5) закріплення в договорах, актах і розписках прав та обов'язків осіб, допущених до комерційної таємниці, та визначення їх відповідальності за володіння такою інформацією та порушення встановлених вимог;

6) створення внутрішніх органів забезпечення захисту комерційної таємниці тощо.

Такі заходи дадуть змогу убезпечити комерційну таємницю від маніпуляцій з нею.

Захист облікової інформації, у тому числі й комерційної таємниці, набуває особливого ваги в нинішніх умовах, коли рівень комп'ютеризації бухгалтерського обліку досить високий. Використання інформаційно-комп'ютерних технологій має багато позитивних сторін, але, разом з тим, воно значно зменшило безпеку інформації, що зберігається на комп'ютерах, серверах та в Інтернеті.

В Україні з'явилося таке поняття, як кібербезпека. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» встановлено, що кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Тобто захист облікової інформації та її кібербезпека пов'язані. Проте захист є більш ширшим поняттям і ґрунтується на безпеці всієї облікової інформації незалежно від її форми, у той час, як кібербезпека бухгалтерських даних пов'язана тільки з даними, що знаходяться на комп'ютерах із доступом до мережі Інтернет.

Науковці визначають різні види, групи, класи заходів захисту облікової інформації (*табл. 1*).

Таблиця 1

Види заходів захисту облікової інформації в наукових джерелах

Автор(-и), джерело	Види заходів захисту
Дикий А. П. [4]	1) кадрова робота (кадрова підтримка та робота із персоналом); 2) організаційно-технічні заходи (захист від акустичного підслуховування, захист інформації в системах зв'язку, від витоку за рахунок засобів масової інформації, від несанкціонованого доступу); 3) організаційно-режимні методи (забезпечення фізичної безпеки облікового персоналу, охорона приміщення бухгалтерії та документів, контроль доступу)
Вітер С. А., Світлишин І. І. [2]	1) організаційні (обмеження несанкціонованого доступу до конфіденційної облікової інформації); 2) технічні (попередження навмисного пошкодження облікової інформації за допомогою спеціально спровокованих порушень працездатності технічних засобів або програмного забезпечення); 3) кадрова робота (підвищення компетентності працівників та їх відповідальності у застосуванні новітніх інформаційних технологій)
Шишкова Н. Л. [8]	1) правові (нормативно-правове та організаційно-правового закріплення у документах, договорах, актах відповідальності щодо конфіденційності інформації, прав та обов'язків працівників); 2) технічні (технічні заходи захисту комп'ютерної техніки, приміщень бухгалтерії та інших будівель, пожежна безпека, виявлення приладів розвідування інформації); 3) програмні (спеціальні продукти програмного захисту, регламентація доступу до електронних баз даних та електронних документів за допомогою паролів та ідентифікаційних програм, криптографічні засоби шифрування); 4) організаційні (формування та регламентація служби безпеки, регламентація переліку конфіденційної інформації, комерційної таємниці, системи обмеження доступу до даних, архівного зберігання, побудова захищеного документообігу, ліцензування програм та інше)
Боримська К. П., Кінзерська Н. В. [1]	1) організаційно-режимна компонента (постійне оновлення та адміністрування головної бази даних, організація оперативного доступу та збереження інформаційного фонду, документальне затвердження переліку відомостей, які становлять комерційну таємницю; контроль за проходженням, передачею, опрацюванням та архівуванням документів; контроль виконання документів; організація фізичного захисту інформаційних систем від витоку інформації та несанкціонованого доступу до них); 2) організаційно-технічна компонента (підготовка друкованих зведень, аналітичних довідок та статистичних звітів про стан документообігу; ведення електронних документів; організація оперативного пошуку інформації по документах за певними реквізитами; визначення типових маршрутів та технологічних схем обробки електронних документів; організація зберігання усіх примірників документів; організація служб копіювання, архівування та відновлення електронних документів, забезпечення їх захисту від несанкціонованого доступу)

Варіативність наведених заходів вимагає чіткої структуризації, яка здійснена на основі аналізу видів заходів із захисту облікової інформації в різних джерелах і з урахуванням мети дослідження. Це дозволило здійснити їх групування за користувачами даних з визначенням суб'єктів забезпечення в умовах аутсорсингу (*рис. 1*).

Поділ заходів із захисту облікової інформації на внутрішні та зовнішні обумовлюється наявністю зовнішніх та внутрішніх користувачів даних. Якщо до внутрішніх належать працівники підприємства, власники, управлінський персонал, то до зовнішніх – в основному контрагенти, які можуть бути конкурентами.

Під внутрішніми організаційними заходами захисту облікової інформації розуміються заходи щодо організації захисту бухгалтерських даних, до яких включаємо:

1) *нормативні заходи захисту облікової інформації:*

- розробка внутрішніх нормативних документів щодо критеріїв визначення конфіденційної інформації;
- розробка форм, бланків та регістрів обліку конфіденційної інформації, наприклад журнал допуску до облікових даних із зазначенням дати, часу отримання доступу до даних та підписом;
- затвердження режимів допуску до конфіденційної інформації та інші;

2) *кадрові заходи захисту:*

- укладання «інсайдерських» договорів та контрактів із працівниками, або договорів про нерозголошення інформації, що регулюють правила щодо оприлюднення «секретів підприємства» працівниками, які володіють конфіденційною інформацією або можуть заволодіти нею під час своєї роботи;
- розробка інструкції щодо роботи з працівниками аутсорсингової компанії;
- спонукання працівників до виявлення власного інтересу щодо захисту інформації методом різних заохочень у вигляді грошових премій, підвищення окладу, професійного зростання, підвищення кваліфікації;
- створення списку осіб, що можуть володіти захищеними даними, розпорошення цих даних таким чином, аби тільки декілька осіб володіли повним обсягом інформації, а інші мали тільки доступ до окремих її частин;
- чітке визначення відповідальності, прав та обов'язків осіб, що володіють такою інформацією тощо;

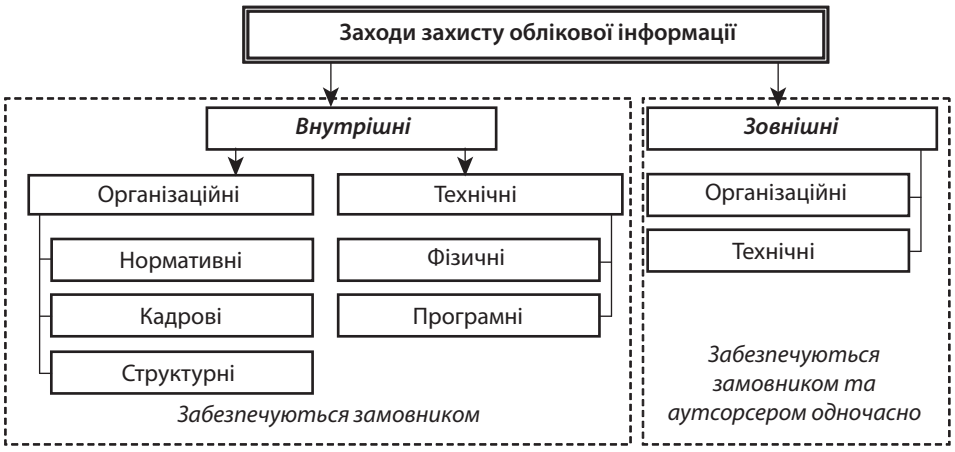

Рис. 1. Класифікація заходів із захисту облікової інформації відповідно до користувачів даних в умовах аутсорсингу

3) *структурні заходи захисту облікової інформації* пов'язані зі створенням служби безпеки інформації на підприємстві, регламентацією її роботи, прав, обов'язків та відповідальності. Зокрема, Дикий А. П. [3] у своїх дослідженнях звертає увагу на важливість служби економічної безпеки на підприємстві щодо захисту облікової інформації.

До складу внутрішніх технічних заходів захисту облікової інформації відносимо фізичні та програмні. Фізичні заходи захисту облікової інформації характеризуються застосуванням різноманітних механічно-технічних засобів захисту, серед яких сигналізація у приміщеннях підприємства, у тому числі бухгалтерії; використання сейфів; застосування картковопропускної системи в приміщеннях підприємства із різним рівнем доступу; захист від різних видів акустичного підслуховування та підглядання; застосування систем відеоспостереження; застосування різноманітних сканерів для ідентифікації працівників та визначення того, що вони приносять/виносять на роботу/з роботи.

Програмні внутрішні технічні заходи захисту облікової інформації пов'язані із використанням програмного забезпечення та різних програмних продуктів для безпеки. Зокрема, використання персональних паролів для працівників на комп'ютерах та у програмах; обмеження доступу до Інтернету із комп'ютерних пристроїв на підприємстві; заборона використання зовнішніх накопичувачів пам'яті, що не належать підприємству, або обмеження їх використання на комп'ютерах (блокування USB рознімів для флешок); створення персоніфікованих паролів для друкування документів на принтерах та їх сканувань; використання антивірусних програм; застосування криптографічних засобів для шифрування документів на основі електронного цифрового підпису та інші. Також сюди можна віднести використання спеціальних захищених носіїв електронного цифрового підпису та інформації, що в Україні тільки почало розвиватися. Після здійснення кібератак влітку 2017 року в українському законодавстві закріплено використання захищених носіїв як засобу захисту інформації, у тому числі облікової, оскільки електронний цифровий підпис використовуються в більшості випадків для підписання та подачі електронних звітів, податкових накладних і первинних документів. Обов'язкове використання захищених носіїв законодавчо встановлене для нотаріусів та державних реєстраторів з 02.11.2016 р. і для органів державної влади, місцевого самоврядування, підприємств державної форми власності – з 17.08.2017 р. відповідно до постанови КМУ № 1452.

Зовнішні організаційні заходи захисту облікової інформації пов'язані зі створенням таких умов відносин із зовнішніми користувачами, за яких вони не можуть заволодіти конфіденційною інформацією. Це може бути чітке прописування в угодах та договорах із контрагентами прав та обов'язків сторін, визначення відповідальності за їх порушення; використання договорів про нерозголошення важливої інформації тощо.

Зовнішніми технічними заходами захисту облікової інформації може бути створення окремих приміщень для переговорів із контрагентами, які будуть технічно захищені та ізольовані від основного приміщення підприємства; застосування тимчасових перепусток для працівників аутсорсингової компанії, що не є працівниками, їх обшуки та обмеження руху всередині будівель підприємства та інші.

ВИСНОВКИ

Розробка заходів із захисту облікової інформації пов'язана із особливостями діяльності підприємства, способами співпраці з контрагентами (зокрема при наданні послуг з бухгалтерського аутсорсингу), характеристиками інформації. Для великих підприємств система захисту повинна включати всі можливі заходи. Для маленьких підприємств, як правило, створення відділу безпеки інформації є недоцільним. У такому випадку можна обмежитися використанням програмних, нормативних, кадрових та фізичних заходів із оглядом на особливості облікової інформації (застосування паролів, захищених носіїв інформації, антивірусних програм, укладання інсайдерських договірів із бухгалтером або договорів про нерозголошення, забезпечення безпеки приміщення бухгалтерії тощо). ■

ЛІТЕРАТУРА

1. Боримська К. П., Кінзерська Н. В. Концептуалізація захисту бухгалтерської інформації при міжкорпоративному електронному документообороті торговельних підприємств: проблемні аспекти. *Вісник Житомирського державного технологічного університету. Сер.: «Економічні науки»*. 2013. № 3. С. 16–25.

2. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. № 11. С. 497–502. URL: http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf

3. Дикий А. П. Роль служби економічної безпеки підприємства при забезпеченні захисту бухгалтерської інформації. *Моделювання регіональної економіки*. 2011. № 1. С. 42–54.

4. 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. Вип. 3. С. 208–214.

5. Колобов Л., Колеснікова І. Комерційна таємниця та питання захисту комерційної таємниці. *Підприємництво, господарство і право*. 2016. № 5. С. 8–13.

6. Цибуляк Б. Захист інформації з обмеженим доступом на засадах аутсорсингу. *Вісник НУ «Львівська політехніка». Сер.: «Автоматика, вимірювання та керування».* 2012. № 741. Ч. 2. С. 246–250.

7. Шинкаренко А. Ю., Ставицький О. В. Кібербезпека як один з механізмів забезпечення стабільного розвитку економіки в Україні. *Актуальні проблеми економіки та управління*. 2017. № 11. URL: http://ape.fmm.kpi.ua/article/download/102862/97979

8. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник Національного гірничого університету*. 2016. № 3. С. 119–127.

REFERENCES

Borymska, K. P., and Kinzerska, N. V. "Kontseptualizatsiia zakhystu bukhhalterskoi informatsii pry mizhkorporatyvnomu elektronnomu dokumentooboroti torhovelnykh pidpryiemstv: problemni aspekty" [Conceptualization of the protection of accounting information in the inter-corporate electronic document circulation of trade enterprises: problem aspects]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Ser.: Ekonomichni nauky*, no. 3 (2013): 16-25.

Dykyi, A. P. "Poriadok zabezpechennia bezpeky bukhhalterskoi informatsii v umovakh zastosuvannia suchasnykh kompiuternykh tekhnolohii" [The procedure for ensuring the security of accounting information in the use of modern computer technology]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu*, no. 3 (2008): 208-214.

Dykyi, A. P. "Rol sluzhby ekonomichnoi bezpeky pidpryiemstva pry zabezpechenni zakhystu bukhhalterskoi informatsii" [The role of the enterprise's economic security service in providing protection of accounting information]. *Modeliuvannia rehionalnoi ekonomiky*, no. 1 (2011): 42-54.

Kolobov, L., and Kolesnikova, I. "Komertsiina taiemnytsia ta pytannia zakhystu komertsiinoi taiemnytsi" [Commercial secret and issues of commercial secrecy protection]. *Pidpryiemnytstvo, hospodarstvo i pravo*, no. 5 (2016): 8-13.

Shynkarenko, A. Yu., and Stavytskyi, O. V. "Kiberbezpeka yak odyn z mekhanizmiv zabezpechennia stabilnoho rozvytku ekonomiky v Ukraini" [Cybersecurity as one of the mechanisms for ensuring stable economic development in Ukraine]. Aktualni problemy ekonomiky ta upravlinnia. 2017. http://ape.fmm.kpi.ua/article/download/102862/97979

Shyshkova, N. L. "Zasoby pidvyshchennia kerovanosti bezpekoiu oblikovoi informatsii" [Tools to increase the manageability of security accounting information]. *Ekonomichnyi visnyk Natsionalnoho hirnychoho universytetu*, no. 3 (2016): 119-127.

Tsybuliak, B. "Zakhyst informatsii z obmezhenym dostupom na zasadakh autsorsynhu" [Protection of Restricted Information on the Basis of Outsourcing]. *Visnyk NU «Lvivska politekhnika». Ser.: Avtomatyka, vymiriuvannia ta keruvannia.* Vol. 2, no. 741 (2012): 246-250.

Viter, S. A., and Svitlyshyn, I. I. "Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva" [Protection of accounting information and cyber security of the enterprise]. Ekonomika i suspilstvo. 2017. http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf