

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.

« ____ » _____ 2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Основні проблеми при побудові моделей захисту інформації в комп'ютерній мережі захищеної лабораторії

Виконав:

студент 4-го курсу, групи КБ-41,
спеціальності 125

«Кібербезпека»

(шифр і назва спеціальності)

Віталій Фарбітнік

(прізвище, ім'я, по батькові)

Керівник Андрій Лагун

(прізвище та ініціали)

Рецензент Рашкевич Марія

(прізвище та ініціали)

АНОТАЦІЯ

Віталій Фарбітнік «Основні проблеми при побудові моделей захисту інформації в комп'ютерній мережі захищеної лабораторії». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи 56 с., 7рис., 20 джерел.

Об'єктом дослідження є захист інформації в комп'ютерній мережі.

Мета роботи – проаналізувати моделі захисту інформації в комп'ютерній мережі на прикладі захищеної лабораторії.

Методи дослідження – дослідити сучасні загрози комп'ютерних мереж, проаналізувати методи захисту інформації в комп'ютерних мережах, розробити рекомендації щодо побудови моделі захисту інформації в комп'ютерній мережі.

У першому розділі розглядаються причини захисту інформації. Досліджуються комп'ютерні мережі та види загроз комп'ютерним мережам. В другому розділі розглядаємо методи захисту інформації в комп'ютерній мережі, основні моделі захисту, проблеми при розробці системи безпеки інформації. У третьому розділі досліджено аналіз та рекомендації до моделі захисту інформації, засоби захисту інформації від несанкціонованого доступу в РОМ, системний підхід до захисту, а також рекомендації щодо покращення безпеки інформації

ANOTATION

Vitaliy Farbitnyk "The main problems in building models of information security in the computer network of a secure laboratory." Thesis on the specialty 125 "Cybersecurity" consists of a text that contains 3 sections of 54 pages, 7 figures, 20 sources.

The object of research is the protection of information in a computer network.

The purpose of the work is to analyze the models of information security in a computer network on the example of a secure laboratory.

Research methods - to investigate modern threats to computer networks, to analyze methods of information security in computer networks, to develop recommendations for building a model of information security in a computer network.

The first section discusses the reasons for protecting information. Computer networks and types of threats to computer networks are studied. In the second section we consider methods of information protection in a computer network, the main models of protection, problems in developing an information security system. The third section examines the analysis and recommendations for the model of information protection, means of protecting information from unauthorized access to ROM, a systematic approach to protection, as well as recommendations for improving information security

Зміст

Оглавление	5
Вступ.....	Помилка! Закладку не визначено.
Розділ 1. Причини захисту інформації.....	Помилка! Закладку не визначено.
1.1 Комп'ютерні мережі	Помилка! Закладку не визначено.
1.2 Види загроз комп'ютерним мережам	Помилка! Закладку не визначено.
Висновок до Розділу 1	Помилка! Закладку не визначено.
Розділ 2. Методи захисту інформації в комп'ютерній мережі.....	Помилка!
Закладку не визначено.	
2.1 Методи захисту інформації	Помилка! Закладку не визначено.
2.2 Основні моделі захисту інформації комп'ютерної мережі.....	Помилка!
Закладку не визначено.	
2.3 Проблеми при розробці системи безпеки інформації.....	Помилка! Закладку не визначено.
Висновок до Розділу 2	Помилка! Закладку не визначено.
Розділ 3. Аналіз та рекомендації до моделі захисту інформації	Помилка!
Закладку не визначено.	
3.1 Аналіз засобів захисту інформації в комп'ютерних мережах.....	Помилка!
Закладку не визначено.	
3.1.1 Засоби захисту інформації від несанкціонованого доступу в РОМ	Помилка! Закладку не визначено.
3.1.2 Системний підхід до захисту	Помилка! Закладку не визначено.
3.2 Рекомендації щодо покращення безпеки інформації.....	Помилка! Закладку не визначено.
Висновок до Розділу 3	Помилка! Закладку не визначено.
Висновки	6

Список використаних джерел	8
----------------------------------	---

Висновки

Застосування інформаційних технологій (ІТ) вимагає підвищеної уваги до питань інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати значних матеріальних збитків. Без належної ступеня захисту інформації впровадження ІТ може виявитися економічно не вигідним в результаті значних втрат конфіденційних даних, що зберігаються і обробляються в комп'ютерних мережах.

Реалізація рішень, що забезпечують безпеку інформаційних ресурсів, істотно підвищує ефективність всього процесу інформатизації в організації, забезпечуючи цілісність, справжність і конфіденційність дорогої інформації, що циркулює в локальних і глобальній інформаційних середовищах.

Таким чином, лабораторія має на увазі комплексну безперервну систему захисту даних. Відповідно, при розробці та побудові комплексної системи захисту інформації необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, виробництва, експлуатації та розвитку захищаються ресурсів. Вибір методів захисту – це досить складна оптимізаційна задача, і при її вирішенні необхідно прораховувати ймовірність виникнення загроз безпеці інформації, вартість реалізації тих чи інших способів захисту та ін. Крім того, система захисту повинна постійно вдосконалюватися разом з розвитком обчислювальної інфраструктури. Проте, основною вразливістю системи захисту лабораторії є люди.

Проблема побудови моделі захисту інформації в комп'ютерній мережі захищеної лабораторії буде вирішена, тільки якщо створена і безвідмовно функціонує комплексна система захисту інформації, що охоплює весь життєвий цикл обчислювальної інфраструктури, починаючи від розробки і до її знищення, а також весь технологічний ланцюжок збору, зберігання і обробки інформації, що захищається.

Ціль дипломної роботи успішно досягнена.

Задачі дипломної роботи виконані:

- 1) Досліджено сучасні загрози комп'ютерних мереж;
- 2) Проаналізовано методи захисту інформації в комп'ютерних мережах;
- 3) Розроблені рекомендації щодо побудови моделі захисту інформації в комп'ютерній мережі.

У цій дипломній роботі були розкриті питання причин захисту інформації, цілей та методів, розглядані основні моделі захисту інформації, зі зверненням уваги на основні проблеми при побудові моделей на прикладі комп'ютерної мережі захищеної лабораторії та надані рекомендації при побудові моделей.

Список використаних джерел

1. Балацька В.С., Шабатура М.М. Сканери вразливості комп'ютерної мережі. Захист інформації в інформаційно-комунікаційних системах: матеріали III Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 р. / ЛДУ БЖД. Львів, 2019.С. 34-36.
2. 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).
3. Войтович В.С., Гриник Р.О. Дослідження надійності використання протоколу IPsec для створення VPN. Зб. тез доповідей Всеукраїнська науково-практична інтернет-конференція “Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку” (м. Черкаси, 13-19 березня 2017 р.). Черкаси, 2017. С. 66-68.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах / Учеб. пособие для вузов. – М., 2001.
5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999.
6. Мирошник М.А. Диагностические эксперименты в системах защиты информации на сетях клеточных автоматов. / М.А. Мирошник, Я.Ю.Королева // Інформаційно-керуючі системи на залізничному транспорті. – 2009. – №4. – С. 142–145.
7. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2014. – №5. – с. 66-70.
8. Мирошник М.А. Методы эффективного кодирования внутренних

состояний микропрограммных автоматов. / М.А. Мирошник, Я.Ю.Королева, // Технология приборостроения. – 2011. – №1. – С. 12–16.

9. Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2008. – 225 с.

10. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.

11. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

12. 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).

13. Miroshnik M. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis. /Miroshnik M., Kovalenko M. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – №6, с.36-45.

14. 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. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

15. 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.

16. 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.

17. Osborn, S., Sandhu, R., and Nunawer, Q. Configuring Role-Based Access

Control To Enforce Mandatory And Discretionary Access Control Policies. ACM Trans. Info. Syst. Security, 3, 2, 2000.

18. Ravi S. Sandhu, Pierangela Samarati: Access Control: Principles and Practice. IEEE Communication Magazine 1994.

19. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., and Youman, C.E. Role-based access control models. Computer, 29:38-47, Feb. 1996.

20. Steve Demurjian: Implementation of Mandatory Access Control in Role-based Security System. 2001.