МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

# МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Методичні вказівки
до виконання розрахунково-графічних робіт
для студентів напряму підготовки (спеціальність)
6.170103 "Управління інформаційною безпекою",
125 «Кібербезпека»

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного моделювання
*Протокол № _8__*
*від « 19 »  02  2019 р.*

Чернігів ЧНТУ 2019

Менеджмент інформаційної безпеки. Методичні вказівки до виконання розрахунково-графічної роботи для студентів напряму підготовки (спеціальність) 6.170103 "Управління інформаційною безпекою", 125 «Кібербезпека» / Укл.: Усов Я.Ю. – Чернігів: ЧНТУ – 16с.

Укладачі: Усов Ярослав Юрійович, викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск: Ткач Юлія Миколаївна,

завідувач кафедри кібербезпеки та математичного моделювання,

доктор педагогічних наук, доцент

Рецензент: Ткач Юлія Миколаївна, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, доцент

**ЗМІСТ**

# ПЕРЕДМОВА

Метою викладання дисципліни є сутність та завдання менеджменту інформаційної безпеки, складові системи менеджменту інформаційної безпеки, процеси ризик-менеджменту, засоби реалізації та підтримки функціонування системи менеджменту інформаційної безпеки та її аудит. Виклад теоретичного матеріалу доповнено практичними завданнями, кожен розділ завершено питаннями для самоконтролю.

Завданнями вивчення навчальної дисципліни є:

- сутність та завдання менеджменту інформаційної безпеки;
- складові системи менеджменту інформаційної безпеки;
- процеси ризик-менеджменту;
- засоби реалізації та підтримки функціонування системи менеджменту інформаційної безпеки;
- аудит системи менеджменту інформаційної безпеки.

Запропоновані завдання для індивідуальної (розрахунково-графічної) роботи студентів включають методичні вказівки до виконання, завдання для розрахунку, критерії оцінювання. За допомогою розрахунково-графічної роботи та запропонованих завдань досягається більш глибоке опанування теорії, що здійснюється за допомогою розвитку логічного мислення через вирішення задач та дає змогу студентам осмислити нові для них поняття. Завдання для розрахунку скомпоновані відповідно до розділів робочої програми «менеджменту інформаційної безпеки», 7 семестр навчання, що полегшує і робить більш зручною організацію навчального процесу і викладачам, і студентам.

Завдання для розрахунково-графічної роботи студентів можуть використовуватися як для аудиторної, так і домашньої роботи. Вони спрямовані на розвиток у студентів організаційних та аналітичних здібностей, а також уміння користуватися теоретичними посиланнями у вирішенні практичних

ситуацій та вміння користуватися статистикою і спеціальною літературою. Завдання для розрахунково-графічної роботи студентів можуть значною мірою полегшити вивчення дисципліни студентами очної форми навчання.

Під час виконання розрахунково-графічної роботи студенти повинні ознайомитися та вивчити лекційний матеріал, запропонований викладачем. Основою для вивчення є літературні джерела, наведені в даній методичній розробці. За наявності незрозумілих питань студентам рекомендується звернутись за консультаціями до викладача з метою отримання всіх необхідних пояснень щодо організації розрахунково-графічної роботи, виконання розрахункових завдань та пошуку додаткових літературних джерел. Викладачем надаються додаткові роз'яснення та індивідуальні консультації для підвищення компетентності студентів та розширення спектру їх знань з даної дисципліни.

## КРИТЕРІЇ ОЦІНЮВАННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Розрахунково-графічні завдання виконуються за окремим графіком. Студент самостійно готується до такого заняття за індивідуальним завданням. Обсяг розрахунково-графічної роботи визначається навчальним планом з дисципліни.

З даного курсу розрахунково-графічної робота проводиться у формі виконання індивідуальних завдань з розв'язування різноманітних задач.

Шкала оцінювання знань студентів при виконанні розрахунково-графічної роботи

| **Рівень виконання розрахункової роботи** | **Кількість балів** | |
|---|---|---|
| - завдання розв'язані повністю і правильно, містять пояснення до розрахунків;<br>- здійснено посилання на нормативну базу;<br>- показано вміння самостійно формулювати висновки за результатами проведеного дослідження;<br>- присутній творчий підхід та використано новітні інформаційні технології. | 9… | 10 |
| - завдання виконані повністю, але при розв'язуванні допущені незначні помилки;<br>- не аргументовано викладено матеріал;<br>- у висновках містяться помилки та недоречності | 6… | 8 |
| - завдання розв'язані, але містять грубі помилки;<br>- завдання розв'язані не у повному обсязі та допущено значні помилки;<br>- не сформульовані висновки за результатами розрахунків | 3… | 5 |
| - завдання виконані частково і неякісно;<br>- записані тільки формули | 0… | 2 |

У зв'язку з тим що, розрахунково-графічна робота містить завдання для розрахунку з різних тем, і може бути виконана після вивчення всіх тем курсу, оцінюється вона після закінчення другого модуля і оцінка за виконання розрахунково-графічної роботи, додається до підсумкової модульної оцінки, переведеної за шкалою ECTS.

## СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| Назви змістових модулів і тем | Кількість годин для денної форми навчання | | | | | |
|---|---|---|---|---|---|---|
| | денна форма | | | | | |
| | усього | у тому числі | | | | |
| | | л | пр | лаб | інд | с.р. |
| **Модуль 1** | | | | | | |
| **Змістовий модуль 1**. | | | | | | |
| 1. Сутність та завдання менеджменту інформаційної безпеки. | | 5 | | 4 | | 20 |
| 2. Складові системи менеджменту інформаційної безпеки (СМІБ). | | 5 | | 5 | | 20 |
| 3. Процеси ризик-менеджменту. | | 5 | | 5 | | 20 |
| 4. Засоби реалізації та підтримки функціонування системи менеджменту інформаційної безпеки. | | 5 | | 5 | | 20 |
| 5. Аудит системи менеджменту інформаційної безпеки. | | 6 | | 5 | | 20 |
| Модульна контрольна робота №1 | | | | | | |
| **Разом за змістовим модулем 1** | 150 | 26 | | 24 | | 100 |
| **Усього годин за дисципліну** | 150 | 26 | | 24 | | 100 |

## ВИМОГИ ДО ОФОРМЛЕННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Робота оформляється на листах А4 з однієї сторони, поля: з лівого боку – 20 мм, з правого боку – 10 мм, зверху – 20 мм, знизу – 20 мм. Завдання повинні бути виконані акуратно, розбірливим почерком (або надруковані), з детальними поясненнями та всіма проміжними розрахунками. В кінці розрахункового завдання пишеться висновок (відповідь).

Вимоги до комп'ютерного набору розрахункової роботи:

– текстовий редактор – WORD;

– гарнітура шрифту – Times New Roman;

– кегль шрифту (розмір) – 14;

– міжрядковий інтервал – полуторний;

– абзац – 1,25 см;

– розташування тексту роботи – вирівнювання по ширині;

– міжрядковий інтервал між заголовком (назвою розділу чи підрозділу) і текстом повинна дорівнювати 1 інтервалу.

Приклад оформлення титульної сторінки розрахунково-графічної роботи наведено у Додатку А.

Повністю оформлена і виконана розрахункова робота подається на кафедру в термін, що визначений у плані-графіку виконання розрахункової роботи для перевірки її викладачем. Якщо робота виконана не вчасно без поважних причин, то студенту ставиться 0 балів («незадовільно») і він повинен виконати додатково один з варіантів, який вкаже викладач. Розрахункова робота оцінюється після особистої співбесіди з викладачем. В разі зауважень з боку викладача, робота повинна бути доопрацьована в зазначений термін і подана на перевірку. До підсумкового контролю допускаються лише студенти, що вчасно здали і захистили свою роботу.

Варіант розрахунково-графічної роботи видається студенту викладачем (згідно порядкового номеру в списку академічної групи або в інший спосіб).

## ВАРІАНТИ ЗАВДАНЬ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

**Варіант: 1**

1. Чим менеджер відрізняється від підприємця?
2. Які переваги можуть бути від впровадження СМІБ на підприємстві?
3. Які політики можуть входити до загальної політики СМІБ?
4. Наведіть кількісні методи оцінювання ризиків?

**Варіант: 2**

1. Що є предметом менеджменту?
2. Що таке рейдерство?
3. Що таке ризик?
4. Що регламентує стандарт ISO / IEC 27001 та ISO / IEC 27002?

**Варіант: 3**

1. Які Ви знаєте основні функції менеджменту?
2. Як визначається місце та область поширення СМІБ в організації?
3. Що таке політика ІБ?
4. Наведіть якісні методи оцінювання ризиків

**Варіант: 4**
1. Назвіть загальні принципи управлінської діяльності.
2. Що спільного між системою менеджменту якості та СМІБ?
3. Які стандарти регламентують процес ризик-менеджменту?
4. Які існують стандарти забезпечення управління активами?

**Варіант: 5**
1. Якій найсуттєвіший внесок у менеджмент зробив А. Файоль?
2. Наведіть п’ять фаз планування кінцевого впровадження СМІБ?
3. Що включає в себе управління доступом?
4. Що входить до системи фізичної безпеки підприємства?

**Варіант: 6**
1. Розкрийте сутність понять конфіденційність, цілісність та доступність?
2. Що таке контекст організації?
3. Що собою являє оцінка CVSS?
4. Які міжнародні організації беруть участь у забезпеченні та підтримки ІБ?

**Варіант: 7**
1. Що таке актив?
2. Як реалізується оцінка ефективності СМІБ?
3. Опишіть процес ідентифікації активів
4. Що таке сертифікований аудит СМІБ?

**Варіант: 8**
1. Розкрийте сутність поняття системи менеджменту інформаційної безпеки?
2. Що таке аудит ІБ?
3. Що таке оцінка ризиків?
4. Які ви знаєте відкриті бази даних вразливостей?

**Варіант: 9**
1. Наведіть приклад складних і простих активів?
2. Який стандарт регламентує проведення внутрішніх аудитів?
3. Що включає в себе управління інцидентами ІБ?
4. Які існують програмні засоби підтримки управління активами?

**Варіант: 10**
1. Що таке цикл PDCA?
2. Які етапи внутрішнього аудиту СМІБ?
3. Як забезпечується безпека виробничих процесів організації?
4. Які дії відображають ризик-менеджмент?

## ДОДАТОК А

Титульна сторінка розрахунково-графічної роботи

**Чернігівський національний технологічний університет**
**Кафедра кібербезпеки та математичного моделювання**

**Розрахунково-графічна робота**

**з дисципліни „ Менеджмент інформаційної безпеки ”**

***варіант* №** _____

виконав(ла)
студент(ка) _____
(прізвище, ім’я, по-батькові)
перевірив
_____
оцінка _____ балів

Підпис викладача _____

Чернігів 2019

## СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

### Базова


1. Завадський Й. С. Менеджмент: «Management». 2-ге вид. Київ: Українсько-фінський інститут менеджменту і бізнесу, 1998.
2. Гольдштейн Г. Я. Основы менеджмента: Конспект лекций. Издание второе дополненное. Таганрог: ТРТУ, 1997.
3. Овсянко Д. В. Классики теории менеджмента. *Вестник Санкт-Петербургского университета*. Сер. 8. 2004. Вып. 2. № 16.
4. Кейнс Дж. М. Общая теория занятости, процента и денег. Москва: Прогресс, 1978.
5. Автономова В., Ананьина О., Макашевой Н. История экономических учений: учебное пособие. Москва: ИНФРА-М, 2004.
6. Прокушев Е. Ф. Менеджмент первичного уровня. Москва: Дашков и К, 1999.
7. Дмитриев А. А. ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях. *Das Management*. 2009. № 1. С. 36-39.
8. Information technology. Security techniques. Information security management systems. Requirements. ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013. 34 p.
9. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общие сведения и словарь. ISO/IEC 27000:2014, ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия), 2014. 41 с.
10. Лебединець В. О., Коваленко С. М., Тахтаулова Н. О. Імплементація циклу Демінга-Шухарта (PDCA) при регламентації процесів системи управління якістю фармацевтичного підприємства», *Управління правління, економіка та забезпечення якості в фармації*. 2012. № 1(21). С. 11-17.
11. Деятельность международных организаций в сфере информационной безопасности / НОУ «ИНТУИТ». 2019. URL: https://www.intuit.ru/studies/courses563/419/lecture/9570?page=2 (дата звернення: 10.01.2019).
12. Деятельность международных организаций в сфере информационной безопасности / НОУ «ИНТУИТ». 2019. URL: https://www.intuit.ru/studies/courses/563/419/lecture/9571 (дата звернення: 10.01.2019).
13. Цвілій О. О. Безпека інформаційних технологій: сучасний стан стандартів ISO27K системи управління інформаційною безпекою. *Телекомунікаційні та інформаційні технології*. 2014. № 2. С. 73-79.

14. Дмитриев А. А. ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях. *Das Management.* 2009. № 1. С. 36-39.
15. «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013. P. 34.
16. «Information technology. Security techniques. Information security management systems implementation guidance», ISO/IEC 27003:2017, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017. P. 45.
17. «IT-Grundschutz Methodology – Community Draft», BSI-Standard 200-2, Federal Office for Information Security (BSI), 2017. P. 131.
18. Системи забезпечення інформаційної безпеки. Огляд / Компанія «Валтек», 2018. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review (дата звернення: 26.12.2018).
19. «Методи захисту системи управління інформаційною безпекою». Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП «УкрНДНЦ», 2016. 28 с.
20. Поспєлов Д. А. Нечёткие множества в моделях управления и искусственного интеллекта. Москва: Наука, 1986. 312 с.
21. Гарасимчук О. І., Костів Ю. М. Оцінка ефективності систем захисту інформації. *Вісник КНУ імені Михайла Остроградського*. 2011. Вип. 2 (67). С. 16-20.
22. «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]», National Institute of Standards and Technology Special Publication 800-30, Falls Church: Natl. Inst. Stand. Technol, 2002, p. 54.
23. «Risk analysis based on IT-Grundschutz», BSI-Standard 100-3, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23.
24. Рекомендации в области стандартизации банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. РС БР ИББС-2.2-2009. Введ. 2010.01.01. Банк России: Официальный сайт. Москва: Банк России. URL: http://www.cbr.ru/ credit/gubzi_docs/st22_09.pdf [дата звернення: 29.12.2011].
25. «Information Technology – Security techniques – Information security risk management (ISO/IEC 27005:2008)». ISO/IEC JTC 1/SC 27, 2008. P. 62.
26. «Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности», BS ISO/IEC 27005:2008. Київ, 2011. С. 70.

27. Луцкий М., Иванченко Е., Корченко А., Казмирчук С., Охрименко А. Современные средства управления информационными рисками. *Захист інформації*. 2012. № 1. С. 5–16.
28. Корченко А., Архипов А., Казмирчук С. Анализ и оценивание рисков информационной безопасности: монография. Киев: ООО «Лазурит-Полиграф», 2013. 275 с.
29. «Risk management», Standard AS/NZS 4360:2004, Nundah: ISO working group – risk management Terminology, 2004. P. 65.
30. «International standard Risk management. Principles and guidelines», ISO/FDIS 31000:2009(E), International Organization for Standardization, JISC, 2009. P. 24.
31. Галатенко В. Стандарты информационной безопасности. Москва: Интернет-Университет Информационных технологий, 2004. 328 с.
32. Казмірчук С., Волянська В. Дослідження методик оцінки ризиків. С*учасні проблеми захисту інформації з обмеженим доступом*: міжвідомча науково-практ. конф., тези доп. Київ, 2008. С. 67–69.
33. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ. SecurityLab. Минск: SecurityLab, 2004. URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml [дата обращения: 18.12.2011].
34. Алексеев А. Управление рисками. Метод CRAMM. *IT Expert*. Москва: ЗАО «ИТ Эксперт», 2010. URL: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. [дата обращения: 19.12.2010].
35. Потій О., Лєншин А. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу. *Збірник наукових праць Харківського університету Повітряних Сил*. 2010. № 2(24). С. 85–91.
36. Частиков А., Леднева И. Использование байесовской сети при разработке экспертных систем с нечеткими знаниями. *Краснодар Кубанский государственный технологический университет*, 2005. URL: http://ito.su/2000/II/5/5152.html).
37. Jeevan Jaising, Jackie Rees Krannert, «Value at Risk: A methodology for Information Security Risk Assessment», Proceedings of The 6th INFORMS Conference on Information Systems and Technology (CIST-2001), Miami Beach, Florida, November 2001. P. 15.
38. «Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA». Security Risk Analysis & Assessment, and ISO 27000 Compliance, Macclesfield: The Leading Security Risk, 2010. URL: http://www.riskworld.net.
39. Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen, «Model-Driven Risk Analysis. Chapter: A Guided Tour of the CORAS Me-thod», 2011, SINTEF ICT, Oslo, Norway, pp. 23-43.

40. «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013. P. 34.

41. Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности: BS ISO/IEC 27005:2011. Киев, 2011. 94 с.

42. «Expression des Besoins et Identification des Objectifs de Sécurité EBIOS», Méthode de gestion des risques, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

43. C. Harpes, A. Adelsbach, S. Zatti, N. Peccia, «Quantitative Risk Assessment with ISAMM on ESA's Operations Data System», Itrust consulting, 2007. URL: https://www.itrust.lu/wp-content/uploads/2007/09/publications_TTC_2007_abstract_risk_assessment_with_ISAMM.pdf (Last accessed: 19- Jan- 2017).

44. «IRAM2 Managing information risk is a business essential», Information Security Forum Limited, 2017. URL: https://www.securityforum.org/ uploads/2015/03/ISF-IRAM2-ES.pdf (Last accessed: 20- Jan- 2017).

45. «Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models», COBIT 4.1., Rolling Meadows: IT Governance Institute, 2007, p. 196.

46. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е изд. Санкт-Петербург: Питер, 2006. 958 с.

47. Нестеров С. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft: учебный курс. Санкт-Петербург: Издательство «INTUIT», 2009. 136 с.

48. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. Москва: Компания АйТи, ДМК Пресс, 2004. 384 с.

49. «Practical Threat Analysis in-depth», PTA Technologies, 2013. URL: http://www.ptatechnologies.com/default.htm (Last accessed: 20-Jan- 2017).

50. Костров Д. Анализ рисков и управление ими. *Byte Россия*. 2003. № 10 (62). С. 15–20.

51. Симонов С. Анализ рисков в информационных системах. Практические аспекты. Защита информации. *Конфидент. Безопасность компьютерных систем*. 2001. № 2. С. 48-53.

52. «Compliant Information Security Risk Assessment Tool: vsRisk». IT Governance Ltd., Boise: IT Governance Ltd, 2011. URL: http://www.27001.com/ products/31.

53. C. Alberts, S. Behrens, R. Pethia, W. Wilson, OC-TAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM), Hanscom : SEI Joint Program Office, 1999, p. 72.

54. «Information technology. Security techniques. Code of practice for information security management. International standard», ISO/IEC 17799:2005, International

Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2005, p. 115.

55. «Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799)». *Callio Technologies*. Москва: Представительство Callio Technologies, 2012. URL: http://businesssoft.ru (дата обращения: 18.03.2011).

56. «Consultative Committee for Space Data Systems. Guide for secure system interconnection informational report», CCSDS 350.4-G-1, Washington: Green book November, 2007, p. 51.

57. Лукашов А. Монте-Карло для аналитиков. Как грамотно моделировать и измерять риски. *Риск-менеджмент*. 2007. № 3. С. 73–77.

58. «Inventory of risk assessment and risk management methods», [Reference document]. Paris: Securing Europe's Information Society Regulation, 2004. 460 p.

59. Руководство по управлению рисками безопасности / Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам; Центр Microsoft security center of excellence, TechNet, Редмонд, США: Корпорация Майкрософт, 2006. URL: http://technet.microsoft.com/ru-ru/library/cc163143.aspx (дата обращения: 29.12.2011].

60. Syalim A., Hori Y., Sakurai K. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. *International Conference on Issue*, Fukuoka: Grad. Sch. of Inf. Sci. & Electr. Eng, P. 726–731.

61. «A Guide to risk assessment and safeguard selection for Information Technology Systems», MG-3 K1G 3Z4, Ontario: Government of Canada, Communications Security Establishment (CSE) P.O., 1996. P. 65.

62. Peltier T. Information security risk analysis. London: Auerbach Publications, 2001. 281 p.

63. Rowe W. An anatomy of risk. NY: John Wiley, 1997. 488 p.

64. Anderson, Alison Shain, Michael Shain, «Anderson Risk Management», Information Security Handbook, New York: Stockton Press, 1991. P. 75–127.

65. «MEHARI – Overview», Club de la Securit ´ e de l'Information Franc¸ais, Paris: CLUSIF, 2010, p. 50.

66. «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. Book I», The Method, [version 2], Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006, p. 140.

67. Гарсия М. Проектирование и оценка систем физической защиты. Москва, Мир, 2002. 386 с.

68. «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. II», Catalogue of Elements, [version 2], Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006. P. 87.

69. «CMS Information Security Risk Assessment (RA) Methodology», [CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)] Baltimore: Centers for Medicare & Medicaid Services, 2002. P. 21.

70. Скулыш Е., Корченко А., Горбенко Ю., Казмирчук С. Средства анализа и оценки риска информационной безопасности. *Інформаційна безпека. Людина, суспільство, держава*. 2011. № 3 (7). С. 31-48.

71. Казмирчук С., Охрименко А. Анализ и оценка риска потер государственных информационных ресурсов. *Інтегровані інтелектуальні робототехнічні комплекси (IIRTC 2012) = Integrated Intellectual Robotechnical Complexes (IIRTC 2012):* V Міжнар. наук.-практ. конф.: тези доп. Киев: НАУ, 2012. С. 325–326.

72. Малюк А., Царегородцев А., Макаренко Е. Один из подходов к оценке рисков информационной безопасности в облачных средах. *Безопасность информационных технологий*. 2014. № 4. С. 68-74.

73. Урзов А., Варлатая С. Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности. *Доклады ТУСУРа*. 2013. № 2 (28). С. 142-146.

74. Федорченко А., Чечулин А., Котенко И. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей. *Информационно-управляющие системы*. 2014. № 5 (72). С. 72-79.

75. Федорченко А., Чечулин А., Котенко И. Построение интегрированной базы уязвимостей. *Известия высших учебных заведений. Приборостроение*. 2014. Т. 57, № 11. С. 62-67.

76. Харченко В., Алаа Мохаммед Абдул-Хади, Поночовный Ю. Формирование подмножеств уязвимостей доступности коммерческих Веб-сервисов. *Системи обробки інформації*. 2013. Вип. 7 (114). С. 112-115.

77. Белобородов А., Горбенко А. Применение баз данных уязвимостей в задачах исследования безопасности программных средств. *Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка*. 2015. Вип. 165. С. 83-85.

78. National Vulnerability Database. *National Institute of Standards and Technology*. Gaithersburg, 2016. URL: https://nvd.nist.gov/home.cfm.

79. Банк данных угроз безопасности информации / Федеральная служба по техническому и экспортному контролю России. Москва, 2016. URL: http://bdu.fstec.ru/.

80. Open Sourced Vulnerability Database. *Open Security Foundation*, Lafayette, 2016. URL: https://http://osvdb.org.

81. IBM X-Force Exchange / IBM Corporation. New York, 2016. Acc URL: https://exchange.xforce.ibmcloud.com/vulnerabilities/109429.

82. Vulnerability Notes Database / United States Computer Emergency Readiness Team, Murray Lane, 2016. URL: https://www.kb.cert.org/vuls/#.

83. Vulnerabilities / SecurityFocus. Mountain View. 2016. URL: http://www.securityfocus.com/-53r4–FallsChurch:Natl.Inst.Stand.Technol, 2013.