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
“_10_” _лютого_2022 року

ДИПЛОМНА РОБОТА
МАГІСТРА

на тему **Дослідження рівня ефективності сучасних систем захисту корпоративних мереж в приватних структурах**

Виконав:
здобувач VI курсу, групи КБ-61м
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління
інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Олег КЛЕНИК
(ім’я та прізвище))
Керівник Ростислав ТКАЧУК
(ім’я та прізвище))
Рецензент Наталя ЛИСА
(ім’я та прізвище)

Львів – 2022 року

АНОТАЦІЯ

Кленик Олег Володимирович «Дослідження рівня ефективності сучасних систем захисту корпоративних мереж в приватних структурах».

Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 4 розділи, 88 с., 7 рис, 8 табл.

Об’єкт – процес створення комплексних систем захисту корпоративних мереж.

Предмет дослідження – методи і засоби захисту корпоративних мереж.

Мета роботи – аналіз шляхів впровадження чи підвищення ефективності систем захисту корпоративних мереж.

Методи дослідження – аналіз літературних джерел та інформаційних WEB-ресурсів з теми дослідження, порівняльний аналіз вимог до побудови корпоративних мереж, існуючих рішень та засобів захисту, математичний апарат теорії імовірності.

У роботі розглянуто питання захисту інформації від несанкціонованого доступу, вдосконалення систем, та використання існуючих технологічних рішень. У роботі виконаний аналіз поточного стану засобів захисту інформації в мережах. Розглянуті їх переваги та недоліки. Також були розглянуті основні типи атак на мережі, з ціллю розуміння принципів їх дії, для побудови якісної системи захисту мереж. Також в роботі був використаний математичний апарат теорії імовірності для визначення порушення критичних властивостей інформаційного активу на основі CVSS.

ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖІ, ТЕХНІЧНИЙ ЗАХИСТ, ІНФОРМАЦІЯ, АТАКИ, ЗАСОБИ ЗАХИСТУ, СТРУКТУРА ЗАХИСТУ.

ABSTRACT

Oleh Klenyk, "Modern systems of corporate networks protection in private structures efficiency level research".

Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 4 sections, 88 pages, 7 figures, 8 table.

Object - the process of creating comprehensive security systems for corporate networks.

The subject of research - methods and means of protection of corporate networks.

The purpose of the work is to analyze ways to implement or increase the effectiveness of corporate network protection systems.

Research methods - analysis of literature sources and information WEB-resources on the research topic, comparative analysis of requirements for building corporate networks, existing solutions and means of protection, mathematical apparatus of probability theory.

The issues of protection of information from unauthorized access, improvement of systems, and use of existing technological solutions are considered in the work. The analysis of the current state of information security in networks is performed in the work. Their advantages and disadvantages are considered. The main types of attacks on the network were also considered, in order to understand the principles of their operation, to build a quality system of network protection. The mathematical apparatus of probability theory was also used to determine the violation of the critical properties of the information asset based on CVSS.

INFORMATION SECURITY, NETWORKS, TECHNICAL PROTECTION, INFORMATION, ATTACKS, MEANS OF PROTECTION, STRUCTURE OF PROTECTION.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

В дипломній роботі було вирішено завдання аналізу та класифікації загроз у комп’ютерних мережах. Також було розглянуто метод загальної оцінки вразливостей CVSS. Крім того, досліджено методи захисту комп’ютерних мереж та надано рекомендації щодо їх впровадження в комп’ютерну мережу. Встановлено, що існуючі методи захисту не повинні застосовуватися поодинці, а для побудови якісної системи захисту слід використовувати комплекс рішень. Також було описано підхід до проектування системи IT-безпеки компанії та запропоновано план дій щодо інцидентів у сфері безпеки. Враховуючи переваги та недоліки засобів мережевої безпеки та рекомендації щодо побудови комплексної системи безпеки мережі, було змодельовано систему безпеки мережі. Потім за допомогою математичного апарату теорії ймовірностей були розраховані ймовірності порушення критичних властивостей для інформаційних значень мережі.

Проведено порівняльний аналіз локальної мережі підприємства до та після впровадження заходів захисту. Показано, що запропонована система інформаційної безпеки має місце через зниження показників ймовірності порушення критичних властивостей інформаційних активів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 8 основних рубежів захисту комп’ютерних мереж [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.it-lines.ru/blogs/security/ osnovnye-metody-zashhity-korporativnoj-seti.

2. А.Кичма, О.Полотай Загрози безпеки Wi-Fi мереж та основні протоколи захисту. "Інформаційна безпека та інформаційні технології": Збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів учених, студентів і курсантів. – Львів, 2021. – С. 49-51.

3. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // 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.121-124).

4. В. Балацька, В. Ящук, О. Полотай. Використання сканерів вразливостей для захисту комп’ютерної мережі навчального закладу. VI Міжнародна науково-практична конференція «Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи», Л. ЛДУ БЖД, 2021.

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. Закон України «Доступ до публічної інформації» [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/ 2939-17.

7. 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.

8. Захист мережі: комплексний підхід [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://goo.su/16VM.

9. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. 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. 52–54.

10. Концепції захисту IT-інфраструктури від сучасних загроз [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://netwave.ua/ru/ kontseptsy-ya-zashhy-ty-y-t-y-nfrastruktury-ot-sovremenny-h-ugroz.

11. Мережні атаки [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html.

12. Методи захисту мереж [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://studopedia.su/6_4733_metodi-zashchiti-setey.html.

13. Рекомендації інформаційної безпеки для малого та середнього бізнесу [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post 348892.

14. Росляков О. О. Віртуальні приватні мережі. Основи побудови та застосування / О. О. Росляков, С. В. Попов. – Київ: Еко-трендз, 2006. – 301 с. Snader J. J. VPNs illustrated: Tunnels, VPN’s and IPsec / John Junior Snader., 2006. – 445 с.

15. Структура локальної мережі підриємства [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.sviaz-expo.ru/ru/articles/struktura-lokalnoj-seti-predpriyatiya.

16. Чому потрібен план реагування на кіберінциденти [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://nv.ua/ukr/biz/experts/chomu-potriben-plan-reaguvannya-na-kiberincidenti-

17. Ящук В.І. Методологія наукового пізнання та онтологія наукових досліджень в процесі професійної підготовки фахівців з кібербезпеки // В. Ящук, М. Навитка / матеріали VI Міжнародної науково-практичної конференції «Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи» 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).

18. 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.

19. 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.

20. 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.

21. 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.

22. Terri W. O. Firewalls. Практичне застосування міжмережевих екранів / William Olgtri Terri. – Київ: ДМК Пресс, 2001. – 400 с. – (Захист та адміністрування).