УДК 338:004.7.056

Микитенко Т. В., к.екон.н.[1];
Петровська І. О., к.екон.н., доцент, с.н.с.[2];
Рогов П. Д., к.т.н.[3];
Гаркуша А. О.[4]

[1] - Університет державної фіскальної служби України, Ірпінь;
[2] - Київський університет ринкових відносин, Київ;
[3] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ;
[4] - Університет конверсії, розвитку освіти та кадрів, Київ.

Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах

Резюме. В статті розглянуто проблеми економічної та інформаційної безпеки суб'єктів господарювання в Україні, а також можливі шляхи їх вирішення в сучасних умовах.

Ключові слова: економічна безпека, інформаційна безпека, суб'єкти господарювання.

Постановка проблеми. В сучасних умовах господарювання підприємства України функціонують у складному, швидкоплинному середовищі, що обумовлює посилення інформаційної безпеки, потреба в забезпеченні якій особливо гостро стоїть в умовах геополітичної нестабільності в Україні. Експоненціальне зростання кількості злочинів у економічній та інформаційній сферах, стрімке розповсюдження систем електронного документообігу, поява глобальних баз даних (у тому числі - персональної та комерційної інформації) вимагають побудови надійної системи інформаційного захисту суб'єктів господарювання, як елемента інформаційної політики держави.

На заваді формування ефективної системи інформаційної, економічної та фінансової безпеки підприємств є низький рівень їх стану, що обумовлено відсутністю широковідомих вітчизняних програмних продуктів (так званого СОФТа), неефективністю системи державного управління у цих сферах, недостатньою зорієнтованістю на захист національних інтересів в інформаційній, економічній і соціальній сферах, а також непослідовність та безсистемність здійснення економічних та інших реформ, недосконаліть національного законодавства щодо забезпечення інформаційної безпеки та ефективного управління економікою; недостатній рівень кваліфікації державних службовців із питань національної безпеки та її складових; корупція в управлінських структурах.

Аналіз останніх досліджень і публікацій. Проблемам забезпечення безпеки суб'єктів господарювання (підприємств) різних форм власності приділяли увагу такі вітчизняні вчені, як: Близнюк І. М., Братель О. Р., Бондаренко В. О., Бучило І. Л., Горбатюк О. М., Гуцалюк М. О., Ляшенко О. М., Камлик М. І., Козаченко Г. В., Остроухов В. В., Пономарьов В. П., Стрельцов А. А., Цимбалюк В. Л., Чубарук Т. І., Щербина В. М. та інші. Зокрема, важливий внесок у розвиток використання інформаційних систем і технологій в системи обліку суб'єктів господарювання зробили такі вчені, як: М. М. Бенько, С. В. Івахненков, В. В. Євдокимов, Т. А. Писаревська, М. Е. Скрипник, В. Д. Шквір та інші. Однак, попри наявності значної кількості робіт та важливості питань, що розглядаються, недостатньо дослідженими залишаються методичні підходи до формування механізмів забезпечення інформаційної безпеки підприємств в сучасних умовах, особливо в умовах економічної нестабільності.

Економічна безпека - стан національної економіки, який дозволяє зберігати стійкість до внутрішніх і зовнішніх загроз, що сприяє створенню надійної та забезпеченої всіма необхідними засобами держави, захищеності

національно-державних інтересів у сфері економіки.

Інформаційна безпека є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства. Забезпечення (у тому числі і гарантія) безпеки підприємства пов'язана з інформаційною безпекою внаслідок широкого використання інформаційних технологій в його діяльності. Крім того, інформаційна безпека підприємницької діяльності є матеріально важливішою основою забезпечення національної економічної безпеки. Її можна визначити як суспільні відносини щодо створення та підтримання на належному рівні життєдіяльності інформаційної системи захисту суб'єкта господарювання від впливу внутрішніх і зовнішніх загроз, який забезпечує його самозбереження та розвиток у поточній й стратегічній перспективах.

Складовими економічної безпеки, згідно Методики розрахунку рівня економічної безпеки України, затвердженої Міністерством економіки України, є: фінансова, науково-технологічна, інвестиційно-інноваційна безпека та інші [1].

Так, *фінансова безпека* - стан фінансової системи держави, за якого створюються необхідні фінансові умови для її стабільного соціально-економічного розвитку, забезпечується її стійкість до фінансових шоків та дисбалансів, створюються умови для збереження цілісності та єдності фінансової системи. Фінансова безпека підприємства є складним та інтегрованим явищем, що синтезує ряд важливих змістовних характеристик економічної безпеки підприємства та фінансів підприємства, зокрема, має такі складові:

банківська безпека - рівень фінансової стійкості банківських установ країни, що дає змогу забезпечити ефективність функціонування банківської системи країни та захист від зовнішніх і внутрішніх дестабілізуючих чинників, незалежно від умов її функціонування;

безпека небанківського фінансового сектору - рівень розвитку фондового та страхового ринків, що дає змогу повною мірою задовольняти потреби суспільства в зазначених фінансових інструментах та послугах;

боргова безпека - відповідний рівень внутрішньої та зовнішньої заборгованості з урахуванням вартості її обслуговування та ефективності використання внутрішніх і зовнішніх запозичень та оптимального співвідношення між ними, достатній для задоволення нагальних соціально-економічних потреб, що не загрожує суверенітету держави та її фінансовій системі;

бюджетна безпека - це стан забезпечення платоспроможності та фінансової стійкості державних фінансів, що надає можливість органам державної влади максимально ефективно виконувати покладені на них функції;

валютна безпека - стан курсоутворення, який характеризується високою довірою суспільства до національної грошової одиниці, її стійкістю, створює оптимальні умови для поступального розвитку вітчизняної економіки, залучення в країну іноземних інвестицій, інтеграції України до світової економічної системи, а також максимально захищає від потрясінь на міжнародних валютних ринках;

грошово-кредитна безпека - стан грошово-кредитної системи, що забезпечує всіх суб'єктів національної економіки якісними та доступними кредитними ресурсами в обсягах та на умовах, сприятливих для досягнення економічного зростання національної економіки.

У ринкових умовах господарювання підприємство, як відкрита система, функціонує у складному зовнішньому середовищі, що характеризується нестабільністю та постійною динамікою. Таке середовище змушує керівництво швидко адаптуватися до нових умов, потребує знання законів розвитку та пошуку шляхів виживання в ринковій економіці, врахування чинників невизначеності і нестійкості економічного середовища.

Найважливішими факторами, що впливають на економічну безпеку підприємства, є ступінь досконалості законодавчої бази, рівень оподаткування, доступ на світові ринки збуту, інвестиційна привабливість регіону, держави тощо. Насамперед, економічна безпека підприємства залежить від економічної безпеки держави, регіону, адже ґрунтується на їхньому фінансовому, сировинному та виробничому потенціалі, перспективах розвитку. Наявність багаторівневої концепції економічної безпеки господарюючих суб'єктів усіх рівнів дає можливість забезпечити передбачуваність зовнішніх загроз підприємствам.

Головна мета управління економічною безпекою - забезпечення найефективнішого функціонування, найпродуктивнішої роботи операційної системи та економічного використання ресурсів, забезпечення певного рівня трудового життя персоналу та якості

господарських процесів підприємства, а також постійного стимулювати нарощування наявного потенціалу та його стабільного розвитку.

До основних функціональних цілей економічної безпеки підприємства належать забезпечення захисту інформаційних ресурсів та інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів та відділів підприємства.

Метою статті є дослідження процесів забезпечення інформаційної безпеки суб'єктів господарювання та розробка пропозицій щодо захисту інформаційних ресурсів і інформаційного поля, комерційної таємниці та досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства за рахунок використання вітчизняних програмних продуктів.

Виклад основного матеріалу. Інформаційна безпека підприємства характеризується рівнем захищеності суб'єкта господарювання, є основою побудови фундаменту для забезпечення необхідних умов стійкого розвитку підприємства та держави в цілому. Головна умова інформаційної безпеки підприємства – здатність протистояти існуючим і виникаючим небезпекам та загрозам, які здібні завдати фінансової шкоди підприємству або посприяти небажаній зміні структури капіталу, примусової ліквідації підприємства тощо [2, 8, 14].

Оскільки комп'ютерні системи прямо інтегровані в інформаційні структури сучасного підприємства, засоби захисту повинні враховувати відповідні форми представлення інформації. Це означає, що системи захисту повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не окремих документів, файлів чи повідомлень. Інформаційну безпеку підприємства слід розглядати у контексті формування безпечних умов існування інформаційних технологій, які включають питання захисту інформації, побудови ефективної інформаційної інфраструктури, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів. Адже, інформаційний захист є значущою складовою інформаційної системи фінансів та бухгалтерського обліку та становить одну з головних функцій сучасної системи управління суб'єктів господарювання [2].

На інституційному рівні у забезпеченні інформаційної безпеки України задіяне цілу низку державних інституцій. Так, питаннями формування інформаційної безпеки України опікуються понад 20 державних органів і центральних органів виконавчої влади.

Україна все частіше стикається з усе більш масштабними проявами комп'ютерної злочинності, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем [3]. Разом з тим, в Україні затверджена та введена в дію Указом Президента України від 15 березня 2016 року № 96/2016 "Стратегія кібербезпеки України", яка має за мету створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, суб'єктів господарювання тощо [16].

Американський уряд у 2016 році вперше офіційно визнав, що до збою у забезпеченні електричною енергією в Україні у грудні 2015 року призвели кіберзловмисники [4]. При чому, Служба безпеки України у грудні 2015 року повідомляла щодо попередження хакерської атаки іноземних спецслужб проти енергетичних об'єктів України. Співробітники СБУ знайшли шкідливе програмне забезпечення в мережах окремих обласних енергетичних підприємств [5].

Високий рівень загроз у кібернетичному просторі підтверджується дослідженнями відомого німецького оператора зв'язку Deutsche Telecom, за даними якого Україна опинилася на четвертій позиції у світі серед країн – об'єктів та джерел кібернетичних атак. Лише протягом лютого 2013 року з території України їх було здійснено 566 тисяч. Підрозділом реагування на комп'ютерні надзвичайні події України CERT-UA, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України, протягом 2012 року зафіксовано та вжито заходів з реагування на 31 комп'ютерний інцидент, які стосувалися захищеності інформаційних ресурсів державних органів [6]. Найбільш розповсюдженими різновидами атак були несанкціонований доступ до автоматизованих систем (17 випадків) та DDoS-атаки (6 випадків) на державні інформаційні ресурси. До того ж, на 150 веб-сайтах українського сегмента мережі Інтернету, з метою протидії несанкціонованому втручанню, спецслужбами України було вжито заходів із блокування/видалення фішингового контенту. При цьому маємо враховувати, що за перше півріччя 2013 року кількість таких інцидентів стала 33, що однозначно свідчить про зростання відповідних загроз. За 2012 рік було

зафіксовано лише п'ять випадків експлуатації технічно вразливих систем, а за першу половину 2013 року кількість таких випадків становила 13. Інший небезпечний показник: якщо протягом 2012 року був зафіксований лише один випадок цільового ураження державних інформаційних ресурсів, то за першу половину 2013 року таких випадків зафіксовано шість, що свідчить не просто про кількісне зростання спроб стороннього впливу на державні інформаційні ресурси, а про збільшення кількості цілком свідомих атак на певні системи з цільовим використанням їх вразливості.

Ситуацію загострення кібербезпекової проблематики для України демонструють і звітні показники Служби безпеки України. Слідчими органами СБУ протягом другого півріччя 2012 року та першого півріччя 2013 року порушено 114 кримінальних справ у сфері використання електронно-обчислюваних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, з них у другому півріччі 2012 року – 45, у першому півріччі 2013 – 59 за статтями 361, 361-1, 361-2, 362, 363 розділу XVI Кримінального Кодексу України [7].

Високий рівень загроз у кіберпросторі підтверджується даними Державного агентства з питань науки, інновацій та інформатизації, наведеними у доповіді про стан інформатизації та розвиток інформаційного суспільства в Україні за 2014 рік. [6]. Фактично кількість злочинів, що скоєні внаслідок несанкціонованого доступу до інформації, сягнула з 74 - у 2012 році до 442 - у 2014 році, кількість злочинів щодо несанкціонованої зміни даних - збільшилася у 7 разів, порушення правил користування інформацією - в 9 разів [7].

За звітами аналітиків Gartner, витрати на інформаційну безпеку у світі в 2015 році зросли на 8,2%, а загальний обсяг глобального ринку кібербезпеки в 2015 році складав 106 млрд. дол. США. У 2017 році обсяг цього ринку за попередніми прогнозам може досягти 120 млрд. дол. США, а до 2020 року ця цифра може зрости до 170 млрд. дол. США [8]. Останнім прикладом хакерської атаки є фальшивий лист Президента України до Надії Савченко щодо її голодування [9]. Ситуація, що склалася свідчить про те, що існуючі підходи не надають дієвого механізму оцінки захищеності інформаційних систем, а суб'єктивні характеристики не спрацьовують, тому актуальним завданням є об'єктивна оцінка рівня захищеності інформаційних ресурсів і стану інформаційної безпеки, що вкрай важливе для формування довіри зовнішніх користувачів до інформації, яка подається у звітності суб'єктів господарювання.

Отже, Україна все частіше стикається з усе більш масштабними проявами комп'ютерної злочинності, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем.

Джерелом загроз і викликів можуть стати програмні продукти "1С", які впроваджує, реалізує та супроводжує російська франчайзингова компанія "1С". Система програм "1С: Підприємство" призначена для автоматизації управління та обліку на підприємствах різних галузей, видів діяльності і типів фінансування, включає в себе рішення для комплексної автоматизації виробничих, торгових та сервісних підприємств, продукти для управління фінансами холдингів і окремих підприємств, ведення бухгалтерського обліку ("1С: Бухгалтерія" найвідоміша облікова програма в ряді країн), розрахунку зарплати та управління кадрами, для обліку в бюджетних установах, різноманітні галузеві і спеціалізовані рішення, розроблені самою фірмою "1С", її партнерами та незалежними організаціями.

Більш, ніж 130 000 підприємств в Україні всіх видів діяльності використовують систему програм "1С: Підприємство". Близько 550 підприємств, що працюють в 50 містах України, входять до партнерської мережі "1С:Франчайзинг" та здійснюють впровадження, налагодження і супровід програм "1 С Підприємство 8". Більш, ніж 430 навчальних закладів проводять навчання студентів з економічних та технічних спеціальностей з використанням програм "1С". Система "1С Підприємство" широко застосовується в Україні, Казахстані, Білорусі та організаціями цих країн. Більше 120 Центрів сертифікованого навчання (ЦСН), які знаходяться в 31 місті України, надають послуги з професійної підготовки технічних фахівців і користувачів для роботи з програмами "1С Підприємство 8" [10, 17].

Можливі ризики для підприємств України. Особливістю функціонування "1С Підприємство 8" є той факт, що код платформи є закритим і без участі розробника (ПАТ "1С") рішення всіх технічних питань (автоматизація виробничих та торгівельних підприємств, фінансових організацій, підприємств сфери обслуговування тощо; підтримка оперативного

управління підприємством; автоматизація організаційної і господарської діяльності; ведення бухгалтерського обліку; підтримка багатовалютного обліку; вирішення завдань планування, бюджетування та фінансового аналізу; розрахунок зарплати, управління персоналом) виявляється непростим. Така побудова програми дає можливість здійснювати пильний контроль з боку іноземного розробника програмних продуктів за всіма аспектами облікової діяльності українських суб'єктів підприємництва.

До того ж, на замовлення українського уряду однією з компаній, що спеціалізується на захисті інформації, проводились дослідження, присвячені безпеці щодо використання розробок "Лабораторії Касперського" в українських державних органах. Висновки експертів досить категоричні - антивірус може віддалено блокувати роботу комп'ютерів і безконтрольно передавати дані користувачів спецслужбам РФ [11]. Крім того, використання антивірусних продуктів виробництва "Лабораторії Касперського" несе високі ризики щодо безконтрольної передачі інформації з ПК користувачів на сервери компанії з можливістю подальшого використання даної інформації, включаючи передачу її правоохоронним органам і силовим структурам. Всі продукти антивірусу "Лабораторії Касперського" працюють в системі з найвищим пріоритетом і не можуть бути обмежені або контролюватися будь-яким зовнішнім програмним забезпеченням або самою операційною системою. Під час роботи продукти проводять обмін даними з серверами, розташованими в США і Росії. Всі дані, що передаються, відправляються з комп'ютера зашифровані та не можуть бути проаналізовані.

Аналогічні інформаційні ризики пов'язані і з використанням бухгалтерської програми "Парус", яка використовується в Україні більшістю бюджетних установ, тобто може мати прямий інформаційний доступ до державних бюджетних показників. Розробником вказаної програми є також іноземний (російський) виробник – Корпорація "Парус", яка була створена у 1990 році. На той час її засновники проходили службу у обчислювальному центрі Головного штабу воєнно-морського флоту Російської Федерації (РФ). В РФ програмні продукти корпорації використовуються у федеральних та регіональних органах влади, органах місцевого самоврядування, бюджетних та комерційних установах [15].

В України Корпорація "Парус" нараховує 28 регіональних представництв та понад два десятки дилерських компаній. Загальна кількість співробітників Корпорації "Парус" в українських представництвах становить понад 550 фахівців, з яких понад 250 працюють у Києві, кількість інсталяцій перевищує 200 000, програмне забезпечення працює в більш, ніж 20000 організацій. На сьогодні програмні продукти Корпорації "Парус" викладаються більш, ніж у 600 навчальних закладах України I-IV рівня акредитації. [15, 18]

Таким чином, можна зробити висновок про масштабну іноземну експансію на ринку українського бухгалтерського СОФТа, що не може не турбувати з точки зору загальної національної безпеки.

Можливі ризики для фондових ринків України з точки зору інформаційної безпеки. Загальновідомо, що ринок цінних паперів є одним з основних механізмів акумулювання і перерозподілу інвестиційного капіталу в світовій економіці. На сучасному етапі розвитку світового господарства можна говорити про перевагу цього джерела формування капіталу, порівняно з кредитом та внутрішнім нагромадженням. Глобалізація світової економіки, що прискорилася протягом останніх десятиліть, стала причиною формування практично єдиного всесвітнього ринку капіталів. Можна говорити і про зворотну закономірність: міжнародний ринок цінних паперів, що стрімко розвивається, є рушійною силою подальшої інтеграції національних економік у єдине світове господарство через інформаційне середовище (простір).

Розвиток сучасних засобів обчислювальної техніки і телекомунікації, що стали можливими через розвиток та широке впровадження інформаційних технологій, дозволив забезпечити можливість практично миттєвого переміщення коштів з одного національного ринку на інший. Поряд з перевагами такої мобільності капіталу, її безпосереднім наслідком є також нестійкість національних ринків цінних паперів внаслідок збільшення їхньої залежності від розвитку економік інших країн, можливості здійснення комп'ютерних злочинів у цієї сфері. Це стає особливо очевидним при розгляді фінансових криз, таких як мексиканська криза 1994-1995 років, що поширилась на всю Латинську Америку, і криза у країнах Південно-Східної Азії 1997-1998 років, яка відобразилась на усіх

фондових ринках країн, що розвиваються і розвинутих країн тощо.

Відповідно до досліджень західних економістів, в останні десятиліття у зв'язку з випереджальним розвитком економік багатьох країн, що розвиваються, спостерігається різке збільшення потреби в інвестиційних ресурсах, тоді як зростання обсягів капіталу, що інвестується, відстає від потреб світової економіки. І хоча боротьба за інвестиційні ресурси між провідними центрами світового господарства: США, Європейським Союзом і Японією в останнє десятиліття також украй загострилася, в особливо важкому стані в конкуренції за інвестиційні ресурси знаходяться країни, що розвиваються. Не останнім за значенням фактором, що породжує дефіцит капіталу в країнах, що розвиваються (та й у багатьох розвинутих), є "ідеологія споживання", що інформаційно нав'язується з-за кордону та приводить до зниження сформованих норм нагромадження в економіці.

Вирішення цього завдання має на увазі як проведення певної інформаційної політики, що спрямована на зміцнення іміджу даної країни в очах інвесторів, так й реалізацію макроекономічної стратегії, що забезпечує підтримку більш високої норми прибутку та/чи зниження ризиків, пов'язаних вкладеннями в економіку країни [14, 17].

Можливі шляхи вирішення проблеми. Уряд України у рамках виконання рішення Ради національної безпеки і оборони України у вересні 2015 року доручив Державній службі спеціального зв'язку та захисту інформації України негайно виключити використання російського програмного забезпечення, відключити оновлення всіх російських програм. Як повідомили в Прес-службі Уряду, таке доручення озвучено в ході урядової наради: "Є пряма заборона на використання російського програмного забезпечення". Мова йде про програмне забезпечення компанії "Лабораторія Касперського". Держслужбі спецзв'язку і телекомунікацій було доручено негайно відключити оновлення програм, їх купівлю та використання в органах влади [12].

Відомо, що вже є результати боротьби з використанням російських поштових серверів у роботі державних службовців: працівника Львівської обласної державної адміністрації у жовтні 2015 року звільнили з посади за використання у роботі сервера Mail.ru. З'ясувалося, що працівник Департаменту міжнародного співробітництва та туризму Львівської ОДА в офіційному листуванні використовував електронну адресу російського поштового сервера Mail.ru. Про це повідомили громадські діячі, які отримали запрошення на офіційний захід ЛОДА із пошти Mail.ru [13].

Однак, питання використання у фінансовій діяльності вітчизняними суб'єктами господарювання російських програм "1С" та "Парус" чомусь не розглядається як загроза національної безпеки. Навіть для рекламування подальшого руху програми "1С" на вітчизняному ринку такі стовпи української свідомості як Київський Національний університет імені Тараса Шевченка надають в оренду свої приміщення (у лютому 2016 року в актовому залі червоного корпусу відбулася конференція щодо просування "1С" у освітянських закладах).

Ризики безпеки суб'єктів економічної діяльності, що існують при використанні російського бухгалтерського СОФТу, полягають, по-перше, у отриманні багаточисельної української фінансової та бухгалтерської інформації, яка може представляти комерційну таємницю, а, по-друге, в будь-який момент розробник програми може як запустити в систему "трояна", так і просто припинити обслуговування та підтримку самої програми. Звичайно, обидва сценарії призведуть до порушення економічної та інформаційної безпеки підприємств і нанесуть суттєву економічну шкоду на мікро- та макрорівні. При цьому, в Україні вищими навчальними закладами готуються та щорічно випускаються фахівці за напрямом "Комп'ютерні науки" спеціальностей "Інформаційні управляючі системи та технології", "Інформаційні технології проектування", напрямом "Комп'ютерна інженерія" спеціальність – "Комп`ютерні системи та мережі" тощо. До того ж за даними Міністерства освіти і науки України станом на І квартал 2014 року за спеціальностями, які належать до ІТ-сфери, було захищено 72 докторських та 381 кандидатських дисертаційних робіт. Понад половина усіх отриманих наукових звань серед зазначених спеціальностей припадає на три: "Інформаційні технології", "Математичне моделювання та обчислювальні методи", "Комп'ютерні системи та компоненти".

За даними НАН України у виконанні наукових досліджень в галузі інформаційних технологій беруть участь 1258 наукових працівників, серед яких 138 докторів та 408 кандидатів наук. Кількість ІТ-фахівців в Україні на початок 2014 року становить

близько 250 тис. чоловік, 40 тис. із них - сертифіковані висококласні спеціалісти, що створюють конкурентоспроможну експортоорієнтовану продукцію.

Згідно зі звітом "Вимірювання інформаційного суспільства" Міжнародного Союзу Електрозв'язку ООН, Україна займає 68 місце в світі з розвитку ІКТ. Усього рейтинг охоплює 157 країн. Лідирує вже третій рік поспіль Південна Корея, на 2-у місці Швеція, Ісландія на 3-у. США перебуває на 17-у місці індексу ІКТ, Польща – на 37-у місці. Росія в рейтингу на 40-у місці [6].

Тобто існують власні вітчизняні спеціалісти, які спроможні розробити оригінальну бухгалтерську програму. Єдине, що потрібне, це створення належних умов, а саме: встановлення державного замовлення на розробку відповідної бухгалтерської програми; тотальна заборона на використання іноземного програмного забезпечення суб'єктами господарювання та контролюючими фіскальними органами.

Впровадження запропонованих заходів дозволить зробити конкретні шаги до створення системи економічної та інформаційної безпеки суб'єктів економічної діяльності, підприємств різної форми власності, національної економіки та суспільства взагалі.

Висновки.

1. В сучасних умовах національне господарство розвинутих країн світу та України знаходиться у значній залежності від інформаційних технологій, кіберпростором охоплено практично всі сфери національного господарства, у першу чергу – стратегічно важливі, включаючи сферу державного управління, оборону, енергетику, управління підприємствами з безперервним циклом виробництва тощо.

2. Проблема забезпечення й гарантування економічної та інформаційної безпеки підприємств в Україні в теперішній час стоїть дуже гостро, враховуючи те, що накопичення, передавання та обмін інформацією, зокрема, бухгалтерський облік, ведеться за допомогою комп'ютерних програм де-факто іноземного виробництва, включаючи ті, які можуть містити в собі програмні модулі для несанкціонованого отримування конфіденційної інформації, а також можуть використовуватися як інструменти та канали для кіберзлочинів.

3. Україна володіє достатнім потенціалом для забезпечення інформаційної безпеки країни та інформаційного забезпечення підприємств, у тому числі сертифікованими висококласними спеціалістами, що можуть створити конкурентоспроможну експортоорієнтовану продукцію. Отже їх необхідно активно залучити для розробки критично важливого для безпеки країни програмного забезпечення, включаючи бухгалтерське.

4. На державному рівні необхідно на Кабінет міністрів України покласти функції координації дій із інформаційного забезпечення установ та підприємств України, включаючи розробку заходів із розвитку національного програмного забезпечення для виробничих підприємств, закладів інфраструктури, фінансових установ, оборонних структур та інших установ, що забезпечують національну безпеку держави.

5. В сучасних умовах інформаційна безпека суб'єктів господарювання різних форм власності може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною, спиратися на систему різних видів власного програмного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Подальші дослідження слід присвятити аналізу та змісту конкретних заходів із розвитку національного програмного забезпечення для виробничих підприємств, бюджетних установ, закладів інфраструктури, фінансових установ, оборонних структур та інших установ, що забезпечують національну безпеку держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації щодо розрахунку рівня економічної безпеки України. Наказ Міністерства економіки України від 29.10.2013 №1277 [Електронний ресурс] // Міністерство економічного розвитку і торгівлі України. – Режим доступу: http://www.me.gov.ua/.
2. Шкарлет С.М. Економічна безпека підприємства: інноваційний аспект: монографія / С.М. Шкарлет. – К.: НАУ, 2007. – 436 с.
3. Костюк І. Україна в полі кібертероризму: загрози, реальність, протидія - [Електронний ресурс]. – Режим доступу: http:// www.science-community.org/uk/node/155962.
4. Правительство США подтвердило, что за отключением электроэнергии в Украине стоят хакеры. - [Електронний ресурс]. – Режим доступу :http://for-ua.com/article/1108323.

5. [Електронний ресурс]. – Режим доступу :http://antivirus.ua/taxonomy/term/556.
6. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2014 рік.- [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/content/shchorichna-dopovid-pro-rozvytok-informaciynogo-suspilstva.
7. Янчев А.В Організаційно-методологічні положення електронного документування у системі бухгалтерського обліку / Дис. на здобуття наук. ступ. док. ек. наук. за спец. 08.00.09. Бух. облік, аналіз та аудит, Харків, 2015.
8. Наконечний В.С. Стан розвитку управління інформаційною безпекою в світовій практиці та її вплив на економічний розвиток України // Сучасний захист інформації. - № 4. - 2015.
9. http://gazeta.ua/articles/comments-newspaper/list-prezidenta-buv-pidrobkoyu/684933.
10. http://www.1c.ru/rus/products/1c/integration/ext.htm.
11. http://articles.antivirus.ua/content/kaspersky-ukraine.
12. http://www.unian.ua/science/1134358-yatsenyuk-doruchiv-pripiniti-vikoristannya-rosiyskogo-programnogo-zabezpechennya.html.
13. http://tsn.ua/ukrayina/chinovnika-lvivskoyi-oda-zvilnili-za-vikoristannya-elektronnoyi-poshti-mail-ru-520871.html.
14. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. - К.: КНТ, 2007.
15. http//parus.ua.
16. Стратегія кібербезпеки України, затверджена та введена в дію Указом Президента України від 15 березня 2016 року № 96/2016.
17. Hansen F. and Oleshchuk V.A.: Conformance Checking of RBAC Policy and its Implementation, The First Information Security Practice and Experience Conference, ISPEC 2005, Singapore, LNCS, Volume 3439, pp. 144–155, 2005.
18. Ru.wikipedia.org.

Стаття надійшла до редакції 14.04.2016

Микитенко Т. В., к.экон.н.[1]**;**
Петровская И. О., к.экон.н., доцент, с.н.с.[2]**;**
Рогов П. Д., к.т.н.[3]**;**
Гаркуша А. О.[4]

[1] - Университет государственной фискальной службы Украины, Киев;
[2] - Киевский университет рыночных отношений, Киев;
[3] - Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев;
[4] - Университет конверсии, развития образования и кадров, Киев

Проблемы информационной безопасности субъектов ведения хозяйства в Украине и возможные пути их решения в современных условиях

Резюме. В статье рассмотрено проблемы экономической и информационной безопасности субъектов ведения хозяйства в Украине, а также возможные пути их решения в современных условиях.

Ключевые слова: экономическая безопасность, информационная безопасность, субъекты ведения хозяйства.

T. Mykytenko, Ph.D[1]**;**
I. Petrovska, Ph.D[2;]
P. Rogov, Ph.D[3]**;**
A. Garqusha[4]**.**

[1] - University of Tax Service of Ukraine, Irpen;
[2] - Kyiv university of market relations, Kyiv;
[3] - Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovskij, Kyiv;
[4] - University of conversion, development of education and shots, Kyiv

Problems of informative safety of subjects of menage in Ukraine and possible ways of their decision are in modern terms

Resume. In the article a problems of economic and informative security of subjects of ménage is considered in Ukraine, and also possible ways of their decision in modern terms.

Keywords: economic security, informative security, subjects of ménage.