УДК 004.056.5

С. С. Бучик, С. В. Мельник

МЕТОДИКА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ В АВТОМАТИЗОВАНІЙ СИСТЕМІ

У статті запропоновано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі. Висвітлено необхідні нормативно-правові документи інформаційної безпеки. Розглянуто роботу прототипу експертної системи, яка дозволяє оцінити рівень інформаційного ризику для певної автоматизованої системи та визначити необхідність застосування додаткових заходів інформаційної безпеки.

Постановка проблеми. У сучасних умовах розвитку комп'ютерної техніки, створення нових зразків програмного та апаратного забезпечення, які використовують з метою добування даних з різноманітних джерел інформації, наявності випадків шпигунства з метою отримання відомостей щодо зразків техніки, програмних засобів, цивільних та військових об'єктів, а також персональних даних та доступу до державних інформаційних ресурсів, досить важливою складовою системи безпеки стала інформаційна безпека (ІБ). Однією із цілей ІБ є реалізація існуючих або розробка нових методологій визначення інформаційного ризику в певній автоматизованій системі (АС).

Саме тому виникає потреба в створенні спеціальних систем, які дозволяли б оцінювати інформаційні ризики та визначати їх кількісний показник, який необхідний для подальшого аналізу рівня ризику в АС та є одним з обов'язкових факторів прийняття рішень спеціалістом з ІБ (у певних випадках системним адміністратором або адміністратором безпеки) щодо необхідності збільшення кількості заходів ІБ.

Таким чином, актуальним є питання оцінювання інформаційного ризику в АС та прийняття рішення щодо необхідності підвищення заходів ІБ.

Огляд останніх досліджень і публікацій. У даний час існують окремі нормативно-правові документи, які регламентують питання ІБ. Вони є основою для створення систем оцінювання як інформаційного ризику окремо, так і ІБ в цілому. Розглядаючи основні нормативні акти, що стосуються ІБ, обов'язково слід виділити такі стандарти: ISO 2700x, 290xx, 13335, 15408, 18044, 18028, 15947, 15443 тощо, загалом більше 100; X.800-816, X.830-835, X.736, X.740, X.1121, X.1051 тощо, загалом більше 40; COBIT, ICM3, BSI-ITBPM, MITS, ISF-SoGP, SAS 70, TruSecure, SysTrust, WebTrust, BBBOnline, TRUSTe тощо, загалом більше 40; NIST SP 800-x, FIPS 140-201 тощо, загалом більше 100 [1].

Розглядаючи нормативно-правову базу ІБ, впроваджену в нашій державі, слід виділити такі документи: "Про Доктрину інформаційної безпеки України" (проект Указу Президента України, попередня редакція втратила чинність на підставі Указу Президента № 504/2014 від 06.06.2014); Закон України "Про інформацію" від 02.10.1992 (чинна редакція від 02.03.2014) № 2657-XII; нормативний документ у сфері технічного захисту інформації (НД ТЗІ) 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого

доступу", затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22 (зі зміною № 1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172) та інші.

У наведених вище документах викладено основну інформацію щодо ІБ, тому без ознайомлення з ними не можливо правильно оцінити інформаційний ризик тієї чи іншої АС.

Як вказано в [2], питанню управління інформаційними ризиками присвячено багато наукових праць, але більшість із них настільки перенасичені формулами та складні, що не можуть бути швидко та ефективно використані на практиці. Тому головною вимогою при розгляді та виборі методики оцінювання ризику в АС є простота та наочність разом з використанням загальноприйнятих стандартів. Питання оцінювання ризику в автоматизованій системі привернуло увагу таких науковців, як: Астахов А. М. [1] (використовує системний підхід до управління інформаційними ризиками, що ґрунтується на міжнародних стандартах BS 7799-3 та ISO/IEC 27005), Гончар С. Ф [3] (застосовує ймовірнісний підхід), Дмитрієв О. А. [4] (розглядає питання ризику відповідно до міжнародного стандарту ISO/IEC 27001), Черней Г. А. [5] (поєднує експертний та ймовірнісний підходи до аналізу інформаційних ризиків), Бєлов В. М. [6] (використовує експертний підхід з урахуванням міжнародних стандартів) тощо.

З аналізу видно, що більшість підходів спирається на міжнародні стандарти, що, у свою чергу, робить визначення ризику простим та доступним, але, на думку авторів, важливим при визначенні факторів ризику ІБ є використання найбільш простого та доступного апарату, який матиме властивість практичної корисності та поєднуватиме в собі кращі аспекти решти підходів.

Формулювання завдання дослідження. Виходячи з наведеного, метою статті є удосконалення методики оцінювання інформаційного ризику в АС з використанням базових методик та вимог міжнародних стандартів, доведення працездатності методики за допомогою програмного продукту, який є прототипом експертної системи.

Виклад основного матеріалу. Для досягнення поставленої мети розберемо, у чому полягає сутність термінів "експертна система" та "інформаційний ризик". Згідно з [7], експертною називають систему, що об'єднує можливості електронної обчислювальної машини із знанням експерта в такій формі, що система може виробити розумні рекомендації або рішення. Щодо поняття "інформаційний ризик", то існує декілька основних визначень. Наведемо їх: ризик – комбінація ймовірності події та наслідків цієї події [8]; ризик ІБ – потенційна можливість використання вразливостей активу або групи активів конкретною загрозою для завдання збитку організації [9]; ризик – функція ймовірності реалізації певної загрози, виду і величини завданих збитків [10]. Визначення, викладене в ISO/IEC 27005, є найбільш повним, тому в подальшому під поняттям "інформаційний ризик" будемо розуміти саме потенційну можливість використання вразливостей активу або групи активів конкретною загрозою для завдання збитку організації. Взагалі, ризик є комплексною величиною, яку характеризують лише за допомогою визначення певної комбінації факторів, таких як: загрози, інциденти, вразливості та види збитків. Ці фактори окремо один від одного не дають змоги правильно описати ризик та визначити його рівень.

У цілому оцінювання ризику полягає у визначенні його рівня та порівнянні з максимально допустимим. За основу методики оцінювання інформаційного ризику в АС

обрано методику, описану в [6], але для оцінювання системи управління ІБ використаємо оцінні вимоги, визначені в стандарті ISO/IEC 27001 (табл. 1). Безпосередню модель загроз та вразливостей побудуємо, виходячи з типових вразливостей ІБ згідно з ISO/IEC 27002 (табл. 2). У методиці описано процес оцінювання ризиків ІБ, а також розглянуто спосіб кількісного оцінювання ризиків ІБ. Вона призначена для оцінювання ризиків ІБ у рамках побудови або вдосконалення системи ІБ на підприємствах малого і середнього бізнесу. Основним завданням методики є визначення кількісного показника ризику ІБ з метою прийняття ефективних заходів щодо захисту інформації (ЗІ). Запропонована методика оцінювання ризиків дозволяє виконати повноцінний аналіз й оцінку ризиків без допомоги висококваліфікованих фахівців і може бути адаптованою для оцінювання ризиків ІБ в АС.

Таблиця 1

Вимоги до ІБ

№	Розділ основних вимог до ІБ	Вимоги до ІБ
1	2	3
1.	Загальні вимоги до СУІБ	1.1. СУІБ створена
		1.2. СУІБ впроваджена
		1.3. СУІБ знаходиться в експлуатації
		1.4. Здійснюється моніторинг СУІБ
		1.5. СУІБ аналізується
		1.6. СУІБ удосконалюється
2.	Створення й управління СУІБ	2.1. Визначені сфери дії та межі СУІБ
		2.2. Визначення дій СУІБ у виняткових ситуаціях
3.	Політика безпеки	3.1. Містить у собі основу для визначення її цілей
		3.2. Встановлює загальні напрямки та принципи діяльності щодо ІБ
		3.3. Враховує вимоги підрозділу
		3.4. Враховує вимоги законодавства та нормативної бази
		3.5. Враховує конкретні обов’язки в сфері безпеки
		3.6. Поєднується зі стратегічним контекстом управління ризиками в організації, у якій буде створюватися СУІБ
		3.7. Встановлює критерії для оцінювання ризиків
		3.8. Затверджена керівництвом
4.	Активи	4.1. Наявні реєстри інформаційних активів
		4.2. Власники активів правильно ідентифіковані
		4.3. Наявні правила маркування конфіденційних документів
		4.4. Наявні правила поведінки з конфіденційними документами
		4.5. Наявна схема класифікації документів

Таблиця 2

Характеристика невідповідності вимогам нормативно-правової бази в сфері ІБ

Сума виконаних вимог	Ризик невідповідності АС вимогам законодавства (R_n)
16–21	0,01
11–15	0,25
<10	0,5
Не виконуються	0,9

Загальний алгоритм оцінювання ризику згідно з даною методикою наведено на рис. 1. Для його розуміння слід розглянути кожну процедуру окремо.

Рис. 1. Схема алгоритму оцінювання ризику ІБ

Ідентифікація активів. На даному етапі експерти проводять інтерв'ю з особовим складом підрозділу або відділу з метою виявлення використовуваних активів. Активи системи інформаційних технологій є компонентом або частиною загальної системи, у яку підрозділ безпосередньо вкладає кошти, що, відповідно, потребують захисту з боку підрозділу. При ідентифікації активів слід мати на увазі, що будь-яка система інформаційних технологій включає в себе не тільки апаратні засоби, але й програмне забезпечення.

Існують такі види активів: інформація (файли, що містять дані про діяльність організації); апаратні засоби (комп'ютери, принтери); програмне забезпечення, включаючи прикладні програми (обробки текстів, цільового призначення); обладнання для забезпечення зв'язку (телефони, мідні та оптико-волоконні кабелі); персонал; престиж організації.

Визначення ризику невідповідності вимогам законодавства в галузі ІБ. Будь-який підрозділ, що має інформаційні системи або робота якого пов'язана з використанням

інформаційних технологій, повинен дотримуватися вимог законодавчих актів у цій галузі. Їх невиконання може спричинити цивільну, кримінальну, адміністративну, дисциплінарну та іншу, передбачену законодавством відповідальність. Ризик невиконання нормативних вимог впливає на загальний ризик ІБ. Алгоритм визначення ризику невідповідності вимогам законодавства у сфері ІБ включає в себе проведення всебічного аналізу стану системи інформаційного захисту з метою виявлення невідповідності. У ході аналізу всім вимогам, які не порушують, присвоюють значення “1”, в іншому випадку – “0”. Усі значення, яким присвоєно “1”, додають, решту – не враховують.

Дізнавшись (підрахувавши) кількість виконаних вимог, можна визначити ризик невідповідності АС вимогам законодавства. Для цього використаємо табл. 2. Оскільки не існує визначеної кількості вимог, а є лише перелік тих (описаний в [11]), що повинні бути виконані, нам слід підібрати їх (їхню кількість) саме під нашу АС. У табл. 1 наведено вимоги до ІБ згідно зі стандартом ISO/IEC 27001 (відповідно до чотирьох розділів, а саме: “Загальні вимоги до системи управління інформаційною безпекою (СУІБ)”, “Створення і управління СУІБ”, “Політика безпеки”, “Активи”), загальна їх кількість становить 21. За методикою, викладеною в [6], отримаємо характеристики невідповідності вимогам нормативно-правової бази у сфері ІБ (табл. 2).

Розробка моделі загроз. При розробці моделі загроз слід визначити вразливості (організаційні та технічні), притаманні визначеній АС. У нашому випадку кількість організаційних та технічних вразливостей обираємо, виходячи з табл. 3, яка описує модель загроз та вразливостей, передбачених стандартом ISO/IEC 27002:2005 [12]. Можливість використання організаційних вразливостей встановлюють експертним методом, аналізуючи застосування організаційних заходів ЗІ. У ході проведення аналізу всім організаційним заходам, які виконують, присвоюють значення “1”, в іншому випадку – “0”. Усі значення, яким присвоєно “1”, додають, решту – не враховують. Використовуючи методику, викладену в [6], отримаємо характеристики організаційних вразливостей ІБ АС (табл. 4).

Таблиця 3

Модель загроз та вразливостей

№	Галузь безпеки	Вразливість	Загроза, що використовує дану вразливість
1	2	3	4
1.	Безпека кадрових ресурсів (ISO/IEC 27002:2005, розділ 8)	1.1. Недостатній рівень навчання персоналу щодо безпеки	1.1. Помилка персоналу технічної підтримки
		1.2. Неосвіченість користувачів у питаннях безпеки	1.2. Помилка користувачів
		1.3. Відсутність політики безпеки в сфері коректного використання засобів телекомунікацій та передачі повідомлень	1.3. Несанкціоноване використання мережевого обладнання

Продовження табл. 3

1	2	3	4
		1.4. Права доступу залишаються в працівника навіть після звільнення	1.4. Несанкціонований доступ
		1.5. Невмотивований та незадоволений персонал	1.5. Зловживання засобами обробки інформації
		1.6. Робота без нагляду персоналу, що працює в неробочий час	1.6. Грабіж
		1.7. Відсутність механізмів моніторингу	1.7. Несанкціоноване використання програмного забезпечення
2.	Фізична безпека і безпека навколишнього середовища (ISO/IEC 27002:2005, розділ 9)	2.1. Відсутність фізичного захисту будівлі, дверей та вікон	2.1. Грабіж
		2.2. Розміщення обладнання в зоні, якій загрожує затоплення	2.2. Затоплення
		2.3. Незахищене зберігання інформації	2.3. Грабіж
		2.4. Відсутність схеми періодичної заміни обладнання	2.4. Закінчення терміну експлуатації засобів зберігання інформації
		2.5. Стрибки напруги	2.5. Флуктуація електроживлення
		2.6. Нестабільне електроживлення (подача електроенергії)	2.6. Флуктуація електроживлення
3.	Управління комунікаціями та операціями (ISO/IEC 27002:2005, розділ 10)	3.1. Складний користувацький інтерфейс	3.1. Помилка персоналу
		3.2. Передача або повторне використання засобів зберігання інформації без потрібного очищення	3.2. Несанкціонований доступ
		3.3. Неадекватний контроль змін	3.3. Збій системи безпеки
		3.4. Неадекватне керування мережею	3.4. Перенавантаження трафіка
		3.5. Відсутність розподілу обов'язків	3.5. Зловживання системою (випадкове чи навмисне)
		3.6. Відсутність процедур резервного копіювання	3.6. Втрата інформації

Продовження табл. 3

1	2	3	4
		3.7. Відсутність оновлень програмного забезпечення, яке використовують для захисту від шкідливих кодів (вірусів)	3.7. Вірусне ураження
		3.8. Неконтрольоване копіювання	3.8. Грабіж
		3.9. Незахищене з'єднання з мережами загального користування	3.9. Використання програмного забезпечення неавторизованими користувачами
4.	Контроль доступу (ISO/IEC 27002:2005, розділ 11)	4.1. Некоректне розмежування доступу в мережах	4.1. Несанкціоноване під'єднання до мережі
		4.2. Відсутність механізмів ідентифікації та аутентифікації	4.2. Присвоєння чужого користувацького ідентифікатора
		4.3. Відсутня чи некоректна політика контролю доступу	4.3. Несанкціонований доступ до інформації, системи чи програмного забезпечення
		4.4. Відсутність чи недостатнє тестування програмного забезпечення	4.4. Використання програмного забезпечення неавторизованими користувачами
		4.5. Незадовільне керування паролями	4.5. Присвоєння чужого користувацького ідентифікатора
		4.6. Відсутність захисту мобільного комп'ютерного устаткування	4.6. Несанкціонований доступ до інформації
		4.7. Відсутність "виходу із системи", коли залишають робоче місце	4.7. Використання програмного забезпечення неавторизованими користувачами
		4.8. Відсутність контролю прав доступу користувачів	4.8. Доступ зі сторони користувачів, які звільнились з організації, або перевелися на інше місце роботи
		4.9. Відсутність відключення та зміни стандартних попередньо встановлених облікових записів та паролів	4.9. Несанкціонований доступ до інформації, системи чи програмного забезпечення

Продовження табл. 3

1	2	3	4
		4.10. Неконтрольоване використання системних утиліт	4.10. Обхід механізмів контролю системи чи додатка
5.	Придбання, розробка та супровід інформаційних систем (ISO/IEC 27002:2005, розділ 12)	5.1. Недосконала політика безпеки в сфері використання криптографії	5.1. Порушення законодавства або нормативної бази
		5.2. Невиконання або виконання в недостатньому обсязі тестування програмного забезпечення	5.2. Використання програмного забезпечення неавторизованими користувачами
		5.3. Відомі дефекти в програмному забезпеченні	5.3. Використання програмного забезпечення неавторизованими користувачами
		5.4. Недостатній захист криптографічних ключів	5.4. Відкритий доступ до інформації
		5.5. Відсутність контролю вхідних та вихідних даних	5.5. Помилка
		5.6. Відсутність перевірки даних, що обробляються	5.6. Викривлення інформації
		5.7. Неконтрольоване завантаження та використання програмного забезпечення	5.7. Шкідливе програмне забезпечення

Таблиця 4

Характеристика організаційних вразливостей ІБ АС

Загальна кількість заходів захисту, що виконують (організаційні вразливості, які відсутні для даної інформаційної системи)	Коефіцієнт вразливості (K_0)
19–23	0,01
11–18	0,25
Менше 10	0,5
Не виконують	0,9

Можливість використання технічних вразливостей встановлюють експертним методом, аналізуючи технічні заходи ЗІ, що застосовують у даній АС. Під час проведення аналізу всім технічним заходам, які виконують, присвоюється значення "1", в іншому випадку – "0". Усі значення, яким присвоєно "1", додають, решту – не враховують. Відповідно до методики, викладеної в [6], отримаємо характеристики технічних вразливостей ІБ АС (табл. 5).

Таблиця 5

Характеристика технічних вразливостей ІБ АС

Загальна кількість заходів захисту, що виконують (технічні вразливості, які відсутні для даної інформаційної системи)	Коефіцієнт вразливості (K_t)
13–16	0,01
8–12	0,25
Менше 8	0,5
Не виконують	0,9

Визначення допустимого рівня ризику. Допустимим ризиком прийнято вважати той, який у даній ситуації є прийнятним при існуючих суспільних цінностях. Для АС рекомендоване значення допустимого ризику не повинне перевищувати 5%. Це обумовлюється, у першу чергу, тим, що кошти, вкладені за звітний період (наприклад, 1 рік), можуть становити десятки мільйонів гривень. У разі реалізації однієї з актуальних загроз завданий збиток може становити більше 5%, а отже, є неприпустимим і вимагає вжиття ефективних заходів.

Визначення кількісного значення ризику. Кількісне значення інформаційного ризику реалізації певної загрози з усього переліку актуальних загроз з урахуванням наявності вразливостей розраховуємо за такою формулою [6]:

$$R = P_{загр} \cdot R_n \cdot C \cdot \frac{K_o + K_t}{2}, \qquad (1)$$

де R – кількісна величина інформаційного ризику;

$P_{загр}$ – імовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз;

R_n – ризик невідповідності вимогам законодавства;

C – цінність активу;

K_0 – імовірність використання організаційних вразливостей;

K_t – імовірність використання технічних вразливостей.

Реалізація прототипу експертної системи оцінювання інформаційного ризику. Результатом перевірки працездатності даної методики є розроблений програмний продукт, який є прототипом експертної системи оцінювання інформаційного ризику в АС. Кінцеві результати роботи програми висвітлені у двох формах (рис. 2), причому на одній з них показано повідомлення, що містить рекомендації щодо необхідної кількості заходів ІБ, а на іншій – графічне зображення отриманих результатів оцінювання.

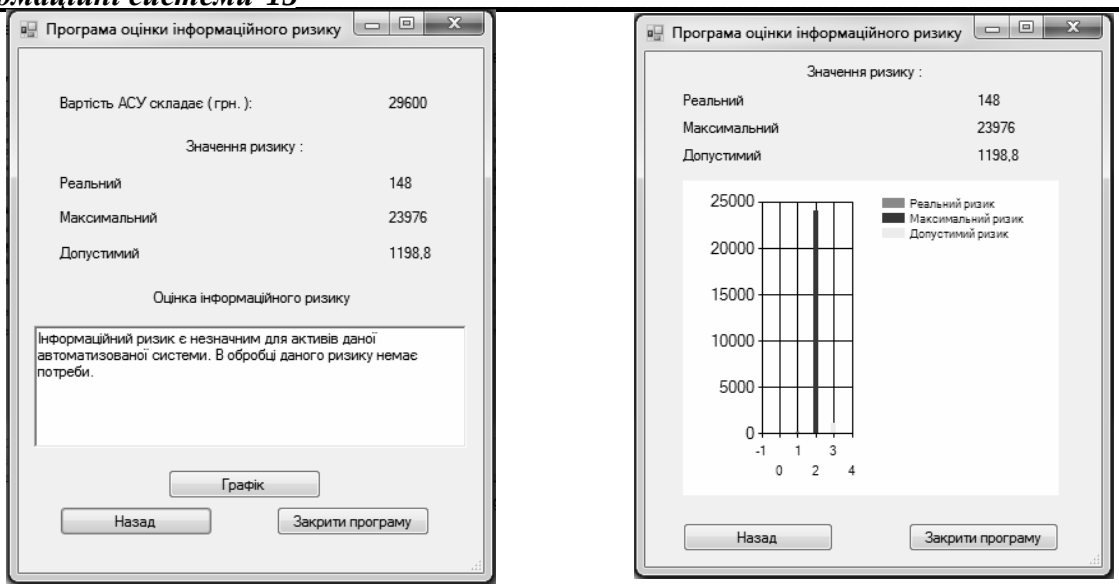

Рис. 2. Кінцевий результат (оцінка інформаційного ризику)

Основними результатами автори вважають удосконалення існуючої методики оцінювання ІБ АС шляхом введення вимог міжнародного стандарту ISO/IEC 27001. Працездатність даної методики підтверджується програмним продуктом.

Висновки. У статті запропоновано удосконалену методику оцінювання інформаційного ризику в АС з використанням базових методик та вимог міжнародних стандартів. Працездатність методики доведено за допомогою програмного продукту, який є прототипом експертної системи оцінювання інформаційного ризику в АС. Його можна використовувати як для безпосереднього оцінювання інформаційного ризику, так і в навчальних цілях. У подальшому на його основі можна створити інтелектуальну систему для прийняття рішень, пов'язаних з визначенням заходів ІБ в АС .

СПИСОК ЛІТЕРАТУРИ

1. Астахов А. М. Искусство управления информационными рисками / А. М. Астахов. – М. : ДМК Пресс, 2010. – 312 с.
2. Бучик С. С. Оцінювання функціональних профілів загроз державним інформаційним ресурсам / С. С. Бучик // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир : ЖВІ ДУТ, 2014. – Вип. 9. – С. 146–155.
3. Гончар С. Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Ф. Гончар // Захист інформації. – 2014. – № 1 (16). – С. 40–46.
4. Дмитриев А. А. Риск-менеджмент по требованиям международного стандарта ISO/IEC 27001. Один из способов увидеть будущее без машины времени [Электронный ресурс] / А. А. Дмитриев. – Режим доступа : http://www.das-management.info.
5. Черней Г. А. Оценка угроз безопасности автоматизированным информационным системам [Электронный ресурс] / Г. А. Черней. – Режим доступа : http://www.ase.md/~osa/publ/ru/pubru01.html.

6. Плетнев П. В. Методика оценки рисков информационной безопасности : докл. ТУСУРа [Электронный ресурс] / П. В. Плетнев, В. М. Белов. – Режим доступа : www.tusur.ru/filearchive/reports-magazine/2012-25-2/083.pdf.
7. Бучик С. С. Системи підтримки прийняття рішень : конспект лекцій / С. С. Бучик, С. О. Кондратенко, О. О. Писарчук. – Житомир : ЖВІРЕ, 2006. – 168 с.
8. Системы управления информационной безопасностью. Ч. 3. Руководство по управлению рисками информационной безопасности : BS 7799-3 : 2006 [Электронный ресурс]. – Режим доступа : http://www.konyakov.ru/konyakov/uploads/2014/01/BS_7799_3_ru.doc.
9. BS ISO/IEC 27005 : 2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс]. – Режим доступа : http://www.klubok.net/Downloads-index-req-viewdownloaddetails-lid-424.html.
10. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. – [Чинний від 28.04.1999]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/doccatalog/list?currDir=41640.
11. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования : ISO/IEC 27001:2005 [Электронный ресурс]. – Режим доступа : http://www.specon.ru/files/ISO27001.pdf.
12. Информационные технологии. Свод правил по управлению защитой информации : ISO/IEC 27002 : 2005 [Электронный ресурс]. – Режим доступа : http://www.pqm-online.com/assets/files/lib/std/iso_iec_27002-2005.pdf.

Подано 16.04.2015

С. С. Бучик, С. В. Мельник

МЕТОДИКА ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

В статье предложена и проанализирована усовершенствованная методика оценивания информационного риска в автоматизированной системе. Освещены необходимые нормативно-правовые документы информационной безопасности. Рассмотрена работа прототипа экспертной системы, которая позволяет оценить уровень информационного риска для определенной автоматизированной системы и определить необходимость использования дополнительных мер информационной безопасности.

S. S. Buchyk, S. V. Melnyk

METHODS OF ESTIMATION OF INFORMATIVE RISKS IN AUTOMATED SYSTEM

In the article the improved methods over of estimation of informative risk in an automated system is brought, shown and analyzed. Needed normatively-legal documents of informative security are represented. The work of prototype of consulting model, which allows to estimate the level of informative risks for a certain automated system and to define the necessity of application of additional informative security measures, is considered.