user profiles. Visitors who will be first to be on the Web site or a web resource of any organization should be judged by the quality and importance of published materials.

For large web resources, there is an urgent task of emergency navigation and search user support. It can be solved by the personalization of content based on the needs and behaviors of the end user. When you personalize the web pages will be dynamically change the content of the web resource to the specific needs of the user. As a result, the user will "communicate" with the web page, but the site itself will appeal to anyone who got to the page, not as part of the total mass, and as to the particular person that has their personal interests, personally. To address the issue of clustering was chosen the algorithm of CLOPE, which is suitable for clustering large amounts of data. The algorithm CLOPE, during operation, is maintained a small amount of data for each cluster, with a minimum number of scans. The purpose of this article is to publish the results of the study of modern trends in the use of clustering in solving the problem of personalization.

Keywords: *site personalization, web resource, algorithm, clustering, user*
Рецензент: доцент, канд. техн. наук Міроненко Д.С.
Статья поступила

УДК 004.42

Міроненко Д. С.[1], Вонярха О.В.[2]

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ І ПРАЦЕЗДАТНОСТІ КОРПОРАТИВНОГО ПОШТОВОЇ СЕРВЕРА

На сьогоднішній день існує достатня кількість різних як платних, так і безкоштовних поштових сервісів, які надають прийнятний рівень зручності використання. У статті описані методи реалізації поштового сервісу на основі досліджень в області структурної організації пошти підприємства, а так само практичних випробувань поштових серверів, бізнес призначення, в середніх і великих IT-компаніях.

Наведено варіант підбору програмного-стека з актуальних на даний момент елементів відкритого програмного забезпечення, які виконують конкретну роль в роботі поштового сервера. Описані передові практики використання сучасних технологій захисту передачі конфіденційної інформації в момент передачі через глобальну мережу. А також актуальні методи валідації власної пошти, та її захисту від підміни третіми особами. Представлені основні методи захисту від спаму, і захисту користувачів від небажаної пошти. Дані методи і практики, можна використовувати як посібник для організації поштового сервера, або ж як рекомендації під час налаштування сервера з подібною специфікою.

Було встановлено, що реалізація зручного поштового сервісу на базі відкритого програмного забезпечення може бути виконано на основі програмного забезпечення Postfix спільно з Dovecot. Postfix повністю відповідає поставленим вимогам, з можливістю роботи в тандемі з іншими елементами стека, він є простим в подальшому адмініструванні. Dovecot – найефективніше рішення прийому електронної пошти у зв'язці з Postfix, в сфері

[1]*завідувач кафедри інформатики, доцент, кандидат технічних наук ДВНЗ «Приазовський державний технічний університет», м. Маріуполь, mironenko_ds@ukr.net*
[2]*бакалавр, ДВНЗ «Приазовський державний технічний університет», м. Маріуполь, happyvaran28@gmail.com*

відкритого програмного забезпечення. Дане рішення було випробувано у декількох середніх компаніях.

В ході випробувань по черзі впроваджувалися технології захисту поштових обмінів, такі як SSL і DKIM, кожна впроваджувана технологія продемонструвала себе як актуальний і важливий елемент роботи сучасних поштових сервісів, відмова від якого наражає користувачів пошти до серйозного ризику.

Результати досліджень звелися до практичної реалізації моделі поштового сервера, яка використовує передові технології в цій галузі і відповідає сучасним вимогам безпеки.

Ключові слова: *програмний-стек, відкрите програмне забезпечення, електронна пошта, сервер, кластер, Postifx, Dovecot, SSL, SpamAssasin, безпека даних, e-mail.*

Вступ. Представники середнього і великого бізнесу рано чи пізно стикаються з питаннями безпеки і зберігання інформації, в свою чергу, одним з основних інструментів обміну інформацією, в діловій сфері, є електронна пошта. І хоча в наш час, пропонується безліч різних сервісів обміну електронною поштою, коли від втрати даних або «витоку» інформації може залежати доля підприємства, продумана реалізація власного поштового сервісу стає невід'ємною необхідністю.

Аналіз останніх досліджень і публікацій. На сьогоднішній день існує достатня кількість різних як платних, так і безкоштовних поштових сервісів, які надають прийнятний рівень зручності використання. Якщо завдання електронної пошти полягає у вирішенні питань бізнес сегмента, де інформація має певну цінність для роботи підприємства, тоді в використанні зовнішніх поштових сервісів виявлені значні мінуси:

– немає можливості керувати поштою повноцінно. Фактично поштовий сервіс не належить підприємству, знаходиться не на його серверах, до нього немає повноцінного доступу;

– немає можливості точно знати, що відбувається в даний момент з файлової частиною електронної пошти;

– немає можливості прогнозування проблем;

– немає гарантій що не відбудеться витоку інформації з боку сервера;

– немає можливості організувати повноцінне резервне копіювання;

– немає повноцінних можливостей розмежування доступів до пошти.

А проблеми в мережевих сегментах можуть і зовсім відрізати підприємство від поштового сервісу. У світлі подібних недоліків, сформовані певні вимоги:

- зручності використання сервісу користувачем;
- безпеки зберігання даних;
- працездатність;
- безпеки передачі даних;
- захист користувача від небажаної пошти.

За підсумками дослідження, було виявлено, що найбільш ефективним рішенням реалізації, корпоративного поштового сервісу підприємства – є об'єднання програмних елементів в програмний стек. У свою чергу, кожен елемент обрано для виконання строго певної ролі, в якій він виявляється найбільш ефективним рішенням.

Було встановлено, що реалізація зручного поштового сервісу на базі відкритого програмного забезпечення може бути виконано на основі програмного забезпечення Postfix спільно з Dovecot [1-3]. Postfix повністю відповідає поставленим вимогам, з можливістю роботи в тандемі з іншими елементами стека, він є простим в подальшому адмініструванні. Dovecot – найефективніше рішення прийому електронної пошти у зв'язці з Postfix, в сфері відкритого програмного забезпечення. Дане рішення було випробувано у декількох середніх компаніях.

Безпека передачі в середовищі всесвітньої мережі забезпечується за рахунок шифрування трафіку на рівні протоколу передачі, для чого була обрана технологія SSL [4] з використанням SSL сертифікатів. Метод дозволяє убезпечити передачу аутентифікаційних даних користувача на поштовому сервері, а також виключає можливість витоку інформації в разі перехоплення листів зловмисником в глобальній мережі, так як без наявності сертифіката, зловмисник не зможе прочитати вміст перехоплених електронних пакетів даних.

Дуже важливим аспектом роботи поштового сервера є фільтрація вхідної пошти. Дане питання розібрано в статті [5], в якій описується необхідність реалізації фільтрації вхідних електронних листів, з метою збереження кінцевого користувача від небажаної пошти, так як це може негативним чином позначитися на зручності в роботі. У сфері відкритого програмного забезпечення, відповідно до цієї концепції, було обрано і випробувано програмний продукт SpamAssasin [6]. Кваліфікована конфігурація цього продукту може повністю покрити вимоги фільтрації. Виходячи з цього, його буде додано в програмний-стек.

Для захисту від підміни електронної пошти може бути застосована технологія: DomainKeys Identified Mail [7] – метод аутентифікації, розроблений для виявлення підробки повідомлень, що пересилаються по email. Метод дає можливість одержувачу перевірити, що лист дійсно було відправлено з заявленого домену. DKIM спрощує боротьбу з підробленими адресами відправників, які часто використовуються в фішингових листах і в поштовому спам. Замість традиційної IP-адреси, для визначення відправника DKIM додає в нього цифровий підпис, пов'язаний з ім'ям домена організації. Підпис автоматично перевіряється на стороні одержувача, після чого, для визначення репутації відправника, застосовуються білі списки і чорні списки.

Також, ефективним рішенням є технологія SPF [8], яка є актуальним інструментом з організації захисту від підміни пошти досліджуваного сервера. SPF розшифровується як Sender Policy Framework, що можна перевести як «інфраструктура політики відправника». Це розширення для протоколу відправки електронної пошти через SMTP, яке дозволяє додати DNS записи типу TXT до доменного імені і вказати в цих записах IP адреси серверів, з яких дозволена відправка електронної пошти.

SPF використовується як фактор підвищення довіри до вихідної від домену пошти, з метою зниження ймовірності попадання листів в «Спам». Репутація домену, яку SPF дозволяє захистити, також має не останнє значення. При розсилці спаму або підроблених листів, зловмисники можуть підставити в поле «Від» будь-яку адресу в будь-якому домені, що може стати причиною проблем для власника такого домену. IP адресу поштового сервера, з іншого боку, підробити неможливо, тому коли SPF запис для домену є, приймаюча сторона перевіряє її і діє відповідно.

Метою даної статті є висвітити основні тенденції, відпрацьовані практики, і практичні рішення в сфері організації та адміністрування поштових серверів корпоративного призначення. У свою чергу, результати дослідження можна використовувати керівництвом підприємства як відправну точку в проектуванні поштового сервісу.

Виклад основного матеріалу. Для аналізу ефективності основних технологій захищеного поштового обміну були проведені тести обміну поштою між випробуваним сервером і популярними в Україні поштовими сервісами gmail.com, ukr.net, i.ua, meta.ua. В ході випробувань основні технології впроваджувалися поступово в порядку черги, і потім отримані результати порівнювалися з аналогічними випробуваннями без використання технологій. Кожен експеримент представляв собою відправку ста листів, де кожен успішно доставлений лист представляв 100% успіху, в свою чергу листи, які не пройшли перевірку помічені спамом, або ж не прийняті, були представлені 0% успіху.

Для генерації і швидкого відправлення листів був використаний php-скрипт:

```
$to= "Mary <mary@example.com>" . ", " ;
$to .= "Kelly <kelly@example.com>";
$subject = "Birthday Reminders for August";
$message = ' <html> <head>  <title>Birthday Reminders for August</title> </head> <body>
<p>Here are the birthdays upcoming in August!</p>
<table>
 <tr> <th>Person</th><th>Day</th><th>Month</th><th>Year</th>  </tr>
 <tr> <td>Joe</td><td>3rd</td><td>August</td><td>1970</td>  </tr>
 <tr> <td>Sally</td><td>17th</td><td>August</td><td>1973</td>  </tr>
</table> </body> </html>';
$headers= "MIME-Version: 1.0\r\n";
$headers .= "Content-type: text/html; charset=iso-8859-1\r\n";
$headers .= "From: Birthday Reminder <birthday@example.com>\r\n";
$headers .= "Cc: birthdayarchive@example.com\r\n";
$headers .= "Bcc: birthdaycheck@example.com\r\n";
mail($to, $subject, $message, $headers);
```

Висновки за результатами випробувань базувалися на відповідях сервера при спробі передачі листа, скануванні трафіку на стороні випробуваного сервера за допомогою TCPDUMP, загального сканування трафіку між клієнтом і сервером за допомогою програми WireShark, а так само дані отримані через веб-інтерфейс поштового сервісу. Для розрахунку працездатності сервера враховувалися втрати поштового трафіку виробленого сервером протягом доби, після чого результат втрат порівнювався з внутрішніми балами сервера.

Експеримент №1 – першим експериментом стала відправка листів з сервера без будь-яких налаштувань доменної валідації. Результати експерименту представлені в таблиці 1 та на рисунку 1.

Таблиця 1 – Результати експерименту без доменної валідації

Поштовий сервіс	Успішне отримання	Позначені як спам	Відкинуто сервером
gmail.com	0%	20%	80%
ukr.net	3%	97%	0%
i.ua	61%	39%	0%
meta.ua	0%	30%	70%

Ситуація, коли кілька листів проходять у вхідні, а потім починають потрапляти в спам, або ж спочатку в спам, а потім листи починають відкидатися, відбувається через те, що після подолання деякого ліміту вхідних листів, які не підлягають валідації на стороні поштового сервісу, адреса відправника заноситься в «сірий список».

Після потрапляння до цього списку, реакція на лист сервера змінюється відповідно до налаштувань безпеки. Дану ситуацію можна побачити шляхом сканування вихідного трафіку, за допомогою утіліти tcpdump.

Слід зазначити, що різниця в результатах дій поштових серверів, полягає в різних налаштуваннях політики реакцій на листи, які не вдалося повністю перевірити, і ідентифікувати.

Після настройки технологій Domain Validation: Dkim, DMARC і SPF експеримент був проведений ще раз, і отримані наступні результати (див. таблицю 2 та рисунок 2).

Експеримент довів працездатність даної технології, тому що після їх впровадження, поштові сервіси стали відкидати підроблені листи. Деякі сервіси прийняли кілька таких листів, позначивши їх як спам, успішних доставок не відбулося не в одному з випадків. Отже можна відзначити актуальність впровадження даної технології.

Експеримент №2 – випробування технології захисту від заміни листів, які надходять від імені випробуваного сервера. Практична реалізація експерименту полягає в тому, що формуємо пакет підроблених листів, представляємося ім'ям випробуваного сервера і розсилаємо листи. Мета виявити чи є можливість підробляти листи та розсилати їх від імені сервера.

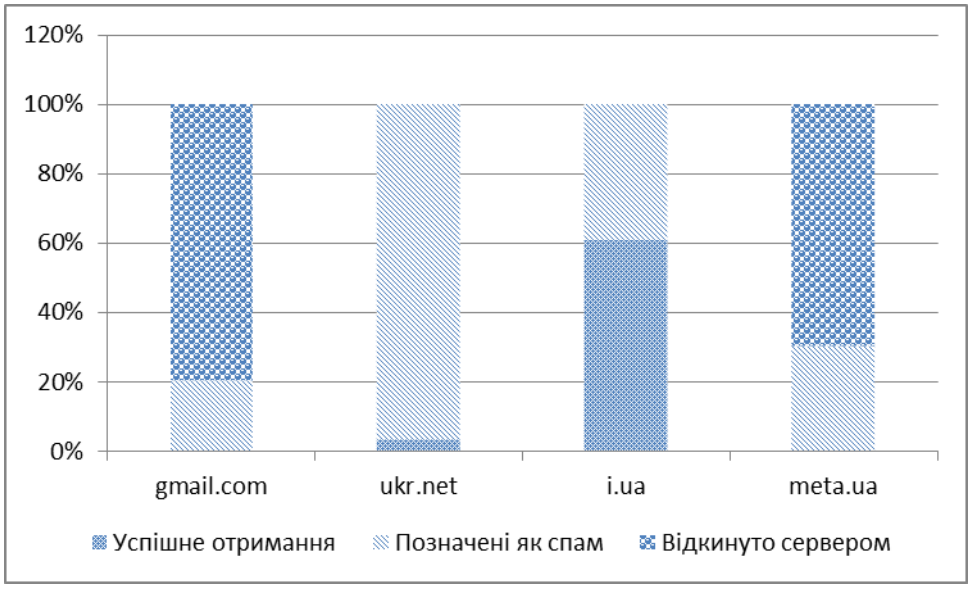

Рисунок 1 – Гістограма результатів експерименту 1 без доменної валідації

Таблиця 2 – результати експерименту з використанням доменної валідації

Поштовий сервіс	Успішне отримання	Позначені як спам	Відкинуто сервером
gmail.com	90%	10%	0%
ukr.net	95%	5%	0%
i.ua	70%	30%	0%
meta.ua	93%	7%	0%

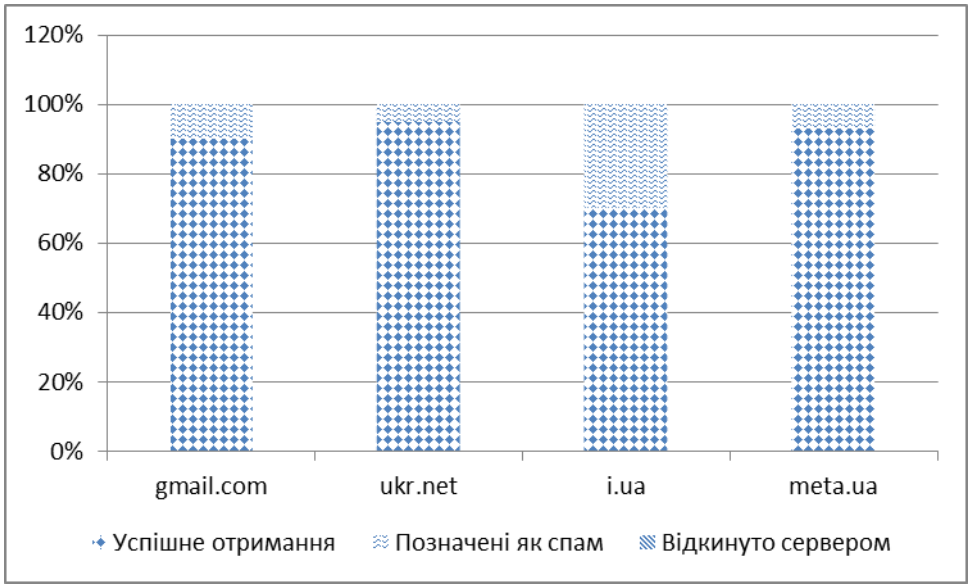

Рисунок 2 – Гістограма експерименту з використанням доменної валідації

За аналогією з першим експериментом, була згенерована і відправлена пошта на чотири популярних поштових сервіси. З тією лише різницею, що в цьому екскременті відправка проводилася з іншого сервера, що не має відношення до випробуваного поштового сервера, тобто випробування в ролі зловмисника.

Після випробувань були отримані наступні результати представлені таблиця 3.

Таблиця 3 – Результат відправки підроблених листів без технології доменної валідації

Поштовий сервіс	Успішне отримання	Позначені як спам	Відкинуто сервером
gmail.com	0%	100%	0%
ukr.net	0%	80%	20%
i.ua	61%	39%	0%
meta.ua	20%	70%	10%

Як видно з експерименту, хоч в більшості випадків лист і позначений як спам, однак при цьому він не відкидається поштовим сервісом, і потрапляє до поштової скриньки, отже зловмисник може передати інформацію жертві від нашого імені. При цьому слід зазначити, що в ряді випадків, коли налаштування безпеки на поштовому сервісі чуть-менш суворі, з боку зловмисника, лист потрапляє в категорію – «вхідні повідомлення» як безпечні, що ще більше погіршує становище.

Після настройки технологій Domain Validation: Dkim, DMARC і SPF експеримент був проведений ще раз, і спостерігалися наступні результати випробувань, які представлені в таблиці 4 та на рисунку 4.

Таблиця 4 – Результат відправки підроблених листів с працюючої технологією доменної валідації

Поштовий сервіс	Успішне отримання	Позначені як спам	Відкинуто сервером
gmail.com	0%	10%	90%
ukr.net	0%	10%	90%
i.ua	10%	90%	0%
meta.ua	0%	80%	20%

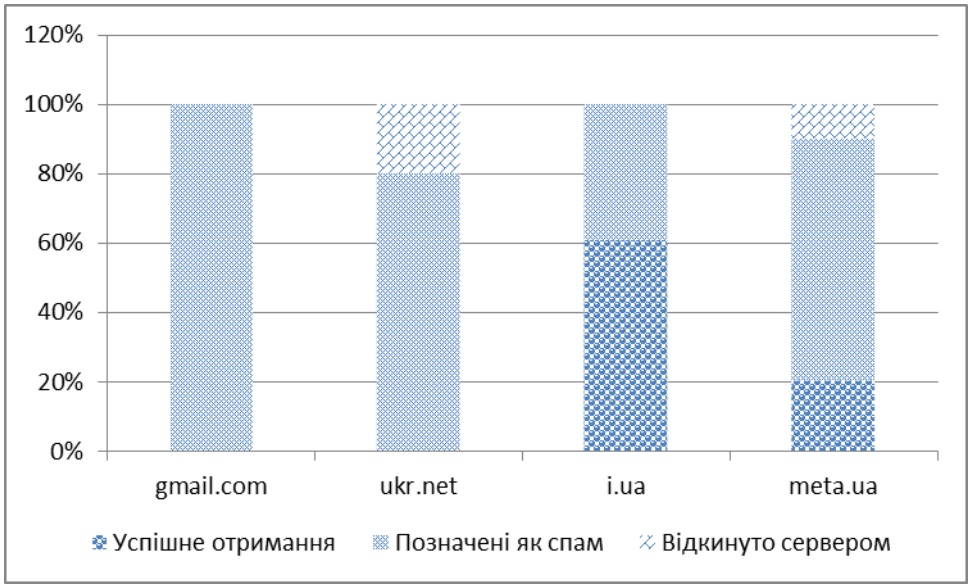

Рисунок 3 – Гістограма експерименту №2 без технології доменної валідації

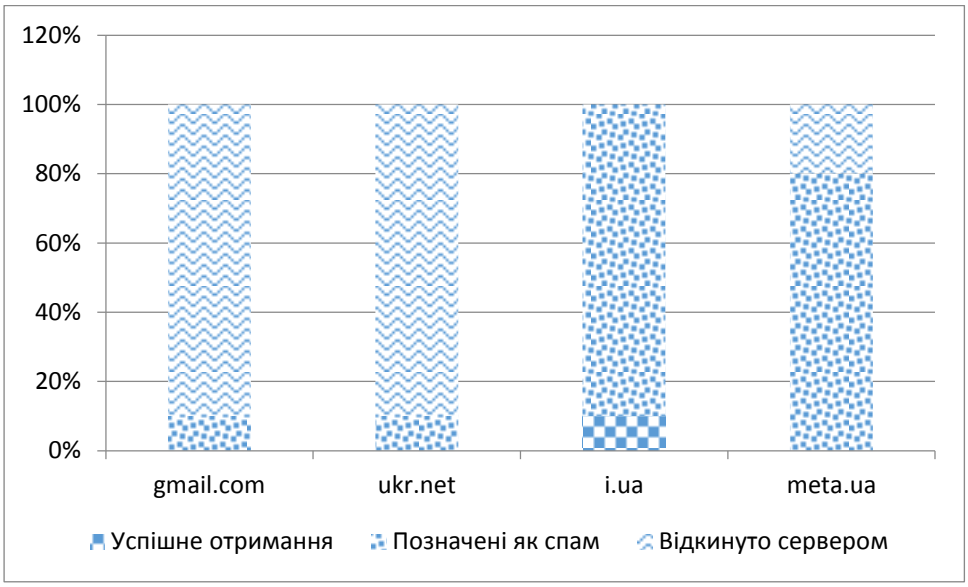

Рисунок 4 – Гістограма експерименту з використанням доменної валідації для підроблених листів

Після впровадження технології захисту від підміни шляхом валідації домену, можливості підмінити лист практично не залишилося, і якщо, слідуючи своїм налаштуванням безпеки, сервер і не відкидав лист, то в такому випадку гарантовано позначав його як спам. Що ще раз підтверджує актуальність обраної технології.

ВИСНОВКИ

Виконано аналіз теоретичної бази в галузі проектування корпоративних поштових серверів. На основі цього аналізу були підібрані і налаштовані необхідні компоненти для побудови актуальної моделі поштового сервісу. Практично вдалося реалізувати модель поштового сервера, з використанням передових технологій в цій галузі, яка відповідає сучасним вимогам безпеки. В ході випробувань по черзі впроваджувалися технології захисту поштових обмінів, такі як SSL і DKIM, кожна впроваджувана технологія продемонструвала

себе як актуальний і важливий елемент, роботи сучасних поштових сервісів, відмова від яких наражає користувачів пошти на серйозний ризик. Описані в статті практики зарекомендували себе як актуальні методи в реалізації сервера з використанням сучасних технологій, що відповідає необхідним стандартам реалізації поштових сервісів

Список використаних джерел:

1. Загальні зведення з Відкритого ПЗ, і його особливості [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Open-source_software
2. Індивідуальні особливості Postfix [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Postfix
3. Технічна документація по Dovecot [Електронний ресурс]. – Режим доступу: https://wiki.dovecot.org/DovecotFeatures
4. Загальні відомості про технології захищеної передачі [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/SSL
5. Левицкая Т. А. Моделирование системы для обработки, анализа и хранения в облаке корпоративных сообщений / Т. А. Левицкая, И. В. Федосова, Д. Е. Кривченков // Міжвузівський тематичний збірник наукових праць. – Маріуполь: ДВНЗ «ПДТУ», 2019. – Вип. 20. – С. 206-210.
6. Опис технології SpamAssasin [Електронний ресурс]. – Режим доступу: https://wiki.dieg.info/spamassassin
7. Опис технології DKIM [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/106589
8. Опис можливостей SPF [Електронний ресурс]. – Режим доступу: https://drupal-admin.ru/blog/nastroyka-ptr-spf-dkim
9. Приклад реалізації кластеризації поштового сервера [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/324538/

Мироненко Д. С.,Вонярха А.В.

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ И РАБОТОСПОСОБНОСТИ КОРПОРАТИВНОГО ПОЧТОВОГО СЕРВЕРА

На сегодняшний день существует достаточное количество различных как платных, так и бесплатных почтовых сервисов, которые предоставляют приемлемый уровень удобства использования. В статье описаны методы реализации почтового сервиса на основе исследований в области структурной организации почты предприятия, а так же практических испытаний почтовых серверов, бизнес назначения, в средних и крупных IT-компаниях.

Приведен вариант подбора программного-стека по актуальным на данный момент элементам открытого программного обеспечения, которые выполняют конкретную роль в работе почтового сервера. Описанные передовые практики использования современных технологий защиты передачи конфиденциальной информации в момент передачи через глобальную сеть. А также актуальные методы валидации собственной почты, и ее защиты от подмены третьими лицами. Представлены основные методы защиты от спама и защиты пользователей от нежелательной почты. Данные методы и практики, можно использовать как пособие для организации почтового сервера, или как рекомендации при настройке сервера с подобной спецификой.

Было установлено, что реализация удобного почтового сервиса на базе открытого программного обеспечения может быть выполнено на основе программного обеспечения Postfix совместно с Dovecot. Postfix полностью соответствует предъявляемым требованиям, с возможностью работы в тандеме с другими элементами стека, он является простым в дальнейшем администрировании. Dovecot - эффективное решение приема электронной почты в связке с Postfix, в сфере открытого программного обеспечения. Данное решение было опробовано в нескольких средних компаниях.

В ходе испытаний по очереди внедрялись технологии защиты почтовых обменов, такие как SSL и DKIM, каждая внедряемая технология продемонстрировала себя как актуальный и важный элемент работы современных почтовых сервисов, отказ от которого подвергает пользователей почты к серьезному риску.

Результаты исследований свелись к практической реализации модели почтового сервера, которая использует передовые технологии в этой области и отвечает современным требованиям безопасности.

Ключевые слова: *программный-стек, открытое программное обеспечение, электронная почта, сервер, кластер, Postifx, Dovecot, SSL, SpamAssasin, безопасность данных, E-mail*

Mironenko D. S.,Vonjarkha A.V.

RESEARCH OF THE POSSIBILITY OF USING MODERN TECHNOLOGIES TO INCREASE THE RELIABILITY AND PERFORMANCE OF THE CORPORATE E-MAIL SERVER

Today, there are a fair number of different paid and free mail services that provide an acceptable level of usability. The article describes methods of implementation of mail service on the basis of researches in the field of structural organization of mail of the enterprise, as well as practical tests of mail servers, business purpose, in medium and large IT companies.

There is a variant of selection of software-stack from current open-source elements that play a specific role in the work of the mail server. Best practices of using modern technologies of protection of transfer of confidential information at the moment of transmission through the global network are described. As well as current methods of validation of own mail, and its protection against spoofing by third parties. The basic methods of protection against spam, and protection of users from spam. These methods and practices can be used as a guide for organizing a mail server, or as a guide when setting up a server with similar specifics.

It has been found that the implementation of a convenient open source mail service can be performed using Postfix software in conjunction with Dovecot. Postfix is fully compliant, with the ability to work in tandem with other elements of the stack, it is easy to administer further. Dovecot is the most effective open source email solution for receiving Postfix email. This solution has been tested in several medium-sized companies.

During the tests, mail security technologies such as SSL and DKIM were introduced in turn, and each technology introduced proved to be a relevant and important element of modern mail services, the failure of which puts mail users at serious risk.

The research results came down to the practical implementation of a mail server model that uses advanced technologies in this field and meets modern security requirements.

Keywords: *Software stack, open source software, email, server, cluster, Postifx, Dovecot, SSL, SpamAssasin, data security, E-mail*

Рецензент: доцент, канд. техн. наук Кривенко О.В.

Принято