УДК 368.03:004.056

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТРАХОВИХ КОМПАНІЙ: УКРАЇНСЬКІ РЕАЛІЇ ТА ДОСВІД США

© 2014 **ЖАБИНЕЦЬ О. Й.**

УДК 368.03:004.056

Жабинець О. Й.

Політика інформаційної безпеки страхових компаній: українські реалії та досвід США

У статті досліджено перспективи реалізації політики інформаційної безпеки українськими страховими компаніями. Зокрема, проаналізовано законодавче забезпечення та міжнародні стандарти інформаційної безпеки ISO/IEC 27001:2013 та ISO/IEC 27002:2013, розглянуто місце політики інформаційної безпеки у новій версії міжнародного стандарту інформаційної безпеки ISO/IEC 27002:2013. Проведено аналіз ключових факторів оцінки ризику у формуванні політики інформаційної безпеки американської компанії сфери ризикового страхування Philadelphia Insurance Companies. Автор робить висновок, що, незважаючи на те, що діяльність страхової компанії як і будь-якої іншої фінансової установи, наприклад, комерційного банку, має свою специфіку, її інформаційна безпека ґрунтується на загальноприйнятих принципах та вимогах міжнародних стандартів. Кожна страхова компанія України сьогодні може самостійно вирішувати питання формування та реалізації політики інформаційної безпеки, керуючись національним законодавством, міжнародними стандартами та досвідом зарубіжних страхових компаній. Водночас з огляду на нестабільність соціально-економічної та політичної ситуації в нашій державі, і як наслідок – невизначеності умов функціонування ринку страхування навіть у найкоротшій перспективі, вітчизняні страхові компанії не можуть стабілізувати і спрогнозувати свої прибутки, що знижує можливості планування і проведення чіткої ІТ-політики, в т. ч. політики інформаційної безпеки.

Ключові слова: *політика інформаційної безпеки, страхові компанії, міжнародні стандарти інформаційної безпеки, законодавче забезпечення інформаційної безпеки, фактори оцінки ризику*

Рис.: *2.* ***Табл.:*** *1.* ***Бібл.:*** *10.*

Жабинець Ольга Йосифівна *– кандидат економічних наук, доцент кафедри фінансів, Львівський державний університет внутрішніх справ (вул. Городоцька, 26, м. Львів, 79007)*

Email: *olza@ukr.net*

УДК 368.03:004.056

Жабинец О. И. Политика информационной безопасности страховых компаний: украинские реалии и опыт США

В статье исследованы перспективы реализации политики информационной безопасности украинскими страховыми компаниями. В частности, проанализированы законодательное обеспечение и международные стандарты информационной безопасности ISO/IEC 27001:2013 и ISO/IEC 27002:2013, рассмотрено место политики информационной безопасности в новой версии международного стандарта информационной безопасности ISO/IEC 27002: 2013. Проведен анализ ключевых факторов оценки риска в формировании политики информационной безопасности американской компании сферы рискового страхования Philadelphia Insurance Companies. Автор делает вывод, что несмотря на то, что деятельность страховой компании как и любой другой финансовой организации, например, коммерческого банка, имеет свою специфику, ее информационная безопасность основывается на общепринятых принципах и требованиях международных стандартов. Каждая страховая компания Украины сегодня может самостоятельно решать вопросы формирования и реализации политики информационной безопасности, руководствуясь национальным законодательством, международными стандартами и опытом зарубежных страховых компаний. В то же время, учитывая нестабильность социально-экономической и политической ситуации в нашем государстве, и как следствие – неопределенность условий функционирования рынка страхования даже в краткосрочной перспективе, отечественные страховые компании не могут стабилизировать и спрогнозировать свои доходы. Это, в свою очередь, снижает возможности планирования и проведения четкой ИТ-политики, в т. ч. политики информационной безопасности.

Ключевые слова: *политика информационной безопасности, страховые компании, международные стандарты информационной безопасности, законодательное обеспечение информационной безопасности, факторы оценки риска*

UDC 368.03:004.056

Zhabynets O. Yo. The Information Security Policy at Insurance Companies: Ukrainian Context and U.S. Experience

The article studies the prospects for the information security policy implemented by Ukrainian insurance companies. In particular, the legal framework and international information security standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013 were analyzed, as well as the role of the information security policy according to the new version of the international information security standard ISO/IEC 27002:2013. The study analyzes key risk evaluation factors in forming the information security policy of Philadelphia Insurance Companies, a U.S.-based risk insurance company. The author concludes that despite the fact that operations of an insurance company, as well as any other financial institution, for example, a commercial bank, have distinctive properties, their information security is based on the generally accepted principles and requirements of international standards. Each Ukrainian insurance company can currently solve the problems of forming and implementing the information security policy in accordance with the national legislation, international standards and the experience of foreign insurance companies. Simultaneously, due to lack of stability in the socio-economic and political situation in our state and the resulting uncertainty of operating conditions of the insurance market even in the most immediate future, domestic insurance companies cannot stabilize and predict their incomes, which restricts the possibility of planning and pursuing a well-defined IT policy, including the information security policy.

Keywords: *information security policy, insurance companies, international information security standards, legal framework for information security, risk evaluation factors*

Pic.: *2.* ***Tabl.:*** *1.* ***Bibl.:*** *10.*

Zhabynets Olga Yo. *– Candidate of Sciences (Economics), Associate Professor, Associate Professor, Department of Finance, Lviv State University of Internal Affairs (vul. Gorodotska, 26, Lviv, 79066, Ukraine)*

Email: *olza@ukr.net*

Рис.: 2. Табл.: 1. Библ.: 10.

***Жабинец Ольга Иосифовна** – кандидат экономических наук, доцент, доцент кафедры финансов, Львовский государственный университет внутренних дел (ул. Городоцкая, 26, г. Львов, 79066)*

***Email:** olza@ukr.net*

Постановка проблеми. Процеси інтеграції вітчизняного страхового ринку до європейського та світового страхового простору вимагають від страхових компаній швидкого реагування на проблеми, що виникають у зв'язку із можливими витоками конфіденційної інформації, а її захист виступає головним пріоритетом у діяльності усіх без винятку страховиків. Ефективність формування захисних механізмів протидії ризикам, що загрожують захисту конфіденційних даних та комерційної таємниці, напряму залежить від розробки та впровадження вітчизняними страховими компаніями політики інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення інформаційної безпеки в різних її аспектах розглядали у своїх працях багато вітчизняних та зарубіжних науковців, зокрема О. О. Войналович, А. Є. Городецький, В. В. Домарьов, О. Б. Курицький, Р. А. Калюжний, Б. А. Кормич, Ю. Є. Максименко, О. І. Мотлях, О. В. Олійник, Ю. А. Нисневич, В. П. Талимончик, Г. А. Титаренко, В. С. Цимбалюк. Водночас, питання законодавчого забезпечення та особливостей реалізації політики інформаційної безпеки вітчизняними страховиками, а також використання зарубіжного досвіду щодо її формування сьогодні залишаються поза увагою вітчизняних дослідників, що обумовило вибір тематики даної наукової статті.

Метою статті є аналіз законодавчого забезпечення та можливостей реалізації політики інформаційної безпеки вітчизняними страховиками на основі використання національного та зарубіжного досвіду, а також міжнародних стандартів з управління інформаційною безпекою.

Основні результати дослідження. У науковій літературі найчастіше використовується таке визначення політики інформаційної безпеки: «Політика інформаційної безпеки – це набір законів, правил, практичних рекомендацій і практичного досвіду, що визначають управлінські та проектні рішення в області захисту інформації» [1, с. 137].

Основними законодавчо-нормативними актами у сфері інформаційної безпеки є сьогодні Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», а також Указ Президента України «Про положення про технічний захист інформації в Україні». Усі вони стосуються загальних аспектів захисту інформації та персональних даних громадян. Щодо фінансової сфери, то з дня опублікування Постанови НБУ «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України» від 28.10.2010 № 474 у банківській діяльності почали діяти такі стандарти:

1) СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IEC 27001:2005, MOD);
2) СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IEC 27002:2005, MOD) [2].

Впровадження в банках України стандартів з управління інформаційною безпекою дозволить, зокрема, розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання, а також забезпечити підвищення репутації та ринкової привабливості банків [3].

Для страхових компаній в Україні поки що не запроваджено єдиних обов'язкових стандартів інформаційної безпеки, хоча такі стандарти уже давно застосовуються зарубіжними страховиками. З огляду на те, що політика інформаційної безпеки банківськими установами розробляється самостійно, як це зазначено у Методичних рекомендаціях, то сьогодні вітчизняні страховики, спираючись на зарубіжний досвід та досвід реалізації політики інформаційної безпеки в банківській та інших видах діяльності, а також міжнародні стандарти інформаційної безпеки, можуть самостійно розробляти власну політику інформаційної безпеки.

Серед міжнародних стандартів інформаційної безпеки (ISO/IEC 27001 та ISO/IEC 27002) політика інформаційної безпеки описується стандартом ISO/IEC 27002, остання версія якого вийшла у 2013 році. Для впровадження системи управління інформаційною безпекою використовується стандарт ISO/IEC 27001. В ньому прописано алгоритми, у відповідності до яких має бути впроваджено систему інформаційної безпеки [4], тоді як ISO/IEC 27002 надає пояснення, детально описує кроки щодо впровадження системи, включає рекомендації та пояснення для оперативного і правильного впровадження усіх вимог [5]. У разі запровадження системи інформаційної безпеки компанія отримує сертифікат про присвоєння стандарту саме ISO/IEC 27001.

Інформація щодо використання стандарту ISO/IEC 27001 страховими компаніями в Україні наразі відсутня [6, с. 35]. Однак перші кроки до процесу використання міжнародних стандартів інформаційної безпеки уже зроблено одним із лідерів вітчизняного ринку страхування НАСК «Оранта», яка з 2010 року використовує програмні рішення компанії Lumension, впровадження яких, за словами представника компанії, повинно стати одним з послідовних етапів підготовки НАСК «Оранта» до сертифікації за міжнародним стандартом ISO 27001 [7].

Місце політики інформаційної безпеки у новій версії міжнародного стандарту інформаційної безпеки ISO/IEC 27002:2013 демонструє рис. 1.

Відповідно до стандарту ISO/IEC 27001:2013, мета політики інформаційної безпеки полягає у забезпеченні напрямку управління інформаційною безпекою та підтримку

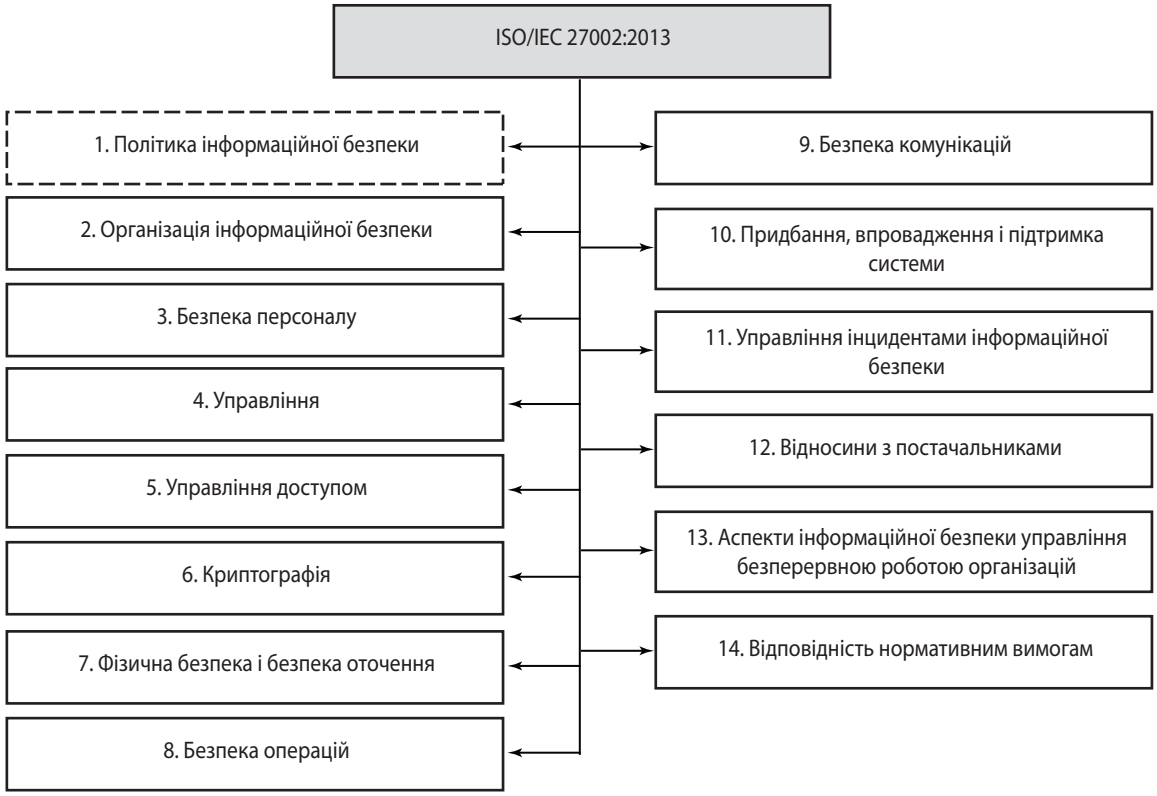

Рис. 1. Місце політики інформаційної безпеки у міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013

Джерело: побудовано автором за [5].

захисту інформації відповідно до вимог бізнесу та відповідних законів і правил [5].

На найвищому рівні стандартом вимагається визначити програмний документ – «політика інформаційної безпеки», в якому буде викладено підхід до управління захистом інформації в організації. Цей документ в області інформаційної безпеки повинен бути визначений та затверджений керівництвом, опублікований і доведений до співробітників і відповідних зовнішніх сторін.

Програмний документ повинен відповідати таким вимогам:

а) бізнес-стратегії;

б) правилам, законодавству та договорам;

в) поточним та прогнозованим загрозам навколишнього середовища щодо інформаційної безпеки.

Політика інформаційної безпеки має містити такі основні відомості:

1) визначення інформаційної безпеки, її цілей і принципів, що охоплюють всі види діяльності, пов'язані із захистом інформації;

2) призначення загальних і спеціальних обов'язків з управління інформаційною безпекою;

3) процесів для обробки відхилень і винятків [5].

Програмний документ має бути «підтриманий» конкретними темами політики, які сприяють реалізації контролю в області інформаційної безпеки і, як правило, структурований з метою задоволення потреб певних цільових груп усередині організації або для охоплення певних тем, наприклад таких як управління доступом, класифікація інформації (і її обробка), фізична безпека та безпека оточення, конфіденційність і захист персональної інформації та ін.

Політика інформаційної безпеки повинна бути доведена до співробітників і відповідних зовнішніх сторін у формі, яка є доступною і зрозумілою.

Крім того, політика інформаційної безпеки може бути оформлена як у вигляді одного документа, так і декількох окремих, але взаємопов'язаних документів; повинна переглядатись через заплановані інтервали або за умови значних змін з метою забезпечення її (політики) постійної придатності, адекватності та ефективності.

За словами Метью Джозефовіча (Matthew Josefowicz), менеджера страхової групи дослідницької компанії Celent: «Інформаційна безпека – головний пріоритет для страхових груп у США; оцінка поточних уразливих місць і розробка комплексної стратегії захисту стають пріоритетом» [8].

З огляду на це розглянемо особливості формування політики інформаційної безпеки американською страховою компанією Philadelphia Insurance Companies (PHLY).

Для початку варто звернути увагу на те, що Philadelphia Insurance Companies (PHLY) – це ризикова страхова компанія зі штаб-квартирою в місті Бала Синвайд (Bala Cynwyd) штату Пенсільванія у США. Компанія налічує 46 офісів в 13 регіонах на всій території США. Має високі рейтинги наступних рейтингових агентств: «A + +» (Superior) за A.M. Best Company, «A +» за Standard & Poor's. Компанія входить до страхової групу «The Tokio Marine

Group», яка є найстарішим страховиком Японії та лідером у майновому страхуванні та страхуванні відповідальності [9].

При створенні політики інформаційної безпеки PHLY розглядає наступні ключові фактори оцінки ризику (табл. 1).

Таблиця 1

Аналіз ключових факторів оцінки ризику PHLY у формуванні політики інформаційної безпеки

№ з/п	Фактори оцінки ризику	Їх характеристика	Особливості забезпечення
1	2	3	4
1	Права доступу до внутрішньої інформації та інформації про клієнтів (далі – конфіденційної інформації)	Права доступу до інформації надаються уповноваженим особам керівництвом компанії	Права надаються за необхідністю
2	Контроль доступу до інформаційних систем (у т.ч. елементів управління для перевірки справжності) та надання доступу лише уповноваженим особам і компаніям	Доступ до інформації обмежений уповноваженими особами. Всі програми компанії використовують технологію аудентифікації для управління доступом	Уповноваженій особі присвоюється унікальне ім'я користувача та пароль, які використовуються при вході в систему для додатків, що містять інформацію. Крім того, після трьох невдалих спроб користувач блокується і відключається системним адміністратором
3	Обмеження доступу в місця, що містять інформацію: будівлі, кабінети з комп'ютерною технікою, сховища записів	Дата-центр компанії розташований в штаб-квартирі. У цьому місці фізичний доступ в будівлю контролюється за допомогою системи карткового доступу. Крім того, приміщення постійно патрулюють охоронці	1)доступ до обчислювальної техніки в дата-центрі контролюється також за допомогою системи карткового доступу. Тільки уповноважені особи (наприклад, персонал IT-відділу) отримують відповідний доступ. 2) в якості віддаленого сховища записів PHLY використовує зовнішніх постачальників. Безпека навколишнього об'єкта постачальника перевіряється шляхом відвідування цього об'єкта
4	Шифрування електронної інформації (під час транспортування та зберігання в мережі або системі), до якої неуповноважені особи не мають доступу	На теперішній час конфіденційна інформація, що зберігається в мережі або системах – зашифрована, й компанія запроваджує технологію, яка захищатиме передачу цих даних	-
5	Процедури, які підтверджують відповідність змін конфіденційної інформації щодо політики інформаційної безпеки фірми	Ці процедури забезпечують доступ до конфіденційної інформації обмеженому колу уповноважених осіб	-
6	Процедури подвійного контролю, розподіл обов'язків і перевірка співробітників, відповідальних за доступ до інформації про клієнтів	Перевірки проводяться щодо всіх потенційних працівників компанії, у тому числі тих, які під час роботи можуть мати доступ до конфіденційної інформації	Процедури відбору нових співробітників тісно пов'язані із відділом персоналу. Належний розподіл обов'язків здійснюється за допомогою докладного опису посадових функцій. Посадові інструкції описують основні обов'язки працівників, при цьому особливу увагу спрямовано на адекватний розподіл обов'язків
7	Системи контролю та процедур для виявлення фактичних вторгнень у конфіденційну інформацію та намагань заволодіння даними цієї інформації	Працівники відділу інформаційних технологій використовують процедури для моніторингу активності брандмауера за підсумками тижня	Під час розгляду журналів діяльності брандмауера, працівники знаходять численні невдалі спроби входу в систему та дивно записані імена користувачів. За всіма підозрілими подіями проводяться ретельні розслідування
8.	Програми реагування, що визначають заходи, які необхідно вжити, коли є підозра щодо несанкціонованого доступу до конфіденційної інформації або виявлено несанкціонований доступ	Персонал відділу інформаційних технологій несе відповідальність за актуальний стан програм реагування на момент, якщо є фактичні вторгнення в інформаційні системи фірми або лише спроби вторгнення	-

Закінчення табл. 1

1	2	3	4
9	Захист від фізичного знищення конфіденційної інформації через ушкодження вогнем і водою	Центр обробки даних захищений за допомогою пожежної техніки гасіння, а також шляхом вибору найліпшого розташування центру на місцевості, його архітектурного планування та будівництва	-
10	Програми реагування щодо збереження цілісності та безпеки конфіденційної інформації у разі відмови комп'ютера або іншого обладнання, у тому числі, при необхідності відновлення втраченої інформації	Компанія підтримує план аварійного відновлення для центру даних у власному офісі. Крім того, для кожного департаменту компанії існує окремий план аварійного відновлення, який узгоджений в межах усієї організації	План аварійного відновлення перевіряється один раз на рік на об'єктах компаній-постачальників програм аварійного відновлення

Джерело: складено автором за [10].

Як свідчить інформація, викладена у табл. 1, політика інформаційної безпеки страховика будується на ключових факторах оцінки ризику, і чим повніше буде зроблений аналіз, тим ефективнішою буде реалізація цієї політики. Крім того, політика інформаційної безпеки повинна будуватися відповідно до специфіки діяльності і узгоджуватись із законодавчою базою держави.

Потреба страховиків України у розробці політики інформаційної безпеки, на нашу думку, зростатиме з кожним роком. Високий рівень конкуренції на ринку страхування спонукатиме страхові компанії боротися за клієнтів – причому не просто за клієнтів, а за надійних, перспективних та «безризикових». Тобто за тих, хто зазвичай є дуже чутливим до якості і рівня обслуговування.

Водночас, з огляду на нестабільність соціально-економічної та політичної ситуації в нашій державі, і як наслідок – невизначеності умов функціонування ринку страхування навіть у найкоротшій перспективі, страхові компанії не можуть стабілізувати і спрогнозувати свої прибутки, що знижує можливості планування і проведення чіткої ІТ-політики, у т. ч. політики інформаційної безпеки.

На основі практичного досвіду з метою підвищення рівня інформаційної безпеки компаніям, в т. ч. страховим, можна рекомендувати використовувати низку наступних заходів захисту даних, які не потребують значних фінансових витрат (рис. 2).

Як видно з рис. 2, без грамотно розробленої політики інформаційної безпеки не можуть обійтися жодні адміністративні заходи захисту.

Отже, незважаючи на те, що діяльність страхової компанії як і будь-якої іншої фінансової установи, наприклад комерційного банку, має свою специфіку, її інформаційна безпека ґрунтується на загальноприйнятих принципах та вимогах міжнародних стандартів. Кожна страхова компанія України сьогодні може самостійно вирішувати питання формування та реалізації політики інформаційної безпеки, керуючись національним законодавством, міжнародними стандартами та досвідом зарубіжних страхових компаній.

Висновки. Важливе значення у створенні механізму протидії ризикам, що загрожують захисту конфіденційних даних страховиків, належить розробці та впровадженню політики інформаційної безпеки. Політика інформаційної безпеки страхової компанії повинна передбачає прийняття необхідних заходів з метою захисту активів від випадкової або навмисної зміни, розкриття чи знищення, а також в цілях дотримання конфіденційності, цілісності та доступності інформації, забезпечення процесу автоматизованої обробки даних. Від ретельності її опрацювання залежатиме дієвість всіх інших рівнів забезпечення інформаційної безпеки – процедурного і програмно-технічного. Водночас складність розробки політики інформаційної безпеки може визначатися проблематичністю використання зарубіжного досвіду, оскільки політика безпеки ґрунтується на виробничих ресурсах і функціональних можливостях програмних продуктів конкретного страховика, а також, на нашу думку, повинна враховувати особливості національного ринку страхування.

ЛІТЕРАТУРА

1. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К. : ООО «ТИД «ДС», 2002. – 688 с.

2. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України : Постанова НБУ від 28.10.2010 р. № 474 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/v0474500-10

3. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0365500-11

4. International standard ISO/IEC 27001. – 2nd edit. – Switzerland, 2013. – 23 p.

5. International standard ISO/IEC 27002. – 2nd edit. – Switzerland, 2013. – 80 p.

6. Жабинець О. Й. Захист інформації та інформаційна безпека страхових компаній / О. Й. Жабинець // Економічний часопис – XXI. – 2014. – № 7 – 8 (2). – С. 32 – 35.

7. НАСК «Оранта» закупила Lumension для обеспечения безопасности конечных точек [Електронний ресурс]. – Режим доступу : http://oranta.ua/rus/pressroom_record.php?news_id=890

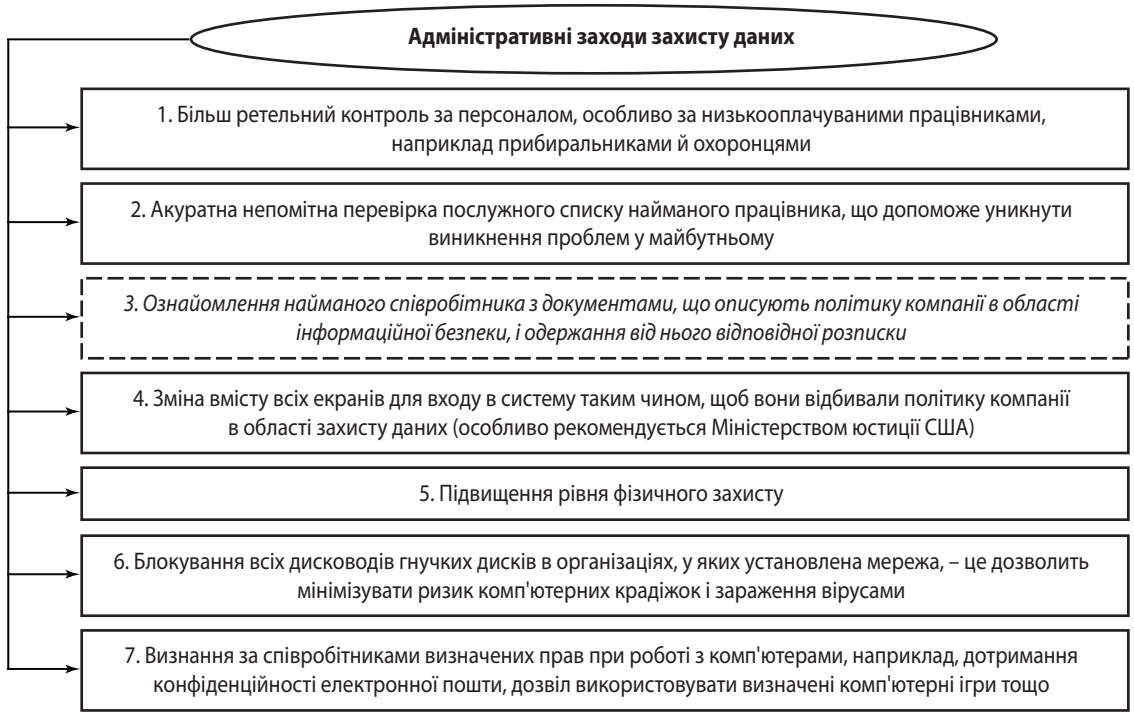

Рис. 2. Адміністративні заходи захисту даних

Джерело: побудовано автором за [1, с. 141].

8. Josefowicz M. IT Security Issues in Insurance [Електронний ресурс]. – Режим доступу : http://www.celent.com/reports/it-security-issues-insurance

9. PHLY at a Glance [Електронний ресурс]. – Режим доступу : https://www.phly.com/Files/PHLY%20at%20a%20Glance%202014_05021431-2900.pdf

10. Philadelphia Insurance Companies. Information Security Policy [Електронний ресурс]. – Режим доступу : http://www.phly.com/Files/infosecurity_policy31-2813.pdf

REFERENCES

Domarev, V. V. Bezopasnost informatsionnykh tekhnologiy. Metodologiia sozdaniia sistem zashchity [Safety of information technology. Methodology for creating protection systems]. Kyiv: TID «DS», 2002.

"HACK "Oranta" zakupila Lumension dlia obespecheniia bezopasnosti konechnykh tochek" [HACK "Orans" bought for Lumension endpoint security]. http://oranta.ua/rus/pressroom_record.php?news_id=890

International standard ISO/IEC 27001Switzerland, 2013.

International standard ISO/IEC 27002Switzerland, 2013.

Josefowicz, M. "IT Security Issues in Insurance" http://www.celent. com/reports/it-security-issues-insurance.

[Legal Act of Ukraine] (2010). http://zakon4.rada.gov.ua/laws/show/v0474500-10

"Metodychni rekomendatsii shchodo vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu ta metodyky otsinky ryzykiv vidpovidno do standartiv Natsionalnoho banku Ukrainy" [Guidelines for implementing information security management system and methods of risk assessment in accordance with the standards of the National Bank of Ukraine]. http://zakon2.rada.gov.ua/laws/show/v0365500-11

"PHLY at a Glance" https://www.phly.com/Files/PHLY%20at%20a%20Glance%202014_05021431-2900.pdf

"Philadelphia Insurance Companies. Information Security Policy" http://www.phly.com/Files/infosecurity_policy31-2813.pdf

Zhabynets, O. I. "Zakhyst informatsii ta informatsiina bezpeka strakhovykh kompanii" [Data protection and information security insurance]. Ekonomichnyi chasopys - XXI, no. 7-8 (2) (2014): 32-35.