УДК 368.03:004.056.5

О. Й. Жабинець
кандидат економічних наук, доцент кафедри фінансів,
Львівський державний університет внутрішніх справ, Україна
olza@ukr.net

ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНА БЕЗПЕКА СТРАХОВИХ КОМПАНІЙ

Анотація. У статті проаналізовано основні канали та види витоків конфіденційної інформації, досліджено особливості використання сучасних технологій захисту інформації вітчизняними страховими компаніями та дотримання ними міжнародних стандартів інформаційної безпеки.
Ключові слова: страхові компанії, захист інформації, інформаційна безпека, DLP-системи, технологія «хмарних обчислень», міжнародні стандарти інформаційної безпеки.

О. И. Жабинец
кандидат экономических наук, доцент кафедры финансов,
Львовский государственный университет внутренних дел, Украина
ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТРАХОВЫХ КОМПАНИЙ
Аннотация. В статье проанализированы основные каналы и виды утечек информации, исследованы особенности использования современных технологий защиты информации отечественными страховыми компаниями и соблюдения ими международных стандартов информационной безопасности.
Ключевые слова: страховые компании, защита информации, информационная безопасность, DLP-системы, технология «облачных вычислений», международные стандарты информационной безопасности.

Olga Zhabynets
PhD (Economics), Associate Professor, Lviv State University of Internal Affairs, Ukraine
26 Horodotska Str., Lviv, 79007, Ukraine
DATA PROTECTION AND INFORMATION SECURITY OF INSURANCE COMPANIES
Abstract. *Introduction.* The development of high-technology provides unlimited opportunities for efficient business, but at the same time it makes some information for espionage more accessible. The insurance companies providing insurance protection and guaranteeing security for their customers, should be the last in the list of financial institutions' confidential information leakage. The author considers that the problem of data protection and information security of insurance companies takes on a special urgency in today's environment.
The purpose of the paper is analysis of channels and types of confidential information leaks, characteristics of modern technologies leaks in information security for domestic insurance companies, and their compliance with international standards of information security.
Results. Rapid development of information technology, insurance services sales through the Internet and other innovations substantiate increased requirements for the protection of personal data and other confidential information by the insurance companies. Realizing the importance of information security, domestic insurers begin to introduce advanced protection technologies for confidential data, including DLP-systems. Practice of international standards of information security has not been very popular in Ukraine yet in comparison with the developed countries, because there is a lack of the legislative requirements in the information security system for the insurers. In the author's opinion, this situation could affect the insurers' reputation adversely and cause the loss of confidence in them among the consumers of insurance services.
Keywords: insurance companies; information security; DLP-systems; cloud computing technology; international standards of information security.
JEL Classification: G22

Постановка проблеми. Розвиток високих технологій створює необмежені можливості для ефективного ведення бізнесу, але водночас робить будь-яку інформацію доступнішою для шпигунства. Страхові компанії, надаючи страховий захист і виступаючи гарантами безпеки для своїх клієнтів, повинні бути останніми у списку фінансових структур щодо можливостей витоку конфіденційної інформації. З огляду на це проблема захисту інформації та інформаційна безпека страхових компаній у сучасних умовах набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. Питання захисту інформації та інформаційної безпеки в різних її аспектах розглядаються у працях таких зарубіжних науковців, як Брассар Ж. (Brassard, 2011), Норткатт С. (Northcutt, 2002), Рівест Р. (Rivest, 2006), Уілхайт А. (Willhite, 2000), Уітті Р. (Witty, 2012), у тому числі російських учених – Войналовича О. О., Городецького А. Є., Курицького О. Б., Нисневича Ю. А., Талимончик В. П., Титаренко Г. А. та ін. Серед українських дослідників забезпечення інформаційної безпеки вивчали Калюжний Р. А., Кормич Б. А., Максименко Ю. Є., Мотлях О. І., Олійник О. В., Цимбалюк В. С. та ін. Розвиток інформаційних технологій у страхуванні досліджували Йолкіна-Старк Л., Фурман В., Ширінян Л. та інші науковці й практики українського страхового бізнесу. Водночас, проблеми інформаційної безпеки страхових компаній в Україні та механізм її забезпечення сьогодні залишаються поза увагою вітчизняних дослідників, що обумовило вибір тематики цієї наукової статті.

Метою статті є аналіз каналів і видів витоків конфіденційної інформації, особливостей використання сучасних технологій захисту інформації вітчизняними страховими компаніями та дотримання ними міжнародних стандартів інформаційної безпеки.

Основні результати дослідження. Під загальним терміном «інформаційна безпека» розуміється комплексний захист будь-яких конфіденційних відомостей, випадковий чи спрямовано санкціонований витік яких може завдати шкоди компанії, її власнику або користувачеві. У зв'язку з тим, що останнім часом ведення документації та робочий процес більшості організацій пов'язаний із комп'ютерною технікою і мережею Інтернет, часто інформаційна безпека асоціюється з інформаційно-технічною безпекою: 1) безпекою інформації на електронних носіях; 2) передачею інформації по електронних мережах; 3) копіюванням інформації з одних видів електронних носіїв на інші. Однак чимало інформації зберігається не лише в еле-

ктронному вигляді. Наприклад, більша частина першоджерел та архівних матеріалів знаходиться в паперовому вигляді. З огляду на це вважаємо, що інформаційна безпека повинна передбачати захист будь-якої конфіденційної інформації незалежно від місць її зберігання, передачі або типу носія (паперовий чи електронний варіант).

За даними InfoWatch, у 2012 році найбільшу частку серед каналів витоку конфіденційної інформації склали паперові документи, персональні комп'ютери, ноутбуки та смартфони (рис. 1).

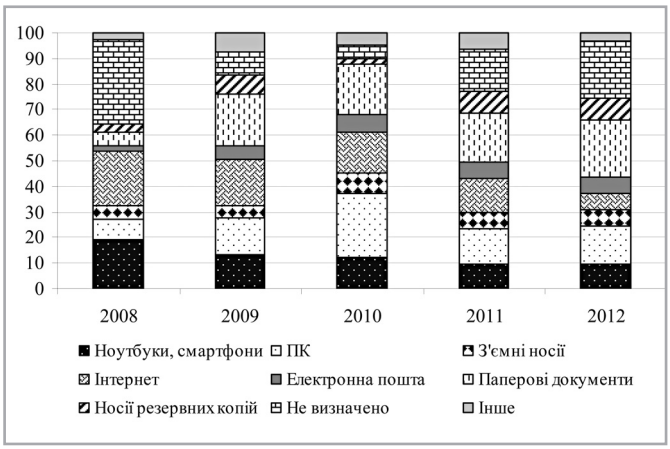

Рис. 1. **Канали витоків конфіденційної інформації у світі протягом 2008-2012 рр., %**
Джерело: Побудовано автором за [1]

На рис. 1 видно, що спостерігається зростання витоків інформації на паперових носіях: якщо у 2008 році цей канал спричинив витоки лише в межах п'яти відсотків, то у 2012 році – понад 20%. При цьому за цей самий період два канали – ноутбуки, смартфони та персональні комп'ютери – знаходяться в незмінних межах – близько 30%. Така динаміка свідчить про те, що протягом п'яти років недостатньо уваги приділялося захисту як власне інформації на паперових носіях, так і місць її зберігання. Водночас більше зусиль було докладено для захисту інформації на персональних комп'ютерах та ноутбуках, що й дало позитивні результати – вдалося запобігти зростанню частки витоків через цей канал. Окрім того, завдяки розробленим технологіям і програмам із захисту інформації частку витоків через Інтернет вдалося знизити від 20% у 2008 році до 5% у 2012 році.

На рис. 2 подано види витоків конфіденційної інформації та їх частка в загальному обсязі витоків у світі. До

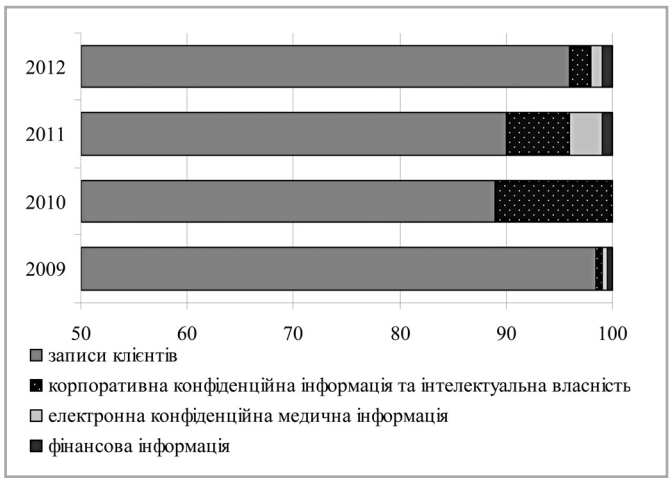

Рис. 2. **Види витоків конфіденційної інформації у світі протягом 2009-2012 рр., %**
Джерело: Побудовано автором за [2]

групи «записи клієнтів» належить така інформація із платіжних карт (від 90% до 95% усіх записів клієнтів), дані страхових полісів, номери соціальних карт, e-mail адреси. Варто зазначити, що за 2010 рік компанія Trustwave здійснила ранжування даних за іншою методикою, тому результати були зведені у дві групи: перша – записи клієнтів, друга – корпоративна конфіденційна інформація та інтелектуальна власність.

На рис. 2 можна побачити, що найчастіше об'єктом викрадення інформації є записи клієнтів. Існує також тенденція до зниження (щоправда досить хаотичного) питомої ваги цієї групи впродовж чотирьох років. У 2010 році зафіксовано зменшення частки витоку інформації із записів клієнтів від 98,5% до 89%, однак до 2012 року вона знову збільшилася і сягнула 96%. Дані рис. 1 вказують на те, що частка інформації, яка може потенційно належати до суто страхової, є незначною. На жаль, жодне дослідження в галузі інформаційної безпеки не виокремлює витоки конфіденційної інформації, що пов'язані зі страхуванням, а дані страхових полісів, що були втрачені, складають незначний відсоток у «записах клієнтів». З огляду на це ми в змозі простежити лише загальні тенденції у витоках інформації та зробити припущення про можливий їх стан у страхових компаніях.

Наприклад, American International Group (AIG) оголосила про втрату особистих даних, у тому числі імен і номерів соціального страхування, що належали 930 тис. клієнтів, а також про втрату десятків тисяч медичних записів. Виток інформації стався внаслідок викрадення 31 березня 2006 року ноутбуку, фотоапарату та комп'ютерного обладнання з офісу страховика у США. Усі 930 тис. клієнтів були співробітниками компаній, які мали корпоративні медичні поліси AIG [3]. Британське відділення страхової компанії Zurich Insurance зізналося у витоку даних про понад півмільйона своїх клієнтів. Дані були загублені під час транспортування у центр зберігання на території Південної Африки. За це управління з фінансових послуг Великобританії зобов'язало страхову компанію виплатити рекордний штраф у розмірі 2,3 млн. фунтів стерлінгів – найвищий (за даними FSA – Financial Services Authority) за всю історію існування законодавства Великобританії про захист даних [4]. Один із вендорів компанії Standard Insurance Company визнав, що був випадково розкритий файл у мережевій системі. Для сторонніх осіб у період від 7 до 18 жовтня 2013 року були доступні імена, номери соціального страхування, адреси та дати народження клієнтів [5]. 13 липня 2012 року компанія Massachusetts Mutual Life Insurance ненавмисно відправила за допомогою безпечної електронної пошти на неправильну адресу звіт, який містив інформацію з іменами клієнтів, номерами соціального страхування та іншими даними [6].

На нашу думку, об'єктом зацікавленості злочинців і надалі буде приватна інформація, а тому страховим компаніям необхідно використовувати сучасні технології її захисту, прописувати правила користування цією інформацією та, найголовніше, стежити за безумовним виконанням цих правил.

Сьогодні для запобігання витоків конфіденційної інформації широко застосовуються DLP-системи (у перекладі з англійської Data Leak Prevention – запобігання витоку даних). Ці інструменти засновані на аналізі потоків даних. У разі виявлення конфіденційної інформації спрацьовує захист, який відстежує повідомлення або блокує його надсилання.

Сутність роботи подібних систем полягає не тільки у блокуванні різних способів передачі інформації, а і в ретельній фільтрації всього трафіку. Найкращі DLP-системи, наприклад, можуть стежити за Інтернет-трафіком, а також за інформацією, що записується з комп'ютерів на зовнішні носії (USB-флеш, оптичні диски тощо), за документами, які роздруковуються, та ін. При цьому в автоматичному режимі си-

стема визначає, чи є в потоці даних документи, що містять конфіденційну інформацію, або такі, які схожі на них за змістом. Виявляючи щось подібне, DLP-система відразу посилає попередження співробітнику, що відповідає за забезпечення інформаційної безпеки, і той вирішує, яких слід вживати заходів.

Можна стверджувати, що саме з появою DLP-систем відбулося формування системи інформаційної безпеки. Адже до цього програмні продукти, які забезпечували інформаційну безпеку, насправді захищали не інформацію, а місця її зберігання. Із появою DLP-систем засоби захисту навчилися відрізняти конфіденційну інформацію від неконфіденційної. Певною мірою це дозволяє навіть економити на захисті даних, наприклад, використовувати шифрування тільки в тих випадках, коли зберігається або передається конфіденційна інформація, в інших – не шифрувати.

Слід зауважити, що саме у страхуванні в Україні можуть активно застосовуватися DLP-системи. Це пов'язано з тим, що найкращі DLP-системи спрямовані, перш за все, на відловлювання структурованої шаблонної інформації та персональних даних, а у сфері страхування здебільшого використовуються стандартизовані форми зберігання і передачі інформації.

Водночас, не можна забувати, що DLP-системи вирішують лише одну частину проблеми – випадкові витоки. Зловмисні витоки не контролюються нею. Отже, DLP-системи не здатні самостійно, без зусиль з боку спеціалістів служби безпеки, запобігати всім видам витоків. Для боротьби із зловмисними витоками передбачається доопрацювання на етапі підготовки, впровадження та супроводу системи, розслідувань інцидентів тощо.

Останнім часом страхові компанії використовують власні сайти не тільки для презентації фірми та її страхових продуктів, розміщення останніх новин тощо. У режимі он-лайн також пропонується заповнити замовлення на придбання страхового продукту, сплатити вартість продукту й отримати страховий поліс. Зрозуміло, що програма, яка забезпечує такий сервіс, повинна мати високий рівень інформаційного захисту.

Саме технологія «хмарних обчислень» (Cloud Computing) забезпечує повсюдний і зручний мережевий доступ на вимогу до обчислювальних ресурсів, таких як мережі передачі даних, сервери, пристрої зберігання даних, додатки й сервіси. Використання «хмарних обчислень» дозволяє споживачам значно зменшити витрати на інфраструктуру інформаційних технологій і гнучко реагувати на зміни обчислювальних потреб завдяки використанню властивостей обчислювальної еластичності «хмарних послуг».

Однак в останні роки все частіше з'являються повідомлення, що технологія «хмарних обчислень» є вразливою й піддається зламу хакерами. Існує інформація від компаній із різних галузей економіки, зокрема Епсілон (Epsilon), Соні (Sony) та Амазон (Amazon), що у квітні 2011 року відбулися витоки даних через використання «хмарних обчислень».

Наприклад, маркетингова компанія Epsilon повідомила, що інформація про близько 2500 осіб, що становить майже 2% клієнтів, була піддана атаці хакерів, у наслідок чого було спотворено мільйони записів [7]. Sony оголосила, що певна інформація облікового запису була викривлена через незаконне та несанкціоноване вторгнення в мережу [8]. Платформа «хмарних обчислень» компанії Amazon (Amazon Elastic Compute Cloud) відчула частковий збій. Було повідомлено, що вона назавжди втратила деякі дані про клієнтів [9].

Нині широко застосовується стандарт ISO/IEC 27001 із організації інформаційної безпеки, остання версія якого вийшла у 2013 році. Стандарт розроблено Міжнародною організацією стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). Станом на кінець 2013 року було видано 17 500 сертифікатів ISO/IEC 27001 у 100 країнах [10].

Використання цього стандарту здійснюється на комерційній основі, що покладає зобов'язання на клієнта суворо виконувати вимоги стандарту ISO, який, своєю чергою, контролює клієнта на предмет їх дотримання.

Упровадження системи управління інформаційною безпекою зумовлено необхідністю захисту бізнес-процесів компаній з метою зниження потенційних ризиків витоку конфіденційної інформації, мінімізації можливості зовнішніх втручань, а також централізованого контролю потоків даних.

ISO/IEC 27001 містить вимоги в галузі захисту інформації для створення, розвитку і підтримки системи менеджменту інформаційної безпеки. Поняття «захисту інформації» трактується цим міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Фактично ISO/IEC 27001 описується система управління ризиками, що пов'язані з інформацією.

Процес сертифікації за стандартом ISO/IEC 27001 складається із трьох стадій:

1) вивчення незалежним аудитором документів системи менеджменту інформаційної безпеки;

2) масштабний аудит, оцінка впроваджених заходів та їх ефективності, повне вивчення документів, яких вимагає стандарт;

3) завершальна стадія аудиту для підтвердження, що сертифікована організація відповідає вимогам.

Популярність цього стандарту можна пояснити й тим, що він інтегрується з іншими стандартами ISO, які були запроваджені в компаніях, наприклад, ISO 9001 (системи менеджменту якості), ISO/IEC 22301 (системи менеджменту безперервності бізнесу), ISO/IEC 20000 (системи менеджменту IT-послуг). У багатьох країнах ISO/IEC 27001 є основою для встановлення національних стандартів інформаційної безпеки.

Страхові компанії для підвищення якості власних послуг намагаються дотримуватися високих міжнародних стандартів, зокрема розроблених Міжнародною організацією стандартизації та Міжнародною електротехнічною комісією. Сертифікація на відповідність ISO/IEC 27001 демонструє діловим партнерам, інвесторам і клієнтам, що захист даних, інформаційна безпека в страховій компанії є пріоритетним напрямом. Це, безперечно, робить таку компанію більш привабливим партнером. Проте для отримання конкурентних переваг компанії можуть встановлювати для себе додаткові стандарти надання послуг.

Стисло розглянемо використання засобів захисту інформації страховиками вітчизняного страхового ринку. Наприклад, з метою підвищення інформаційної безпеки НАСК «Оранта» від 2010 року використовує такі програмні рішення компанії Lumension, як контролювання знімних носіїв інформації Lumension Device Control, управління запуском додатків Lumension Application Control. За допомогою цих рішень можна відслідковувати, які пристрої постійно підключені, який тип і обсяг інформації знаходиться у трафіку компанії, які співробітники порушують правила доступу до інформації. Як результат, НАСК «Оранта» вказує на поліпшення інформаційної безпеки: знизилася кількість зловживань через підключення знімних носіїв, скоротилися випадки зараження вірусними програмами та витоків даних [11].

Починаючи з 2011 року, «хмарні технології» були запроваджені у страховій компанії «Гарант-Авто» [12]. Від 2013 року істотна частина IT-процесів страхової компанії «УНІКА» переведена на платформу гібридних «хмарних технологій». Перехід від традиційної моделі обчислень до «хмарних технологій» дозволив страховій компанії «УНІКА» отримати безперервно доступний сервіс, уніфікувати IT-компоненти, скоротити витрати на IT. Усе це в комплексі сприяло підвищенню якості обслуговування клієнтів компанії, зокрема оперативності продажу страхових полісів [13].

У 2013 році страхова компанія «АХА Страхування Життя» повідомила про те, що переводить IT-інфраструктуру на «хмарні технології». Із переходом на нові технології

«АХА Страхування Життя» відмовилася від використання традиційної ІТ-інфраструктури, перевівши на «хмарну платформу» навіть файл- і прінт-сервери [14].

У 2011 році страхова компанія «ПЗУ Україна» впровадила систему захисту від витоку конфіденційної інформації на базі McAfee Host Data Loss Prevention. Як і всі страхові компанії, СК «ПЗУ Україна» зберігає на базі своєї ІТ-інфраструктури велику кількість конфіденційної інформації про клієнтів, а тому, згідно із Законом України «Про захист персональних даних», несе відповідальність за збереження та безпеку цих даних. Упроваджена страховиком система захисту запобігатиме потенційному витоку конфіденційних даних відповідно до технічних можливостей [15].

Інформація щодо використання стандарту ISO/IEC 27001 страховими компаніями в Україні наразі відсутня. Обов'язкове введення адаптованого варіанту стандарту ISO/IEC 27001 в нашій державі вимагається лише для банківських установ. Для небанківських фінансових посередників, у т. ч. страхових компаній, в Україні поки що не запроваджено єдиних обов'язкових стандартів інформаційної безпеки.

Висновки. Стрімкий розвиток інформаційних технологій, продаж страхових послуг через Інтернет і численні новації вимагають сьогодні від страхових компаній надійного захисту персональних даних клієнтів та іншої конфіденційної інформації. Розуміючи значущість забезпечення інформаційної безпеки, вітчизняні страховики у своїй діяльності починають упроваджувати передові технології захисту конфіденційних даних, у т. ч. DLP-системи. Через відсутність в Україні законодавчих вимог до страховиків у системі захисту інформації практика застосування міжнародних стандартів інформаційної безпеки не набула такого поширення, як у розвинених державах світу, що, на нашу думку, може негативно вплинути на репутацію страховиків та призвести до ще більшої втрати довіри до них з боку споживачів страхових послуг.

Перспективи подальших досліджень будуть стосуватися можливостей застосування зарубіжного досвіду щодо формування політики інформаційної безпеки у страховій сфері.

Література

1. InfoWatch / Офіційний сайт. – Режим доступу : http://www.infowatch.ru
2. Trustwave / Офіційний сайт. – Режим доступу : http:// www.trustwave.com
3. Treaster J. Insurer Reports Theft of Data on 930 000 [Electronic resource]. – 2006. – Accessed mode : http://www.nytimes.com
4. Martin I. Insurer given record fine for losing 46 000 customers' details [Electronic resource]. – 2010. – Accessed mode : http://citywire.co.uk
5. Standard Insurance Company [Electronic resource]. – 2013. – Accessed mode : www.privacyrights.org
6. Massachusetts Mutual Life Insurance Company [Electronic resource]. – 2013. – Accessed mode : www.privacyrights.org
7. Mills E. Who Is Epsilon And Why Does It Have My Data? [Electronic resource] / E. Mills. – 2011. – Accessed mode : http://news.cnet.com/8301-27080_3-20051038-245.html
8. Sony Customer Notification US States (excluding Puerto Rico and Massachusetts) [Electronic resource]. – 2011. – Accessed mode : http://us.playstation.com/news/consumeralerts/#us
9. Eunice J. The Cloud Backlash [Electronic resource] / J. Eunice. – 2011. – Accessed mode : http://news.cnet.com/8301-31114_3-20058674-258.html#ixzz1LPsfKptq
10. ISO/IEC 27001:2013 information security management system standard arrives [Electronic resource]. – 2013. – Accessed mode : http://www.reuters.com
11. Oranta National Joint Stock Insurance Company [Electronic resource]. – 2012. – Accessed mode : https://www.lumension.com
12. Хмарні сервіси Microsoft допомагають «ГАРАНТ-АВТО» удосконалити систему корпоративних комунікацій без капітальних інвестицій [Електронний ресурс]. – 2011. – Режим доступу : http://www.microsoft.com
13. «УНИКА» перевела ИТ-процессы на облачные технологии [Электронный ресурс]. – 2013. – Режим доступа : http://www.de-novo.biz
14. Страховая компания АХА выбирает надежность Облака De Novo [Электронный ресурс]. – 2013. – Режим доступа : http://www.de-novo.biz
15. В СК «ПЗУ Украина» внедрили систему защиты от утечки данных [Электронный ресурс]. – 2011. – Режим доступа: http://www.pcweek.ua

Стаття надійшла до редакції 15.06.2014

References

1. InfoWatch *(Official website).* Retrieved from http://infowatch.ru (in Russ.).
2. Trustwave *(Official website).* Retrieved from http://trustwave.com
3. Treaster, J. (2006). *Insurer Reports Theft of Data on 930,000.* Retrieved from www.nytimes.com
4. Martin, I. (2010). *Insurer given record fine for losing 46,000 customers' details*. Retrieved from: http://citywire.co.uk
5. Privacy Rights Clearinghouse (2013). *Standard Insurance Company.* Retrieved from http://privacyrights.org/content/standard-insurance-company
6. Privacy Rights Clearinghouse (2013). *Massachusetts Mutual Life Insurance Company.* Retrieved from https://privacyrights.org/content/massachusetts-mutual-life-insurance-company
7. Mills, E. (2011). *Who Is Epsilon And Why Does It Have My Data?* Retrieved from http://news.cnet.com/8301-27080_3-20051038-245.html
8. PlayStation (2011). *Sony Customer Notification US States (excluding Puerto Rico and Massachusetts).* Retrieved from http://us.playstation.com/news/consumeralerts/#us
9. Eunice, J. (2011). *The Cloud Backlash.* Retrieved from http://news.cnet.com/8301-31114_3-20058674-258.html#ixzz1LPsfKptq
10. Reuters (2013). *ISO/IEC 27001:2013 information security management system standard arrives.* Retrieved from http://www.reuters.com
11. Lumension (2012). *Customer Success Story. Oranta National Joint Stock Insurance Company.* Retrieved from https://lumension.com/Customers/lumension-customer-success-stories/Oranta-National-Joint-Stock-Insurance-Company.aspx
12. Microsoft (2011). *Microsoft cloud services help «Garant-AUTO» to improve the system of corporate communications without capital investment.* Retrieved from https://microsoft.com/Ukraine/CaseStudies/CaseStudy.aspx?id=93 (in Ukr.).
13. De Novo (2013). *«UNIQA» moved IT processes to the cloud services.* Retrieved from http://www.de-novo.biz (in Russ.).
14. De Novo (2013). *AXA insurance company chooses the reliability of De Novo's cloud.* Retrieved from http://www.de-novo.biz (in Russ.).
15. PC Week (2011). *IC «PZU Ukraine» implemented a system of protection against data leakage.* Retrieved from http://www.pcweek.ua (in Russ.).

Received 15.06.2014