ВОЛОТ О.І.,
КОЛОТОК В.О.

Інформаційне забезпечення інформаційної безпеки підприємств малого бізнесу в умовах ринкових відносин

Предметом *дослідження є теоретичні аспекти, методичні положення та прикладні аспекти формування інформаційного забезпечення інформаційної безпеки підприємств малого бізнесу та шляхи їх удосконалення в умовах ринкових відносин.*

Метою дослідження є *обґрунтування теоретико-методичних засад інформаційного забезпечення підприємств малого бізнесу та розробка рекомендацій щодо удосконалення існуючих заходів та засобів інформаційного забезпечення безпеки інформаційних потоків, спрямованих на підвищення ефективності їх функціонування і безпеки.*

Методи дослідження*. Теоретичну та методичну основу дослідження становлять наукові праці вчених із проблематики інформаційної безпеки підприємств У роботі застосовано сукупність наукових методів і підходів, у тому числі системний, логічний, що дозволило забезпечити концептуальну єдність і ефективність дослідження.*

Результати роботи. *В статті наведено та проаналізовано потенційні загрози від зовнішнього та внутрішнього втручання в інформаційну систему підприємств малого бізнесу. Знання загроз, причин та умов скоєння таких злочинів, як викрадання інформації через комп'ютерні мережі і прослуховування ліній зв'язку та інші дозволить працівникам підрозділів служб безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарюючого суб'єкта.*

Досліджено та класифіковано заходи та засоби забезпечення безпеки інформаційних потоків. Обґрунтовано завдання забезпечення інформаційної безпеки, які необхідно вирішувати системно.

Розглянуто поняття фейкової інформації; з'ясовано методи поширення фейкової інформації в мережі Інтернету в сучасних умовах.

Галузь застосування результатів. *Система наук з галузі економічної безпеки, широке коло проблем соціально-економічних наук з дослідження дисфункціонального розвитку.*

Висновки. *Основні висновки дослідження можна звести до формулювання:*
Визначено загрози від зовнішнього та внутрішнього втручання в інформаційну систему малих підприємств. Розглянуто та класифіковано заходи та засоби забезпечення безпеки інформаційних потоків суб'єктів малого підприємництва.
Доведено, що зростання важливості підготовки аналітиків, інформаційних працівників до сучасних тенденцій в провадженні інформації, аналізу, її захисту та збереженні, підвищення їхнього фахового рівня й готовності до глибокого аналізу контенту при підготовці інформаційно-аналітичних матеріалів та інформаційної безпеки є актуальним питанням сьогодення.

Ключові слова: *інформаційно-комунікаційні технології, інформаційна безпека, інформаційне забезпечення, фейкова інформація*.

ВОЛОТ Е.И.,
КОЛОТОК В.О.

Информационное обеспечение информационной безопасности предприятий малого бизнеса в условиях рыночных отношений

Предметом *исследования являются теоретические аспекты, методические положения и прикладные аспекты формирования информационного обеспечения информационной безопасности предприятий малого бизнеса и пути их совершенствования в условиях рыночных отношений.*

Целью исследования является *обоснование теоретико-методических основ информационного обеспечения предприятий малого бизнеса и разработка рекомендаций по совершенствованию существующих мер и средств информационного обеспечения безопасности информационных потоков, направленных на повышение эффективности их функционирования и безопасности.*

Методы исследования*. Теоретическую и методическую основу исследования составляют научные труды ученых по проблематике информационной безопасности предприятий. В работе применена совокупность научных методов и подходов, в том числе системный, логический, что позволило обеспечить концептуальное единство и эффективность исследования.*

Результаты работы. *В статье приведены и проанализированы потенциальные угрозы внешнего и внутреннего вмешательства в информационную систему предприятий малого бизнеса. Знание угроз, причин и условий совершения таких преступлений, как похищение информации через компьютерные сети и прослушивания линий связи и других, позволит работникам подразделений служб безопасности предприятий в пределах своей компетенции принять меры, которые станут препятствием на пути к злонамеренным покушениям на информационные ресурсы и потоки хозяйствующего субъекта.*

Исследованы и классифицированы меры и средства обеспечения безопасности информационных потоков. Обоснованно задачи обеспечения информационной безопасности, какие необходимо решать системно.

Рассмотрены понятия фейковой информации; выяснено методы распространения фейковой информации в сети Интернета в современных условиях.

Область применения результатов. *Система наук в области экономической безопасности, широкий круг проблем социально-экономических наук по исследованию дисфункционального развития.*

Выводы. *Основные выводы исследования можно свести к формулировке:*
Определены угрозы внешнего и внутреннего вмешательства в информационную систему малых предприятий. Рассмотрены и классифицированы меры и средства обеспечения безопасности информационных потоков субъектов малого предпринимательства. Доказано, что рост важности подготовки аналитиков, информационных работников с современными тенденциями в производстве информации, анализа, ее защиты и сохранения, повышения их профессионального уровня и готовности к глубокому анализу контента при подготовке информационно-аналитических материалов и информационной безопасности является актуальным вопросом современности.

Ключевые слова: *информационно-коммуникационные технологии, информационная безопасность, информационное обеспечение, фейкова информация*.

VOLOT O.I.,
KOLOTOK V.O.

Data support of information security for small business under conditions of market relations

The subject *of research involves theoretical issues, methodological provisions and applied aspects for development of data support of information security at small business enterprises and ways of their improvement under conditions of market relations.*

The purpose *of research is to substantiate theoretical and methodological foundations of information support for small business and to develop recommendations for improvement of existing measures and tools for data support of the information flow security aimed at enhancing their functioning and safety.*

Research methods. *The theoretical and methodological basis of research are scientific works of experts on the problems of information security of enterprises. A set of scientific methods and approaches, including systemic and logical ones, has been applied in the following work, which allowed to ensure the conceptual unity and effectiveness of research.*

Results of work. *The article presents and analyzes potential threats from external and internal interference into the information system of small business enterprises. Knowledge of threats, causes and conditions of such crimes as stealing of information through computer networks and telecommunications monitoring as well as others will enable employees of the enterprise security units, within their competence, to take certain measures in order to block malicious attacks on information resources and flows of the business entity.*

Measures and means of ensuring the information flow security have been investigated and classified. Tasks of supporting the information security that need to be solved systematically have been substantiated.

The concept of fake information has been considered; methods of distributing fake information on the Internet under modern conditions have been determined.

Application area of results. *System of sciences in the field of economic security, a wide range of issues of social and economic sciences in the research of dysfunctional development.*

Conclusions. *The main conclusions of research can be summarized as follows: Threats from external and internal interference into the information system of small business enterprises have been identified. Measures and means of data support of information security for the information flows at small business entities have been reviewed and classified.*

It has been proved that increasing importance of training of analysts and information workers to modern trends in the information production, its analysis, protection and preservation, increase of their professional level and readiness for deep content analysis in the preparation of informational and analytical materials and information security is a relevant issue of today.

Key words: *information and communication technologies, information security, data support, fake information.*

«За безпеку платять, а за її відсутність – розплачуються».
У. Черчилль

Постановка проблеми**.** Проблема інформаційної безпеки підприємств є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, інформаційних систем (ІС) і мереж. Це пояснюється дедалі зростаючими технічними і програмними можливостями доступу до інформації, що не завжди є правомірним і законним [1].

Знання потенційних загроз, причин та умов скоєння таких злочинів, як викрадання інформації через комп'ютерні мережі і прослуховування ліній зв'язку та інші дозволить працівникам підрозділів служб безпеки підприємств малого бізнесу у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарюючого суб'єкта, що обумовлює актуальність та доцільність теми дослідження.

Аналіз досліджень та публікацій з проблеми. Нині створено достатній пласт наукових робіт з проблематики інформаційної безпеки підприємств. Дослідженнями даного питання займалися такі видатні науковці, як Бондаренко В.О., Бучило І.Л., Горбатюк О.М., Дибкова Л. М., Стрельцов А.А., Копитко М.І. Кавун С. В., Носов В. В., Манжай О. В., Пономарьов В.П., Пилипенко А. А., С.П., Цимбалюк В.Л., Чубарук Т.І., Щербина В. М. та інші. Однак, враховуючи наявні теоретичні розробки, питання інформаційного забезпечення інформаційної безпеки підприємств малого бізнесу потребують систематизації, а також додаткового дослідження й удосконалення.

Метою статті є подальший розвиток теоретичного вивчення сутності Інформаційного забезпечення інформаційної безпеки підприємств, аналіз, класифікація та удосконалення існуючих заходів та засобів інформаційного забезпечення безпеки інформаційних потоків суб'єктів малого підприємництва.

Виклад основного матеріалу. Функціонування будь-якої системи керування вимагає правильної організації інформаційного забезпечення, тобто наявності сукупності оброблених зведень про стан об'єктів фінансово-господарської діяльності, що задовольняють вимоги керуючого блоку. У свою чергу інформаційне забезпечення містить у собі інформаційну систему, що володіє необхідним інформаційним фондом (персоналом і технічними засобами) і системою інформаційних потоків.

Інформаційна система являє собою комунікації персоналу підприємства щодо питань, що стосується їх професійної діяльності. Система інформаційних потоків - це сукупність фізичних переміщень інформації, яка дає можливість здійснити який-небудь процес, реалізувати яке-небудь рішення [2].

Під інформаційною безпекою можна розуміти стан захищеності інформаційного середовища підприємства та забезпечення його нормального функціонування та динамічного розвитку [3].

При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта, в умовах якого можлива дія загроз. Досягається це системою заходів, спрямованих на попередження, вияв та ліквідацію інформаційних загроз [4].

Метою інформаційної безпеки є збереження цілісності, повноти та точності інформації, мінімізація ризику несанкціонованих змін у інформаційних системах [5].

Копитко М.І. розмежовує загрози інформаційній безпеці об'єкта на внутрішні і зовнішні [6]. Іванченко Н. О. їх умовно розділяє на чотири основні групи:

- програмні - впровадження "вірусів", апаратних і програмних закладок; знищення і модифікація даних в інформаційних системах;

- технічні, в т.ч. радіоелектронні, - перехоплення інформації в лініях зв'язку; радіоелектронне придушення сигналу в лініях зв'язку і системах управління;
- фізичні - знищення засобів обробки і носіїв інформації;
- режимні - порушення регламентів інформаційного обміну; незаконні збір і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; розкрадання носіїв, а також апаратних або програмних парольних ключів; дезінформація, приховування або спотворення інформації; розкрадання інформації з баз даних [7].

Можливість зовнішнього і внутрішнього втручання в інформаційну систему підприємства може вплинути на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність та ін. Це може привести до негативних наслідків у діяльності підприємства, а саме: збоїв у функціонуванні систем управління технологічними та управлінськими процесами; розголошення відомостей, що становлять комерційну та інші види таємниць; порушення достовірності фінансової звітності; несанкціонованого доступу до бази даних підприємства; викривлення публічної інформації, тощо [8].

Тому підприємства малого бізнесу повинні здійснювати заходи, щодо забезпечення інформаційної безпеки інформаційних потоків від різноманітних загроз. Взагалі, заходи зі забезпечення інформаційної безпеки на підприємствах малого бізнесу можна поділити на такі групи (таблиця 1).

Таблиця 1

Характеристика основних заходів зі забезпечення інформаційної безпеки на підприємствах малого бізнесу

Технічні	Організаційні	Правові
- захист від несанкціонованого доступу до системи (створення умов він втручання сторонніх осіб до конференційної інформації); - резервування особливих комп'ютерних підсистем (необхідність створювання резервних копій даних на змінних носіях чи хмарних сервісах); - організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; - встановлення устаткування для виявлення і гасіння пожежі; - вживання конструктивних заходів захисту від крадіжок, саботажу, диверсій, вибухів; - встановлення сигналізації.	- охорона обчислюваних центрів; - ретельний добір освіченого персоналу; - наявність плану відновлення працездатності обчислювального центру після виходу його з ладу; - універсальність засобів захисту від усіх користувачів, в тому числі вищих посадових осіб, розподіл прав доступу персоналу до інформаційних ресурсів підприємства; - проведення аналітичної роботи, що дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки підприємства.	- захист авторських прав програмістів; - контроль за розробниками комп'ютерних систем; - удосконалення адміністративного, цивільного, законодавства в галузі комп'ютерного права.

Джерело: класифіковано авторами на основі [9,10].

Доцільно зауважити, що на підприємствах малого бізнесу, які мають дуже обмежені ресурси не є доцільним створення відділу інформаційної безпеки організації. Таку функцію можна покласти на окрему особу, яка не відповідає за обробку конфіденційної інформації. В її рольовій функції можна виділити чотири напрями: розробка методології аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення; організація і здійснення конкретних видів діяльності із захисту інформації; експлуатація технічних засобів захисту інформації; аудит і контроль функціонування системи інформаційної безпеки підприємства.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. Заходи з інформаційної безпеки на підприємствах здійснюються за допомогою відповідних заходів (таблиця 2).

Таблиця 2

Характеристика основних засобів зі забезпечення інформаційної безпеки на підприємствах малого бізнесу

Засоби	Характеристика
Фізичні	Засоби, які необхідні для зовнішнього захисту обчислювальної техніки, території та об’єктів. Реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються
Апаратно-програмні	Засоби, які працюють в взаємодії. Вони включають як і апаратні компоненти персонального комп’ютера так і програмну складову (різні електронні, електронно-механічні та інші пристрої, що вмонтовуються в серійні блоки електронних систем обробки і передачі)
Криптографічні	Спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту здійснюється за допомогою криптографічних систем, які встановлюються на підприємстві. Це самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї. Даний метод захисту реалізується у вигляді програм або пакетів програм.
Адміністративно-організаційні	Можна віднести накази, інструкції, розпорядження менеджменту, які спрямовані на регулювання заходів з інформаційної безпеки підприємства. Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу.
Біометричні	До них належать: розпізнавання сітківки ока, яке відбувається за допомогою інфрачервоного світла кровоносних судин на задній стінці ока; сканування відбитків пальців та геометрії руки; визначення динаміки підпису та інші. Сканування відбитків пальців передбачає порівняння відерників на пальцях зі збереженим в ІС для доступу до даних. Визначення динаміки підпису відбувається шляхом порівняння кривизни написів на документі з внесеними в систему.
Правові	Чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання інформаційних технологій (ІТ).
Морально-етичні	До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни

Джерело: побудовано авторами на основі [11-15].

Використання управлінцями малого бізнесу інформації з Інтернету наражає їх на таку сучасну загрозу як фейкову інформацію. Термін «фейк» (англ. fake – підробка) має багато значень. Часто фейком називають недостовірну, неправдиву інформацію,. але таке визначення не відображає суті фейку. Адже фейк – це підробка, фальшивка, яка поширюється спеціально для того, щоб дезінформувати аудиторію, яка може спонукати для прийняття невірного управлінського рішення Зважаючи на це боротьба з фейками є однією з важливих компонентів забезпечення інформаційної безпеки на підприємствах малого бізнесу.

Ефективним способом боротьби з фейком є своєчасне його виявлення. Для того, аби запобігти поширенню фейкових новин в соцмережах, видання The Huffington Post склало перелік простих правил, як їх розпізнавати [16]:

- читайте більше, ніж заголовок. Одна з причин, чому фейкові новини так швидко поширюються - тому що заклопотані читачі не дивляться далі заголовка або врізу, перш ніж поширити матеріал;
- перевірте, яке видання опублікувало новину. Незнайомі сайти, заповнені оголошеннями та заголовками, написаними капсолоком, повинні негайно викликати скепсис;
- перевірте дату публікації та час. Інший поширений елемент фейкових новин - видавати старі публікації за нові. Читачі сприймають їх як такі, що сталися щойно. Зверніть увагу на час публікації - це не займає багато часу і допоможе уникнути помилки;
- хто автор? Дивлячись на те, хто написав статтю, можна виявити багато інформації про джерело новин. Пошукайте попередні публікації автора - його бекграунд допоможе зрозуміти, чи дійсно автор є журналістом, чи не писав він фейкових статей до цього;
- дивіться на які джерела посилається новина. Відсутність посилань або джерел, з яких були взяті ті чи інші заяви, є очевидним сигналом того, що пост, швидше за все, є фейком;
- звертайте увагу на сумнівні цитати та фотографії. Вигадувати цитати для фейкових новин дуже просто. Скептично ставтеся до шокуючих або підозрілих цитат, прогляньте, чи публікувалися вони в інших виданнях, якщо так - то яких;
- бережіться упередженості. Люди часто звертають увагу та поширюють ті публікації, які відображають їх погляди та світогляд. Фейкові новини - не виняток;
- подивіться, чи інші видання пишуть про це. Якщо новина виглядає підозрілою або в ній є неймовірні факти, пошукайте, що з цього приводу писали інші видання;

- подумайте, перш ніж робити репост. Новинні сайти, які поширюють дезінформацію, працюють в розрахунку на те, що читачі будуть поширювати їх новини.

Отже, зростає важливість підготовки аналітиків, інформаційних працівників до сучасних тенденцій у висвітленні новин, підвищення їхнього фахового рівня й готовності до глибокого аналізу контенту при підготовці інформаційно-аналітичних матеріалів на базі інформації із соціальних медіа. Аналітик повинен володіти навичками грамотного пошуку інформації, аналізу джерел, уміти критично відбирати й оцінювати.

Висновки. Становлення інформаційної цивілізації зумовлює зміну підходів до безпекового середовища підприємств малого бізнесу, спонукає їх до вирішення загроз, які націлені на їхні інформаційні потоки. Тому малі підприємства, в міру фінансових можливостей, потребують застосування таких заходів та засобів, які б допомогли їм вберегти власні інформаційні потоки від загроз, допомогли зберегти конфіденційність, цілісність та доступність інформації.

Малодослідженим напрямком залишається вивчення питання використання технології блокчейн на підприємствах малого бізнесу за для захисту потоків інформації від підробки та спотворення. Тому цей напрямок потребує подальшого вивчення.

Список використаних джерел

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій /Г. Я. Аніловська// Науковий вісник НЛТУ України. – 2008. - вип. 18.9. - С. 270-273.

2. Маркіна І. А. Контролінг для менеджерів [текст] : навч. посіб. / І. А. Маркіна, О. М. Таран-Лала, М. В. Гунченко - К. : "Центр учбової літератури", 2013. - 304 с.

3. Сухорукова, О. А. Напрями економічної оцінки інформаційної та інтелектуальної безпеки медіапідприємств / Сухорукова О. А. // Science and education: trends and prospects : Collection of scientific articles. – Ascona Publishing, New York, United States of America, 2018. – Pp. 196–202.

4. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві /Ю. О. Коваленко // Економіка промисловості. - 2010. - № 3.

5. Герасименко О.В., Козак А.В. Інформаційна безпека підприємства: поняття та методи її забезпечення /О. В. Герасименко, А. В. Козак// XIV Міжнародна наукова інтернет-конференція ADVANCED TECHNOLOGIES OF SCIENCE AND EDUCATION (19-21.04.2018). [Електронний ресурс]. - Режим доступу: http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/.

6. Копитко М.І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств. Навчально-методичний посібник. – Львів: Ліга-Прес, 2016. – 172 с.

7. Іванченко Н. О. Інформаційна складова економічної безпеки підприємства та її значення для забезпечення стійкого розвитку національної економіки /Н. О. Іванченко// Стратегія розвитку України. Економіка, соціологія, право. - 2011. -№3. - С.125-129.

8. Нехай В. А. Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств /В. А. Нехай, В. В. Нехай// Науковий вісник Міжнародного гуманітарного університету. - 2017. - С.137-140. [Електронний ресурс]. - Режим доступу: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf.

9. Інформаційна безпека комп'ютерних систем [Електронний ресурс]. - Режим доступу: https://studfiles.net/preview/7152686/page:44/.

10. Мехед Д. Б. Захист інформації на підприємстві / Д. Б. Мехед // Вісник Чернігівського державного технологічного університету. Серія : Технічні науки. - 2014. - № 2. - С. 143-148.

11. Северина С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина // Вісник Запорізького національного університету. Економічні науки. - 2016. - № 1. - С. 155-161

12. Чемолосова А. В. Алгоритми та структури даних. Методичні рекомендації до вивчення курсу для студентів заочної форми навчання. 2012. - С. 140. [Електронний ресурс]. - Режим доступу: https://studfiles.net/preview/5462915/.

13. 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.

14. Дибкова Л. М. Інформатика і комп’ютерна техніка: навч. посіб. / Л. М. Дибкова. – 4-те вид., стереотип. – К.: Академ-видав, 2012. – 464 с. – (Серія «Альма матер»).

15. Технології захисту інформації / Сайт Ужгородського національного університету [Електронний ресурс]. - Режим доступу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

16. Як розпізнати фейкову новину в соцмережах - рекомендації The Huffington Post. / Сайт ГО «Детектор Медія» [Електронний ресурс]. - Режим доступу: https://ms.detector.media/web/online_media/yak_rozpiznati_feykovu_novinu_v_sotsmerezhakh_rekomendatsii_the_huffington_post/.

References

1. Anilovska H.Ia. Informatsiina bezpeka pidpryiemstva v umovakh vykorystannia suchasnykh informatsiinykh tekhnolohii /H. Ya. Anilovska// Naukovyi visnyk NLTU Ukrainy. – 2008. - vyp. 18.9. - S. 270-273.

2. Markina I. A. Kontrolinh dlia menedzheriv [tekst] : navch. posib. / I. A. Markina, O. M. Taran-Lala, M. V. Hunchenko - K. : "Tsentr uchbovoi literatury", 2013. - 304 s.

3. Sukhorukova, O. A. Napriamy ekonomichnoi otsinky informatsiinoi ta intelektualnoi bezpeky mediapidpryiemstv / Sukhorukova O. A. // Science and education: trends and prospects : Collection of scientific articles. – Ascona Publishing, New York, United States of America, 2018. – Pp. 196–202.

4. Kovalenko Yu. O. Zabezpechennia informatsiinoi bezpeky na pidpryiemstvi /Iu. O. Kovalenko // Ekonomika promyslovosti. - 2010. - № 3.

5. Herasymenko O.V., Kozak A.V. Informatsiina bezpeka pidpryiemstva: poniattia ta metody yii zabezpechennia /O. V. Herasymenko, A. V. Kozak// XIV Mizhnarodna naukova internet-konferentsiia ADVANCED TECHNOLOGIES OF SCIENCE AND EDUCATION (19-21.04.2018). [Elektronnyi resurs]. - Rezhym dostupu: http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/.

6. Kopytko M.I. Menedzhment informatsiinykh resursiv ta informatsiina bezpeka pidpryiemstv. Navchalno-metodychnyi posibnyk. – Lviv: Liha-Pres, 2016. – 172 c.

7. Ivanchenko N. O. Informatsiina skladova ekonomichnoi bezpeky pidpryiemstva ta yii znachennia dlia zabezpechennia stiikoho rozvytku natsionalnoi ekonomiky /N. O. Ivanchenko// Stratehiia rozvytku Ukrainy. Ekonomika, sotsiolohiia, pravo. - 2011. -№3. - S.125-129.

8. Nekhai V. A. Nekhai V. V. Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstv /V. A. Nekhai, V. V. Nekhai// Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. - 2017. - S.137-140. [Elektronnyi resurs]. - Rezhym dostupu: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf.

9. Informatsiina bezpeka kompiuternykh system [Elektronnyi resurs]. - Rezhym dostupu: https://studfiles.net/preview/7152686/page:44/.

10. Mekhed D. B. Zakhyst informatsii na pidpryiemstvi / D. B. Mekhed // Visnyk Chernihivskoho derzhavnoho tekhnolohichnoho universytetu. Seriia : Tekhnichni nauky. - 2014. - № 2. - S. 143-148.

11. Severyna S. V. Informatsiina bezpeka ta metody zakhystu informatsii / S. V. Severyna // Visnyk Zaporizkoho natsionalnoho universytetu. Ekonomichni nauky. - 2016. - № 1. - S. 155-161

12. Chemolosova A. V. Alhorytmy ta struktury danykh. Metodychni rekomendatsii do vyvchennia kursu dlia studentiv zaochnoi formy navchannia. 2012. - S. 140. [Elektronnyi resurs]. - Rezhym dostupu: https://studfiles.net/preview/5462915/.

13. Zakharkin O. O. Informatsiini systemy ta tekhnolohii u finansovykh ustanovakh : konspekt lektsii [Elektronnyi resurs] / O. O. Zakharkin, M. Yu. Abramchuk, M. A. Derkach. — Sumy : Vyd-vo SumDU, 2007. — 80 s. — Rezhym dostupu : http://elkniga.info/book_188.html.

14. Dybkova L. M. Informatyka i kompiuterna tekhnika: navch. posib. / L. M. Dybkova. – 4-te vyd., stereotyp. – K.: Akadem-vydav, 2012. – 464 s. – (Seriia «Alma mater»).

15. Tekhnolohii zakhystu informatsii / Sait Uzhhorodskoho natsionalnoho universytetu [Elektronnyi resurs]. - Rezhym dostupu: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

16. Yak rozpiznaty feikovu novynu v sotsmerezhakh - rekomendatsii The Huffington Post. / Sait HO «Detektor Mediia» [Elektronnyi resurs]. - Rezhym dostupu: https://ms.detector.media/web/online_media/yak_rozpiznati_feykovu_novinu_v_sotsmerezhakh_rekomendatsii_the_huffington_post/.

Дані про авторів

Волот Олена Ігорівна,
доцент кафедри бухгалтерського обліку, оподаткування та аудиту, Чернігівський національний технологічний університет, к.е.н., доцент
e-mail: e_volot@ukr.net

Колоток Вадим Олександрович,
аспірант кафедри бухгалтерського обліку, оподаткування та аудиту, Чернігівський національний технологічний університет
e-mail: kolotokvo@ukr.net

Данные об авторах

Волот Елена Игоревна,
доцент кафедры бухгалтерского учета, налогообложения и аудита, Черниговский национальный технологический университет, к.э.н., доцент
e-mail: e_volot@ukr.net

Колоток Вадим Александрович,
аспирант кафедры бухгалтерского учета, налогообложения и аудита, Черниговский национальный технологический университет
e-mail: kolotokvo@ukr.net

Data about the authors

Volot Olena,
Associate Professor, Department of Accounting, Taxation and Auditing, Chernihiv National University of Technology, Candidate of Economic Sciences, Associate Professor
e-mail: e_volot@ukr.net

Kolotok Vadym,
Postgraduate Student of the Department of Accounting, Taxation and Auditing, Chernihiv National University of Technology
e-mail: kolotokvo@ukr.net