УДК 004.77
DOI https://doi.org/10.32782/2663-5941/2025.1.2/25

Омецинская Н.В.
Таврійський національний університет імені В.І. Вернадського

Гуйда О.Г.
Таврійський національний університет імені В.І. Вернадського

Кучерявий В.М.
Таврійський національний університет імені В.І. Вернадського

Вишемірська Я.С.
Таврійський національний університет імені В.І. Вернадського

Боженко М.І.
Senior Infrastructure Engineer, Lotusflare

ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ SMTP-СЕРВЕРУ (POSTFIX)

У зв'язку з постійним зростанням кількості кібератак і загроз інформаційної безпеки, захист обчислювальних ресурсів поштових серверів стає критично важливим завданням для організацій різного масштабу.

У статті розглянуто роль та місце SMTP-сервера в параметризації поштового сервера як ключового елемента електронної поштової системи. SMTP (Simple Mail Transfer Protocol) є основним протоколом для передавання електронної пошти між серверами, що забезпечує доставку повідомлень у глобальній мережі Інтернет. Параметризація поштового сервера, зокрема SMTP-сервера, є важливим аспектом для забезпечення його надійності, безпеки, продуктивності та масштабованості. Правильна конфігурація SMTP-сервера визначає, як обробляються, надсилаються та отримуються електронні листи, а також як забезпечується захист від спаму, фішингу та інших кіберзагроз.

Стаття присвячена вивченню методів і засобів захисту SMTP-сервера на прикладі Postfix – одного з найпоширеніших і гнучких рішень для обробки електронної пошти. Postfix забезпечує високу продуктивність і надійність роботи, проте в умовах сучасних загроз потребує додаткових заходів безпеки для протидії різним типам атак, таким як спам, фішинг, DoS-атаки та спроби несанкціонованого доступу.

Проведено аналіз архітектури Postfix та його основних компонентів, що дозволяє виявити потенційні вразливості і шляхи їх усунення. Розглянуто механізми автентифікації (SMTP AUTH), авторизації та контролю доступу, включаючи використання SSL/TLS для забезпечення безпечного з'єднання, захисту від атак типу "людина посередині" та шифрування даних під час передачі. Належний моніторинг дозволяє виявляти аномалії у функціонуванні сервера та своєчасно реагувати на можливі загрози, такі як спроби несанкціонованого доступу або атаки типу DoS.

Визначено ефективні підходи до конфігурації Postfix для зменшення навантаження на сервер та підвищення його продуктивності, зокрема за рахунок оптимізації роботи з чергами, управління потоками та використання механізмів кешування.

Результати цього дослідження можуть бути корисними для системних адміністраторів, фахівців з інформаційної безпеки, а також дослідників, які займаються вивченням проблем захисту інформаційних систем і мереж.

Ключові слова: *захист SMTP-сервера, Postfix, кібербезпека, авторизація та контроль доступу, шифрування SSL/TLS, фільтрація спаму, захист від фітингу, DoS-атаки, інформаційна безпека поштових серверів, протидія кібератакам.*

Постановка проблеми. У сучасному цифровому світі електронна пошта залишається одним із ключових засобів комунікації як для особистих, так і для корпоративних потреб. Однак зростання кількості кібератак і їхня складність значно підвищують ризики, пов’язані з використанням поштових серверів. SMTP-сервери [1, 2], такі як Postfix [3, 4], регулярно стають мішенями для різних типів атак, включаючи спуфінг, фішинг, розсилку спаму, DoS-атаки та спроби несанкціо-

нованого доступу [5]. Це зумовлює необхідність аналізу, розробки та впровадження ефективних механізмів захисту, які здатні забезпечити надійний захист обчислювальних ресурсів поштового сервера та захистити конфіденційну інформацію від компрометації.

Аналіз останніх досліджень і публікацій: На сьогоднішній день захист SMTP-серверів від кіберзагроз є однією з актуальних тем у сфері інформаційної безпеки. Останні дослідження зосереджуються на розробці та впровадженні нових методів і технологій для підвищення захищеності поштових серверів, зокрема на прикладі широко використовуваного SMTP-сервера Postfix. У цьому контексті варто відзначити кілька ключових напрямів досліджень [6]:

– Автентифікація та захист переданої інформації

– Реалізація політик безпеки SPF, DKIM і DMARC

– Методи фільтрації спаму та шкідливого ПЗ

– Моніторинг та журналювання

– Оптимізація продуктивності SMTP-серверів

– Інтеграція з іншими технологіями**.**

Постановка завдання. Метою даної статті є аналіз існуючих засобів і технологій захисту обчислювальних ресурсів SMTP-серверу (Postfix) від несанкціонованого використання у контексті ОС Linux. Розглянуто основні методи захисту, перспективи їх розвитку та надано рекомендації щодо покращення конфігурації та впровадження нових технологій.

Виклад основного матеріалу. Комп'ютерна безпека, також знана як кібербезпека або безпека інформаційних технологій (IT-безпека), спрямована на забезпечення захисту комп'ютерних систем і мереж від витоку, крадіжки або пошкодження даних, апаратного та програмного забезпечення, а також від порушень чи неправильного використання наданих послуг. Ця галузь отримала значний розвиток завдяки зростанню залежності від комп'ютерних систем, Інтернету та бездротових мереж, таких як Bluetooth і Wi-Fi, а також завдяки поширенню "розумних" пристроїв, включно зі смартфонами, телевізорами та різноманітними пристроями Інтернету речей (IoT). Кібербезпека є важливим викликом сучасного світу через її складність як з політичної, так і з технологічної точки зору. Основна мета кібербезпеки – забезпечити конфіденційність, цілісність і доступність даних у системі [8].

З моменту виникнення Інтернету та поширення цифрових технологій питання кібербезпеки стали невід'ємною частиною як професійної, так і приватної діяльності. Кібербезпека та кіберзагрози зберігають свою актуальність протягом останніх півстоліття, супроводжуючи розвиток технологій. У 1970-х та 1980-х роках комп'ютерна безпека здебільшого цікавила наукові установи, але із розширенням доступу до Інтернету почали виникати комп'ютерні віруси та атаки на мережі. 1990-ті роки ознаменувалися поширенням вірусів, а у 2000-х роках спостерігалася інституціоналізація кіберзагроз і впровадження механізмів кібербезпеки. З 2010-х років стали звичними масштабні атаки та урядові регуляторні ініціативи. Важливою віхою у становленні кібербезпеки було засідання у квітні 1967 року, організоване Віллісом Уером на Весняній конференції з питань комп'ютерів. Публікація його звіту стала основою для розвитку галузі [9].

У 1977 році Національний інститут стандартів і технологій (NIST) представив концепцію "тріади ЦРУ" (конфіденційність, цілісність, доступність), яка стала базовою для визначення цілей безпеки. У 1970-х і 1980-х роках основні загрози комп'ютерній безпеці були обмеженими, оскільки технології лише починали свій розвиток. У той час основними проблемами були несанкціонований доступ до даних та файлів. Проте вже у другій половині 1970-х років компанії, такі як IBM, почали пропонувати системи контролю доступу та програмне забезпечення для безпеки [10].

Першою комп'ютерною програмою, яка ілюструє загрози безпеці, був хробак Creeper, створений у 1971 році Бобом Томасом з BBN. У 1972 році Рей Томлінсон розробив антивірус Reaper для боротьби з Creeper. Згодом у 1986–1987 роках було зафіксовано перший випадок кібершпигунства, здійснений групою німецьких хакерів під керівництвом Маркуса Гесса. У 1988 році хробак Морріса привернув широку увагу до кіберзагроз, а у 1990-х розпочалася розробка протоколів безпеки, таких як SSL, для захисту інформації в Інтернеті.

У 1993 році компанія Netscape розпочала розробку протоколу SSL після того, як Національний центр суперкомп'ютерних додатків (NCSA) запустив Mosaic 1.0 – перший веб-браузер. У 1994 році Netscape підготувала першу версію SSL 1.0, яка, однак, не була випущена через численні вразливості, зокрема атаки повторного відтворення та можливість модифікації незашифрованих повідомлень хакерами. У лютому 1995 року була опублікована версія SSL 2.0.

Агентство національної безпеки (АНБ) США відповідає за захист національних інформаційних

систем і водночас здійснює збір іноземної розвідки. Ці функції часто конфліктують між собою: забезпечення безпеки включає виявлення вразливостей і їх усунення, тоді як розвідка вимагає використання цих слабких місць для отримання інформації. Усунення вразливостей позбавляє АНБ можливості використовувати їх у наступальних цілях.

АНБ аналізує популярне програмне забезпечення, шукаючи вразливості, які можуть бути використані для конкурентних переваг США. У більшості випадків агенція не повідомляє розробників про знайдені слабкі місця, зберігаючи їх у таємниці. Такий підхід працював до певного часу, але згодом інші країни, такі як Росія, Іран, Північна Корея та Китай, також здобули наступальні можливості та почали використовувати їх проти США. Інструменти АНБ для атак, спочатку створені для американських установ, зрештою опинилися в руках супротивників. Наприклад, у 2016 році інструменти АНБ були зламані та використані Росією й Північною Кореєю. Крім того, деякі співробітники АНБ перейшли на роботу до іноземних організацій, сприяючи розвитку їхніх кіберздатностей.

У сучасному світі Агентство національної безпеки (АНБ) відіграє подвійну роль у кібербезпеці: воно одночасно відповідає за захист інформаційних систем США та за збір іноземної розвідки. Це створює суперечність між оборонними та наступальними діями, такими як використання вразливостей у програмному забезпеченні для збору даних. Наприклад, у 2007 році Сполучені Штати та Ізраїль використали недоліки в операційній системі Microsoft Windows для атаки на ядерну інфраструктуру Ірану, що спонукало Іран до розробки власних кібервійськових потужностей.

Для захисту комп'ютерних систем важливо розуміти потенційні атаки, які поділяються на такі категорії:

- **Бекдори** – приховані механізми, що дозволяють обійти стандартні процедури автентифікації чи інші засоби безпеки. Вони можуть бути створені навмисно розробниками для забезпечення доступу до системи або виникати через неправильну конфігурацію програмного забезпечення. Наприклад, бекдори можуть використовуватися для законного віддаленого управління системою, але у випадку, коли такі механізми потрапляють у руки зловмисників, це створює значну загрозу. Вразливість бекдорів полягає у тому, що їх важко виявити – найчастіше їх можуть ідентифікувати лише фахівці з доступом до вихідного коду чи глибоким знанням операційної системи. Існують програмні засоби для виявлення бекдорів, однак їх ефективність залежить від складності самої загрози. Приховані бекдори можуть бути використані для крадіжки конфіденційних даних, створення бот-мереж або для інших шкідливих дій.
- **Атаки відмови в обслуговуванні (DoS)** – це тип атак, спрямованих на те, щоб зробити комп'ютерну систему або мережевий ресурс недоступним для законних користувачів. Зловмисники здійснюють такі атаки, створюючи перевантаження ресурсів системи. Це може включати надмірну кількість запитів, що призводить до виснаження ресурсів (процесорної потужності, оперативної пам'яті чи пропускної здатності мережі). Більш складним варіантом є **розподілені атаки відмови в обслуговуванні (DDoS)**, які реалізуються за допомогою численних джерел, таких як зомбі-комп'ютери в бот-мережах. Такі атаки ускладнюють ідентифікацію джерела та нейтралізацію загрози. Існують різні види DoS-атак:
  - **Флудинг-атаки**, під час яких система отримує надмірну кількість трафіку.
  - **Атаки виснаження ресурсів**, спрямовані на знищення апаратних чи програмних можливостей.
  - **Протокольні атаки**, що використовують уразливості у протоколах зв'язку.

  Методи захисту від таких атак включають використання міжмережевих екранів (брандмауерів), систем виявлення аномалій, балансування навантаження та інші стратегії. Хмарні сервіси також пропонують спеціалізовані інструменти для боротьби з DDoS-атаками, забезпечуючи масштабованість ресурсів і автоматичне реагування.
- **Фізичний доступ** – несанкціонований користувач, отримавши доступ до обладнання, може копіювати дані або змінювати систему, встановлюючи шкідливе програмне забезпечення. Для запобігання таким атакам використовують шифрування та модулі захисту, як-от Trusted Platform Module.
- **Підслуховування** – перехоплення комунікацій між системами, включаючи використання електромагнітних випромінювань (наприклад, за стандартом TEMPEST).
- **Поліморфні загрози** – новий тип багатовекторних атак, що змінюють форму для обходу систем захисту.
- **Фішинг** – отримання конфіденційної інформації через обман, зазвичай за допомогою підроблених електронних листів або веб-сайтів.
- **Підвищення привілеїв** – несанкціоноване збільшення прав доступу, що дозволяє звичайним користувачам отримати контроль над системою.

- **Зворотна інженерія** – аналіз програмного забезпечення для виявлення його структури та принципів роботи, що може використовуватися як для досліджень, так і для злочинних цілей.

Висновки. У статті було розглянуто та проаналізовано сучасні методи й технології захисту ресурсів SMTP-сервера (Postfix) від несанкціонованого використання.

Список літератури:

1. Simple Mail Transfer Protocol URL: https://datatracker.ietf.org/doc/html/rfc5321 (date of access: 19.01.2025).

2. TCP SYN Flooding Attacks and Common Mitigations URL: https://datatracker.ietf.org/doc/html/rfc4987#appendix-A (date of access: 19.01.2025).

3. Postfix Documentation URL: http://www.postfix.org/documentation.html (date of access: 19.01.2025).

4. Postfix SMTP relay and access control. *The Postfix Home Page*. URL: https://www.postfix.org/SMTPD_ACCESS_README.html (date of access: 19.01.2025).

5. Deploying mail servers | Red Hat Product Documentation. *Red Hat Product Documentation*. URL: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/deploying_mail_servers/index (date of access: 01.02.2025).

6. Cartier G., Cartier J. F., Fernandez J. M. Next-Generation DoS at the Higher Layers: A Study of SMTP Flooding. Network and System Security. NSS 2013. Lecture Notes in Computer Science. – Berlin, Heidelberg: Springer, 2013. Vol. 7873. P. 149–163. DOI: 10.1007/978-3-642-38631-2_12.

7. Deibert R. J. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*. 2018. Vol. 32, no. 4. P. 411–424. URL: https://doi.org/10.1017/s0892679418000618 (date of access: 19.01.2025).

8. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)

9. Гуйда О. Г., Кисельов В. Б., Омецинська Н.В. Інформаційні системи для оцінювання кіберзагроз. Challenges and threats to critical infrastructure. Collective monograph. Detroit, Michigan, USA, 2023. P. 161–163.

10. Омецинська Н. В., Гуйда О. Г., Прокопенко І. Ю. «Дослідження технологій інформаційного пошуку для використання в семантичній мережі», The 4th International scientific and practical conference “Current challenges of science and education” (December 11-13, 2023) MDPC Publishing, Berlin, Germany.

Ometsinska N.V., Guida O.G., Kucheriavyi V.M., Vishemirska Ya.S., Bozhenko M.I. MISSCE SMTP SERVER IN THE MAIL SERVER PARAMETERS

Due to the constant increase in the number of cyber attacks and threats to information security, protecting the computing resources of mail servers is becoming critically important m for organizations of various sizes.

The article examines the role of the SMTP server in the parameterization of the mail server as a key element of the electronic mail system. SMTP (Simple Mail Transfer Protocol) is the main protocol for transferring electronic mail between servers, which ensures delivery across the global Internet. Parameterization of the mail server, or SMTP server, is an important aspect for ensuring its reliability, security, productivity and scalability. The correct configuration of the SMTP server determines how emails are processed, manipulated, and deleted, as well as how protection against spam, phishing, and other cyber threats is ensured.

The article is devoted to the development of methods and features of protecting the SMTP server on the Postfix application – one of the most advanced and flexible solutions for processing electronic mail. Postfix ensures high productivity and reliability of the robot, protecting against current threats will require additional security steps to counter various types of attacks, such as spam, phishing, DoS attacks and unauthorized access attempts.

An analysis of the Postfix architecture and its main components was carried out, which allows us to identify potential applications and ways of their subtraction. The mechanisms of authentication (SMTP AUTH), authorization and access control are reviewed, including the use of SSL/TLS to ensure secure connection, protection from man-in-the-middle attacks and encryption of data during transmission. Proper monitoring allows you to detect anomalies in a functioning server and promptly respond to possible threats, such as unauthorized access attempts or DoS attacks.

Effective approaches to configuring Postfix have been identified to change the focus on the server and increase its productivity, focusing on the optimization of work with drawers, flow control and alternative caching mechanisms.

The results of this investigation may be of benefit to system administrators, information security officers, and investigators who investigate security problems in information systems and security systems.

Key words: *SMTP server protection, Postfix, cyber security, authorization and access control, SSL/TLS encryption, spam filtering, fitting protection, DoS attacks, information security of mail servers, prevention of cyber attacks.*