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 УІБ
д.т.н. доц. Ткачук Р.Л.
_____
“____” _____2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Дослідження стану інформаційної безпеки мережевих протоколів системи електронної пошти

Виконав:
студент 4 курсу,
групи КБ-41, спеціальності 125
«Кібербезпека»
(шифр і назва спеціальності)
Владислав МЕЛЬНИК
(прізвище, ім’я, по батькові)

Керівник Володимир САМОТИЙ
(прізвище та ініціали)

Рецензент Богдан МІЗЮК
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Владислав Мельник «Дослідження стану інформаційної безпеки мережевих протоколів системи електронної пошти». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 73 с., 8 рис., 6 табл., 44 джерел.

Об'єктом дослідження є мережеві протоколи системи електронної пошти.

Мета роботи – розглянути методи і засоби захисту мережевих протоколів системи електронної пошти.

Методи дослідження – вивчення наукової літератури з теми дослідження, нормативно-правової бази, аналітичний і порівняльний методи, методи системного аналізу.

У першому розділі досліджено організацію служби електронної пошти в мережі Інтернет, зокрема описано роль і функції електронної пошти та ризики, які пов’язані з використанням електронної пошти. В другому розділі описані мережеві протоколи системи електронної пошти, а саме протокол SMTP та POP3. В третьому розділі проведено дослідження, щодо основних методів і засобів захисту мережевих протоколів системи електронної пошти. Захист розглядався через призму додатків та IP.

СИСТЕМА ЕЛЕКТРОННОЇ ПОШТИ, МЕРЕЖЕВІ ПРОТОКОЛИ, ЗАХИСТ ІНФОРМАЦІЇ

ABSTRACT

Vladislav Melnyk "Investigation of the information security status of network protocols of the e-mail system". Thesis in the specialty of 125 "Cybersecurity" consists of textual part that contains 3 sections, 73 pages, 8 figures, 6 tables, 44 sources.

The object of the study are network protocols of the e-mail system.

The purpose of the work is to consider the methods and means of protection of network protocols of the e-mail system.

Research methods - the study of scientific literature on the research topic, regulatory framework, analytical and comparative methods, methods of systems analysis.

The first section examines the organization of e-mail on the Internet, including the role and functions of e-mail and the risks associated with the use of e-mail. The second section describes the network protocols of the e-mail system, namely SMTP and POP3. The third section conducts research on the main methods and means of protection of network protocols of the e-mail system. Protection was considered through the prism of applications and IP.

E-MAIL SYSTEM, NETWORK PROTOCOLS, INFORMATION PROTECTION

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

Таким чином, електронна пошта - це служба пересилання повідомлень між зареєстрованими адресами. Спочатку мова йде тільки про текстових повідомленнях у вузькому сенсі; про пересилання двійкового вмісту. Під текстовими повідомленнями у вузькому сенсі розуміються повідомлення, що складаються з рядків обмеженої довжини, кожен рядок складається з алфавітно-цифрових символів базового набору ASCII і розділових знаків (такі повідомлення також називають 7-бітовими).

Електронна пошта (E-mail) - сервіс передачі електронних повідомлень, для використання якого потрібна поштова програма. Лист може містити не тільки текстову інформацію, але і будь-який приєднаний до нього файл. Розвиток технології Internet привело до появи сучасних протоколів для обміну повідомленнями. Ці протоколи надають великі можливості для обробки листів, різноманітні сервіси та зручність у роботі. Зараз приблизно з однаковою ймовірністю можна зустріти приклади роботи електронної пошти по протоколу UUCP (Unix to Unix cp, де cp - команда, яка використовується в системі UNIX для копіювання файлів) і сучасні протоколи - SMTP (Simple Mail Transport Protocol), POP3 (Post Office Protocol, version 3) і IMAP (Internet Mesage Access Protocol).

Протокол обміну поштової інформацією POP3 призначений для розбору пошти з поштових скриньок користувачів на їх робочі місця за допомогою програм-клієнтів. Якщо по протоколу SMTP користувачі відправляють кореспонденцію через Internet, то по протоколу POP3 користувачі отримують кореспонденцію зі своїх поштових скриньок на поштовому сервері в локальні файли

Протокол SMTP призначений для відправки повідомлень з комп'ютера далі до адресата. Працює він у відповідності з архітектурою клієнт-сервер. Звичайно доступ до сервера SMTP не захищається паролем, так що ви можете використовувати для відправки ваших листів будь-який відомий сервер в мережі.

На відміну від серверів для відправки листів, доступ до серверів для зберігання ваших повідомлень захищається паролем. Тому необхідно використовувати сервер або службу, в якій існує ваш обліковий запис. Ці сервери працюють по протоколах POP і IMAP, які розрізняються способом зберігання листів.

У дипломній роботі були розглянуті системи захисту, що існують в даний час і забезпечують надійну передачу даних (по e-mail).

У захисті на рівні додатків були розглянуті системи PGP і S / MIME. PGP (англ. Pretty Good Privacy) - комп'ютерна програма, що дозволяє виконувати операції шифрування (кодування) і цифрового підпису повідомлень, файлів та іншої інформації, представленої в електронному вигляді.

У PGP застосовується принцип використання двох взаємопов'язаних ключів: відкритого і закритого. Це означає, що якийсь користувач може повідомити про своє публічному ключі всьому світу, при цьому інші користувачі програми можуть надсилати йому зашифровані повідомлення, які ніхто, крім нього, розшифрувати не зможе.

S / MIME призначена для забезпечення криптографічного безпеки електронної пошти. Забезпечуються аутентифікація, цілісність повідомлення та гарантія збереження авторства, безпеку даних (за допомогою шифрування). Велика частина сучасних поштових програм підтримує S / MIME. Стандарт S / MIME включає в себе дві служби безпеки: цифрові підписи, шифрування повідомлень. Ці дві служби є головними компонентами системи безпеки, заснованої на стандарті S / MIME.

Іншим рішенням є розміщення засобів забезпечення безпеки стандарт SSL (Secure Socket Layer - протокол захищених сокетів) і його більш нова вер¬сія - стандарт TLS (Transport Layer Security - протокол захисту транспортно¬го рівня) безпечної передачі даних в Internet. На цьому рівні для практичної реалізації даного підходу є дві можливості. Найбільш загальним рішенням є впровадження засобів SSL (або TLS) в набір відповідних протоколів, що забезпечує прозорість засобів захисту для додатків. У той же

час кошти SSL можна вбудовувати і в прикладні програми. Різні засоби захисту можуть вбудовуватися і в додатки. Перевага даного підходу полягає в тому, що відповідні засоби захисту можуть бути налаштовані оптимальним чином в залежності від вимог конкретного застосування.

Захист на рівні IP Security - це комплект протоколів, що стосуються питань шифрування, аутентифікації і забезпечення захисту при транспортуванні IP-пакетів; в його склад зараз входять майже 20 пропозицій по стандартам і 18 RFC.

Перевага використання IPSec полягає в тому, що цей протокол прозорий для кінцевого користувача і додатків і обеспечі¬вает універсальне рішення. Крім того, протокол IPSec включає засоби фільтрації, що дозволяють використовувати його тільки для тієї частини потоку дан¬них, для якої це дійсно необхідно.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акулов О.А., Медведев Н.В. Информатика: базовый курс. –М.: Омега, 2004. –551 с.

2. Андрончик, А. Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков ; под общ. ред. Н. И. Синадского. – Екатеринбург : Изд-во Урал. ун-та, 2014. – 180 с..

3. Бен-Ари М. Языки программирования. Практический сравнительный анализ. –М.: Мир, 2000. –366 с.

4. Березин С. Internet у вас дома - СПб, 1997. - 400 с.

5. Бройдо В.Л., Матвеев Л.А., Макарова Н.В. Информатика. –М.: Финансы и статистика, 2001. –768 с.

6. 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).

7. 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.

8. 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.

9. 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.

10. 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.

11. Галатенко В.А. «Основы информационной безопасности», изд. Интуит, 2005г.

12. Галатенко В.А. «Стандарты информационной безопасности», изд. Интуит, 2005г.

13. Герасименко В.А., Малюк А.А. Основы защиты информации.М.: МОПО РФ, МИФИ, 1997, 537 с.

14. Гордеев А.В. Операционные системы. Учебник для ВУЗов. –М. Питер, 2004. –416 с.

15. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

16. Гулевич Д. С. Сети связи следующего поколения - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2007 г., 184 с.

17. Информатика. Учебник под ред. А.П.Алексеев, М. «Солон-р», 2002 г.

18. Кнут Д.Э. Искусство программирования, т. 1. Основные алгоритмы, 3-е изд. -М.: Вильямс, 2000. -720 с.

19. Кнут Д.Э. Искусство программирования, т. 3. Сортировка и поиск, 2-е изд. -М.: Вильямс, 2000. -832 с.

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. Лапонина О.Р. «Межсетевое экранирование», 2006г. М. ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 343с

22. Лапонина О.Р. «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия», 2005г. М. ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 672с.

23. Левин Д.Р., Бароди К. Секреты Интернет. - К.: Диалектика, ICE, 1996.

24. Миков А.И., Королев Л.Н. Информатика. Введение в компьютерные науки. – М: Высшая школа, 2003. –341 с.

25. Новиков Ю.В., Кондратенко С.В Основы локальных сетей - ИНТУИТ.ру, 2005 г., 360 с.

26. О.Белей, Н.Мальцева, О.Полотай Фізичний зміст комп'ютерної стеганографії. Вісник Львівського Державного університету безпеки життєдіяльності Том 23 (2021):. С. 27-32.

27. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Спб.: Издательский дом Питер, 2002

28. Олифер Н.А., Олифер В.Г. Сетевые операционные системы. Изд-во «Питер», 2003

29. Основы криптографии: Учебное пособие. /Алферов А.П., Зубов А.Ю., Кузьмин А.С. Черемушкин А.В. - М.: Гелиос, 2001.

30. Петраков А.В. Основы практической защиты информации. М.: Радио и связь, 1999, 368с.

31. Прикладная криптография. /Б. Шнайер. - М.: Издательство ТРИУМФ,2002.

32. Себеста У. Основные концепции языков программирования. – М.: Вильямс, 2001. –672 с.

33. Семенов. Ю.А. Протоколы и ресурсы Интернет. - М.: Радио и Связь, 1996.

34. Столингс В., Криптография и защита сетей: принципы и практика, 2-е издание: пер. с английского – М, : Издательский дом «Вильямс», 2001.

35. Таненбаум Э.Компьютерные сети. СПб.: Издательский дом Питер, 2003

36. Темерев А. Интернет из Книги рекордов Гиннеса // Мир Internet. – 2001. – №11.

37. Ульман Д., Хопкрофт Д., Ахо А. Структуры данных и алгоритмы. – М.: Вильямс, 2000. –384 с.

38. Хаулет Т. Защитные средства с открытыми исходными текстами - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2007 г., 608 с.

39. 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).

40. Anthes C.H.. Интернет: история будущего // ComputerWorld. – 1994. – №45. – С. 22–23.

41. Bryan Costales, Eric Allman «Sendmail Desktop Reference» - O'Reilly, First Edition, March 1997

42. Bryan Costales, Eric Allman «Sendmail» - O'Reilly, Second Edition, January 1997.

43. Craig Hunt «TCP/IP Network Administration», 3.4. Mail Services; 10. sendmail; Appendix E. A sendmail Reference - O'Reilly, Second Edition, December 1997.

44. 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.