УДК 681.321;322:621.395

МОДЕЛЬ СТРАХУВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

КОПИТІН Ю.В.

Одеська національна академія зв'язку ім. О.С. Попова

MODEL OF INSURANCE OF INFORMATION SECURITY RISK

KOPYTIN Y.V.

Odessa national academy of telecommunications n.a. O.S. Popov

Анотація. *В статті акцентовано увагу на швидкі тенденції зростання обсягів цифрової інформації, розкривається сутність і важливість страхування як одного із варіантів обробки ризиків та економічно вигідного методу захисту інформації. Обґрунтовується необхідність впровадження системи страхування ризиків інформаційної безпеки. Запропонована модель страхування ризиків інформаційної безпеки.*

Annotation. *The article accentuates the rapid trend growth of digital information, the essence and importance of insurance as option of risk treatment and economically viable method of information protection. The necessity of introduction of the system of information security risk's insurance is grounded. Model of insurance of information security risk is proposed.*

ПОСТАНОВКА ПРОБЛЕМИ

Сучасна цивілізація виробляє величезну кількість цифрової інформації, яка на сьогоднішній день досягла зеттабайтового діапазону (трильйони гігабайт). Експоненціальне зростання кількості цифрової інформації пов`язане зі збільшенням залежності від інтернет-сервісів, розповсюдженням смартфонів з відеокамерами, зростаючими вимогами корпоративних інформаційних систем, що скоро приведе світ до "йоттабайтової ери", коли кількість інформації перевищить йоттабайт – квадрильон гігабайт [1].

Бурхливі темпи створення нових інформаційно-комунікаційних технологій (ІКТ), зростання обсягів цифрової інформації і підвищення її значимості несуть у собі ризики, потенційно створюють передумови для витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання і блокування інформації і, як наслідок, ведуть до заподіяння шкоди.

Проблеми ризиків інформаційної безпеки (РІБ) і знаходження шляхів зниження шкоди стають з кожним роком все гостріше. Однак не всі власники, володільці і користувачі інформаційних ресурсів можуть самостійно забезпечити надійний захист інформації та гарантоване покриття ризиків.

Частково вирішити дані проблеми можливо шляхом створення дієвого страхового захисту – системи страхування ризиків інформаційної безпеки, яка є важливим і перспективним інструментом управління РІБ організації, економічно вигідним методом компенсації збитку власникам інформаційних активів.

Питанням страхування ризиків інформаційної безпеки присвячені роботи Косарєва А.В., Конявского В.А., Хованова В.М., Кудрявцева О.А., Подчерніна В.М., Скрініка А.П., Мервінського А.І., Ларіної І.Е. та ін.. Тематика даної статті зумовлена тим, що сьогодні страхування сприймається одним із найважливіших чинників сучасного й особливо майбутнього суспільства [2]. Також, до основних чинників, що визначають актуальність зазначеної проблеми, можна віднести й постійно зростаючу кількість інформаційних загроз і ризиків, недостатній рівень забезпечення інформаційної безпеки в організаціях. Страхування ризиків інформаційної безпеки - практично неосвоєна сфера українського страхового ринку, оскільки відсутні нормативно-правова, методична база та комплексні ґрунтовні дослідження цих питань.

Мета роботи – побудувати модель страхування ризиків інформаційної безпеки; обґрунтувати необхідність створення нормативно-правової та методичної бази, розробки та впровадження системи страхування ризиків інформаційної безпеки в Україні; показати сутність і важливість страхування як метода захисту інформації; залучення науковців, спеціалістів до обговорення та вирішення цієї проблеми.

1.АНАЛІЗ СТАНУ ПРОБЛЕМИ

На даний час серед науковців і фахівців не існує однозначного тлумачення понять «інформаційна безпека», «ризик», «ризик інформаційної безпеки», «страхування ризиків інформаційної безпеки», «система страхування ризиків інформаційної безпеки». В літературі широко вживаються такі поняття як «страхування інформаційних ризиків», «страхування інформаційних ресурсів та систем», «страхування електронних пристроїв», «страхування цифрових активів» тощо. В даній роботі будемо використовувати визначення, які наведені в міжнародних стандартах.

Згідно ISO/IEC 27000:2009 *інформаційна безпека* - збереження конфіденційності, цілісності і доступності інформації.

Ризик – комбінація імовірності події та її наслідків [3]. Зауважимо, що ризики властиві всім без виключення сферам діяльності організацій, що законодавчо закріплено в ст.42 Господарського Кодексу України.

Під *ризиком інформаційної безпеки* [4] розуміють імовірність того, що дана загроза буде експлуатувати вразливість активу або групи активів і тим самим завдасть шкоду організації.

На думку автора *страхування ризиків інформаційної безпеки* є одним із варіантів обробки ризиків та економічно вигідним методом захисту інформації, заснованим на видачі страховими компаніями гарантій суб'єктам інформаційних відносин за відшкодування матеріального збитку у разі реалізації загроз інформаційної безпеки.

Вбачається більш правильним розглядати страхування ризиків інформаційної безпеки у широкому сенсі – *страхування інформаційних активів організації*. Страхування ризиків інформаційної безпеки зводиться не тільки до страхування інформації. Страхуються взагалі ризики, пов'язані з інформаційними активами і ризики втрати фінансових активів, і ризики зупинки комерційної діяльності, і ризики, пов'язані з виникненням цивільної відповідальності. Це дозволяє розглядати проблему в комплексі.

Створення та розвиток ринку страхування в інформаційній сфері, нормативно-методичної бази та проведення заходів, спрямованих на впровадження в державах-учасниках СНД системи страхування інформаційних ризиків було передбачено ще в 1999 році [5], яка на жаль, до цього часу не реалізована.

Система страхування ризиків інформаційної безпеки, на нашу думку, – це організаційно впорядкована сукупність суб'єктів (страхових компаній, страхувальників, експертних, консалтингових і брокерських компаній тощо), об’єктів (активів організації) та комплекс законодавчих, нормативно-правових та методичних документів, які визначають умови і порядок проведення страхування ризиків інформаційної безпеки.

2. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ СТВОРЕННЯ СИСТЕМИ СТРАХУВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Існування ризиків інформаційної безпеки робить необхідним управління ними. Управління ризиками (ризик-менеджмент) застосовується для захисту активів організації від ризиків, тобто подій випадкового і непередбачуваного характеру, які можуть завдати шкоди її діяльності. Процес управління РІБ та варіанти оброблення ризиків представлено на рис. 1.

Для кожного з ризиків, ідентифікованих після оцінки ризику, треба прийняти рішення щодо оброблення ризиків. Оброблення ризику (risk treatment) - процес вибору та

впровадження заходів щодо модифікації ризику. Можливі варіанти оброблення ризиків включають: a) застосування належних контролів для зниження ризиків; b) свідоме й об'єктивне прийняття ризиків із забезпеченням, що вони чітко задовольняють політику організації та критерії прийняття ризику; c) уникнення ризиків не дозволяючи дії, які можуть спричинити виникнення ризиків; d) перенесення пов'язаних ризиків на інші сторони, наприклад, страхувальників або постачальників [6].

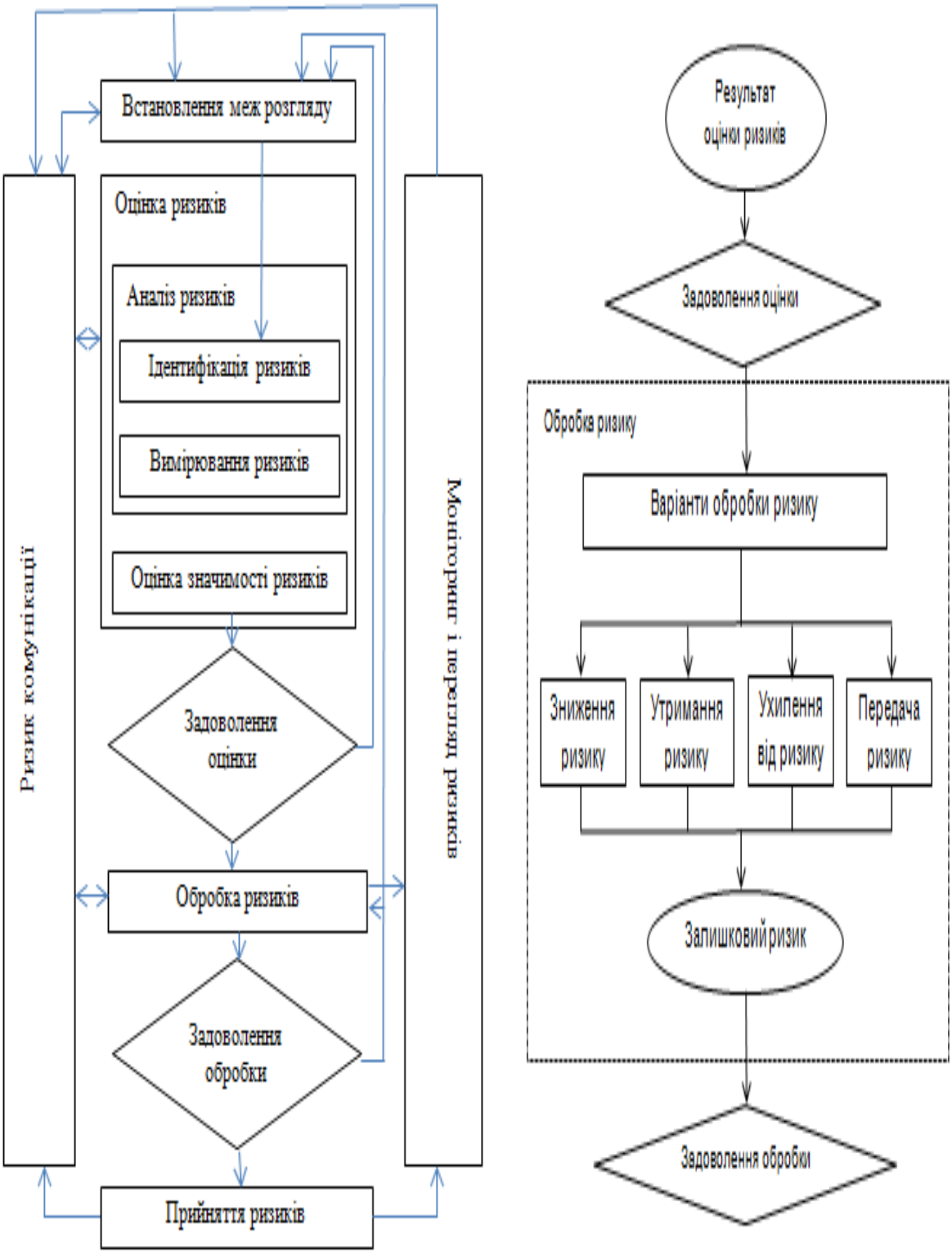

Рисунок 1 - Процес управління ризиком та варіанти оброблення ризиків(за ISO 27005 [6])

Даний стандарт прямо передбачає процес вибору та впровадження заходів щодо мінімізації наслідків ризиків шляхом їх *страхування*, суть якого полягає в передачі страхувальником за певну плату страховикові матеріальної відповідальності за наслідки ризику, зумовленого подіями (страховими випадками), перелік яких передбачено чинним законодавством або договором.

Для кращого розуміння проблеми нижче продемонструємо графічне обґрунтування необхідності створення системи страхування РІБ.

Початкові положення та основні параметри моделі страхування ризиків інформаційної безпеки можна визначити з наступних міркувань: чим більший необхідний рівень захищеності інформаційних активів P_3, тим потрібні більші витрати на побудову системи захисту. Для простоти будемо вважати залежність витрат на захист від рівня захищеності $B(P_3)$ лінійною (пряма 1 на рис. 2 зліва). Залежність можливих витрат, пов'язаних з відшкодуванням збитків, від рівня захищеності $З(P_3)$ більш складна і може бути апроксимована експоненційною кривою (крива 2 на рис. 2 зліва). Загальні імовірні збитки виражаються сумою витрат на захист та витрат на відшкодування збитків (крива 3 на рис. 2 зліва).

Точка *О* на рис. 2 – точка економічної рівноваги, яка відповідає випадку, коли величина можливих витрат, пов'язаних з відшкодуванням збитків, дорівнює витратам на впровадження системи захисту. Вона є межею області розумної достатності витрат на інформаційну безпеку. Однак, сумарні імовірні збитки можна зменшити шляхом перерозподілу витрат, а саме, використавши механізм страхування ризиків інформаційної безпеки. При цьому вартість страхування ризиків інформаційної безпеки залежить від ліміту відповідальності страховика та страхового тарифу, який напряму залежить від рівня захищеності $СТ(P_3)$ та на практиці складає від 1,5 до 5% страхової суми (рис. 2 справа).

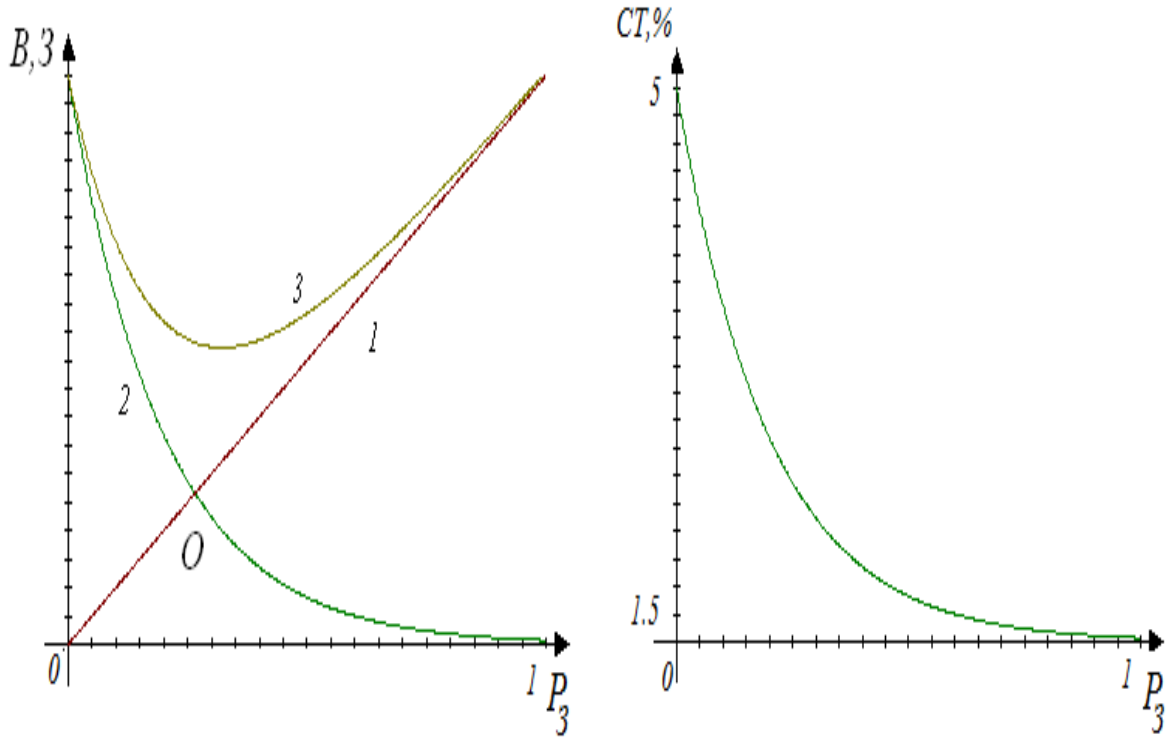

Рисунок 2 - Модель витрат на захист інформаційних активів та залежність страхового тарифу від рівня захищеності

Використовуючи механізм страхування, загальний ризик зменшується в результаті двох чинників: - витрати на страхування нижче витрат на побудову системи захисту, у випадку, коли існує велика кількість загроз, імовірність реалізації яких невисока; - організація отримує можливість за рахунок страхових виплат компенсувати (хоча б частково) збиток від вимушеного простою і втрати інформаційних активів. Виходячи з цього, загальний ризик після страхування ризиків інформаційної безпеки прийме вигляд кривої *1'* (рис. 3).

Зазначимо, що метод страхування ризиків інформаційної безпеки доцільно застосовувати: якщо ймовірність нанесення збитку невисока, але його розмір досить великий; якщо існує велика кількість ризиків та ймовірність їх реалізації (нанесення збитку) висока, але розмір можливого збитку невеликий; за наявності катастрофічних ризиків, тобто коли ймовірність і (або) розмір можливого збитку перевищує задані порогові значення [7].

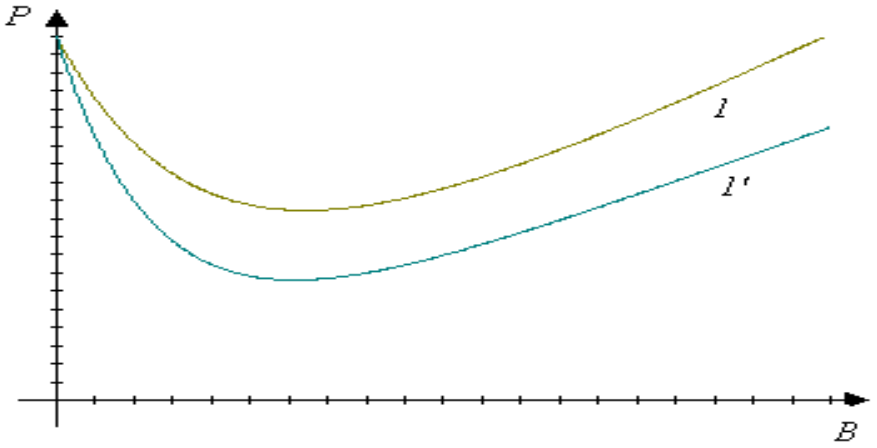

Рисунок 3 - Залежність ризику від вартості системи захисту

3.МОДЕЛЬ СТРАХУВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В даному випадку під моделлю будемо розуміти умовний опис процесу страхування РІБ [8]. Вважаємо можливим при страхуванні РІБ діяти за аналогією з традиційними принципами та методами страхування. На нашу думку, умовна модель страхування РІБ могла б мати вигляд, зображений на рис. 4.

Коротко опишемо дані етапи, оскільки кожен із них може стати темою окремого дослідження.

Ініціювання страхування та вибір страховика. Відносини в сфері інформації, інформаційної безпеки та страхування регулюються Конституцією України, Цивільним Кодексом України, Господарським кодексом України, Кримінальним кодексом України, ЗУ «Про інформацію», ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», ЗУ «Про стандарти, технічні регламенти та процедури відповідності», ЗУ «Про страхування», міжнародними договорами, згоду на обов'язковість яких надана Верховною Радою України, міжнародними нормами і стандартами та іншими законодавчими актами, що регулюють відносини в цих сферах.

Серед міжнародних стандартів у сфері ІБ найбільшою популярністю користуються: стандарти серії ISO 27000, ISO 20000, ISO 18044, ISO 15408, CobiT, NIST SP 800, BS, BSI, PCI DSS, ISF, ITU, EBIOS та ін. Якщо система захисту організації відповідає вимогам стандартів ISO, то це вселяє впевненість, що вона володіє такими характеристиками, як якість, безпека користувача, надійність, ефективність, простота у використанні та ін. Сертифікація на відповідність стандарту дозволить наочно показати як діловим партнерам, інвесторам і клієнтам, так і державі, як гаранту безпеки, що на підприємстві налагоджено ефективне управління інформаційною безпекою.

Перш ніж ініціювати питання страхування РІБ, слід розібратися, що саме треба захищати й страхувати, яка інформація обробляється в організації і де виконується її обробка й ким; визначити, що є цінним активом організації з точки зору інформаційної безпеки.

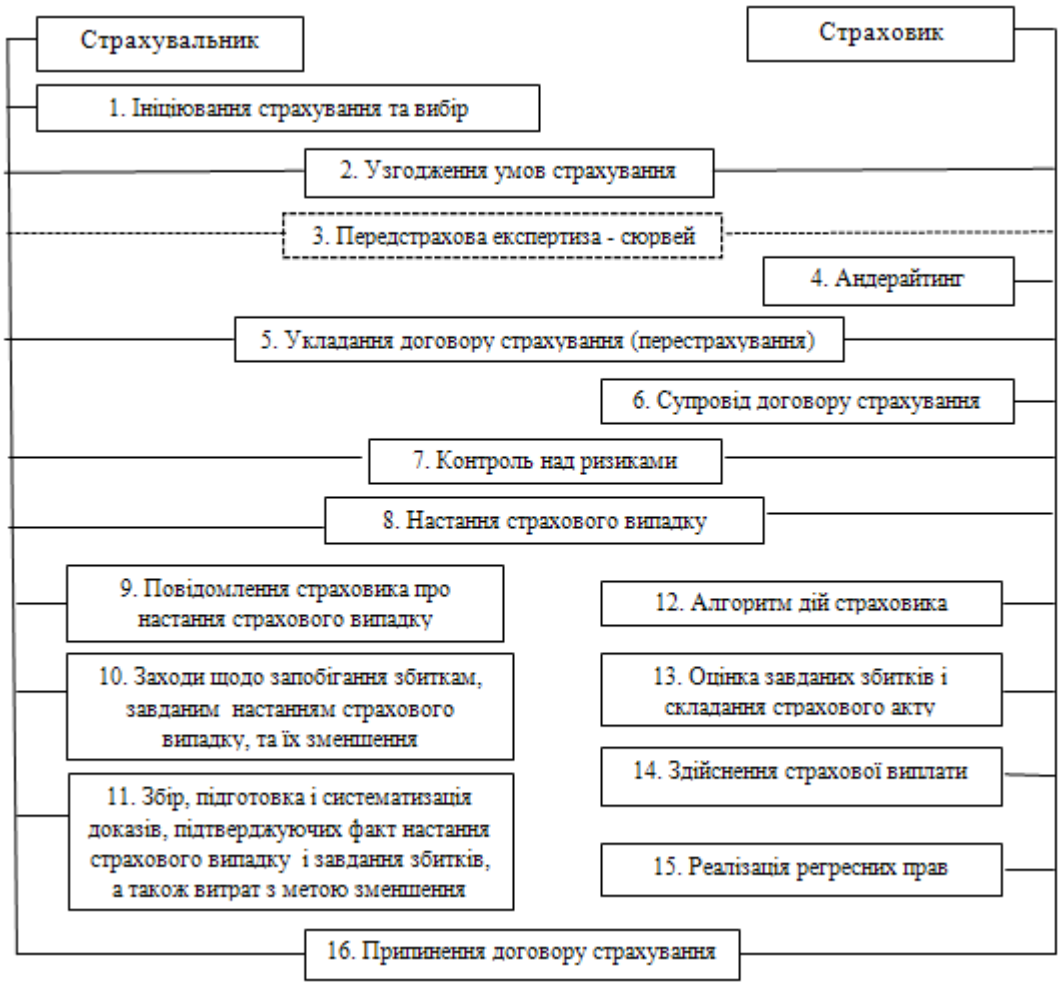

Рисунок 4 - Модель страхування ризиків інформаційної безпеки

Інформація може бути присутня в організації в різних формах. Незалежно від того, яку форму інформація приймає, якими засобами вона поширюється або зберігається, вона завжди повинна бути належним чином захищена й, зокрема, шляхом страхування.

Для цього необхідно провести інвентаризацію та класифікацію інформаційних активів організації. Інвентаризація полягає у складанні переліку цінних активів. Як правило, даний процес виконують власники активів.

Згідно [6] актив (asset) - те, що має цінність для організації. Стандарт ISO 27002 виділяє наступні види активів: інформація: бази даних і файли даних, договори та угоди, системна документація, науково-дослідна інформація, керівництва користувача, навчальний матеріал, процедур експлуатації або допоміжні процедури, плани забезпечення безперервності бізнесу, заходи щодо нейтралізації несправності, контрольні журнали і архівована інформація; програмні активи: прикладні програми, системні програми, інструментальні засоби розробки і утиліти; фізичні активи: комп'ютерне обладнання, апаратура зв'язку, змінні носії інформації та інше обладнання; послуги: обробка даних та послуги зв'язку, загальні комунальні послуги, наприклад, обігрів, освітлення, енергія і кондиціювання повітря; люди, їх кваліфікація, здібності та досвід; нематеріальні активи, такі як репутація та імідж організації.

Повинні бути чітко визначені всі активи, складений їх опис і підтримуватися в робочому стані. Опис активів допомагає забезпечити наявність результативного захисту

активів та також може бути необхідний для інших ділових цілей, таких як техніка безпеки та охорона праці, *страхування* або фінансові причини (менеджмент активів). Процес складання опису активів є важливою попередньою умовою управління ризиками та ініціювання страхування [6].

Класифікація - це процес співвіднесення тих чи інших активів за класами відповідно до певних ознак, які дозволяють визначити подібність або відмінність активів. Мета класифікації: забезпечити належний рівень захисту інформації.

У відповідності зі схемою класифікації, прийнятою організацією, повинен бути розроблений і реалізований відповідний набір процедур для маркування інформації та поводження з інформацією. Далі слід здійснити класифікацію користувачів, які так чи інакше задіяні в процесі збору, введення, обробки, передачі, зберігання, розповсюдження, відображення, використання, модифікації і знищення інформації. Наступним кроком є створення профілів доступу користувачів (профілювання користувачів). Класифікація активів і профілювання користувачів - це два істотних процеси для подальшого успішного аналізу ризиків, управління інформаційними ризиками і страхування.

Діяльність будь-якої страхової компанії найкращим чином характеризують такі головні показники, як платоспроможність, рентабельність, ліквідність активів, розмір статутного капіталу, величина і динаміка зміни страхових резервів, власний капітал компанії, обсяг страхових внесків, види страхування (перестрахування), власники компанії, термін роботи на ринку, кваліфікація виконавців, підтверджена міжнародними сертифікатами, імідж (репутація) компанії, якість і культура обслуговування. Оприлюднення надійної та своєчасної інформації дозволяє страхувальникам та іншим учасникам ринку зрозуміти фінансовий стан страхової компанії та ризики, на які вони можуть наразитися [9].

Узгодження умов страхування. Вибравши страхову компанію (СК), страхувальнику необхідно погодити з нею умови страхування. На цьому етапі визначається необхідний обсяг страхового захисту: розробляються, погоджуються і формуються пропозиції по страхуванню, визначається вартість страхування, ліміт відповідальності СК, готується і узгоджується проект договору страхування (страхового полісу) та інші умови страхування. При узгодженні умов страхування визначають об'єкти страхування. Об'єктом страхування в даному випадку є майнові інтереси, пов'язані з володінням, користуванням і розпорядженням документованою інформацією та іншими активами страхувальника.

На практиці об'єктами страхування можуть бути активи, описані вище. Договір страхування (страховий поліс) може передбачати відшкодування прямих збитків у разі настання різних страхових випадків, таких як: вихід з ладу (збої в роботі) інформаційних систем, зумовлені недостатньою якістю використовуваних програмних і апаратних засобів, помилками при їх проектуванні, розробці, виробництві, установленні, налаштуванні, обслуговуванні або експлуатації; навмисні протиправні дії співробітників підприємства, вчинені з метою завдати шкоди підприємству або отримати певну вигоду; напади (атаки) на інформаційні системи підприємства, які здійснені третіми особами з метою завдати шкоди інформаційним ресурсам організації та її інформаційним системам (пошкодити або знищити інформацію, що зберігається в електронному вигляді, отримати конфіденційні відомості, вивести з ладу програмні та апаратні засоби з метою припинити їх роботу або припинити функціонування певних сервісів тощо); вплив шкідливих програм і макросів, що спричиняють порушення роботи інформаційних систем, втрату інформації або розголошення конфіденційної інформації; розкрадання фінансових активів (грошових коштів), вчинене шляхом здійснення різних неправомірних дій: крадіжки паролів і ключів, присвоєння особистості, внесення змін в програмне забезпечення і т.п. [10].

Більш детально про об’єкти, умови та правила страхування можна дізнатися на сайтах компаній «Ингосстрах» [11], «ALSKOM» [12].

Передстрахова експертиза ризиків (Сюрвей). Неодмінною умовою страхування РІБ є проведення спеціальної експертизи з аналізу ризиків страхового об'єкта. Дана експертиза називається - "Сюрвей" (від англійського "survey" - "огляд"), яку проводить сюрвейєр (від

англ. Surveyor). Він займається інспектуванням, дослідженням, перевіркою об'єктів страхування, виявляє недоліки в процесах або системах безпеки. Найчастіше сюрвейєм в області інформаційного страхування займаються консалтингові та інтеграційні компанії. Як правило, незалежний сюрвейєр залучається в таких ситуаціях: коли існують великі ризики; в маркетингових цілях, коли компанія повинна продемонструвати клієнту високу якість своєї роботи; коли страхова компанія вперше стикається з нехарактерним для себе ризиком, але з міркувань розвитку бізнесу хоче цей ризик прийняти.

Результатом експертизи ризиків є сюрвей-репорт (з англ. «Survey report») - письмова доповідь (репорт), складений сюрвейєром на прохання страхувальника або страховика. Містить матеріали з оцінки ризику (тобто фактичного огляду, експертизи об'єкта, що приймається на страхування), що передує укладенню договору страхування, а також рекомендації, спрямовані на вдосконалення системи інформаційної безпеки потенційного страхувальника. На підставі висновку сюрвейєра страховик порекомендує ряд превентивних заходів (організаційних або інженерно-технічних), спрямованих на вдосконалення системи інформаційної безпеки потенційного страхувальника. Страховик, на підставі висновку сюрвейєра, приймає рішення про прийняття або відмову у страхуванні того чи іншого ризику. Висновки сюрвейєра важливі для укладання договору перестрахування і передують укладенню договору страхування.

Андерайтинг. Ключовим бізнес-процесом страхової компанії є андерайтинг. Важливість андерайтингу для страхової компанії пов'язана з тим, що це та діяльність, яка дозволяє компанії взяти ризик на страхування не збитковою ціною. Незважаючи на значимість даного процесу, однозначного поняття "андерайтинг" не існує. Так, наприклад, даний термін однозначно не закріплений ні в одному галузевому стандарті [13].

Термін андерайтинг був взятий в економічну термінологію із англійської мови. В перекладі з англ. Underwrinting має декілька значень – підписка, гарантування.

У широкому сенсі процес страхового андерайтингу представлено автором на рис. 5.

Всі ці операції тісно пов'язані між собою і взаємозалежні. Перелічені вище операції здійснює андерайтер - кваліфікований спеціаліст або спеціальна організація, що діють від імені страховика. У повному циклі андерайтингу беруть участь не тільки андерайтери, але й інші служби СК.

Суть андерайтингу полягає у діяльності страховика, спрямованої на оцінку ризиків, що приймаються на страхування, визначенні адекватного страхового тарифу та умов страхування, формування прибуткового страхового портфеля, надання рекомендацій страхувальникові по зниженню ризиків. З точки зору страхувальника андерайтинг представляється системою знань з управління ризиками від якості та професіоналізму володіння якої, залежить його вибір того чи іншого страховика [14]. Найбільш важливим і складним етапом процесу андерайтингу є аналіз ризиків, оскільки від правильної оцінки ризику залежить розмір страхової ставки.

Укладання договору страхування (перестрахування). Поняття договору страхування, перестрахування; предмет, форма договору страхування; істотні умови договору страхування; сторони в договорі страхування, обов’язки страховика і страхувальника наведені в Цивільному Кодексі (ЦК) України [15] та Законі України «Про страхування» [16].

Супровід договорів страхування. Ще один важливий бізнес-процес у роботі СК - супровід договорів страхування. Бізнес-процес «супровід договорів страхування» складається з наступних етапів: отримання заяви та анкети, оформлення договору страхування, введення в базу, узгодження договору з андерайтером і юристом, вручення договору, пролонгація договору страхування та укладання додаткових угод. Необхідно відзначити, що узгодження договору страхування з андерайтером і юристом відбувається у випадку, якщо укладається нетиповий договір. На підставі описаного бізнес-процесу визначаються функції підрозділу супроводу договорів страхування [17].

Контроль над ризиками. Після укладення договору страхування андерайтер бере участь у його супроводі, здійснюючи моніторинг стану об'єкта (предмета) страхування та контроль

виконання плану заходів щодо зниження ризиків, і, у разі зміни параметрів прийнятих на страхування ризиків, перераховує страховий тариф і готує зміни в договір. При порушеннях страхувальником своїх зобов'язань за договором страхування андерайтер складає висновок про розірвання договору або про зменшення страхової виплати при настанні страхового випадку.

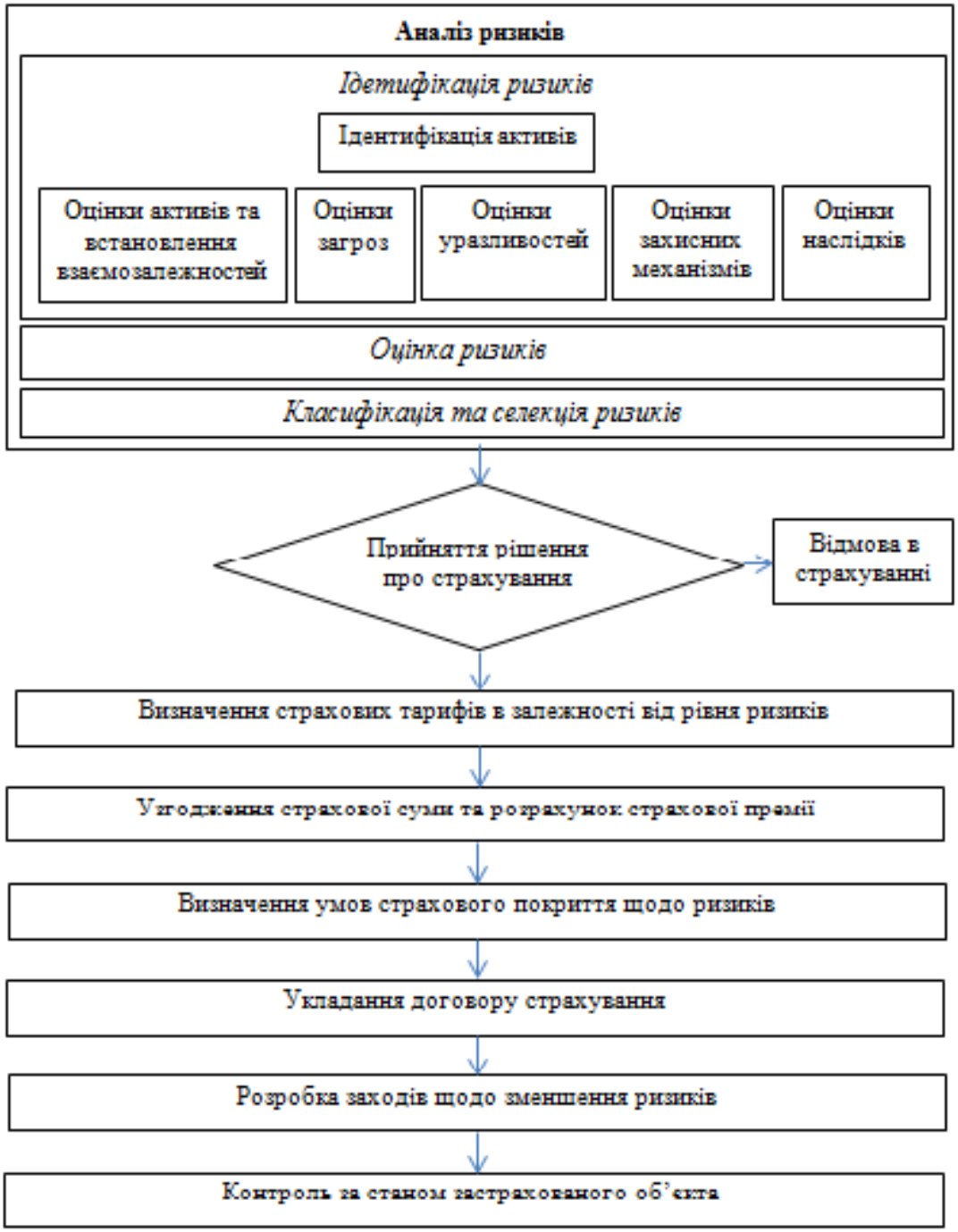

Рисунок 5 - Процес страхового андерайтингу

Настання страхового випадку. Згідно ст.8 Закону України «Про страхування» - Страховий випадок - подія, передбачена договором страхування або законодавчо, яка відбулася і з настанням якої виникає обов'язок страховика здійснити виплату страхової суми (страхового відшкодування) страхувальнику, застрахованій або іншій третій особі. Правовий аналіз викладених понять страхового випадку дозволяє зробити висновок, що страховий випадок як категорія страхування являє собою складний юридичний склад, тобто

правову конструкцію, що складається з самостійних правових елементів: перший елемент - страхова подія; другий елемент - збиток; третій елемент - причинний зв'язок між двома вказаними вище елементами [18].

Повідомлення страховика про настання страхового випадку. Згідно ст. 989 ЦК України страхувальник зобов'язаний повідомити страховика про настання страхового випадку у строк, встановлений договором. Несвоєчасне повідомлення страхувальником без поважних на те причин про настання страхового випадку або створення страховикові перешкод у визначенні обставин, характеру та розміру збитків, дає право страховику відмовитися від здійснення страхової виплати.

Крім повідомлення в усній формі про настання страхового випадку страхувальник зобов'язаний направити страховикові офіційну заяву про настання страхового випадку у письмовій формі. Необхідність подачі заяви у письмовій формі обумовлена тим, що особа, яка повідомляє про настання страхового випадку, має докладно описати в заяві обставини його настання, а саме час і місце виникнення події, хто був присутній у момент настання події, передбачуваний розмір пошкодження майна або іншого збитку, який наступив в результаті впливу події і т.д. Зауважимо, що в разі вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, слід звертатися до Computer Emergency Response Team of Ukraine (CERT-UA). Проблема реагування на інциденти безпеки також є предметом окремого дослідження.

Згодом відомості, викладені в заяві, можуть послужити неспростовними доказами фактичних обставин страхової події, які були отримані за так званими гарячими слідами, що знадобляться для встановлення факту настання страхового випадку, передбаченого договором страхування.

Одним з істотних обов'язків страхувальника при настанні страхової події є збереження місця страхової події в незмінному вигляді до прибуття представників страховика. Обстановку страхової події змінювати не можна, за винятком тих обставин, які пов'язані з ліквідацією небезпеки, що продовжує впливати на предмет або об'єкт страхування, і з проведенням необхідних дій, спрямованих на зменшення збитків від страхового випадку.

Заходи щодо запобігання збиткам, завданим настанням страхового випадку, та їх зменшення. У період дії договору страхування законодавцем на страхувальника покладається ще один обов'язок - це прийняття заходів, необхідних для зменшення збитків від страхового випадку. Даний обов'язок окрім того, що може бути передбачений договором страхування, додатково передбачається законодавцем, а саме ст. 989 ЦК України. Витрати з метою зменшення збитків, що підлягають відшкодуванню страховиком, якщо такі витрати були необхідні або були зроблені для виконання вказівок страховика, повинні бути відшкодовані страховиком, навіть якщо відповідні заходи виявилися безуспішними. Такі витрати відшкодовуються пропорційно відношенню страхової суми до страхової вартості незалежно від того, що разом з відшкодуванням інших збитків вони можуть перевищити страхову суму. Страховик звільняється від відшкодування збитків, що виникли внаслідок того, що страхувальник умисно не прийняв розумні і доступні йому заходи, щоб зменшити можливі збитки.

Збір, підготовка і систематизація доказів, підтверджуючих факт настання страхового випадку і завдання збитків, а також витрат з метою зменшення збитків. Наступним етапом в діях страхувальника є заходи пов'язані зі збором, підготовкою та систематизацією доказів, більшою мірою документальних, що підтверджують факт настання страхового випадку та заподіяння збитку, а також витрат з метою зменшення збитку. Такими документами можуть слугувати: - постанови, довідки, протоколи огляду та інші документи, видані державними органами, установами; - документи, що підтверджують дійсну вартість майна (бухгалтерські документи), висновок про оцінку майна, виданий спеціалізованою оціночною організацією і т.д.; - платіжно-грошові документи, що підтверджують витрати страхувальника спрямовані на зменшення збитку - договори, рахунки, накладні, чеки і т.д. ; -

необхідний пакет документів з передачі прав вимоги (суброгації) до особи, з вини якої виникли збитки; - експертні висновки, якщо за ініціативою страхувальника була призначена і проведена експертиза для встановлення факту настання страхового випадку; - остаточний розрахунок збитку (збитків) або вартості відновлювального ремонту пошкоджених застрахованих інформаційних активів, складений експертами або оцінювачами тощо.

Для проведення всіх зазначених дій і заходів у договорі страхування повинні бути зумовлені, причому абсолютно чітко і виразно, терміни, протягом яких страхувальник або його представник зобов'язаний здійснювати поетапно кожну із перелічених дій.

Алгоритм дій страховика. Страховик при настанні страхового випадку зобов'язаний здійснити наступні дії, які повинні бути обумовлені в договорі страхування в якості необхідних і суттєвих умов страхування, причому у вигляді самостійної глави або розділу договору.

Страховик після отримання повідомлення про настання страхової події зобов'язаний виїхати на місце страхової події в термін, передбачений договором страхування, провести огляд місця страхової події та скласти акт огляду, який підписують всі особи, присутні на огляді. В акті повинні відображатися відомості про те, яка подія відбулася, в який час доби, хто був при цьому присутній, які служби і в який час були викликані, які заходи були вжиті для локалізації небезпеки або зменшення збитку, попередній розмір збитку (збитків) за сумою, повний і докладний опис пошкодженого майна, його залишки тощо. Крім того, в акті докладно виявлені упущення при експлуатації об’єкту страхування та інші обставини, пов'язані з виникненням страхового випадку. Наступним етапом в діях страховика є збирання всіх необхідних документів, в тому числі представлених офіційними державними органами, що описують небезпечну подію і причини її настання. Після того, як страховик встановив факт настання передбаченого в договорі страхування страхової події, він приступає до наступного кроку - встановлення розміру заподіяної страховою подією збитку або шкоди.

У необхідних випадках страховик має право залучати незалежних сюрвейєрів для проведення всієї процедури страхового розслідування. В даному випадку сюрвейєр виступає в ролі аварійного комісара.

Оцінка завданих збитків і складання страхового акту (аварійного сертифікату). Наступним етапом в діях страховика при настанні страхового випадку є складання за результатами проведеного розслідування страхового акту. Якщо за результатами страхового розслідування страховик визнав заявлену подію в якості настання страхового випадку, а також встановив розмір заподіяної даною подією шкоди, він згідно ст.990 ЦК України складає страховий акт (аварійний сертифікат). У тих випадках, коли страховик у результаті страхового розслідування приходить до висновку, що страховий випадок не настав, він складає страховий акт про відмову у виплаті страхового відшкодування. Відповідно ст. 991 рішення страховика про відмову здійснити страхову виплату повідомляється страхувальникові у письмовій формі з обґрунтуванням причин відмови.

Здійснення страхової виплати. Завершальним етапом в діях страховика при настанні страхового випадку є страхова виплата, яка повинна бути здійснена відповідно договору страхування, у тому числі в терміни, встановлені договором. Відповідно ст. 988 ЦК України страховик зобов’язаний протягом двох робочих днів , як тільки стане відомо про настання страхового випадку, вжити заходів щодо оформлення всіх необхідних документів для своєчасного здійснення страхової виплати страхувальникові та здійснити страхову виплату у строк, встановлений договором. Умови та порядок здійснення страхової виплати передбачені ст. 990 ЦК України.

Реалізація регресних прав. Реалізація регресних прав страхової компанії передбачена ст. 993, 1191 Цивільного кодексу України, а також ст. 27 Закону України «Про страхування». Регрес (страхова суброгація) - це право зворотної вимоги страховика до особи, відповідальної за заподіяння шкоди, страховик отримує право на регрес тільки після виплати страхового відшкодування і тільки у розмірі своєї виплати.

Припинення договору страхування. Правовідносини сторін по договору страхування припиняються по двом підставам: згідно загальних правил припинення зобов'язання, передбачених главою 50 ЦК України; відповідно правилам, встановлених тільки для страхових зобов'язань, які передбачені ст. 997 ЦК України.

Загальною підставою для припинення договору страхування є його належне і повне виконання. Дане правило випливає не тільки з самої суті цивільно-правових зобов'язань, метою яких є досягнення остаточного результату, пов'язаного з виконанням, а й підкріплюється законом. Так, в ст. 599 ЦК України прямо визначено, що зобов'язання припиняється виконанням, належним чином.

ВИСНОВКИ

Таким чином, побудована модель страхування ризиків інформаційної безпеки може бути відправною точкою проектування, розробки, впровадження та супроводу системи страхування ризиків ІБ.

Створення та впровадження моделі, механізму, системи страхування ризиків інформаційної безпеки може захистити організації, що використовують високі інформаційні технології, від втрат і збитків, що виникають у результаті збоїв технічних і програмних компонентів інформаційних систем, розкрадання і модифікації інформації, несанкціонованого доступу до інформаційних ресурсів та ін., а також грати попереджувальну і мотиваційну роль.

На даний момент в Україні гостро відчувається потреба в науковому узагальнені чинних норм національного і міжнародного права, здобутків правової думки у цій галузі з метою створення та впровадження у діючу практику загальнодержавної системи страхування ризиків інформаційної безпеки, чіткого визначення методів та механізмів страхування ризиків інформаційної безпеки. Для цього слід провести комплекс науково-дослідних робіт з аналізу проблем страхування інформаційних ризиків, класифікувати їх і виділити основні; дослідити ринок послуг в галузі страхування; розробити теоретичну, нормативну та методичну бази системи страхування ризиків інформаційної безпеки, організувати та забезпечити підготовку фахівців – андерайтерів в ВНЗ, запозичивши позитивний міжнародний досвід.

Проблема створення системи страхування ризиків інформаційної безпеки є актуальною темою сьогодення і потребує концептуального вирішення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Електронний ресурс: http://www.unian.net/ukr/news/news-375431.html
2. Мних М.В. Розвиток теорії страхування у сучасних умовах *[Електронний ресурс]* : *[Журнал «Економіка та держава»]* - Режим доступу до журн.: http://www.economy.in.ua/index.php?iid=10&operation=9.
3. Information technology — Security techniques — Information security management systems — Overview and vocabulary : ISO/IEC 27000:2009(E). – 26 с.
4. Information technology. Security techniques. Information security risk management : BS ISO/IEC 27005:2008 . – 64 с.
5. Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств – участников Содружества Независимых Государств в сфере информатизации *[Електронний ресурс]* : — Режим доступу: *http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=997_842*
6. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [проект]. - К.: Національний банк України 2010. – 163 с. *: табл.* – (Галузевий стандарт України).
7. Чернова Г.В. Управление рисками: Учебное пособие./ Чернова Г.В., Кудрявцев А.А — М.: ТК Велби, Проспект, 2003. - 160 с. - ISBN 5-98032-067-9
8. Советский энциклопедический словарь [гл. ред. А.М. Прохоров]. – 3-є вид. – М.: «Советская энциклопедия», 1985.- 1600с., іл..
9. Електронний ресурс: http://www.ufin.com.ua/analit_mat/strah_rynok/049.htm

10. Анисимов А.А. Предоставление услуг в сфере информационной безопасности *[Електронний ресурс]* : *(курс лекцій)* Режим доступу.: http://www.intuit.ru/department/itmngt/manofis/13/3.html.
11. Електронний ресурс: http://www.ingos.ru/ru/corporate/it/
12. Електронний ресурс: http://alscom.uz/new/?q=ru/node/141
13. Андеррайтинг в страховании *[Електронний ресурс]* : — Режим доступу: http://www.insur-info.ru/management/press/39502.
14. В. Веретнов Андеррайтинг *[Електронний ресурс] :* — Режим доступу: http://riskm.blox.ua/2009/10/Anderrajting.html. – Назва з екрану. – Андеррайтинг.
15. Цивільний кодекс України *[Електронний ресурс] :* — Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=435-15
16. Закон України «Про страхування» *[Електронний ресурс]:*—Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=85%2F96-%E2%F0
17. Николенко Н. П. Сопровождение договоров страхования. *[Електронний ресурс]* : . - Режим доступу.: Електронний ресурс: http://www.insur-info.ru/comments/391/
18. Абрамов В.Ю. Страхование: теория и практика *[Електронний ресурс] :* . - Режим доступу.: http://www.vuzl.org/books/insurance/46-strahovanie-teoria-i-praktika