Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління інформаційною безпекою, д.т.н.,
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“____” _____2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему **Вплив людського фактору на системи організації інформаційної безпеки та способи його оптимізації**

Виконав:
здобувач IVкурсу, групи КБ-41
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Оксана ЗАНИК
(прізвище та ініціали)
Керівник Ростислав ТКАЧУК
(прізвище та ініціали)
Рецензент Ірина АРТИЩУК
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Заник (Сас) Оксана «Вплив людського фактору на системи організації інформаційної безпеки та способи його оптимізації». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 62 с., 5 рис, 2 табл.

Об’єкт – системи організації інформаційної безпеки.

Предметом дослідження – людський фактор.

Мета роботи – оптимізація впливу людського фактору на системи організації інформаційної безпеки.

Методи дослідження – аналіз літературних джерел з теми дослідження, порівняльний аналіз вимог до впровадження систем управління інформаційною безпекою.

В дипломній роботі описані ризики пов’язані з людським фактором. Проведено аналіз моделей та процесів забезпечення кібербезпеки. Наведені методи оцінки інформаційної безпеки. Визначені процеси забезпечення кібербезпеки на підприємстві. Проаналізовано міжнародне законодавство у сфері інформаційної безпеки. Розглянуті аспекти впровадження системи управління інформаційною безпекою на підприємстві. Виконаний аналіз методів збору експертної інформації для розслідування інцидентів кібербезпеки, наведений аналіз загроз, висунуті вимоги до критерії захисту інформації. Для виявлення загроз інформаційної безпеки та каналів витоку інформації розроблено лист опитувальник працівників підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЛЮДСЬКИЙ ФАКТОР, РИЗИК, ЗАХИСТ ІНФОРМАЦІЇ, РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ.

ABSTRACT

Zanyk (Sas) Oksana "The impact of the human factor on the systems of information security and ways to optimize it." Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 62 pages, 5 figures, 2 tables.

Object - information security systems.

The subject of research - the human factor.

The purpose of the work is to optimize the impact of the human factor on the systems of information security.

Research methods - analysis of literature sources on the research topic, comparative analysis of requirements for the implementation of information security management systems.

The thesis describes the risks associated with the human factor. The analysis of models and processes of cybersecurity is carried out. Methods of information security assessment are given. The processes of cybersecurity at the enterprise are defined. The international legislation in the field of information security is analyzed. Aspects of implementation of information security management system at the enterprise are considered. The analysis of methods of collecting expert information for the investigation of cybersecurity incidents is performed, the analysis of threats is given, the requirements to the criteria of information protection are put forward. To identify threats to information security and channels of information leakage, a questionnaire was developed for employees of the enterprise.

INFORMATION SECURITY, HUMAN FACTOR, RISK, INFORMATION PROTECTION, INCIDENT INVESTIGATION.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

Як показали результати аналізу літературних даних та статистики, значна частина інцидентів кібербезпеки, що приводили до витоку конфіденційних даних, відбувалася з вини співробітників компанії, випадково або навмисно провокували втрату цінної інформації.

Описані ризики пов’язані з людським фактором. Проведено аналіз моделей та процесів забезпечення кібербезпеки. Наведені методи оцінки інформаційної безпеки.

Визначені процеси забезпечення кібербезпеки на підприємстві. Проаналізовано міжнародне законодавство у сфері інформаційної безпеки. Розглянуті аспекти впровадження системи управління інформаційною безпекою на підприємстві.

Виконаний аналіз методів збору експертної інформації для розслідування інцидентів кібербезпеки, наведений аналіз загроз, висунуті вимоги до критерії захисту інформації.

Для експерта з розслідування інцидентів розроблено лист для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації.

Дана робота дає можливість сформувати загальні представлення про процес розслідування інцидентів кібербезпеки пов’язані з людським фактором.

Запровадження організаціями процесу розслідування інцидентів кібербезпеки дозволить:

- підвищити рівень кібербезпеки;
- посилити увагу до попередження інцидентів шляхом віднаходження винних у його виникненні та його причин;
- знизити негативні наслідки на бізнес-процеси організації;
- дозволить скоректувати політику інформаційної безпеки організації.

За результатами дипломної роботи були досягнуті наступні завдання:

- проведено аналіз законодавчої бази та міжнародних стандартів з

розслідування інцидентів кібербезпеки;

- проведено аналіз методів збору експертної інформації для розслідування інцидентів кібербезпеки;
- наведений аналіз загроз;
- розроблено лист для опитування працівників підприємства (менеджер, економіст, програміст, системний адміністратор та інші) для виявлення загроз ІБ та каналів витоку інформації пов’язаних із людським фактором;
- визначено основні моделі розслідування інцидентів кібербезпеки;
- проаналізовано процес розслідування інцидентів кібербезпеки;

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. Реагування та обробка інцидентів інформаційної безпеки в мережі GSM // Вісник Державного університету інформаційно - комунікаційних технологій. - 2008. - № 1. - с. 58-72.

4 Гладиш С.В., Кононович В.Г., Тардаскін М.Ф. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2013. - № 15. - с. 31-39.

5 Довганич М. О. Методи та засоби захисту персонального інформаційного простору в контексті мережевої розвідки / М. О. Довганич, В. І. Ящук // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С. 79-81).

6 Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. - К. : НІСД, 2011. - 30 с.

7 Єрохін А.Л. Модель візуалізації нештатних подій у складних інформаційних системах // Зв’язок. - 2009. - № 6. - С. 52-56.

8 Закон України «Про захист інформації в інформаційно - телекомунікаційних системах» № 2594-IV від 31.05.2006.

2009. Интеллектуальные системы управления организационно-техническими системами / Под ред. проф. А.А. Большакова. - М.: Горячая Линия - Телеком, -160 с.

9 Конвенція про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575.

10 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= 6D68FCE54A40938081139F546DD E47B?art_id=38814&cat_id=38712.

11 Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв'язок. - 2011. - № 1. - С. 39-45.

12 Кримінальний кодекс України: Закон України // Відомості Верховної Ради України - 2001. - № 25-26. - Ст. 131.

13 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.

2010. Малюк А. Информационная безопасность: концептуальные и методологические основы защит информации. - М.: Горячая линия - Телеком, - 280 с.

14 Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки: зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). - К. : Вид-во НА СБ України, 2011. - Ч. 2. - С. 43-48.

15 Национальная стратегия кибербезопасности (NCSS). От понимания к возможности.- Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. - [Електронний ресурс]. - Режим доступу: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security- strategies-

ncsss/NCSS2Engelseversie.

16 НД ТЗІ 1.3-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

17 НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

18 Офіційний сайт Міжнародного фонду збору інформації про комп'ютерні інциденти в світі DataLossDB [Електронний ресурс]. - Режим доступу: http://Datalossdb.org/statistics.

19 Полотай О., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у2 ч. Ч. 2. – Київ: Нац. акад. СБУ, 2016. – С. 204-205.

20 Порядок захисту державних інформаційних ресурсів у інформаційно - телекомунікаційних системах. - Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р.

21 Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373.

22 Про Доктрину інформаційної безпеки України : указ Президента України [Електронний ресурс]. - Режим доступу: http ://zakon2.rada.gov.ua/laws/show/514/2009.

- Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : закон України від 9.01.2007 р. № 537-V [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/ laws/show/537-16.

23 Про Стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007.

24 Сакович Л.М., Політов В.І. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. - 2012. - № 5. - С. 37-39.

25 СБУ: Головні проблеми для України - тероризм і кіберзлочинність // Українська Правда [Електронний ресурс]. - Режим доступу: http ://www.pravda.com.ua/news/2012/03/23/6961285.

26 Соколов М.С. Кибернетическая безопасность - понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. - 2012. - № 1. - [Електронний ресурс]. - Режим доступу: http ://db.inforeg .ru/ eni/ artList.asp ?j =4&id=0220913464&idfull=0421200099.

27 Статистичні дані країн, які є постачальниками спаму [Електронний ресурс]. - Режим доступу: https://securelist.ru/analysis/ksb/24580/kaspersky- security-bulletin-2014-osnovnaya-statistika-za-2015-god/.

28 Статистичні дані щодо DDoS-атак у країнах світу [Електронний ресурс]. - Режим доступу: https://www.infowatch.ru/report2015-2016.

29 Статистичні дані, щодо витоку конфіденційної інформації [Електронний ресурс]. - Режим доступу: https://www.antimalware.ru/.

30 Статистичні данні про ризики зіткнення з веб-програмами[Електронний ресурс]. - Режим доступу: https://securelist.ru/analysis/ksb/27543/kaspersky- security-bulletin-2015-osnovnaya-statistika-za-2015-god/.

31 Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. - Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754.

32 Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. - 2012. - № 2. - С. 162-169.

33 Ящук В.І. Принципи проектування автоматизованих інформаційних систем управління об'єктами критичної інфраструктури матеріали Міжнародної науково-практичної конференції "Сучасні напрями розвитку економіки,

підприємництва, технологій та їх правового забезпечення” 02-03 червня 2021 року м. Львів.

34 Canada’s Cyber Security Strategy: For a stronger and more prosperous Canada. - Her Majesty the Queen in Right of Canada, 2010. - 14 с. - [Електронний ресурс]. - Режим доступу: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

35 COBIT - Цілі контролю за інформаційними та суміжними технологіями, 2012 р.

36 ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги».

37 ISO/IEC 27032:2012 «Інформаційні технології - Методи забезпечення безпеки - Керівництво з кібербезпеки».

38 ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки».

39 Securing Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies [Електронний ресурс]. - Режим доступу: http://csis.org/files/media/csis/pubs/081208securingcyberspace_44.pdf.

40 U.S. Department of Justice, Federal Bureau of Investigation Internet Crime Report 2015.