Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри УІБ
д.т.н. доц. Ткачук Р.Л.
_____
“____” _____2022 року

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему

МОДЕЛЬ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виконав:
студент IV курсу, групи КБ-41,
спеціальності (освітньої-професійної програми)
125 “Кібербезпека”_____
(Управління інформаційною безпекою)_____
(шифр і назва спеціальності (освітньої-професійної програми)
Тичина Юрій Богданович_____
(прізвище, ім’я, по батькові)

Керівник_____Ящук В.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Львів – 2022

АНОТАЦІЯ

Тичина Юрій Богданович «**Модель системи управління інцидентами інформаційної безпеки»**
(П.І.Б.) (тема кваліфікаційної роботи)

Кваліфікаційна робота на здобуття вищої освіти ступеня “бакалавр” за освітньо-професійною програмою Управління інформаційною безпекою зі спеціальності 125 - Кібербезпека. – Львівський державний університет безпеки життєдіяльності. Львів. 2022.

У роботі розглянуто теоретичні, науково-методичні та організаційно-функціональні основи моделювання системи управління інцидентами інформаційної безпеки. Окреслено інструментарій наукового пізнання інформаційної безпеки та процесу її забезпечення. Узагальнено класифікаційні ознаки джерел інцидентів інформаційної безпеки. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки. Проаналізовано стандарти, рекомендації, етапи та світові практики щодо управління інцидентами інформаційної безпеки. Запропоновано модель управління інцидентами інформаційної безпеки та наведено методику розслідування інцидентів інформаційної безпеки. Розроблено та обґрунтовано практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки.

Ключові слова: інформаційна безпека, інцидент інформаційної безпеки, система управління інцидентами інформаційної безпеки, модель системи управління інцидентами.

ANNOTATION

Tychyna Yurii Bohdanovych «Model of Information Security Incident Management System»

(Name) (topic of qualification work)

Qualification work for obtaining a bachelor's degree in higher education according to the educational and professional program of the Information Security Department in the specialty 125 - Cybersecurity. - Lviv State University of Life Safety. Lviv. 2022

Theoretical, scientific-methodical and organizational-functional bases of modeling of information security incident management system are considered in the work. The tools of scientific knowledge of information security and the process of its provision are outlined. The classification features of sources of information security incidents are generalized. Modern approaches to information security incident management are identified. Methodical approaches to the formation of the concept and structure of the automated information security incident management system are presented. Standards, recommendations, stages and world practices in information security incident management are analyzed. An information security incident management model is proposed and a methodology for investigating information security incidents is presented. Practical recommendations for the construction and operation of information security incident management systems have been developed and substantiated.

Key words: information security, information security incident, information security incident management system, incident management system model.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ 7

ВСТУП 8

Розділ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 12

1.1 Поняття інформаційної безпеки та процес її забезпечення 12

1.2 Класифікація джерел інцидентів інформаційної безпеки 14

1.3 Сучасні підходи до управління інцидентами інформаційної безпеки 20

Розділ 2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 30

2.1 Аналіз стандартів, рекомендацій та світових практик щодо управління інцидентами інформаційної безпеки 30

2.2 Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035 33

2.3 Методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки 39

Розділ 3 ОРГАНІЗАЦІЙНО - ТЕХНОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 46

3.1 Методика розслідування інцидентів інформаційної безпеки 46

3.2 Модель управління інцидентами інформаційної безпеки 59

3.3 Практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки 65

ВИСНОВКИ 75

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 78

ДОДАТКИ 84

ВИСНОВКИ

Проблема формування системи управління інформаційною безпекою має велике значення для стабільного та максимально ефективного функціонування підприємств та створення високого потенціалу розвитку в майбутньому.

Узагальнення отриманих результатів дослідження дозволило сформулювати та обґрунтувати такі висновки і рекомендації.

1. Аналіз науково-методичних та нормативно-правових джерел показав необхідність та дозволив систематизувати теоретичні засади розроблення СУІБ. У роботі також визначено фази життєвого циклу інциденту ІБ та наведено компоненти типової СУІБ. Ефективне функціонування останньої дозволить акумулювати інформацію щодо інцидентів ІБ, категоризувати їх та визначити найбільш актуальні загрози і, як результат, максимально ефективно впроваджувати превентивні заходи, що дасть можливість підвищити рівень захищеності ІКС організації в цілому.

2. Розкрито сутність поняття «інцидент інформаційної безпеки». Продемонстровано процес розслідування інцидентів інформаційної безпеки на етапах ініціювання, перевірки політики безпеки, формування групи, збирання фахівців, аналізу та складання звітів.

3. Встановлено, що традиційні моделі управління інформаційною безпекою не враховують зростання кількості сучасних кіберзагроз, а також ризиків досягнення цілей. Запропоновано комплексну модель управління інформаційною безпекою та обґрунтовано необхідність її впровадження в організації. Сформульовано пропозиції щодо вдосконалення стратегічного управління інформаційною безпекою організацій.

4. Проаналізовано вимоги і методичні матеріали щодо розробки СУІБ підприємства. Були розглянуті проблеми побудови СУІБ та досліджені процеси УІБ підприємства, які показали, що стандарти побудови СУІБ постійно розвиваються з року в рік і проблема побудови більше не в застарілості нормативної бази, не в актуальності стандартів, а в халатному відношенні

керівництва підприємства до організації забезпечення ІБ або надмірною економією на її складових.

5. Розроблено рекомендації щодо покращення побудови системи управління інформаційною безпекою. Особливу увагу треба виділити знаходженню та оцінки ризиків, загроз та можливих матеріальних та репутаційних втрат організації, щоб правильно оцінити економічну доцільність побудови СУІБ. Для управління будь-якої складної системою необхідно створити жорсткий, але простий регламент обслуговування цієї системи і забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту.

6. На основі узагальнення запропоновано структурну модель інформаційної безпеки систем, що базується на положеннях комплексного підходу. Пропонована структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах полягає в аналізі її основних компонентів: визначенні головних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту.

7. Окрім системного підходу, доцільно врахувати і положення процесного підходу до моделювання систем інформаційної безпеки: наявність мети процесу, тобто бажаного результату захисту інформації, зміни предметної області, в якій реалізується процес, обмеженість необхідних ресурсів на виконання операцій і дій, безперервність процесу, комплексність та розмежування процесу.

8. На основі інтеграції зазначених підходів запропоновано формалізовану модель інформаційної безпеки, яка є функцією з множини області значень складових системи інформаційної безпеки і передбачає, що постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування

інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

9. На основі аналізу наукових джерел, міжнародних та вітчизняних стандартів і рекомендацій, зроблено спробу систематизації принципів та формалізації процедур розробки систем управління інцидентами інформаційної безпеки. Також, на базі часткових узагальнень, визначено фази життєвого циклу інцидентів та наведено компоненти типової системи управління інцидентами інформаційної безпеки. Крім того, показано номенклатуру європейських груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

Таким чином, отримані результати та рекомендації є науково-методичною та практичною базою для вдосконалення процесу управління інцидентами інформаційної безпеки підприємств та спрямовані на підвищення ефективності їх господарської діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

2. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

3. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах / Гладиш С.В. // Реєстрація, зберігання і обробка даних. — 2018 — Т. 10, № 1. — С. 116–124.

4. Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ "ЗІДМУ", 2012. - 292 с.

5. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Х.: «ФОЛІО», 2012. – 296 с.

6. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

7. ДСТУ ISO/IEC 27035-2:2018 Информационные технологии. Методы защиты. Управление инцидентами информационной безопасности. Часть 2. Руководство по планированию и подготовке к реагированию на инциденты (ISO/IEC 27035-2:2016, IDT) від 10.12.2018.

8. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 21–22.

9. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. — К.: НАН України 209. — 149 с.

10. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. — К.: НАН України 2019. — 149 с.

11. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2020. — 163 с. — (Галузевий стандарт України).

12. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [проект]. - К.: Національний банк України 2020. – 163 с. : табл. – (Галузевий стандарт України).

13. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2010. — 163 с. — (Галузевий стандарт України).

14. Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерсово освіти і науки України, СБУ. – К. – 2017. – С. 17-21.

15. Ковтун С. В. Інформаційна безпека: підручник / С.В. Ковтун. – Харків. Вид. ХНЕУ, 2019. – 368 с.

16. Кожунова О.О. Забезпечення інформаційної безпеки на сучасному підприємстві // Школа науки. - 2018. - №2. - С. 19-21.

17. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

18. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. — Одеса : ОНАЗ ім. О.С. Попова, 2019. — 208 с.

19. Концепція створення та забезпечення функціонування інфраструктури захисту державних інформаційних ресурсів в інформаційно - телекомунікаційних системах. [Електронний ресурс] – Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=16D68 FCE54A40938081139F546DD E47B?art_id=38814&cat_id=38712

20. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

21. Малькевич Р. Проблеми забезпечення безпеки інформації підприємства в умовах пандемії / Р. Малькевич, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.69-72).

22. Мамаєва Л.М., Кондратьєва О.А. Основні напрями забезпечення інформаційної безпеки підприємства // Інформаційна безпека регіонів. - 2016. - №2. - С. 5-9.

23. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки

життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

24. Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій / І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк // Восточноевропейский журнал передовых технологий. — 2012. — № 2 (56). — С. 18–21.

25. Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій / І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк // Восточноевропейский журнал передовых технологий. — 2012. — № 2 (56). — С. 18–21.

26. Морозов А. В. Сохранность ресурсов автоматизированных информационных финансово-экономических и бухгалтерских систем / А. В. Морозов, Ю. А. Родичев // Междунар. науч.-техн. конф. «Измерение, контроль, информатизация». – ИКИ-2000. – Барнаул, 2020. – С . 148-151.

27. НД ТЗІ 1.3-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – 30 с.

28. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі. – 32 с.

29. Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв’язку. Рекомендація МСЭ-Т Е.409 (ITU-T E.409. — [Чинне від 2004-28-05]. — Женева. — 22 с. — (Рекомендація Міжнародної організації телекомунікацій (ITU)).

30. Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв’язку. Рекомендація МСЭ-Т Е.409 (ITU-T E.409. — [Чинне від 2004-28-05]. — Женева. — 22 с. — (Рекомендація Міжнародної організації телекомунікацій (ITU)).

31. Потий А. В. Формальная модель процесса защиты информации / А. В. Потий // Радіоелектрон. і комп'ют. системи. – 2016. – №5. – С. 128-133.

32. Пошаговое руководство по созданию CSIRT (Европейское агентство по сетевой и информационной безопасности (ENISA) в рамках программы WP-2006), 2016. — 86 с.

33. Пошаговое руководство по созданию CSIRT (Европейское агентство по сетевой и информационной безопасности (ENISA) в рамках программы WP-2006), 2016. — 86 с.

34. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. [Електронний ресурс] – 2009. – 143 с. – Режим доступу: www.isofts.kiev.ua

35. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

36. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

37. Critical infrastructure companies and the global cybersecurity threat // McKinsey Global Institute. 2019. Жовтень. - [Електронний ресурс]. - Режим доступу: https://www.mckinsey.com/business-functions/risk/our-insights/critical-nfrastructurecompanies-and-the-global-cybersecurity-threat# (дата звернення 20.12.2019).

38. European Network and Information Security Agency [Electronic resource] : ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2018]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.

39. European Network and Information Security Agency [Electronic resource] : ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2012]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.

40. GFI Security survey in the United States. [Електронний ресурс] – 2017. – Режим доступу: www.gfi.com

41. Harrison M. Protection in operating systems / M. Harrison, W. Ruzzo, J. Ullman // Communication of ACM. – 1976. – № 19(8). – P. 461-471.

42. Information technology - Security techniques - Information security incident management (IDT) : ISO/IEC TR 18044:2014. – 76 с.

43. Information technology. Security techniques. Information security incident management (ISO 18044:2004) : ГОСТ Р ИСО/МЭК 18044:2004. — [Чинний від 2008-07-01]. — М. : Федеральное агенство по техническому регулированию и метрологии 2017. — 50 с. — (Нац. стандарт РФ).

44. Information technology. Security techniques. Information security incident management (ISO 18044:2004) : ГОСТ Р ИСО/МЭК 18044:2004. — [Чинний від 2008-07-01]. — М. : Федеральное агенство по техническому регулированию и метрологии 2017. — 50 с. — (Нац. стандарт РФ).

45. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST). – Publ. 800-86. – 2016.

46. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2013. — 223 p.

47. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2013. — 223 p.

48. O.Polotai, Kukharska, N., Lagun, A. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 174–177.

49. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE

16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

50. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

51. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.