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
“_28_” _травня_2021 року

ДИПЛОМНА РОБОТА
БАКАЛАВРА

на тему **Дослідження та оптимізація систем виявлення та захисту інформації від несанкціонованого доступу до серверу ЦОЗТС та ІТ ГУ ДСНС України у Херсонській області**

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Сергій ЖИГІН
(прізвище та ініціали)
Керівник Ростислав ТКАЧУК
(прізвище та ініціали)
Рецензент Наталя ЛИСА
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Жигін Сергій «Дослідження та оптимізація систем виявлення та захисту інформації від несанкціонованого доступу до серверу ЦОЗТС та ІТ ГУ ДСНС України у Херсонській області».

Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 65 с., 17 рис, 1 табл.

Об’єкт – серверне приміщення та сервер.

Предмет дослідження – вибір доступних і запровадження додаткових систем для захисту інформації від несанкціонованого доступу.

Мета роботи – вдосконалити технічну систему захисту інформації в локальній мережі та серверній.

Методи дослідження – аналіз літературних джерел та інформаційних WEB-ресурсів з теми дослідження, порівняльний аналіз вимог до побудови серверних приміщень, існуючих рішень та засобів захисту до локальної мережі серверів.

У даній дипломній роботі розглянуто питання захисту інформації від несанкціонованого доступу, вдосконалення систем, та використання існуючих технологічних рішень. Розглянуто та проаналізовано склад системи її функціональні та технічні особливості під час її створення. Проведено порівняльний аналіз існуючих вимог і методів захисту серверних приміщень та серверів. Зокрема проведений аналіз рівня криптографічного та технічного захистів інформації.

ІНФОРМАЦІЙНА БЕЗПЕКА, ТЕХНІЧНИЙ ЗАХИСТ, ІНФОРМАЦІЯ, ТЕХНІЧНО-ПРОГРАМНИЙ ЗАХИСТ, СЕРВЕР, СЕРВЕРНЕ ПРИМІЩЕННЯ.

ABSTRACT

Zhyhin Serhiy, "Research and optimization of systems for detection and protection of information from unauthorized access to the server of the Center for Emergency Situations and IT of the State Emergency Service of Ukraine in Kherson region."

Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 65 pages, 17 figures, 1 table.

Object - server room and server.

The subject of research - the selection of available and the introduction of additional systems to protect information from unauthorized access to the local network of the server.

The purpose of the work is to improve the technical system of information protection in the local network and on the server.

Research methods - analysis of literature sources and information WEB-resources on the research topic, comparative analysis of requirements for the construction of server rooms, existing solutions and security tools for the local network of servers.

This thesis considers the protection of information from unauthorized access, improvement of systems and use of existing technological solutions. The composition of the system, its functional and technical features during its creation are considered and analyzed. A comparative analysis of existing requirements and methods of protection of server rooms and servers. In particular, an analysis of the level of cryptographic and technical protection of information.

INFORMATION SECURITY, TECHNICAL PROTECTION, INFORMATION, TECHNICAL AND SOFTWARE PROTECTION, SERVER, SERVER PREMISES.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

За період виконання дипломної роботи бакалавра ми дослідили тему захисту серверу та серверного приміщення ЦОЗТС та ІТ ГУ ДСНС України у Херсонській області від несанкціонованого доступу. Дізналися можливі слабкі місця локальної мережі головного управління, через які кіберзлочинець або порушник може здійснити атаку, вивівши з ладу сервер зменшуючи його дієздатність, знищити важливу інформацію або викриваючи секретну інформацію з пристроїв для її зберігання, наносячи непоправної шкоди репутації управління, та дискредитувавши роботу відділу захисту інформації.

Згідно нашого дослідження основними такими слабкими місцями можуть бути:

- доступ до машин, за допомогою "чорних ходів"– атаки, яка може загрожувати виконанням користувачами несанкціонованих операцій на сервері, що атакується; застосування можливостей ПЗ, не задекларованих розробниками;
- помилки в програмах – SMTP-серверах (SMTP problems);
- фізичний доступ до серверного приміщення користувачів які не мають спеціального допуску до роботи з апаратним забеспеченням

Використовуючи вимоги та будову банківської мережі, і наданою керівником документацією про побудову серверного приміщення у структурі ДСНС та Нормативних документів Технічного захисту інформації і різної методичної літератури, ми прийшли до висновку, що для оптимізації захисту інформації, необхідно додаткове грошове забезпечення відділу для купівлі:

- Raid-контролера;
- міжмережевого екрану Cisco;
- встановлення ліцензійного програмного забезпечення Cisco;
- застосування системи контролю та управління для унеможливлення доступу до серверного приміщення фахівцями з інших відділів або сторонніми особами, які не мають на це відповідного дозволу.

Основним нашим рішенням було написання сторінки скриптовою мовою програмування PHP створеною для генерації HTML-сторінок на стороні веб-сервера, розробленої нами для :

- адміністрування системи керування та управління доступом до серверного приміщення
- створення єдиної бази номерів карток ідентифікаторів, закріплених за кожним працівником кому він виданий, за його прізвищем
- авторизації та ідентифікації працівників для входу, за допомогою брелка або картки ідентифікатора;
- автоматичного відкривання дверей, у разі вдалої автентифікації
- ведення таблиці з Датою та Часом входу і виходу користувача до серверного приміщення
- автоматичного закривання дверей

За допомогою цієї оптимізації захисту серверу, та серверного приміщення ЦОЗ та ІТ ГУ ДСНС України у Херсонській області, можна бути впевненим у тому що, захист від несанкціонованого доступу побудований згідно вимог, з використанням найсучасніших технологій, і ми готові до протидії атакам, головне постійне оновлення програмного забезпечення, постійний пошук вразливостей та негайне їх усунення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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).

2. 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.

3. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.

4. 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

5. Денис Колисниченко, Linux От новичка к профессионалу. 7 изд.

6. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України. – 1994. – № 16. – с. 93.

7. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.

8. Закон України “Про основи національної безпеки України”// Урядовий кур’єр, 30 липня 2003 р.

9. Закон України “Про основи національної безпеки України”// Урядовий кур’єр, 30 липня 2003 р.

10. 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.

11. Звіт Cisco “Оцінка рівня інцидентів ІБ за 2018 рік”

12. Зубок М. І. Безпека банківської діяльності: Навч. Посібник / М. І. Зубок. – К.: КНЕУ, 2002. – 190 с.

13. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. –Харків: Вид. ХНЕУ, 2008. –352 с.

14. Конституція України. – Урядовий кур’єр. – 13 липня 1996 р.

15. Левицкий Н. Удаленный сервер своими руками. От азов создания до практической работы - М.: ДМК Пресс, 2019. - 476с.

16. Наказ 20.07.2004 N 466 «Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнання»

17. Наказ ДСНС 23.10.2019 № 608 «Вимоги до інженерної інфраструктури технологічних приміщень (серверних) для розміщення серверного та телекомунікаційного обладнання ВЦТМ»

18. Платонов В.В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж: навч. посібник для студ. вищ.навч. закладів / В.В. Платонов. -М. : Видавничий центр «Академія», 2006. - 240

19. Полотай О., Довганик С. SIEM-системи, як елемент аналізу та управління подіями CSOC. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції. – Черкаси, 2020. - С.60-61.

20. Полотай О., Довганик С. Системи збору інформації про безпеку та управління подіями. Захист інформації в інформаційно-комунікаційних системах : зб. тез. ІІІ Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С. 7-9.

21. Проектування та монтаж локальних комп'ютерних мереж І. М. Журавська

22. Секрети і брехня. Безпека даних в цифровому світі / Б. Шнайер. СПб : Пітер, 2003. - 368 с.

23. Средства противодействия атакам Семенов Ю.А. (ГНЦ ИТЭФ) [Електронний ресурс] Режим доступу: http://book.itep.ru/6/defence.htm

24. Страхарчук А.Я. Інформаційні системи і технології в банках.

25. Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічні науки. – 2016. – № 3. – С. 120-127.

26. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

27. Nam H Nguyen: Essential Cyber Security Handbook In Ukrainian Стаття Wikipedia, RAID (англ. *Redundant Array of Independent Disks*) — технологія віртуалізації даних [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/RAID

28. 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.

29. 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.

30. 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.