УДК 519.872, 519.688, 681.63

БАГАТОКРИТЕРІАЛЬНИЙ АНАЛІЗ РИЗИКІВ ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В GRID-СИСТЕМАХ

С.І. Лавренюк, А.Ю. Шелестов, А.М. Лавренюк

Інститут кібернетики імені В.М. Глушкова НАН України,
тел. +38(044) 526 3603, Mail lsi@bigmir.net
Інститут космічних досліджень НАН України та НКА України,
Національний технічний університет України "КПІ"

Запропоновано використання багатокритеріального аналізу ризиків порушення безпеки інформації в Grid-системах, придатного для ефективного розв'язування задачі оцінювання рівня доступності та перевірки функціональної дієздатності компонентів Grid-системи. Запропонований підхід дозволяє виявити та ранжувати основні загрози порушення безпеки інформації в Grid-системах.

In this paper multi-criteria risk analysis of information security violation in Grid systems is proposed. This approach can be used for availability level estimation task solving and functional activity check of Grid system components. Proposed method provides possibilities for information violation threats investigation and arrangement in Grid systems.

Вступ

Сьогодні для України, як і для багатьох інших країн, актуальним є створення нових Grid-систем, а також оновлення вже існуючих. Зростає складність задач, вирішуваних такими системами, а коло користувачів постійно розширюється, що робить їх привабливими для зловмисників та конкурентів.

Інформація, що використовується в таких системах, здебільшого є досить цінною. До такої інформації насамперед слід віднести реєстраційні дані користувачів та сертифікати, що є ще більш критичним за умов використання механізмів єдиної реєстрації та передачі повноважень. Впливи, що зумовлюють зниження цінності інформації, є несприятливими, а потенційна можливість виникнення та реалізації цих впливів – загрозою. Щоб наслідки можливих несприятливих впливів не наносили відчутної шкоди, треба підтримувати постійну захищеність (безпеку) всієї інформації. Згідно [1], при забезпеченні інформаційної безпеки насамперед треба враховувати наступні властивості [2]: конфіденційність (інформацію не можуть отримати неавторизовані користувачі), цілісність (інформацію не може модифікувати неавторизований користувач) та доступність (користувач з відповідними повноваженнями може використовувати інформацію, коли вона знаходиться у вигляді та місці, які потрібні користувачу в той час, коли він її потребує).

Цінність і важливість збереження окремих властивостей інформації в різних системах може суттєво різнитися. Наприклад, в системах, що обробляють деякі відомості про персонал, найбільш важливим може виявитися захист конфіденційності цієї інформації, а в системах прийняття рішень найбільш важливою може виявитися доступність інформації.

Захищеність інформації від потенційних несприятливих впливів (загроз) забезпечується захистом інформаційних ресурсів, що її обробляють. Для забезпечення захищеності інформації проводять комплекс заходів, унаслідок якого створюється система захисту інформації (СЗІ).

Передусім необхідно встановити, які загрози є найбільш небезпечними для інформаційної системи, і що потрібно захищати насамперед. Для цього треба визначити цінність усіх інформаційних ресурсів, проаналізувати можливі загрози та визначити ризики, пов'язані з їх реалізацією. Результатом здійснення цього етапу є список усіх загроз, відсортований у порядку спадання показника ризику реалізації кожної загрози. Такий аналіз є основою подальшого вибору заходів забезпечення захищеності інформації [3].

Важливим фактором роботи розподілених систем є доступність інформації, сервісів, системи в цілому, оскільки розміщення обчислювальних ресурсів у відносно віддалених місцях збільшує час доступу до них за рахунок наявності проміжних мереж. Це справедливо і для Grid-систем. Наприклад, специфікація „The Open Grid Services Architecture" [4] висуває цілий ряд вимог, щодо доступності (availability) Grid-сервісів. Подібні вимоги згадано у численних статтях (наприклад, [5. 6]), які описують взаємодію різноманітних розподілених систем.

Ця робота націлена на використання багатокритеріального аналізу ризиків порушення безпеки інформації в Grid-системах та їх окремих сервісах. Як об'єкт досліджень з позицій порушення інформаційної безпеки розглянуто Grid-систему на основі програмного забезпечення проміжного рівня g-Lite та GLOBUS Toolkit 4.0. Приклад – система екологічного моніторингу [7], пілотна версія якої розроблена в Інституті космічних досліджень НАН України та Національного космічного агентства України. Ця система складається з кластерного комплексу (обчислювальних вузлів з центральним керівним вузлом, які відповідають за проведення розрахунків згідно з математичною моделлю та містять екземпляр сервісу GRAM,

використовуваного для отримання та виконання завдань); сервера баз даних, що містить усі метадані [8], необхідні для роботи Grid-системи та метеорологічні наземні дані; файлового сервера, що містить архів супутникових знімків; станції прийому EumetCAST, яка забезпечує систему актуальними знімками земної поверхні. Grid-система регулярно отримує дані про стан погоди, супутникові знімки через мережу Інтернет та зберігає їх у файловому архіві й базі даних. У випадку появи нових даних центральний сервер створює завдання на обробку та розподіляє серед обчислювальних вузлів які виконують обчислення, після чого центральний сервер ініціює передачу готових результатів до файлового архіву та за потреби може забезпечити їх візуалізацію.

Аналіз ризиків порушення безпеки інформації Grid-системи

Згідно [1] рішення про те, яким чином забезпечувати захист інформації у комп'ютерній системі (КС), де реалізовувати ці механізми та якими вони мають бути, сприймають як результат комплексного аналізу. Аналіз має включати визначення загроз інформації, оцінку ймовірності реалізації таких загроз та величини можливих втрат, а також оцінку ризиків, пов'язаних із реалізацією цих загроз як функції ймовірності та величини можливих втрат.

Для оцінювання ризиків є багато різних підходів. Так, в [9] для обчислення ризику запропоновано наступну формулу:

$$R = \sum_{j=1}^{N} R_j g_j , \tag{1}$$

де $\sum_j g_j = 1$, R – узагальнений показник ($0 \le R \le 1$), R_j – кількісна оцінка j-го виду ризику ($0 \le R_j \le 1$), g_j – його вага.

У свою чергу, кількісна оцінка j-го виду ризику становить:

$$R_j = \frac{1}{m} \sum_{i=1}^{n_j} R_{ij} g_{ij} , \tag{2}$$

де $\sum_i g_{ij} = 1$, R_{ij} – бальна оцінка i-го фактора в j-у виді ризику, g_{ij} – вага i-го фактора в j-у виді ризику, n_j – кількість врахованих факторів у j-у виді ризику, m – розмах бальної шкали, в межах якої здійснюється оцінка факторів.

Методика оцінювання базового та залишкового ризику. Найпоширенішою та використовуваною за відсутності СЗІ є формула базового ризику (за умов, що загрози складають повну групу подій, [10]):

$$R = \sum_{i=1}^{N} P_i Q_i , \tag{3}$$

де P_i – ймовірність реалізації i-ї загрози, Q_i – втрати, що можуть виникнути за умови реалізації i-ї загрози. Сама ймовірність реалізації i-ї загрози становить добуток:

$$P_i = P_{\partial_i} P_{\partial\phi_i} , \tag{4}$$

де P_{∂_i} – ймовірність появи джерела створення сприятливих умов (середовища) для проявлення i-го фактора, $P_{\partial\phi_i}$ – ймовірність проявлення i-го дестабілізуючого фактора.

Щодо вразливості системи, то згідно [10] її характеризує залишковий ризик:

$$R_o = \sum_{i=1}^{N} p_i P_i Q_i , \tag{5}$$

де R_o – залишковий ризик, p_i – ймовірність реалізації i-ї загрози після встановлення СЗІ, тобто залишкова ймовірність, оскільки нульової досягнути неможливо.

Оцінка залишкового ризику, отримана таким чином, теоретично дає змогу визначити найбільш небезпечні загрози інформації в системі, а це дає змогу використати деякі конкретні механізми захисту.

Методика визначення ризику за двома факторами з використанням експертного оцінювання. У реальних системах кількісне оцінювання вищезгаданих величин може виявитися дуже складним, а іноді навіть неможливим. Наприклад, оцінка величини можливих втрат, викликаних реалізаціями різноманітних загроз, дуже важко піддається прямому розрахунку, оскільки невідома вартісна оцінка тієї чи іншої інформації. Тоді для розв'язання задачі звертаються до методів теорії прийняття рішень та використовують експертні оцінки.

Так, в [11] розглянуто показник ефективності реалізації загрози інформації E_{ij}, який визначено як показник оцінки ризику, пов'язаного з реалізацією даної загрози:

$$E_{ij} = Q_{ij} R_{ij}, \tag{6}$$

де Q_{ij} – показник, що характеризує відносний внесок *i*-ї загрози інформації, реалізованій на протоколі *j*-го рівня КС, до сумарного ефекту дій зловмисника; R_{ij} – показник, що характеризує статистичну ймовірність реалізації *i*-ї загрози інформації, реалізованій на протоколі *j*-го рівня КС.

Значення показника Q_{ij} можна знайти за допомогою методу аналізу ієрархій (MAI) [12], причому ієрархію пріоритетів характеристик загроз інформації доцільно побудувати наступним чином:

- 1-й рівень – пріоритет цілі загрози (порушення конфіденційності, цілісності чи доступності);
- 2-й рівень – пріоритет інформаційного об'єкта, стосовно якого реалізується загроза;
- 3-й рівень – пріоритет компонента КС, в якому реалізується загроза;
- 4-й рівень – пріоритет рівня стека протоколу, на якому реалізується загроза.

Саме значення показника Q_{ij} для *i*-ї загрози інформації *n*-го типу, реалізованої щодо *k*-го інформаційного об'єкта в *m*-у компоненті КС на протоколі *j*-го рівня, визначається за формулою:

$$Q_{ij} = T_n O_{kn} C_{mk} P_{jm}, \tag{7}$$

де T_n – елемент вектора приоритетів типів загроз $\{T_n\}$, що відповідає *n*-у типу загрози; O_k – елемент відповідаючого *n*-у типу загрози вектора пріоритетів $\{O_{kn}\}$, що відповідає інформаційному об'єкту *k*-го типу; C_{mk} – елемент відповідаючого інформаційному об'єкту *k*-го типу вектора пріоритетів $\{C_{mk}\}$, що відповідає компоненту КС *m*-го типу; P_{jm} – елемент відповідаючого компонента КС *m*-го типу вектора пріоритетів $\{P_{jm}\}$, що відповідає *j*–му рівню стеку протоколів.

Значення показника R_{ij} можна знайти за формулою:

$$R_{ij}(j) = aj^3, \tag{8}$$

де $a = \dfrac{1}{\sum_{k=1}^{N} k^3}$ – коефіцієнт нормування, N – кількість рівнів стека протоколів (для стека TCP/IP – 4), j – номер рівня стека протоколів.

Цей метод має особливості, які негативно впливають на рішення про його вибір як методу аналізу ризиків порушення безпеки інформації Grid-системи, розглянутої в даній роботі як приклад.

По-перше, в цьому методі розглядається оцінювання ризиків реалізації загроз лише за двома факторами. Ці фактори – статистична оцінка ймовірності реалізації загрози та оцінка відносної величини втрат, що можуть бути у випадку успішної реалізації загрози. Такий підхід виправданий лише, коли аналізована обчислювальна систем не має взагалі жодних засобів захисту. Наприклад, коли є тільки її проект. Якщо система вже існує певний час та використовує програмне забезпечення (наприклад, GT 4), що включає певні механізми захисту, то треба розглядати питання про оцінку залишкового ризику. В такому випадку треба врахувати не тільки статистичну ймовірність реалізації загрози, а й імовірність реалізації такої загрози за наявності деяких засобів захисту від неї. По-друге, даний метод ґрунтується на припущенні, що статистичні оцінки реалізації *i*-ї загрози, отримані в одній КС з багаторівневою архітектурою, є справедливі з високою достовірністю для будь-якої іншої системи, побудованої за подібною архітектурою. Це не є справедливим в конкретному випадку, оскільки особливість Grid-систем полягає в тому, що вони будуються з використанням деякого додаткового стека протоколів у рамках прикладного рівня моделі OSI, що мають свою багаторівневу архітектуру.

Існує ще один підхід до оцінювання ризиків, пов'язаних з реалізацією загроз інформації, який досить поширений на практиці та описаний у [13]. У даному підході використовують модель оцінювання ризику за трьома факторами: загроза, вразливість, ціна втрати.

Тут під загрозою розуміють усю сукупність умов і факторів, що можуть стати причиною порушення конфіденційності, цілісності чи доступності інформації. Під вразливістю розуміють слабкість у системі захисту, яка робить можливою реалізацію деякої загрози.

Ймовірність деякої події в цьому підході може бути як об'єктивною, так і суб'єктивною величиною. Об'єктивна ймовірність – відносна частота прояву якоїсь події в загальному обсязі спостережень або відношення числа позитивних результатів до загальної їх кількості. Суб'єктивна ймовірність – міра впевненості деякої людини чи групи людей у тому, що дана подія буде мати місце. В останньому випадку йдеться про уявлення експерта чи групи експертів. Експерти повинні мати відповідний досвід та знання індивідуальних особливостей предметної області та побудови даної конкретної системи.

Імовірність реалізації загрози залежить від імовірностей (у випадку статистичного визначення) або рівнів загроз та вразливостей (у випадку застосування експертної оцінки), які є незалежними величинами. Рівень P_i реалізацій деякої загрози визначається за формулою [14]:

$$P_i = P_{зі} P_{ві}, \tag{9}$$

де $P_{зі}$ – рівень (ймовірність) реалізації *i*-ї загрози, $P_{ві}$ – ступінь вразливості або легкості (ймовірність), з якою реалізація *i*-ї загрози може привести до негативних наслідків.

Тоді залишковий ризик R_o визначається за формулою:

$$R_o = \sum_{i=1}^{N} P_{зі} P_{ві} Q_i , \qquad (10)$$

Даний вираз можна розглядати як математичну формулу, аналогічну до формули (5), якщо використовуються кількісні шкали, або як формулювання загальної ідеї при проведенні експертного оцінювання, якщо хоча б одна з шкал є якісною.

Дійсно, якщо змінні в даній формулі є кількісними величинами, то ризик є оцінкою математичного очікування втрат у випадку успішної реалізації деякої сукупності загроз. Якщо змінні є якісними величинами, то метрична операція множення не визначена і в явному вигляді ця формула використовуватися не повинна. В останньому випадку використовуються різноманітні табличні методи визначення ризику.

Оскільки вищерозглянуті методики є досить складними для реалізації, для практичного оцінювання ризику порушення безпеки розподіленої системи слід використати методику [13] проведення якісного оцінювання ризику реалізації загроз інформації в залежності від трьох факторів – загроза, вразливість, ціна втрати.

У рамках цієї методики визначено наступні якісні шкали: рівні втрат, рівні загроз, рівні вразливостей та рівні ризиків.

Рівні втрат – це відносні ступені серйозності наслідків несприятливого впливу на деякий ресурс організації, тобто, інакше кажучи, відносну ціну втрат цього ресурсу (табл. 1).

Таблиця 1. Рівні втрат

Назва рівня	Опис
Відсутній (В)	Негативним впливом на діяльність організації можна знехтувати.
Малий (М)	Невеликий вплив на діяльність організації. Ліквідація наслідків не потребує значних фінансових витрат
Помірний (П)	Відчутний вплив на діяльність організації, який можна ліквідувати швидко, але це потребує фінансових витрат
Серйозний (С)	Сильний негативний вплив на діяльність організацій, який неможливо ліквідувати негайно, але з часом можна нейтралізувати
Критичний (К)	Діяльність організації може опинитися під загрозою припинення

Рівні загроз – це оцінки ймовірності реалізації, яку надають експерти, виходячи з їхнього досвіду роботи з системою (табл. 2). Наприклад, наявність історії попередніх атак та знання сучасних тенденцій захисту інформації.

Таблиця 2. Рівні загроз

Назва рівня	Опис
Низький (Н)	Реалізація даної загрози малоймовірна, за останні кілька років подібних випадків не зафіксовано
Середній (С)	Реалізація даної загрози є потенційно можливою. Спробу реалізації загрози зафіксовано один чи два рази за останні декілька років
Високий (В)	Загроза є досить реальною. Спроби реалізації загрози зафіксовано декілька разів за останній рік

Рівні вразливостей визначає легкість, з якою цю загрозу можна реалізувати в системі, що призведе до негативних наслідків (табл. 3).

Таблиця 3. Рівні вразливостей

Назва рівня	Опис
Низький (Н)	Захищеність системи проти цього типу загроз є досить високою. У системі є спеціальні механізми захисту. Практично неможливо провести успішну атаку
Середній (С)	Захищеність системи проти цього типу загроз є достатньою. У системі присутні деякі механізми захисту. Для проведення успішної атаки потрібен досить високий рівень компетенції та оснащення нападника
Високий (В)	Захищеність системи проти цього типу загроз є низькою. У системі майже відсутні механізми захисту. Для проведення успішної атаки достатньо середнього рівня компетенції та оснащення нападника

Рівні ризику визначаються за табл. 4:

Таблиця 4. Рівні ризику

Показник ризику	Опис
0	Ризик відсутній. Успішна реалізація загрози неможлива
1	Ризик майже відсутній. Успішна реалізація загрози практично не можлива, а наслідки відсутні
2	Ризиком можна знехтувати. Успішна реалізація загрози є досить рідкісною, а наслідки незначні
3	Ризик є малим. Ймовірність успішної реалізації загрози та наслідки досить малі
4	Ризик є помірним. Успішна реалізація загрози практично можлива, але за певних умов. Наслідки будуть середніми
5	Ризик є серйозним. Успішна реалізація загрози може потенційно відбутися і наслідки будуть відчутними
6	Ризик є досить серйозним. Успішна реалізація загрози скоріше за все можлива, а її наслідки будуть серйозними
7	Ризик є значним. Успішна реалізація загрози можлива, а наслідки скоріше за все будуть катастрофічними
8	Ризик є досить значним. Успішна реалізація загрози скоріше за все відбудеться, а наслідки будуть катастрофічними

За запропонованою методикою формується список усіх можливих у даній обчислювальній системі загроз інформації. Такий список може бути отримано на основі переліку загроз з [15, 16].

Для кожної можливої загрози експерти мають оцінити рівень загрози, вразливості системи та втрат, які можуть наступити у разі її реалізації. Оцінювання проводиться у вищевизначених якісних шкалах.

На наступному етапі розраховується відповідна оцінка рівня ризику реалізації кожної загрози згідно матриці, яка наведена у табл. 5.

Отриманий таким чином перелік загроз та відповідних їм показників ризику сортується за показником ризику в порядку спадання. Загрози, що опинилися у верхній частині списку є найбільш небезпечними для даної інформаційної системи.

Таблиця 5. Визначення ризику в залежності від трьох факторів

Рівень втрат (ціна втрати)	Рівень загрози								
	Низький			Середній			Високий		
	Рівень вразливостей			Рівень вразливостей			Рівень вразливостей		
	Н	С	В	Н	С	В	Н	С	В
Відсутній	0	1	2	1	2	3	2	3	4
Малий	1	2	3	2	3	4	3	4	5
Помірний	2	3	4	3	4	5	4	5	6
Серйозний	3	4	5	4	5	6	5	6	7
Критичний	4	5	6	5	6	7	6	7	8

Результати оцінювання ризиків за трьома факторами. Саме експертне оцінювання зазначених трьох факторів (загроза, вразливість, ціна втрати) та застосування описаної методики оцінювання ризиків дасть можливість прийняти до уваги індивідуальні особливості обчислювальної системи, що розглядається у даній роботі. Цей метод не має вищеописаних недоліків. По-перше, при побудові оцінки ризику реалізації загроз інформації приймаються до уваги існуючі в системі механізми захисту (завдяки оцінюванню рівня вразливості системи щодо деякої загрози). По-друге враховуються особливості архітектури даної системи щодо додаткового стека протоколів у рамках прикладного рівня (завдяки оцінюванню рівня загрози на базі досвіду експертів). Тому ця методика була вибрана як методика оцінювання ризиків порушення безпеки інформації.

Зазначимо, що в даній роботі не розглядаються загрози, пов’язані з побічними електромагнітними випромінюваннями та наводками. Вважається, що всі зовнішні канали зв’язку багатократно дублюються й доступ до них зловмисником значно ускладнений або практично неможливий. Вважається також, що всі внутрішні приміщення знаходяться під постійним контролем.

У результаті використання наведеної методики аналізу ризиків порушення безпеки інформації за трьома факторами (загроза, вразливість, ціна втрати) з використанням експертних оцінок для Grid-системи ІКД НАН України та НКА України отримано наступний перелік найбільш небезпечних загроз (показник ризику > 6) (табл. 6).

Таблиця 6. Перелік найбільш небезпечних загроз

№	Назва	Власти-вість	Компонент / Ресурс	*Qi*	*Рзі*	*Рві*	*Ro*
1.	Посилка запитів, що складно виконати	Д	GRAM/ центр. сервер	К	В	В	8
2.	Посилка запитів, що складно виконати	Д	RFT/ центральний сервер	К	В	В	8
3.	Посилка запитів, що складно виконати	Д	GridFTP/центр. сервер	К	В	В	8
4.	Посилка беззмістовних або невірних запитів	Д	GRAM/ центр. сервер	К	В	В	8
5.	Посилка беззмістовних або невірних запитів	Д	RFT/ центр. Сервер	К	В	В	8
6.	Посилка беззмістовних або невірних запитів	Д	GridFTP/ центр. сервер	К	В	В	8
7.	Посилка беззмістовних або невірних запитів	Д	WS–MDS/ центр. сервер	К	В	В	8
8.	Розподілена атака типу „Відмова в обслуговуванні”	Д	ОС/ центр. Сервер	К	В	С	7
9.	Атаки на вичерпання ресурсів ОС	Д	ОС/ центр. Сервер	К	С	В	7
10.	Захоплення мережних підключень	Д	ОС/ центр. Сервер	С	В	В	7

Висновки

Результат оцінювання ризиків показав, що найбільш важливим для безпеки інформації в Grid-системі є підтримка доступності інформації та сервісів. Тобто насамперед необхідно забезпечити безперервну роботу всіх Grid-сервісів, причому дані, які поступають в систему ззовні, мають постійно залишатися актуальними. При цьому цілісність та конфіденційність таких даних – це другорядна мета. На даний час проведено серію активних експериментів з оцінювання рівня доступності Grid-системи та її окремих сервісів. Заплановано розробити методи та моделі захисту Grid-системи для зниження виявлених ризиків.

1. *НД* ТЗІ 1.1–002–99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – К.: ДСТСЗІ СБ України, 1999. – 16 с.
2. *НД* ТЗІ 1.1–003–99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – К.: ДСТСЗІ СБ України, 1999. – 26 с.
3. *ISO/IEC* 27005:2008, Information technology – Security techniques – Information security risk management.
4. *Foster I., Kishimoto H., Savva A., Berry D*. The Open Grid Services Architecture – http://www.ogf.org/documents/GFD.80.pdf.
5. *Foster I., Kesselman C., Nick J. M., Tuecke S.* Grid Services for Distributed System Integration // Computer. 2002. – Vol. 35(6). – P. 37–46.
6. *Foster I.* The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration – http://www.globus.org.
7. *Куссуль Н.Н., Шелестов А.Ю.* Grid-системы для задач исследования Земли. Архитектура, модели и технологии. – К.: Наук. думка, 2008. – 452 с.
8. *Куссуль Н.Н., Лавренюк А.Н., Лавренюк С.И., Грипич Ю.А.* Каталог метаданных системы GEO-Ukraine.// Сборник трудов ДонНТУ серии “Информатика, кибернетика и вычислительная техника”. – 2009. – Вып. 10(153). – С. 92–100.
9. *Гранатуров В.М*. Экономический риск. – М.: Дело и Сервис, 1999. – 112 с.
10. *Архипов А.Е., Ворожко В.П.* Системный подход к оцениванию эффективности защиты гос. тайны // К.: Научно-техн. сб. „Правовое, нормативное и метрологическое обеспечение систем защиты информации в Украине“. – 2005. – Вып. 10. – С. 18–22.
11. *Новиков А.Н., Тимошенко А.А.* Оценка эффективности действий злоумышленника при реализации угроз информации в распределенных компьютерных системах с открытой архитектурой // К.: Науково-техн. зб. „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні“. – 2001. – Вип. 3. – С. 65–66.
12. *Саати Т.* Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 278 с.
13. Замула А.А. Методология анализа рисков и управления рисками // К.: Всеукр. межвед. науч.-техн. сб. „Радиотехника“. – 2002. – Вып. 126. – С. 1–10.
14. *Венцель Е.С.* Теория вероятностей: Учебник. для студ. вузов. – М: Издательский центр „Академия“, 2003. – 576 с.
15. ISO/IEC 15408-1:2005 – Information technology – Security techniques – Evaluation criteria for IT security.
16. *IT* Baseline Protection Manual Standard // http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm.pdf