View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repository of Vinnytsia National Technical University

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056

О.Є. АРХИПОВ, С.М. КУЩ, В.О. ШУТОВСЬКИЙ

Національний технічний університет України «Київський політехнічний інститут», Київ

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МІЖНАРОДНІ СТАНДАРТИ ТА УКРАЇНСЬКЕ ЗАКОНОДАВСТВО

Анотація. Розглянуто вимоги, викладені у нормативних документах, та рекомендації міжнародних стандартів до методики оцінювання ризиків інформаційної безпеки. Наведено умови відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC.
Ключові слова: інформаційна безпека, оцінка ризиків, нормативно-правове забезпечення, українське законодавство, міжнародні стандарти.
Аннотация. Рассмотрены требования, изложенные в нормативных документах, и рекомендации международных стандартов относительно методики оценивания рисков информационной безопасности. Представлены условия соответствия методик оценки рисков информационной безопасности отечественным нормативным документам и международным стандартам ISO/IEC.
Ключові слова: информационная безопасность, оценка рисков, нормативно-правовое обеспечение, украинское законодательство, международные стандарты.
Annotation. The information security risk assessment technique requirements of the Ukrainian legislation acts and international standards are reviewed. The conditions of information security risk assessment technique correspondence to the requirements of the Ukrainian legislation acts and international standards ISO/IEC are given.
Keywords: information security, risks assessment, regulatory support, Ukrainian legislation, international standards.

Вступ

Вдосконалення технологій передачі і обробки інформації, щорічне зростання числа кіберзагроз, необхідність забезпечення інформаційної безпеки незалежно від місця її зберігання є причиною особливої уваги до проблеми оцінки ризиків і вдосконалення систем управління ризиками. За результатами дослідження компанії «Ернст енд Янг» в області інформаційної безпеки (ІБ) за 2009 рік [1], наслідки глобальної економічної кризи змусили керівників великих міжнародних компаній переглянути своє відношення до ІБ, зокрема і до процесу управління ризиками ІБ. Так, наприклад, 50% з опитаних керівників планують в майбутньому збільшити фінансування, а 39% збережуть фінансування на попередньому рівні в цьому напрямі.

У відповідності до стандарту ISO 27001 в моделі PDCA (Plan-Do-Check-Act) (так званий цикл Шухарта-Демінга [2]), що описує циклічний процес забезпечення ІБ, етап оцінки ризиків і прийняття рішень займає основне місце. Державний стандарт України [3], певною мірою відповідає основним міжнародним вимогам у галузі ІБ і містить наступний перелік етапів побудови комплексної системи захисту інформації (КСЗІ):

1. Визначення й аналіз загроз.
2. Розроблення системи захисту інформації.
3. Реалізація плану захисту інформації.
4. Контроль функціонування та керування системою захисту інформації.

Відповідно до Державного стандарту України аналіз і оцінка ризиків (п.1- "визначення й аналіз загроз") є першим етапом побудови комплексної системи захисту інформації. Циклічне проведення оцінки ризиків системи дає можливість проводити контроль її функціонування та оптимізувати КСЗІ за встановленими критеріями. Такий механізм оцінки ризиків дозволяє приймати найбільш ефективні рішення, обираючи оптимальні механізми захисту від загроз і розставляючи пріоритети при створенні системи захисту [4]. Адекватна оцінка ризиків для інформаційно-комунікаційної системи (ІКС) є основною умовою побудови економічно обґрунтованої системи захисту інформації (СЗІ) [5].

Актуальність

Актуальність задачі дослідження метрик безпеки (одною з яких є ризик) відмічена у ряді зарубіжних публікацій [6-8]. Дослідження по цій темі ведуться вже декілька десятиліть, але слід відмітити, що одержано відносно мало результатів, які б виявилися корисними для практичного використання, в той час як метрики безпеки є важливим фактором при прийнятті рішень в області інформаційної безпеки [6]. Так, науково-дослідна рада з інформаційної безпеки уряду США включила проблему метрик безпеки на корпоративному рівні до свого останнього списку проблем [7]. Інститутом захисту інформаційної інфраструктури США метрики безпеки визначені як один з чотирьох науково-дослідних пріоритетів на наступні п'ять-десять років [8]. У аналітичному огляді Національного інституту стандартів і технологій (США) "Напрямки досліджень метрик безпеки" [6] наведено перелік умов, які необхідно враховувати при розробці метрик інформаційної безпеки. Цей перелік визначає широкий діапазон проблем від вико-

ристання економічних індикаторів різного типу до особливостей вимірювання показників ІБ систем різної потужності.

На сьогоднішній день запропоновано багато методик оцінки ризиків, які відображені у стандартах [9,10], викладені у звітах науково-дослідних робіт [11,12] та комплексних робіт, виконаних на замовлення комерційних організацій [13,14]. У цих методиках розглянуто питання аналізу і управління інформаційними ризиками, але вони мають ряд недоліків: є недостатньо ефективними, складними, відірваними від практики або навпаки — пристосованими до конкретної організації і конкретної ІКС. Як зазначено у роботах [15,16], на даний час відсутня універсальна методика, яка є однаково придатною для організацій і компаній різних типів.

Мета

Аналіз вимог, викладених у нормативних документах, та рекомендацій міжнародних стандартів до методики оцінювання ризиків інформаційної безпеки, виділення умов відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC.

Постановка задач

4. Провести аналіз нормативних документів українського законодавства у області оцінки ризиків ІБ.
5. Провести аналіз міжнародних стандартів в області оцінки ризиків ІБ.
6. Сформулювати умови відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC, провести аналіз напрямів розробки методики оцінки ризиків ІБ.

Аналіз нормативних документів українського законодавства у області оцінки ризиків ІБ

Діяльність юридичних і фізичних осіб у сфері інформаційної безпеки в Україні регламентується системою документів: Законами України, Постановами Кабінету Міністрів, Державними стандартами, нормативними документами технічного захисту інформації (НД ТЗІ).

Розгляд питання оцінки ризиків необхідно починати з визначень базових понять. Однак, у перших вітчизняних документах з ТЗІ [3,17,18] терміни «ризик» та «аналіз ризиків» відсутні взагалі, а управління системою захисту інформації (ЗІ) розглядається виключно як адаптація заходів ТЗІ до поточних завдань ЗІ (п.4.4.1 ДСТУ 3396.0), питання економічної доцільності ЗІ зустрічаються в п.3.2 ДСТУ 3396.1 лише в рамках переліку можливих варіантів постановки задачі ЗІ: мінімальні, допустимі або ж необхідні витрати на ТЗІ, оцінка шкоди від реалізації загроз інформації згадується тільки у якості складової частини моделі загроз п.4.5 ДСТУ 3396.0.

Лише з появою у 1999 р. серії документів з захисту інформації в комп’ютерних системах (КС) від несанкціонованого доступу (НСД) тематика оцінки ризиків в галузі ТЗІ стає легітимною [19,20]. Відповідно до нормативного документу [20] ризик визначається як функція ймовірності реалізації певної загрози, виду і величини завданих збитків. Аналіз ризиків у цьому документі визначається як процес визначення загроз безпеці інформації та їх характеристик, слабких сторін комплексної системи захисту інформації (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації автоматизованої системи. Визначення поняття оцінки ризиків у [20] не наводиться, в той час як воно широко використовується у інших НД ТЗІ та літературі, присвяченій проблемам ІБ. На основі розглянутих визначень можна зробити висновок, що формалізованого визначення ризику і моделі взаємозв’язку процесів задачі управління ризиками не запропоновано, що допускає можливість варіювання трактування цього поняття. В загальному випадку обчислення ризику проводиться на основі ймовірності реалізації загрози (або набору загроз) та відповідних збитків організації. Проте, на сьогоднішній день не існує надійного методу визначення ймовірності реалізації ідентифікованих загроз, а також адекватного методу обчислення повного збитку від їхньої реалізації. Складною є задача доведення повноти множини розглянутих загроз і, відповідно, повноти оцінки ризиків [21].

Серед НД ТЗІ безпосередньо оцінки ризиків стосуються [22-25].

Оцінка ризиків в [22] розглядається як одне з завдань, яке необхідно розв’язати при розробці політики безпеки. Відмічено необхідність проведення оцінки гранично припустимих і реальних ризиків у вигляді ймовірності здійснення загроз впродовж заданого проміжку часу, для чого рекомендується вводити дискретні градації. Ймовірності реалізації загроз визначаються на основі експертних оцінок або евристичних даних. Допускається використання як кількісних, так і якісних шкал. У цьому документі аналіз ризиків розглядається як аналіз ймовірностей реалізації загроз. Окремо вимагається проведення оцінки можливих збитків, пов’язаних з реалізацією загроз, аналогічно аналізу ймовірностей реалізації загроз.

У документі [23] введено порівняльну шкалу для оцінки надійності механізмів захисту інформації в комп'ютерних системах від несанкціонованого доступу. КСЗІ представляється у вигляді сукупності функціональних послуг захисту (ФПЗ), кожна з яких є набором функцій, що дозволяють протистояти певній сукупності загроз. Таким чином, не йдеться про оцінку ризиків для системи як таку, а про доведення

реалізації в системі необхідного набору ФПЗ. Оцінка надійності функціонування ФПЗ у [23] не регламентується і віддається у повноваження Експертної комісії, дії якої регламентуються іншими документами.

Відповідно до нормативного документу [24] перелік основних робіт при формуванні технічного завдання включає експертну оцінку очікуваних втрат у разі здійснення загроз, і вибір необхідних функціональних послуг захисту, а також оцінку вартості і ефективності обраних засобів захисту інформації.

У НД ТЗІ [25] на етапі формування технічного завдання на створення КСЗІ на основі вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків і створення переліку суттєвих загроз передбачається необхідність здійснення аналізу ризиків. На етапі формування політики безпеки передбачається уточнення моделей загроз, потенційного порушника та результатів аналізу можливості керування ризиками.

У 2003-2005 роках в якості державних стандартів України було прийнято переклади стандарту ISO/IEC TR 13335, який містить загально прийняту світову термінологію і підходи до оцінки ризиків. Однак ця термінологія не є гармонізованою з серією НД ТЗІ, а підходи ДСТУ не часто застосовуються на практиці.

На основі аналізу українських нормативних документів в області інформаційної безпеки можна зробити декілька висновків. По-перше, аналіз і оцінка ризиків є невід'ємним етапом проектування системи захисту інформації. По-друге, допускається використання як кількісних, так і якісних шкал, об'єктивних та суб'єктивних підходів до отримання оцінки ймовірностей реалізації загроз. По-третє, відсутній НД ТЗІ, який би регламентував процес оцінки ризиків [26], і на поточний момент відсутня гармонізація між основною масою вітчизняних документів (наприклад, НД ТЗІ) та п'ятьма ДСТУ серії ISO. Таким чином, можна зробити висновок про необхідність досліджень по розробці методики оцінки ризиків інформаційної безпеки

Аналіз міжнародних стандартів в області оцінки ризиків ІБ

Сучасні світові стандарти в області інформаційної безпеки передбачають в якості обов'язкового компонента забезпечення режиму ІБ створення системи управління інформаційною безпекою (СУІБ) або її аналогу. Обов'язковою підсистемою останньої є система управління інформаційними ризиками (СУІР), що може включати як кількісні, так і якісні показники і повинна використовувати прозорі метрики [27]. Міжнародною організацією зі стандартизації (International Organization for Standardization, ISO) розроблено близько сотні стандартів, що стосуються інформаційної безпеки і зокрема оцінки ризиків.

Міжнародний стандарт ISO/IEC 27002:2005 [28] визначає ризик як комбінацію ймовірності події і її наслідків. Аналіз ризиків у [28] визначається як систематичне використання інформації для виявлення джерела і оцінки ступеня ризику, а оцінка ризиків — як цілісний процес аналізу ризиків і оцінки їхньої критичності. Наведені визначення в цілому ідентичні вищенаведеним визначенням вітчизняних НД ТЗІ.

Серія стандартів ISO/IEC 2700x включає рекомендації на основі best practices (найкращих практик світового досвіду) у сфері управління інформаційною безпекою, ризиками та засобами контролю як частини загальної системи управління інформаційною безпекою, побудова і функціонування якої здійснюється на основі оцінки ризиків [4]. Розробка СУІБ узгоджена з розробкою систем забезпечення якості та систем захисту навколишнього середовища. У серії стандартів ISO/IEC 2700x опубліковано 8 стандартів і ще 13 готуються до друку. Головні стандарти серії 2700x ISO/IEC 27001:2005 [2], ISO/IEC 27002:2005 [28] та ISO/IEC 27005:2008 [29] базуються на британському стандарті BS-7799. У стандарті [30] до заходів, необхідних для побудови, технічної підтримки та модернізації системи управління інформаційною безпекою, як важливий пункт, включено оцінку ризиків, яка виконується у два основних послідовних етапи: аналіз ризиків та оцінювання ризиків.

У стандартах [2,28] наведено основні етапи оцінки ризиків для СУІБ, а саме:

- визначення методики оцінки ризиків (зазначається, що можна застосовувати різні методики, але головними вимогами до них, є можливість повторення результату оцінки ризиків і порівняння його з результатами оцінок, отриманими за допомогою інших методик);
- ідентифікація ризиків та їхніх складових (активів організації, загроз, вразливостей системи та їхнього впливу на активи);
- аналіз та оцінка ризиків;
- аналіз та оцінка можливості мінімізації ризиків.

Стандарт [29] присвячено управлінню ризиками інформаційної безпеки. У цьому документі розкрито вище перераховані пункти. Стандарт не регламентує вибору конкретної методології оцінки ризиків, і організація може сама вибирати підхід, який би забезпечував необхідні результати і відповідав описаному у стандарті набору критеріїв. Стандарт не віддає перевагу методикам, які використовують кількісні або якісні оцінки ризиків, і в тому числі передбачає можливість використання декількох методик в процесі оцінки ризиків. У ньому визначається структурована та системна послідовність дій від визначення границь системи до розробки плану обробки ризиків. У додатках до стандарту [29] наведено орієнтовні переліки активів, загроз, вразливостей, можливих підходів до оцінки ризиків, а також можливі обме-

ження застосування контрзаходів. Представляє інтерес використання розглянутого в стандарті підходу по формуванню матриць ризиків. Переліки активів, загроз, вразливостей, наведені у стандарті, можуть бути корисними при розробці методики оцінки ризиків ІБ.

У серії стандартів 2700х описано алгоритм управління ризиками, а також довідковий матеріал, необхідний для проведення розрахунків на різних етапах процесу управління ризиками. Згідно вимог стандарту існує можливість вибору однієї з методик, яка відповідає вимогам документованості, раціональності, всебічності та стабільності.

У стандарті ISO/IEC 13335 “Information technology. Security techniques.” визначено набір настанов по управлінню інформаційною безпекою без побудови СУІБ. У стандарті приведені загальні поняття і описані моделі управління безпекою інформаційно-телекомунікаційних систем. Цей стандарт не пропонує конкретних підходів до управління інформаційною безпекою. Частина перша стандарту ISO/IEC 13335-1:2004 [31] відносить управління ризиками до одного з фундаментальних високорівневих принципів інформаційної безпеки. Ризик визначається через ймовірність події і її наслідки. У стандарті запропоновано чотири можливих стратегії аналізу ризиків (базовий підхід, неформальний підхід, детальний аналіз ризику, комбінований підхід). Докладно описано комбінований підхід, який полягає у застосуванні базового підходу для некритичних підсистем і детального аналізу ризиків для критичних підсистем. Комбінований підхід до оцінки ризиків є оптимальним серед запропонованих у стандарті. У додатках до стандарту наведено довідкові матеріали, в тому числі, приведені табличні методики оцінки ризиків, які можуть бути корисними при розробці та тестуванні власної методики оцінки ризиків. Стандарт ISO/IEC 13335 містить огляд загально прийнятих заходів захисту для забезпечення базового рівня захищеності системи, опис різних шляхів досягнення базової захищеності організації, переваги і недоліки різних підходів до побудови системи захисту інформації. Деякі частини стандарту ISO/IEC 13335 на даний момент втратили чинність і частково були замінені на стандарти ISO/IEC 27005:2008. Тим не менш, переклади стандарту ISO/IEC 13335 прийняті у Росії [9,32,33] та Україні в якості національних стандартів.

Стандарт ISO/IEC 18028:2005 “Information technology - Security techniques - IT network security” розширює набір настанов по управлінню інформаційною безпекою, наведених у стандартах ISO/IEC 27002:2005 та ISO/IEC 13335, деталізуючи особливості функціонування і механізми, необхідні для реалізації захисних заходів і елементів управління у більш широкому спектрі мережевого оточення. Цей стандарт є своєрідною з’єднувальною ланкою між загальними положеннями системи управління безпекою інформаційних технологій та способами їхньої технічної реалізації [34]. Аналіз ризиків та вибір на основі положень цього стандарту методики оцінки ризиків ІБ є найбільш ефективним для при оцінці ризиків у окремих конкретних випадках.

У «Загальних критеріях оцінки безпеки інформаційних технологій» (Стандарті ISO/IEC 15408:2002) визначається набір критеріїв безпеки, за якими проводиться сертифікація програмних продуктів, прийнятих у більшості країн світу. Треба відзначити, що процес оцінки є дорогим і довгостроковим, тому він не знайшов широкого застосування за межами ринку урядових і оборонних програмних продуктів. Для розробки методики оцінки ризиків ІБ цей стандарт практично не використовується [34].

На основі аналізу міжнародних стандартів ISO серії 2700х можна зробити висновок, що методика оцінки ризиків повинна відповідати загальноприйнятим вимогам. Основними з них є обґрунтованість методики, повторюваність результатів та їхнє представлення в такій формі, в якій їх можна порівнювати з результатами, отриманими з використанням інших методик. Загальні принципи побудови методики оцінки ризиків стандарту ISO/IEC 13335 (та його російських аналогів) можна покласти в основу розроблюваної методики оцінки ризиків, а стандарт ISO/IEC 18028:2005 зручно використовувати при оцінці ризиків обчислювальної мережі.

Серед зарубіжних стандартів також слід виділити стандарти оцінки ризиків від провідних організацій в області інформаційної безпеки: стандарт BS 7799 від британського інституту BSI, стандарт BSI-100-4 [35] німецької організації BSI, стандарт NIST SP 800-30 [10].

Стандарт від британського інституту BSI BS 7799 лежить в основі серії стандартів ISO/IEC 2700х, які його на цей момент і замінила. Діючою залишається третя частина стандарту BS 7799-3, хоча більша частина його положень увійшла до міжнародного стандарту ISO/IEC 27005:2008 [34].

Відповідно до стандарту німецької організації BSI BSI-100-4 [35] оцінка ризиків проводиться тільки для додаткових ризиків для систем, до яких висуваються підвищені вимоги до забезпечення інформаційної безпеки [34]. Окрім стандарту інститутом BSI розроблено детальний каталог активів, загроз і контрзаходів IT-Grundschutz [36], який представлено у гіпер-текстовому форматі, при чому обсяг каталогу становить понад 4000 сторінок. Цей каталог є найбільш повним з загальнодоступних і його матеріал слід використовувати при розробці методик аналізу ризиків, управління ризиками та аудиті інформаційної безпеки.

Національний інститут стандартів і технологій США (NIST) розробив і опублікував велику кількість стандартів у різних областях для державних, військових та комерційних організацій. Інформаційній безпеці присвячено серію стандартів 800-. В рамках статті найбільший інтерес представляє стандарт

NIST SP 800-30 [10], який регламентує управління ризиками. Оцінка ризиків у цьому документі є першим пріоритетом серед процесів управління ризиками. Ризик визначається як функція ймовірності реалізації заданого джерела загрози через конкретну потенційну вразливість і результуючого впливу цієї шкідливої події на діяльність організації. У стандарті докладно описано методику управління ризиками на основі якісних шкал оцінки ймовірностей загроз та величини збитків (хоча не виключається можливість використання кількісних шкал), а також табличний метод розрахунку ризиків. Наведено приклади розрахунків для ряду випадків. Ефективність контрзаходів запропоновано по результатам проведення аналізу затрати-вигоди. Методика управління ризиками узгоджена з процесом побудови СУІБ, описаним у стандартах серії 2700х.

Серед перерахованих стандартів перспективними для використання при оцінці і управління ризиками є каталог активів, загроз, вразливостей і контрзаходів IT-Grundschutz [36] та методики стандарту SP 800-30 [10].

Не зважаючи, на існування великої кількості стандартів, що регламентують оцінку ризиків, єдиної формалізованої і загальноприйнятої методики або апарату оцінки ризиків не запропоновано. Методика оцінки ризиків створюється для конкретної інформаційної системи. Основними вимогами до методики оцінки ризиків є її обґрунтованість та повторюваність результатів методики, а також представлення результатів у такій формі, в якій їх можна буде порівнювати з результатами, отриманими з використанням інших методик. Цими вимогами слід керуватися при розробці апарату оцінки ризиків інформаційної безпеки.

Аналіз напрямів розробки методики оцінки ризиків ІБ

У роботі, присвяченій визначенню напрямів досліджень метрик безпеки, наведено перелік вимог, які необхідно враховувати при розробці методики оцінки ризиків [6]:

- визначення надійних оціночних функцій безпеки системи;
- зменшення впливу людського фактору та притаманній йому суб'єктивності у вимірах;
- використання системних та ефективних засобів проведення змістовних вимірювань;
- забезпечення прозорості процесів впроваджуваних механізмів безпеки.

В цьому дослідженні також визначені наступні задачі, які необхідно вирішити при розробці методик оцінки ризиків ІБ:

1. Формалізація моделей вимірювань та метрик безпеки.
2. Збір та аналіз статистичної інформації по загрозах та збиткам від них.
3. Використання інтелектуальних технологій.
4. Використання методик, в яких передбачені прямі вимірювання, та інші.

Серед перерахованих задач виділимо використання інтелектуальних технологій для оцінки ризиків ІБ [37-39]. Основною перевагою застосування таких технологій для вимірювання ризику є зменшення суб'єктивного фактору у процесі оцінки ризиків інформаційної безпеки. Дослідження в області інтелектуальних систем [40] особливо бурхливо розвивалися за останні роки. Головною перевагою інтелектуальних систем перед традиційними системами є відсутність програмування у загально прийнятому вигляді. Замість нього проводиться «навчання системи» і забезпечується можливість її пристосування до умов середовища, що змінюються. Основними областями застосування інтелектуальних систем є: інтерпретація даних, діагностика, моніторинг, проектування, прогнозування, планування, навчання, керування, підтримка прийняття рішень, оптимізація. З середини двадцятого століття було запропоновано, реалізовано і успішно застосовано для розв'язання різних задач наступні основні види інтелектуальних систем:

1) експертні системи;
2) штучні нейронні мережі;
3) нечіткі системи;
4) генетичні алгоритми та еволюційне програмування.

Дослідження по застосуванню інтелектуальних технологій в області оцінки ризиків і розробка апарату оцінки ризиків на основі одного або декількох типів інтелектуальних систем були поведені у роботах [37-39].

Висновки:

4. Задача оцінки ризиків інформаційної безпеки на даний момент не має універсального розв'язку і надзвичайно актуальною, як відзначено у зарубіжних і вітчизняних дослідженнях [6-8,27].
5. В Україні оцінку ризиків регламентує ряд нормативних документів технічного захисту інформації [22-25]. На основі аналізу українських нормативних документів в області інформаційної безпеки можна зробити декілька висновків. По-перше, аналіз і оцінка ризиків є невід'ємним етапом проектування системи захисту інформації. По-друге, допускається використання як кількісних, так і якісних шкал, об'єктивних та суб'єктивних методів визначення ймовірностей. По-третє, відсутній НД ТЗІ, який би регламентував процес оцінки

ризиків [26], і на поточний момент відсутня гармонізація між основною масою вітчизняних документів (наприклад, НД ТЗІ) та п’ятьма ДСТУ серії ISO. Обґрунтована методика оцінки ризиків буде задовольняти вимогам вітчизняних нормативних документів.

6. У серії стандартів ISO 2700x [2,28-30] наведено алгоритм процесу управління ризиками, а також довідковий матеріал, який може використовуватися на різних етапах процесу управління ризиками. Методика оцінки ризиків повинна відповідати загальним вимогам, основними з них є обґрунтованість методики, повторюваність результатів та їхнє представлення у такій формі, в якій їх можна порівнювати з результатами, отриманими з використанням інших методик. Загальні принципи побудови методики оцінки ризиків стандарту ISO/IEC 13335 (та його російських аналогів) можна покласти в основу узагальненої методики оцінки ризиків, а стандарт ISO/IEC 18028:2005 можливо використовувати при оцінці ризиків обчислювальної мережі. Серед розглянутих іноземних стандартів перспективними для використання при оцінці ризиків ІБ є каталог активів, загроз, вразливостей і контрзаходів IT-Grundschutz [36] і методики та підходи стандарту SP 800-30 [10].
7. На основі аналізу принципів, які покладено в основу розробки методики оцінки ризиків інформаційної безпеки визначено, що найбільш перспективним є застосування інтелектуальних технологій, зокрема нейронних мереж, нечітких систем та генетичних алгоритмів, а також гібридних інтелектуальних систем.

Список літератури

1. Outpacing change Ernst & Young’s 12th annual global information security survey [Електронний ресурс] // Home - Ernst & Young - Ukraine [сайт] — Режим доступу: http://www.ey.com/Publication/vwLUAssets/12th_annual_global_information_security_survey_brochure/$FILE/12th%20annual%20global%20information%20security%20survey.pdf (29.06.2010). — Назва з екрану.
2. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. — [Чинний від 15-10-2005]. — Женева: [б.в.], 2005. — 42 с. — (Міжнародні стандарти ISO/IEC).
3. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. — [Чинний від 01-01-1997]. — К.: Держстандарт України, 1996. — 6 с. — (Національні стандарти України).
4. Астахов А. Искусство управления информационными рисками / Астахов А. — М.: ДМК Пресс, 2010. - 312 с.
5. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 30 с. — (Нормативні документи системи технічного захисту інформації).
6. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf (10.06.2010). — Назва з екрану.
7. Hard Problem List, INFOSEC Research Council, November 2005 [Електронний ресурс] // Cyber Security Research and Development Center [сайт] — Режим доступу: http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf (10.06.2010). — Назва з екрану.
8. National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective, The Institute for Information Infrastructure Protection, 2009 [Електронний ресурс] // I3P: Institute for Information Infrastructure Protection [сайт] / Martin N. Wybourne , Martha F. Austin , Charles C. Palmer ; The Institute for Information Infrastructure Protection — Режим доступу: http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf (10.06.2010). — Назва з екрану.
9. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3-2007. — [Чинний від 01-09-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2007. — 84 с. — (Національні стандарти Російської Федерації).
10. Gary Stoneburner. Risk Management Guide for Information Technology Systems . Recommendations of the National Institute of Standards and Technology : NIST SP 800-30 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Gary Stoneburner, Alice Goguen, and Alexis Feringa ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (10.06.2010). — Назва з екрану.
11. Корченко А.Г. Построение систем защиты информации на нечетких множествах / Корченко А.Г. – К.:«МК-Пресс», 2006. – 316 с.
12. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики / Балашов П.А., Кислов Р.И., Безгузиков В.П. // Конфидент. – 2003. – 53,№ 4. – С. 56-60; 54,№ 6. – С. 60-66.
13. Control system cyber vulnerabilities and potential mitigation of risk for utilities, Juniper Networks [Електронний ресурс] // Network Security Solutions - Networking Performance Optimization - Juniper Networks [сайт] — Режим доступу: http://www.juniper.net/us/en/local/pdf/whitepapers/2000267-en.pdf (10.06.2010). — Назва з екрану.
14. More Realistic Estimating: Separating Risks and Opportunities from Uncertainty , An Oracle White Paper , March 2009 [Електронний ресурс] // Oracle | Software. Hardware. Complete. [сайт] — Режим доступу: http://www.oracle.com/us/products/applications/042767.pdf (10.06.2010). — Назва з екрану.
15. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с. - (Информационные технологии для инженеров).
16. Петренко С.А. Новые инициативы российских компаний в области защиты конфиденциальной информации / Петренко С.А., Симонов С.В. // Конфидент. – 2003. – 49,№ 1. –С. 56-62.
17. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. — [Чинний від 01-07-1997]. — К.: Держстандарт України, 1996. — 6 с. — (Національні стандарти України).
18. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. — [Чинний від 01-01-1998]. — К.: Держстандарт України, 1997. — 10 с. — (Національні стандарти України).
19. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 21 с. — (Нормативні документи системи технічного захисту інформації).
20. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 30 с. — (Нормативні документи системи технічного захисту інформації).
21. Лукацкий А. О заблуждениях в безопасности, ставших классикой [Електронний ресурс] // Bankir.Ru: Технологии, Риск-Менеджмент, Информационная безопасность [сайт] / Лукацкий А.; Bankir.Ru — Режим доступу: http://www.bankir.ru/technology/article/1367694 (10.06.2010). — Назва з екрану.
22. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-00. — [Чинний від 15-12-2000]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000. — 32 с. — (Нормативні документи системи технічного захисту інформації).
23. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 58 с. — (Нормативні документи системи технічного захисту інформації).
24. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 14 с. — (Нормативні документи системи технічного захисту інформації).
25. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. — [Чинний від 08-11-2005]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. — 25 с. — (Нормативні документи системи технічного захисту інформації).
26. Єрмошин В. Питання розробки методики оцінки ризиків системи управління інформаційною безпекою / Єрмошин В., Капустян М. // Безопасность информации в информационно-телекоммуникационных системах, сборник тезисов докладов XIII Международной научно-практической конференции. – 2010. – С. 67.
27. Петренко С.А. Анализ рисков в области защиты информации, Информационно-методическое

пособие по курсу повышения квалификации “Управление информационными рисками” / Сергей Анатольевич Петренко. — Санкт-Петербург: ООО «Издательский Дом «Афина», 2009. — 153 с.
28. Информационные технологии. Свод правил по управлению защитой информации : ISO/IEC 27002:2005 . — [Чинний від 01-07-2007]. — М.: “Технонорматив”, 2007. — 183 с. — (Міжнародні стандарти ISO/IEC).
29. Information technology — Security techniques — Information security risk management: ISO/IEC 27005:2008. — [Чинний від 15-06-2008]. — Женева: [б.в.], 2008. — 64 с. — (Міжнародні стандарти ISO/IEC).
30. Information technology — Security techniques — Information security management systems — Overview and vocabulary: ISO/IEC 27000:2009. — [Чинний від 01-05-2009]. — Женева: [б.в.], 2009. — 26 с. — (Міжнародні стандарти ISO/IEC).
31. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management: ISO/IEC 13335-1:2004. — [Чинний від 15-11-2004]. — Женева: [б.в.], 2004. — 33 с. — (Міжнародні стандарти ISO/IEC).
32. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер: ГОСТ Р ИСО/МЭК ТО 13335-4-2007. — [Чинний від 01-09-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2007. — 107 с. — (Національні стандарти Російської Федерації).
33. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети: ГОСТ Р ИСО/МЭК ТО 13335-5-2006. — [Чинний від 01-06-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2006. — 40 с. — (Національні стандарти Російської Федерації).
34. Other ISMS Standarts [Електронний ресурс] // ISO27k infosec management standards [сайт] — Режим доступу: http://www.iso27001security.com/html/others.html (10.06.2010). — Назва з екрану.
35. Business Continuity Management: BSI-Standart 100-4. — [Чинний від 01-11-2008]. — Бонн: [б.в.], 2008. — 120 с.
36. BSI: IT-Grundschutz-Kataloge [Електронний ресурс] // BSI: Homepage [сайт] — Режим доступу: https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/kataloge.html (10.06.2010). — Назва з екрану.
37. Корченко А.Г. Построение систем защиты информации на нечетких множествах / Корченко А.Г. – К.:«МК-Пресс», 2006. – 316 с.
38. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики / Балашов П.А., Кислов Р.И., Безгузиков В.П. // Конфидент. – 2003. – 53,№ 4. – С. 56-60; 54,№ 6. – С. 60-66.
39. Кущ С.М. Застосування генетичних алгоритмів для оптимізації нечіткої системи кількісної оцінки ризиків / Кущ С.М., Шутовський В.О. // VII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». Збірка тез доповідей. – 2010. – С. 156-157.
40. Гаврилова Т. А. Базы знаний интеллектуальных систем / Гаврилова Т. А., Хорошевский В. Ф. — СПб.: Питер, 2000. - 384 с.

Стаття надійшла 01.10.10.

Відомості про авторів

Архипов Олександр Євгенович – д.т.н., професор, директор Навчального центру перепідготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна.

Кущ Сергій Миколайович – к.т.н., доцент кафедри фізико-технічних засобів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна, тел.:(044) 406-81-04.

Шутовський Василь Олегович – аспірант, асистент кафедри фізико-технічних засобів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна, тел.:(044) 406-81-04, e-mail: v.shutovskyi@gmail.com.