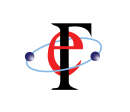
****СОФИЙСКА ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЕЛЕКТРОНИКА**

**„ДЖОН АТАНАСОВ“**

***ул.„Райко Алексиев“ № 48 е – mail*** [***spgelectron@yahoo.co.uk***](mailto:spgelectron@yahoo.co.uk)***; spge – bg.com***

**ДЪРЖАВЕН ИЗПИТ ЗА ПРИДОБИВАНЕ НА ТРЕТА СТЕПЕН НА ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ**

**по професията код** 523050 „Техник на компютърни системи“

**по специалността код** 5230501 „Компютърна техника и технологии“

Д И П Л О М Е Н П Р О Е К Т

**ТЕМА: ИМПЛЕМЕНТАЦИЯ НА СИГУРЕН MAIL СЪРВЪР ПОД LINUX**

**ИЗГОТВИЛ: АЛЕКСАНДЪР ИВАНОВ ИВАНОВ УЧЕНИК ОТ 12„Д“ КЛАС**

**Дипломант:**

*/ Александър Иванов /*

**Научен ръководител:**

*/инж. Цветана Пунева/*

**град София,2022г.**

**СЪДЪРЖАНИЕ**

УВОД...................................................................................................................стр.4-5

ПЪРВА ЧАСТ - СЪРВЪРИ И СЪРВЪРНИ КОНФИГУРАЦИИ...................................стр.6 – 31

# 1. Архитектура на сървъра………………………………………………………………..стр.6

# Изисквания към сървъра – хардуерни и софтуерни……………………………....стр.7

1.2. Средства улесняващи инсталирането………………………………………………стр.7

* 1. Средства за наблюдение и контрол…………………………………………………стр.7

1.4. Организация на данните и защита на информацията…………………………....стр.7

1.5. Средства за отдалечен контрол…………………………………………………….стр.15

# 1.6. Допълнителни осигуровки на сървъра……………………………………………стр.16

1. Видове сървъри……………………………………………………………………...стр.16
   1. Файлов сървър ……………………………………………………………………....стр.16
   2. Сървър за ІР адресиране (DNS Domain Name Server)………………………...….стр.16
   3. Web сървър…………………………………………………………………………..стр.16
   4. Сървър, осъществяващ защитната стена…………………………………………стр.16
   5. Упълномощен сървър (Proxy сървър)……………………………………………..стр.16
   6. Сървър за електронна поща………………………………………………………..стр.16
   7. Факс сървър………………………………………………………………………….стр.16
   8. Сървъри за директорийни услуги………………………………………………....стр.16
   9. . Сървър за приложения…………………………………………………………....стр.17
   10. Други сървъри …………………………………………………………………..стр.17
2. СЪЩНОСТ НА МЕЙЛ СЪРВЪР………………………………………………….стр.17
   1. Mail Submission Agent (MSA……………………………………………………….стр.17
   2. . Mail Transfer/Transport Agent (MTA)………………………..…………………..стр.18
   3. Mail Delivery Agent (MDA)………………………………………………………...стр.18
3. Linux………………………………………………………………………….………стр.21
   1. Дистрибуции………………………………………………………………………..стр.21
      1. Десктоп - насочени дистрибуции…………………………………………......стр.21
4. Видове мрежови атаки…………………………………………………………….......стр.21
5. Защита на мрежата, сървъра и архива……………………………………………...…стр.23
6. Мерки за сигурност…………………………………………………………….……….стр.23

7.1.Модел на информационната сигурност………………………………………….стр.24

8.Управление на риска ………………………………………………………………...стр.25

9.Мерки за налагане на информационна сигурност………………………….……..стр.25

9.1.Класификация на информацията…………………………………………….......стр.25

10.Основни заплахи за сигурността на информацията……………………………..стр.26

11.Криптиране…………………………………………………………………………..стр.27

# II. ВТОРА ЧАСТ ИМПЛЕМЕНТАЦИЯ НА СИГУРЕН MAIL – SERVER ПОД LINUX……………………………………………………………………………...……стр.33-43

1. Проектно предложение…………………………………………………………………стр.33
2. Техническо решение………………………………………………………………..стр.34-43

ИЗВОДИ, ОБОБЩЕНИЕ И ЗАКЛЮЧЕНИЕ…………………………………………стр.43-47

# ИЗТОЧНИЦИ……………………………………………………………………………стр.49

# УВОД

Имплементация е термин, който в различни области му се предава различно значение. В информатиката, имплементацията е реализирането на техническа задача или алгоритъм, като програма, софтуерен компонент или друга компютърна система с помощта на програмиране и внедряване. В областта на информационните технологии, имплементацията означава процеса след закупуване на софтуера, при който клиентът се обучава как да използва софтуера или хардуера, които са били закупени.

[Сървърите](http://tuj.asenevtsi.com/CA/CA030.htm) са обслужващи мрежите устройства. Отдавна отмина времето, когато файл сървърът беше единственият представител на този клас оборудване. Днес съществува голямо разнообразие от сървъри. Зад всяка една функция на мрежата или предлагана услуга стои съответен сървър. Разпределението на  дейностите в мрежата значително облекчава работата й и я прави по - ефективна.Сървърите са  програмни или програмно -апаратни комплекси. Мрежовият сървър и операционната система работят като едно цяло.

Независимо колко е мощен сървърът, той е неизползваем без операционната система, която да се възползва от физическите му ресурси. Сървърът е компютър, който работи съвместно с други компютри в компютърна мрежа, като се различава от тях по това, че за работата му не е необходимо човешко участие.

В мрежите сървърът предоставя услуги към останалите компютри, наричани клиенти. Терминът *„сървър“* е пряко свързван с архитектурата  клиент - сървър. Сървърът е [компютърна програма](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0), която предоставя услуги на други програми, наречени в този контекст [клиентски софтуер](https://bg.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D1%8A%D1%80%D0%B2%D1%8A%D1%80) (Client). Сървърът стартира като услуга, която обслужва заявки на други програми („клиенти“), които могат, а могат и да не бъдат стартирани на същия компютър.

Сървърът е също така [компютър](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80), стартиращ [сървърен софтуер](https://bg.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D1%8A%D1%80%D0%B2%D1%8A%D1%80)  и предоставящ една или повече услуги (като например [хост](https://bg.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82)) на други компютри в същата [мрежа](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B0_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0). В повечето случаи [хардуерните](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%B5%D0%BD_%D1%85%D0%B0%D1%80%D0%B4%D1%83%D0%B5%D1%80) изисквания към този компютър са по-високи от изискванията към хардуера на стандартния настолен компютър, който не функционира като сървър. В допълнение, може да има специални изисквания за [архивиране](https://bg.wikipedia.org/w/index.php?title=%D0%90%D1%80%D1%85%D0%B8%D0%B2%D0%B8%D1%80%D0%B0%D0%BD%D0%B5&action=edit&redlink=1), защити  и др.

Днес този термин се използва най-вече за завършени [компютърни системи](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0). Една такава [софтуерна](https://bg.wikipedia.org/wiki/%D0%A1%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80)/[хардуерна](https://bg.wikipedia.org/wiki/%D0%A5%D0%B0%D1%80%D0%B4%D1%83%D0%B5%D1%80) система представлява софтуерна услуга, стартираща на специално предназначен за нея компютър. Това са например [сървър база данни](https://bg.wikipedia.org/wiki/%D0%A1%D1%8A%D1%80%D0%B2%D1%8A%D1%80_%D0%B1%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8), [файлов сървър](https://bg.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2_%D1%81%D1%8A%D1%80%D0%B2%D1%8A%D1%80&action=edit&redlink=1), [mail сървър](https://bg.wikipedia.org/w/index.php?title=Mail_%D1%81%D1%8A%D1%80%D0%B2%D1%8A%D1%80&action=edit&redlink=1) или [print сървър](https://bg.wikipedia.org/w/index.php?title=Print_%D1%81%D1%8A%D1%80%D0%B2%D1%8A%D1%80&action=edit&redlink=1). Linux или **[**GNU**]/**Linux е общото название на всички [операционни системи](https://bg.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), основаващи се на [ядрото „Linux“](https://bg.wikipedia.org/wiki/%D0%9B%D0%B8%D0%BD%D1%83%D0%BA%D1%81_(%D1%8F%D0%B4%D1%80%D0%BE)) (Linux kernel) и системните инструменти и [библиотеки](https://bg.wikipedia.org/wiki/%D0%A1%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B8%D0%B1%D0%BB%D0%B8%D0%BE%D1%82%D0%B5%D0%BA%D0%B0), обикновено от проекта [GNU](https://bg.wikipedia.org/wiki/GNU). Повечето от тези операционни системи се наричат Linux дистрибуции, но [Фондацията за свободен софтуер](https://bg.wikipedia.org/wiki/%D0%A4%D0%BE%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D1%8F_%D0%B7%D0%B0_%D1%81%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B5%D0%BD_%D1%81%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80) използва наименованието GNU**/**Linux, за да подчертае значимостта на GNU софтуера, което предизвиква известни противоречия.

Linux е флагман и един от най-известните представители на [свободния софтуер](https://bg.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B5%D0%BD_%D1%81%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80) и софтуера с отворен код (F(L)OSS – free software, libre software, and open-source software). Проектът и движение GNU, чиято цел е създаване на нова операционна система свободен софтуер, е основан от Ричард Столман през 1984 г. Системата съдържа голям брой инструменти и програми, например компилатори, текстови редактори и сървъри. Софтуерът се разпространява с лиценза GNU GPL, което гарантира бъдещата му свободна достъпност. С Linux, GNU става напълно работеща операционна система и това спомага за бързото ѝ разпространение.

## Фактът, че повечето от най-бързите суперкомпютри в света, работещи на Linux, може да се отдаде на скоростта му. Linux има репутацията на бърз и гладък, докато за Windows 10 е известно, че с времето става бавен и бавен.

Linux работи по-бързо от Windows 8.1 и Windows 10, заедно с модерна работна среда и качества на операционната система, докато Windows е бавен за по - стария хардуер.

Говорейки за основните възможности на операционната система като планиране на нишки, управление на паметта, обработка на входове и изходи, управление на файлова система и основни инструменти, като цяло Linux превъзхожда Windows.

Има много причини Linux да бъде по-бърз от Windows:

**Първо**, Linux е много лек, докато Windows е дебел. В Windows много програми работят във фонов режим и те изяждат RAM.

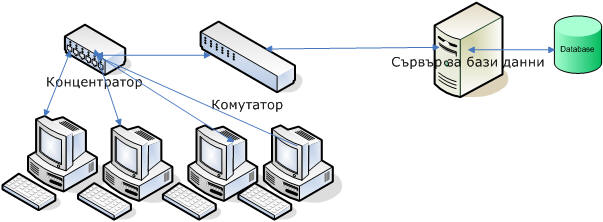
**Второ**, в Linux файловата система е много организирана. Файловете се намират на парчета, които са много близо един до друг. Това прави операциите за четене и запис много бързи. От друга страна, Windows е dumpster и файловете присъстват навсякъде.

# I. ПЪРВА ЧАСТ - СЪРВЪРИ И СЪРВЪРНИ КОНФИГУРАЦИИ

**1. Архитектура на сървъра**

***Правило:*** *Нещата вървят добре, когато е налице излишък. Излишъкът е гаранция за това, че сървърът винаги ще е в добро състояние!*

* [**Паралелна компютърна архитектура**](http://tuj.asenevtsi.com/CA/CA024.htm)**.** [Операционната система](http://tuj.asenevtsi.com/CA/CA018.htm) работеща с четири и повече [процесора](http://tuj.asenevtsi.com/CA/CA052.htm) ще балансира товара на задачата така, че да се постига добра производителност на сървъра.
* **Код за коригиране на грешките** /ЕСС/ подсилва сигурността на сървъра и целостта на данните.
* [**Кеширането**](http://tuj.asenevtsi.com/CA/CA086.htm) **на данните** в паметта оптимизира [производителността на сървъра](http://tuj.asenevtsi.com/CA/CA053.htm).
* Два [мрежови адаптери](http://tuj.asenevtsi.com/CN/N093.htm) позволяват сегментиране товара на клиентите на сървъра. Софтуерът обединява двата порта в един. Вторият адаптер служи за осигуряване на по-висока честотна лента или като резервен.
* Смяна на дисковете по време на работа. Използване на технологията RAID Leve l5.
* Връзка към устройства за бързо съхранение на данни.
* Непрекъсваеми по време на работа захранвания с двойни мрежови кабели и два допълнителни вентилатора.



**1.1. Изисквания към сървъра – хардуерни и софтуерни**

Изискванията са валидни за сървър с 3 клиентски машини и 1 база с до 300 служители. Минимални изисквания:

* **Сървър:** − Компютър с двуядрен процесор Intel / AMD с работна честота ≥2000 MHz, 4096 MB RAM, − MS Windows 7 − Поне 50 GB свободно дисково пространство.
* **Клиент:** − Компютър с двуядрен процесор Intel / AMD с работна честота ≥1800 MHz, 2048 MB RAM, − MS Windows 7 − Поне 2 GB свободно дисково пространство. Препоръчителна конфигурация: Сървър: − Компютър с четири- или повече ядрен процесор Intel / AMD с работна честота ≥3000 MHz , ≥4096 MB − MS Windows 10, MS Windows Server 2012, 2016, 2019 − Около 100 GB свободно дисково пространство. Клиент: − Компютър с четириядрен процесор Intel / AMD с работна честота ≥2400 MHz, 4096 MB − MS Windows 10 − Поне 2 GB свободно дисково пространство.

**1.2. Средства улесняващи инсталирането.**

Софтуерни пакети, които предпазват от допускане на големи грешки при инсталиране и експлоатация на сървъра и оказват ценна помощ на мрежовия администратор.

**1.3. Средства за наблюдение и контрол.**

Продукти за визуализиране състоянието на сървъра. Те позволяват автоматизиране на отделни задачи, които претоварените системни администратори пренебрегват.

**1.4. Организация на данните и защита на информацията.**

Прилагат се различни техники за дублиране на информацията, без това да се отразява чувствително върху крайната цена на сървъра.

Използват се техники за организиране на данните като **DataMiroring и Data Striping** с които данните се организират в RAID масиви - стандартни и хибридни нива, т.е данните се записват на няколко диска по определена схема. RAID масивите представляват организирани няколко физически диска в обща логическа единица.

|  |  |
| --- | --- |
| Стандартни RAID нива: | Схема: |
| RAID 0:  *Минимум 2 устройства, няма защита*  *на информацията.*  *Предлага най-добрата производителност, но не позволява защита на данните.*  *При увеличаване на броя на дисковете в масива,расте и скоростта на запис/четене*. | https://upload.wikimedia.org/wikipedia/commons/thumb/9/9b/RAID_0.svg/150px-RAID_0.svg.png |
| RAID 1:  *Минимум 2 устройства, опростена защита на данните.*  *Недостатъкът на това ниво е, че ефективният свободен обем ще бъде двойно по-малък от сбора на инсталираните устройства.*  *Производителността при запис е същата както при единичен диск.* | https://upload.wikimedia.org/wikipedia/commons/thumb/b/b7/RAID_1.svg/150px-RAID_1.svg.png |
| RAID 2:  *Препоръчват се поне 10 диска за съхранение на данни и още 4 за генерираните кодове.*  *Това прави общ дисков масив от 14 устройства.*  *Информацията се разделя на блокове и се записва последователно на дисковете от масива.*  *Това ниво не се използва от дълги години, защото употребата му е от времето,когато дисковите устройства не предлагаха своевременна корекция на четената от тях информация.* | https://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/RAID2_arch.svg/350px-RAID2_arch.svg.png |

|  |  |
| --- | --- |
| RAID 3:  *Принципът на действие е подобен на този на ниво 2.*  *Надеждността на съхранение на информация е същата като в предходното ниво 2.*  *Един от дисковете е заделен за съхранение на битове за четност.* | https://upload.wikimedia.org/wikipedia/commons/thumb/f/f9/RAID_3.svg/300px-RAID_3.svg.png |

|  |  |
| --- | --- |
| RAID 4:  *Изискват се поне 3 твърди диска с еднакъв капацитет*  *Разпределянето на информацията се осъществява като предходните две нива(2, 3), като отново е предвидено устройство за съхранение на кодовете за четност.*  *Едновременното обработване на две заявки е възможно.*  *Ефективността при това ниво се увеличава с добавяне на повече устройства към масива.* | https://upload.wikimedia.org/wikipedia/commons/thumb/a/ad/RAID_4.svg/300px-RAID_4.svg.png |

|  |  |
| --- | --- |
| RAID 5:  Необходими са минимум 3 диска.  Основава се на разпределянето на блокове от данни с кодове за четност.  Както при останалите нива, блоковете от данни се записват последователно в дисковете от масива, кодовете за четност се разпределят последователно по дисковете в масива.  Функционирането се запазва дори при отпадането на един от дисковете.  При отпадне на един от дисковете и бива заменен с друг, производителността на масива рязко спада през времето, което е необходимо за възстановяването на отпадналия диск.  По времето през което се възстановява изгубеният диск, масива е много податлив към отпадане на втори диск, като в този случай информацията се изгубва безвъзвратно*.* | https://upload.wikimedia.org/wikipedia/commons/thumb/6/64/RAID_5.svg/300px-RAID_5.svg.png |

|  |  |
| --- | --- |
| RAID 6:  *Минималният брой необходими устройства са четири.*  *подобен на RAID 5, но при него има двойно разпределяне на битовете за четност.*  *Нивото предлага по-голяма надеждност на съхраняваната информация за сметка на по-малко ефективно пространство и по-ниска производителност в сравнение с RAID 5.* | https://upload.wikimedia.org/wikipedia/commons/thumb/7/70/RAID_6.svg/300px-RAID_6.svg.png |

|  |  |
| --- | --- |
| **Хибридни RAID нива (Комбинация от RAID нива):** | **Схема:** |
| **RAID 1+0 (10):**  *Необходимостта от минимум 4 диска*  *Това ниво представлява комбинация от RAID 1 и RAID 0.*  *В този случай блоковете от данни се записват огледално (информацията се дублира) и едновременно с това се разпределят между двойка дискове.*  *Тук има по-голяма производителност и защита на данните от RAID 1, но цената му е много по-висока.*  *Масивът може да понесе множество загуби на устройства, стига едно огледално копие да не загуби всичките дискове.* | C:\Users\Vili\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EFC6C3BE.tmp |
| **RAID 0+1:**  *Отново минималното изискване е 4 дискови устройства*  *Тук схемата на функциониране е обратна на 1+0.*  *Първо информацията се разпределя последователно на блокове и след това те се дублират.*  *Рискът от загуба на информация е по-голям, отколкото при RAID 1+0.* | C:\Users\Vili\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9C38E67C.tmp |
| **RAID 0+3:**  *Нивото обединява начинът на работа на RAID 0 и RAID 3.*  *Използва се разделяне (striping) както при RAID 0, но при разпределение на блоковете по схемата на RAID 3.*  *Така се увеличава надеждността на RAID 3, но респективно с това се повишава и цената.* | Nested RAID levels - Wikipedia |
| **RAID 5+0:**  *Съчетание между разпределението на битовете за четност при RAID 5 със stiping - a на RAID 0.*  *Подобрява се надеждността на RAID 5 без да се намалява защитата на данните.* | https://upload.wikimedia.org/wikipedia/commons/thumb/9/9d/RAID_50.png/510px-RAID_50.png |
| **RAID 7:**  *Този RAID е запазена марка на Storage Computer Corporation.*  *Показателите на максималния трансфер при четене на файлове, независимо малки или големи, е изключително висок. Начинът на работа обединява РАЙД 3 и РАЙД 4, но предлага много по-голяма производителност от тях.*  *Той трудно се намира на пазара и държи висока цена.* | Giải thích các cấp độ RAID (phần 1) |

**Предимства:**

* Висока производителност при по-сложни RAID системи и при ползването на битове за четност;
* Не се използват ресурсите на системата (процесор, памет);
* Възможност за замяна на дискове в работещо състояние (disk hot swapping);
* По- малко време за възстановяване на масива при отпадане на някой от дисковете;
* Лесен за инсталация – не е нужно инсталиране и конфигуриране на допълнителен софтуер;
* При наличие на батерия (BBU) изчакващите записи в кеша на контролера няма да бъдат загубени при спиране на захранването;

**Недостатъци:**

* Допълнителни разходи- хардуерните RAID контролери, струват повече отколкото обикновените дискове контролери;
* Алгоритмите и кодът са затворени собственически от компанията произвела контролера;
* Ограничена възможност за замяна и миграция на дисковия масив;
* Липса на гъвкавост (невъзможност за по-големи промени на масива);
* Високият клас контролери могат да бъдат доста скъпи;

**Софтуерен RAID** - Един RAID масив също може да бъде изграден с помощта на отворен код, който се вписва към операционната система. Софтуерният RAID използва споделените ресурси на системата – памет и процесор. Той е по-евтиният вариант в сравнение с хардуерния RAID.

**Предимства:**

* По-евтин в сравнение с хардуерния RAID, част е от операционната система и не се изискват допълнителни средства за хардуер;
* отворен код – RAID масивът е независим от хардуера на системата;
* Стандартизирана конфигурация за всяка една операционна система;
* Сравнително добра производителност – процесорите стават все по-бързи;
* Добра производителност при сравнително неголеми и натоварващи програми.
* Гъвкав метод – позволява преконфигурираното на RAID масива по множество различни начини;

**Недостатъци:**

* По-голяма сложност за изграждане в сравнение с хардуерния RAID; При по-сложни RAID системи и по-високи натоварвания отстъпва по производителност спрямо хардуерните контролери;
* Невъзможна замяна на диск в работещо положение;
* Използва част от ресурсите на системата (процесор и памет);
* Няма възможност за BBU, т.е. при спиране на захранването; незаписаната информация в кеша се губи;
* По-бавно възстановяване на масива;
* По-голяма подготовка при инсталацията на операционната система;

**Заключение:**

RAID технологията предлага сравнително голяма производителност и надеждност на съхраняваната информация. Възможните конфигурации между различните нива, позволяват да се подобрят дадени параметри, в зависимост от нуждите на конкретния потребител. Технологията е гъвкава и не случайно използването ѝ има толкова много предимства.

Но е много важно да се отбележи, че RAID не бива да се използва като резервно копие на данните. Технологията осигурява защита при повреда на някой от дисковете, но не предпазва от злонамерена дейност в уеб пространството, хакери и други. Задължително съхранявайте пълно копие на най-ценната си информация на отделен хард диск и не разчитайте изцяло на RAID. Неговото предназначение е да подобри производителността и да намали риска от загуба на данни, но не и да осигури пълна защита на информацията.

* **Огледален** [**диск**](http://tuj.asenevtsi.com/CA/CA098.htm) **-** два диска използват един и същи контролер, като и двата записват напълно идентично копие на данните. Недостатък - при повреда на контролера информацията се губи.
* **Дублиране на дискове -** Всеки от дублиращите дискове разполага със собствен контролер. Методът е по - скъп, но по надежден и осигурява по-голямо бързодействие.

**1.5. Средства за отдалечен контрол**

Много полезни, когато мрежовия администратор не е наблизо. Той може да се свърже по телефона и да получи информация за състоянието на мрежата, да тества или рестартира системата. Предвидена е и възможност при възникване на проблем, сървърът автоматично да потърси помощ по телефона.

**1.6. Допълнителни осигуровки на сървъра**

Хардуер който сам фиксира възникналите проблеми в сървъра.

[Оперативна памет](http://tuj.asenevtsi.com/CA/CA080.htm) с автоматична корекция на грешките.

Ако това не може да стане повредения чип се изолира и се сигнализира за събитието. Двойна осигуровка на [захранването](http://tuj.asenevtsi.com/CA/CA047.htm) на сървъра. Включване на два UPS, като допълнителна осигуровка на захранването.

Двете устройства работят в паралел.

Дублиране на сървъра **(**клъстъриране**)**- две или повече машини се свързват чрез високоскоростна връзка и се прави абсолютно огледален образ на данните и паметта Дейностите, които се изпълняватот мрежите са разнообразни и сложни. Те се реализират от специализирани сървъри, с цел задоволяване нарастващите нужди на потребителите.

**2. Видове сървъри**:

* 1. **Файлов сървър** - компютър изпълняващ ролята на съвместно хранилище на файлове за потребителите. Синхронизира достъпа до общите ресурси.
  2. Сървър за ІР адресиране (DNS Domain Name Server) - извършва услуги по управление на ІР адреси
  3. **Web сървър** - удобно и икономично средство за публикуване на документи, достъпни са за всеки, който разполага с Web браузър
  4. **Сървър, осъществяващ защитната стена**

**Сървърът може да има три адаптера**

* За връзка с Интернет - създава защитна стена и пълен контрол върху маршрутизирането на постъпващите пакети;
* Адаптер за локална мрежа, който дава възможност на потребителите да се включват в други корпоративни локални мрежи;
* Адаптер за защитаваната LAN.
  1. **Упълномощен сървър (Proxy сървър)** - сървър, който обслужва заявки вместо друг сървър.
  2. **Сървър за електронна поща** - управлява електронните съобщения между потребителите на мрежата.
  3. **Факс сървър** - управлява трафика на факсове към и от мрежата. Може чрез обществената телефонна мрежа да предава факсове към факс апарати.
  4. **Сървъри за директорийни услуги** - позволяват на потребителите да локализират, съхраняват и защитават информацията в мрежата.

**2.9. Сървър за приложени**я - правят данните и сървърната част на приложенията от типа клиент/сървър достъпни за клиентите. При сървъра за приложения базата данни се намира на сървъра, а на клиентският компютър чрез форми се попълват данни или чрез заявки се извлича информация.

* 1. **Други сървъри** - както вече бе споменато, колкото функции изпълнява мрежата, толкова вида сървъри могат да бъдат създадени. Това е въпрос на проектиране, оптимизация на структурата и естествено пари.

1. **СЪЩНОСТ НА МЕЙЛ СЪРВЪР**

Имейл сървър (или само мейл сървър), подобно на други сървъри в интернет, е приложение, което е инсталирано на физически сървър и предоставя определена услуга (в случая електронна поща).Мейл сървърът е виртуален пощенски офис, който едновременно приема и разпраща имейл съобщения, постъпили към него от локални или отдалечени имейл потребители. Мейл сървърът стандартно е съвкупност от няколко приложения или комуникационни модула/пощенски агента:

* MSA – изходящ мейл сървър (SMTP сървър)
* MTA – изпращащ/получаващ мейл сървър
* MDA – входящ мейл сървър (POP3/IMAP сървър)

За комуникацията между имейл клиент и изходящия мейл сървър (MSA) се използва протокол SMTP/ESMTP.За комуникацията между имейл клиент и входящия мейл сървър (MDA) се използват протоколи POP3 или IMAP.За системната комуникация между различните пощенски агенти – изходящ (MSA), изпращащ/получаващ (MTA) и входящ (MDA) мейл сървър се използва протокола SMTP.

**3.1. Mail Submission Agent (MSA)** – пощенски агент, приемащ заявки

* MSA агентът (изходящият мейл сървър) приема заявки за изпращане на имейл съобщения от MUA (Mail User Agent);
* Mail User Agent (MUA) – потребителски агент (имейл клиент);
* MUA или имейл клиент (Mozilla Thunderbird, Microsoft Outlook и други) представлява приложение, което е инсталирано на компютъра на крайния потребител. Имейл клиентът предоставя средата, в която крайният потребител може да създава, изпраща и получава имейл съобщения. След като дадено имейл съобщение е създадено, имейл клиентът има отговорността да го провери, подготви и изпрати към MSA (изходящия мейл сървър).

За да може имейл клиентът да се свърже с MSA, потребителят трябва предварително да направи настройка, като въведете информация:име на изходящия мейл сървър,порт на изходящия мейл сървър(25, 26 или 587),потребителско име и парола.Когато MUA е уеб приложение, инсталирано на сървъра, тогава то се нарича webmail клиент (RoundCube, Horde и други).

MSA извършва последна проверка и подготовка на имейл съобщението, преди да го предаде към MTA (изпращащия агент). Също така MSA е агентът, който може да идентифицира дали потребителят може да изпраща имейли, например чрез потребителско име и парола. Такава идентификация не се извършва при MTA, поради това MSA е добър защитен механизъм против изпращане на спам.

Идентификацията на мейл сървърите на СуперХостинг.БГ е чрез SMTP-AUTH.За MSA е определен порт 587 в спецификацията за системата за електронни съобщения. За разлика от порт 25, който е определен за MTA, този порт не се блокира от доставчиците на интернет услуги.

**3.2. Mail Transfer/Transport Agent (MTA)** – изпращащ/получаващ пощенски агент

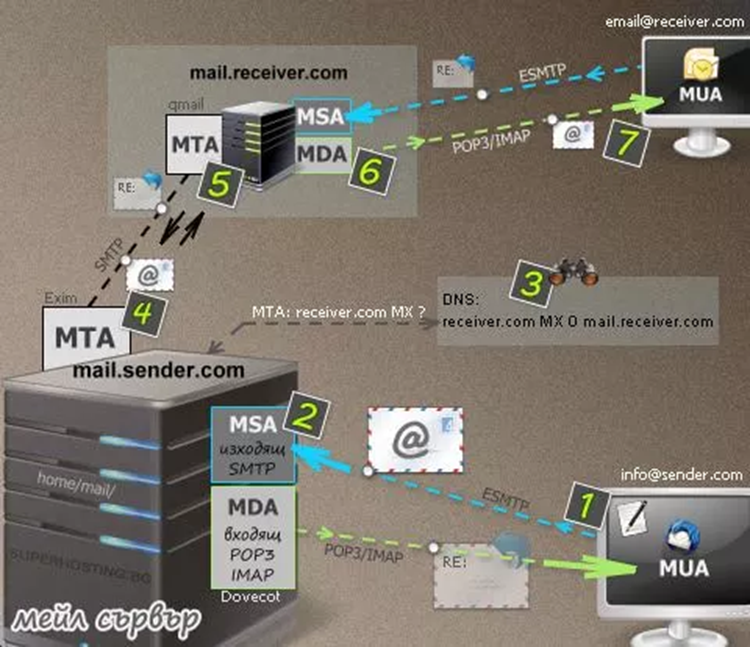
След като получи подготвеното за изпращане имейл съобщение, MTA ще изпрати писмото към дестинацията му.

MTA отговаря за получаването и изпращането на имейл съобщения от и до други MTA.MTA може да получи имейл от друг MTA, от MSA или дори директно от MUA.Когато пощенската кутия на получателя не се намира локално на този MTA, тогава съобщението ще бъде препратено към друг MTA.

**3.3. Mail Delivery Agent (MDA)** – доставящ пощенски агент.

След като мейл сървъра (MTA) на получателя получи писмото, то се предава на доставящия агент MDA (входящия мейл сървър), който от своя страна доставя писмото до пощенската кутия на получателя.

Пощенската кутия се намира на мейл сървъра, а чрез имейл клиент потребителят може да достъпи пощенската кутия.Когато MTA получи имейл от локален потребител (същият домейн, например от info@mydomain.com до office@mydomain.com), тогава директно предава писмото на MDA. В този случай доставянето на писмото се нарича Local Delivery.



* След като имейл съобщението е готово и потребителят е кликнал „Изпрати“, MUA (имейл клиентът) ще го провери и подготви за изпращане. След това ще се свърже с MSA (изходящия сървър) и ще му предаде съобщението.
* MSA ще изиска идентификация на потребителя, например с въвеждане на потребителско име и парола (SMTP-AUTH). Ако потребителят се идентифицира успешно, MSA ще провери съобщението, ще добави още няколко мейл хедъри и ще го предаде към MTA за изпращане. За комуникацията между MUA и MSA се ползва протокол ESMTP.
* MTA или MSA, в зависимост от използвания софтуер, ще направи проверка в DNS за мейл сървъра отговарящ за домейна на получателя (receiver.com). След като дестинацията е известна (mail.receiver.com), MTA на подателя изпраща имейл съобщението до MTA на получателя.
* MTA на получателя получава имейл съобщението и го предава на MDA за доставяне във входящата кутия на получателя. Ако кутията на получателя не се намира на същия този мейл сървър, MTA ще препрати имейл съобщението към следващ MTA. Докато писмото не достигне до MTA, където реално се намира кутията на получателя. Всеки MTA, през който преминава имейл съобщението, ще постави специфична заглавна част (мейл хедър) в него. Тези заглавни части служат за проследяване на пътя, по който е преминало дадено имейл съобщение.
* Когато получателят стартира имейл клиента си и се свърже с входящия си мейл сървър (MDA) писмото се доставя до MUA.
* MUA се е свързал с MDA и получава имейл съобщението.
* Dovecot е пример за входящ мейл сървър, който поддържа POP3 и IMAP и може да се добавя към други приложения за мейл сървъри;
* Например Exim, Postfix, qmail (+POP3) и sendmail са мейл сървъри с вградена функционалност за SMTP изходящ мейл сървър, но за входящ мейл сървър могат да ползват Dovecot (POP3, IMAP). В следната сравнителна таблица можете да видите всички най-известни мейл сървъри и техните функции: Comparison of mail servers.

**4. Linux**

**4.1. Дистрибуции:**

Различните Linux дистрибуции са насочени към различни целеви потребителски групи. Могат да се различават по графичния интерфейс, който използват, [приложните програми](https://bg.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0&action=edit&redlink=1), които идват при инсталацията, системните инструменти, които използват (напр. мениджъри на пакети), както и по много други показатели.

**4.1.1. Десктоп - насочени дистрибуции**

Десктоп - насочените (т.е. насочени към употреба с настолни компютри, лаптопи и нетбукове, най-често използващи процесори x86 или по-новите x86\_64) Linux дистрибуции са тези дистрибуции, които са предвидени за крайни потребители на персонални компютри в дома или офиса, пакетирани с разнообразни приложни програми, често и несвободни кодеци и драйвери. Отдолу са изброени някои от тях:

* **Linux Mint -** Линукс Минт (на английски: Linux Mint) е безплатна GNU/Linux дистрибуция, базирана на Debian и Ubuntu, която има за цел да бъде „модерна, елегантна и удобна операционна система, която е едновременно мощна и лесна за употреба“ За разлика от някои други Linux дистрибуции, Mint предоставя пълна мултимедийна поддръжка, включвайки софтуер не само с отворен, но и със затворен код Целта е потребителят да започне работа веднага след инсталацията, без да се налагат допълнителни настройки или инсталация на софтуер. Mint е подходящ както за професионалисти, така и за обикновени потребители.

Проектът е замислен от Clément Lefèbvre и се разработва активно от Linux Mint общността.

* **Ubuntu**

Ubuntu е една от най-популярните дистрибуции, чиято цел е да предостави безплатна, бързо стартираща, лесна за използване, поддържаща повечето езици и достъпна за всички Linux дистрибуцияДумата „Ubuntu“ означава „човечност“ на езика [зулу](https://bg.wikipedia.org/wiki/%D0%97%D1%83%D0%BB%D1%83). Официални подпроекти на Ubuntu са Kubuntu, Xubuntu и Lubuntu. По подразбиране Ubuntu пристига с графична среда [GNOME](https://bg.wikipedia.org/wiki/GNOME), докато Kubuntu e с [KDE](https://bg.wikipedia.org/wiki/KDE), Xubuntu с [Xfce](https://bg.wikipedia.org/wiki/Xfce), а Lubuntu с [LXDE](https://bg.wikipedia.org/wiki/LXDE).

Това е единствената разлика между тях. Друг официален подпроект е Edubuntu, която включва много образователен софтуер. Благодарение на спонсора си, [Canonical](https://bg.wikipedia.org/wiki/Canonical) Ltd., компания, собственост на основателя на Ubuntu – [Марк Шътълърт](https://bg.wikipedia.org/w/index.php?title=%D0%9C%D0%B0%D1%80%D0%BA_%D0%A8%D1%8A%D1%82%D1%8A%D0%BB%D1%8A%D1%80%D1%82&action=edit&redlink=1), инсталационни Live CD се разпращат безплатно до целия свят

1. **Видове мрежови атаки:**

*Повечето атаки могат да бъдат категоризирани в един от следните шест класа:*

* **Злонамерен софтуер** (Malware): - това е основен термин за софтуер, който е създаден със злонамерени цели. Той включва вирусни атаки, червеи, рекламен софтуер, троянски коне и шпионски софтуер. Това са най-често срещаните опасности за една компютърна система.
* **Пробив в сигурността: -**  тази група атаки включва всеки опит за получаване на неоторизиран достъп до системата.

Това включва разкриване на пароли, превишаване на права, проникване в сървър, всички дейности, които най-често се свързват с термина „хакерство“.

* **Атаки от тип „отказ от услуга**“ (DoS): - вид атака, която причинява загуба на услуга или невъзможност на мрежата да функционира. При тази атака зложелателите нямат достъп до системата, а блокират достъпа на легитимните потребители. Един от начините да се блокира дадена легитимна услуга е да се наводни целевата система с множество фалшиви заявки за свързване. При това тя неможе да отговори на легитимните заявки. DoS е най-често срещаната атака в уеб.
* **Уеб атаки: -**  това е всяка атака, която се опитва да наруши/промени даден уеб сайт. Две от най-често срещаните такива атаки са: SQL injection (SQLi) Това е метод за уеб атака, чрез която хакерът може да внедри и изпълни SQL команди върху базата данни на даденият сайт и XSS (cross-site scripting) атака, която използва уязвимост на приложението, за да “вмъкне“ нежелан код, който се изпълнява в браузъра на крайния потребител.
* **“Отвличане”** на HTTP сесии (Session hijacking): - тези атаки представляват отвличане на идентификатора на потребителската сесия (session hijacking), при което е възможно злонамерени потребители да осъществят достъп до чужди данни, принадлежащи на даден потребител.
* **DNS отравяне** (DNS poisoning): - този тип атаки компрометират DNS сървъра така, че потребителите могат да бъдат пренасочени към зловредни уеб сайтове, включително и към уеб сайтове с цел фишинг.

Фишинг атаките са най-разпространената форма на интернет измама. Това е широко използван похват от компютърни престъпници за получаване на важна информация.

Te целят да подмамят хората да предоставят важна лична информация, най-често подробности по кредитни карти и банкови сметки. Злонамерен софтуер (Malware) Вредното програмно осигуряване е общ термин за програми, които умишлено нанасят вреда на компютърните системи и мрежи. Malware е основен термин за софтуер, който има злонамерени цели.

Следва описание на трите типа злонамерен софтуер: вируси, троянски коне и шпионски софтуер. Вируси Според Symantec (създателите на Norton antivirus и други софтуерни продукти) вирусът е „малка програма, която се размножава и се скрива в други програми, обикновено без знанието на потребителя“.

* **Троянски кон** - получава името си от мита за Троянската война. Компютърният троянски кон изглежда привидно като нормален софтуер, а всъщност тайно прехвърля вируси или друг тип зловреден софтуер на компютъра.

Троянските коне най-общо казано са програми, които работят като скрити процеси на даден компютър и дават пряк или косвен достъп на външни лица до личната информация на потребителя.

Много често се използват за получаване на таен достъп до системата, на която са инсталирани, т.е. някой отдалечено контролира компютъра.

Троянските коне са тип зловреден код с универсално приложение – първоначално представящ се за легитимно и полезно приложение, което всъщност извършва подмолни действия.

Постепенно се появяват и такива, които не изискват потребителят да ги стартира, а се възползват от уязвимостите в операционната система и определени програми, за да се наместят незабелязано в системата.

Троянските коне могат да изпълняват различни задачи: отваряне на задна врата, следене на натиснати клавиши и/или запис на екрана (ако разполага с вграден метод за това), изтегляне или публикуване на файлове на/от компютъра, кражба на ценни данни, изтриване на файлове, забавяне и/или блокиране на системата и др. Именно затова са и много често срещани във виртуалното пространство.

* **Шпионски софтуер -**  друга категория зловреден софтуер е шпионският софтуер (spyware). Това е софтуер, който следи какво прави потребителя на компютъра си.

Той може да бъде под формата на обикновена бисквитка (cookie), която уеб сайтът, който потребителят посещава, поставя на компютъра му и използва, за да го разпознае, когато той го посети отново. Друга форма на шпионския софтуер са програмите, които записват натиснатите клавиши на клавиатурата. Действието се нарича keystroke logging, а програмите - keylogger. Подобни програми са тези за запис на екрана – това са най-често снимки на определена област около курсора.

Данните се съхраняват, за да се изпратят покъсно на източника, инсталирал шпионския софтуер или директно се изпращат чрез e-mail.

Това е един от най-често срещаните начини за кражба на акаунти и/или пароли, номера на кредитни карти и други лични за даден потребител данни. Програмите за запис на дейности (най-често натиснати клавиши) често се инсталират от шпионския софтуер.

* **Логическа бомба** - е софтуер, който остава скрит докато не настъпи някакво специфично събитие. Това събитие може да е дата и време. При настъпване на това събитие софтуерът извършва злонамерени дейности като например, изтриване на файлове, промяна на системните конфигурации или дори пускане на вирус.

## 6. Защита на мрежата, сървъра и архива – защита се прави на сървъра, мрежата и архива.Защита на мрежата на физическо и логическо ниво.

## Информационна сигурност e защитата на информацията и информационните системи от неоторизиран достъп, използване, разкриване, промяна, прочитане, запис и унищожаване.

## 7. Мерки за сигурност - Външните и вътрешните заплахи могат да бъдат избегнати при прилагане на определени мерки за сигурност, като:

* **Използване на операционни системи с висока степен на сигурност** - Съвременните операционни системи удовлетворяват това изискване.

Например разновидностите на **Windows или Linux** очакват въвеждането на валидно потребителско име и парола, за да позволят зареждане и работа със системата.

Съхранението на паролите e във вид, неудобен за осъществяване на лесен достъп до тях;

* **Автентикация и идентификация -** автентикацията е процес на удостоверяване на правилния потребител.

В качеството на синоним на термина автентификация понякога се използва термина "проверка на идентичност".

Идентификацията позволява на субекта да назове себе си. За целта се използват различни идентификатори, като парола, личен идентификационен номер, криптографски ключ и др. Например правилността на паролата за определено потребителско име гарантира, че потребителят е автентичен. Друг често използван идентификатор за удостоверяване на самоличността на регистриран вече потребител на даден уебсайт, като част от процеса на влизане, е използването на „бисквитки“ (cookies).

Те могат да спестят повторно въвеждане на потребителско име и парола при всеки следващ достъп до този сайт.

Представляват текстови данни, които се съхраняват на клиентската система, обвързват се с конкретен браузър и сайт, и съдържат информация, която браузъра изпраща към сървъра при всяка негова заявка.

Бисквитките имат различен период на валидност, от временни файлове, съществуващи до момента на напускане на уебсайта или деактивирате на използвания уеб браузър, до запазени за указан срок.

* **Криптиране на данните -** криптирането на данните е технология, базирана на науката криптография.

Криптирането използва код или ключ за разбъркване (шифриране) и след това за подреждане (дешифриране) на данните, с цел представянето им в първоначалната им форма. Данните се криптират с помощта на алгоритъм или шифър;

* **Използване на защитна стена (Firewalls) и прокси сървър -** защитната стена филтрира входящите и изходящите пакети и определя дали да разреши преминаването на даден пакет. Тя се настройва от администратора на мрежата и обикновено се разполага на шлюза (gateway) на мрежата.

Прокси сървърът функционира като посредник между системите от вътрешната мрежа и тези от външната. Например една от функциите на такъв сървър е свързана с кеширане (съхраняване) на Web страници за подобряване на качеството на Web услугата;

* **Използване на антивирусен софтуер -** в днешно време е задължително използването на антивирусни програми за защита на системата от вируси.

Антивирусният софтуер, открива вирусни инфекции, сигнализира за тях и се опитва да предотврати евентуални техни поражения;

* **Ограничаване на физическия достъп -** тази стъпка е свързана с определяне на степента на директен физически достъп на лица до ресурсите на мрежата.

При висока степен на сигурност сървърите и устройствата за връзка трябва да се поставят в зони без достъп на физически лица, освен упълномощените за това. Работните станции, които се намират в незащитени райони трябва да ограничават по софтуерен начин достъпа до важните данни в мрежата.

* 1. **Модел на информационната сигурност:**

Най-използваният модел на информационна сигурност включва три основни компонента – конфиденциалност, интегритет и достъпност

* **Конфиденциалност** - предотвратяване разкриването на информация на неоторизирани лица или системи.

Примери могат да бъдат - надничане в компютърен екран при наличие на чувствителна информация, загуба на мобилен компютър или флаш памет, както и предаване на данни през компютърна или телефонна мрежа, когато няма физически контрол върху преносната среда.

* **Интегритет -** невъзможността за промяна на информацията без разрешение. Интегритета е нарушен, когато служител несъзнателно или съзнателно изтрие или унищожи важна информация.
* **Достъпност -** представлява възможността информацията да бъде достъпна, когато е необходима.

Прекъсването на ток, техническите проблеми, свързани със софтуер и хардуер, не трябва да прекъсват работните процеси, свързани с обработка и съхранение на информацията.

1. **Управление на риска -** това е процес по установяване на уязвимостите и заплахите, както и мерки за намаляването на риска до приемливи нива.

Той е важна част от защитата на информацията. Управлението на риска и сигурността са непрекъснати процеси.

1. **Мерки за налагане на информационна сигурност:**

* **Административни мерки -** тези мерки включват одобрени процедури, стандарти и указания.

Те информират персонала какво трябва и какво не трябва да прави при всекидневната си работа. Пример за такива мерки са политиките за сигурност.

Тези мерки формират базата за техническите и физическите мерки.

* **Логически мерки -** тези мерки включват използването на софтуер, мониторинг и контрол на достъп до информацията и компютърните системи.

Примери за това са пароли, антивирусен софтуер, защитни стени, контроли за достъп, криптиране и други.

Чрез ограничаване на правата на всеки потребител или програма, се предоставят само необходимите права за изпълнение на определените задачи.

Пример за нарушение е използването на компютър за всекидневни задачи с администраторски права.

* **Физически мерки -** тези мерки включват контрола над работната среда като контрол на достъп, видео наблюдение, алармена инсталация, системи за противопожарна охрана, заграждания и жива охрана са пример за такива мерки.
  1. **Класификация на информацията:**

Елемент от информационната сигурност и управлението на риска е класификацията на информацията и дефинирането на процедури за защитата в зависимост от тази оценка.

* **Служебна информация** – може да обработва, съхранява и предава информация само върху компютърни системи и мрежи и електронни носители, собственост на организацията. Не се разрешава публикуване и предаване в Интернет без разрешение;
* **Публична информация** - може да се обработва, съхранява и предава свободно;
* **Конфиденциална информация** - може да се обработва, съхранява и предава само върху компютърни системи и мрежи, собственост на организацията, които не са свързани с Интернет.

Забранява се записа, съхранението, публикуването или предаването на информацията без одобрението на организацията.

1. **Основни заплахи за сигурността на информацията:**

* **Зловреден софтуер** - Това е софтуер, който работи без знанието и информираното съгласие на потребителите на дадена компютърна система. Това включва компютърни вируси, червеи, троянски коне, софтуер за шпиониране и други;
* **Нелоялни служители -** Служител, който съзнателно се стреми да навреди на конкретния бизнес или работодател. Такъв служител може да запише и изнесе чувствителна информация, до която има достъп.

Може технически (вреден софтуер, прихващане на трафик) или по друг начин да придобие неоторизиран достъп до такава информация. Изнасянето може да стане с помощта на външен електронен носител (флаш памет, преносим диск, мобилен телефон) или чрез изпращане през интернет;

* **Човешка грешка -** несъзнателно действие или бездействие на служител, което вреди на организацията.

Това може да е в следствие подвеждане, немарливост или незнание. Тези грешки могат да доведат до заразяване с вреден софтуер, да спомогнат на нелоялни или външни лица, целящи да навредят на организацията, да предизвика техническа неизправност или да унищожи информация, като се даде достъп до нея през интернет или се изгуби електронен носител;

* **Техническа неизправност -** може да се получи в следствие на софтуерна грешка, отказ на хардуера, природно бедствие, човешка грешка, злоумишлени действия на служител или външно лице. Техническите неизправности водят до спирането на услуги и прекъсват дадени процеси. Неизправност може да доведе и до загуба на информация;
* **Външни атаки -** това са действия на софтуер или трети лица, които целят да навредят на дадена организация.

Тези действия могат да доведат до изтичане или унищожаване на важна информация. Това може да стане отдалечено – с използване на уязвимост в операционната система, в системния и приложния софтуер, с прихващане на пароли, с използване на вреден софтуер;

* **Локално съхранени данни -** обичайните мерки се прилагат към копията от имейли (изпратени и получени), които са запазени на вашата собствена машина.

Криптирайте драйвърите си, решавайте и следвайте подходяща политика за изтриване на информация.

* **Данни по кабела -** имейлът обикновено пътува през число от отделни подскоци между изпращача и получателя. Тази диаграма илюстрира обичайните стъпки, които съобщението би трябвало да измине, предавателните протоколи, използвани за тези стъпки и възможните типове криптиране за тях.

**11. Криптиране: -** криптирането на данни е най- сигурния метод за защита на архивите на сървърите.

Криптиране може да се прави на данните които се съхраняват на масива, както и на съобщенията които се предават по mail – serverite.

Криптирането има за цел да преобразува информацията преди предаване по канала за връзка така, че тя да не може да бъде разчетена от друг, освен от получателя, за който е предназначена.

Обикновено криптирането разчита на два компонента – алгоритъм за криптиране, който в повечето случаи е известен и ключ (парола), с която се прави криптирането.

Науката за шифриране на съобщения се нарича криптография.

Няма алгоритъм, който не може да бъде разбит, целта на всеки алгоритъм за криптиране е да се увеличи времето за разбиване на кода до толкова, че да не си струва влагането на толкова усилия или информацията вече да бъде неизпозлваема. Някои методи за атаки имат за цел да разкрият криприраното съобщение, а други атакуват самия ключ.

В повечето случаи целта на криптографията е преобразуването на информацията да бъде без загуби – т.е. от криптираната информация да може да бъде възстановена оригиналната.

В някои частни случаи целта е да се удостовери изпращаната информация и/или самият изпращач.

Тогава криптирането може да използва алгоритми със загуба на информация.

Тъй като криптирането променя структурата на предаваната информация, както и компресията на данните, двете функции могат да се използват едновременно – например ако се компресира един файл с използване на парола, той е едновременно компресиран и криптиран.

*! В съвременния свят се използват няколко вида алгоритми за криприране на информацията:*

* **Симетрична криптография. -** Принципът на работа е следния: източникът и получателят имат предварително избран алгоритъм и ключ.

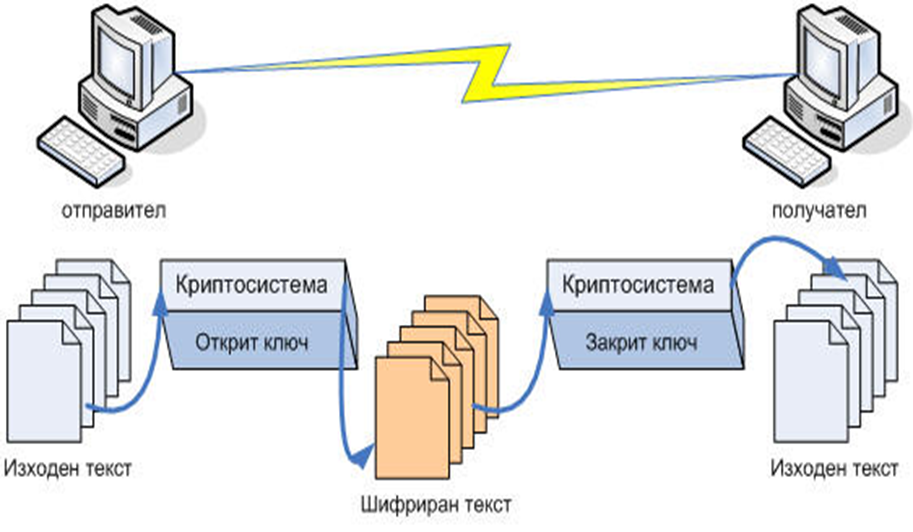
Източникът стартира алгоритъма за криптиране в права посока и криптира информацията, използвайки ключа.

Получателят декриптира информацията със същия ключ, използвайки същия алгоритъм в обратна посока.

Недостатък на метода е необходимостта от предварителен контакт (обмен на парола) между кореспондентите.

* **Несиметрични алгоритми** – криптирането и декриптирането се извършва по различен начин, а паролите за криптиране и декриптиране са различни.

Най- популярните представители на този клас са алгоритмите с открит ключ (Public-key cryptography), например алгоъмъ RSA.



Сървърът (получателят) изработва двойка ключове – частен и публичен.

Те са така подбрани, че с публичния ключ се криптира информацията, а с частния се декриптира. Публичният ключ се предава през мрежата към източника, който криптира информацията с него и я изпраща така по канала. Получателят декриптира информацията с частния ключ.

Така не е необходим предварителен контакт между двете страни, тъй като ключа за криптиране се предава по мрежата, но дори някой да го прихване – с него не може да се декриптира предаваната информация.

* **Криптиране от край до край на специфични имейли -** криптирането на имейли през целия път от подателя до получателя е било трудно в миналото, въпреки че инструментите за осъществяване на този вид „от край до край” криптиране стават по-доби и по-лесни за използване.

Pretty Good Privacy (PGP) и неговият безплатен братовчед GNU Privacy Guard (GnuPG) са стандартни инструменти, за да се направи това. И двете програми могат да осигурят защита на вашия имейл по пътя и също да защитят вашата съхранена информация.

Главни имейл клиенти като Microsoft Outlook и Mozilla Thunderbird могат да бъдат конфигурирани да работят гладко с криптиращ софтуер, който с просто кликане на бутон да означи, потвърди, кодира и декодира имейл съобщения.

Най-доброто при криптирането от край до край е, че е сигурно, че съдържанието на вашия имейл ще бъде защитено не само срещу прихващане по кабела, но също и срещу някои от заплахите към съдържанието на копия от вашите имейли, съхранявани на вашата машина или на машината на трета страна.

Има две уловки при GnuPG/PGP.

**Първата** е, че те работят само ако другите страни, с които кореспондирате също ги използват.

Неминуемо много от хората, с които разменяте имейли не използват GPG/PGP, дори и да е известен и употребяван между вашите приятели или в организацията.

**Втората** е, че вие трябва да намерите и потвърдите публичен ключ за хората, на които пращате имейл, за да сте уверен, че подслушващите не могат да ви надхитрят с използването на грешен ключ.

Тази хитрост е известна като атака „човек по средата”. Вероятно най-лесният начин да започнете да изполвате GnuPG е да използвате Mozilla Thunderbird with the Enigmail плъгин. Можете да намерите бърз начален гайд за инсталиране и конфигуриране на Enigmail.

* **Сървър към сървър криптиран транзит. -** след като натиснете **"SEND",** имейлите обикновено се предават по веригата от SMTP мейл сървъри преди да достигнат дестинацията си.

Можете чрез своя имейл клиент да разгледате в главата на всеки имейл, който получавате, за да видите веригата от сървъри, по която е пътувало съобщението.

В повечето случаи съобщенията са преминали през мейл сървърите без криптиране.

Но има стандарт, наречен SMTP over TLS, който позволява криптиране, когато изпращате и получавате сървъри за даден подскок от веригата, който той поддържа. Ако вие или вашата организация оперирате с мейл сървър, трябва да се убедите, че той поддържа TLS криптиране, когато общува с други мейл сървъри.

Прегледайте документацията на своя SMTP сървър софтуер, за да разберете как да упълномощите TLS.

* **Клиент към мейл сървър – криптиране -** Ако използвате POP или IMAP, за да получите имейла си, уверете се, че това е криптиран POP или IMAP. Ако вашият мейл сървър не поддържа криптирана версия на този протокол, нека вашият доставчик или системен администратор да поправи това.

Ако използвате уеб мейл услуга, уверете се, че имате достъп до нея само като използвате HTTPS, а не HTTP. Hushmail.com е уеб мейл доставчик, който винаги използва HTTPS и предлага и от край до крак криптиране (въпреки че те са неподатливи на съдебни разпореждания).

Много уеб мейл доставчици използват HTTPS само за страницата, на която се логвате и след това се връщат към HTTP.

Това не е сигурно. Потърсете опция в конфигурацията на вашия акаунт (или browser plugin), осигуряваща на вашия уеб мейл перманентна употреба на HTTPS. Ако не можете да намерите начин да се убедите, че виждате своя уеб мейл само през https, преминете на друг уеб мейл доставчик.

* **Информация, съхранявана на машините на втори и трети страни -** съществуват две главни причини, поради които вашите имейли да бъдат съхранявани на компютри, контролирани от трети страни.
* **Съхранение от вашия доставчик на услуги -** Ако няма да стартирате свой собствен мейл сървър, тогава има трета страна, която получава (или може да съхранява) копия от всички ваши имейли.

Това обикновено би могъл да е интернет доставчик, наемник или уеб мейл доставчик. Копия от съобщенията ще бъдат разпръснати и по компютри, контролирани от интернет доставчици, наемници и уеб мейл хостове на тези, с които си кореспондирате.

Уверете се, че вашият имейл софтуер е конфигуриран така, че да изтрива съобщенията от мейл сървъра на вашия интернет доставчик след като ги свали.

Това е най-повсеместната договорка, ако използвате POP, за да изтеглите своя имейл, но е обичайно за хора, използващи IMAP или уеб мейл да оставят копия от своите съобщения на сървъра.

Ако използвате уеб мейл или IMAP, уверете се, че триете съобщенията веднага след като ги прочетете.

Имайте на ум, че с големите уеб мейл услуги може да отнеме много време, вероятно месеци, преди съобщението да бъде наистина изтрито, независимо дали вие все още имате достъп до него или не.

С по-малък IMAP или уеб мейл сървър е възможен юридически достъп до копия от съобщения, взети с призовка години след като потребителят ги е изтрил. Съдържанието на кодираните PGP/GnuPG имейли не е достъпно през тези трети страни, въпреки че главите на мейлите (като „до”: и „относно” линиите) ще бъдат. Стартирането на собствен мейл сървър с криптиран хард или използването на криптиране „от край до край” за комуникации с висока степен на поверителност, са най-добрите начини за да смекчите тези рискове.

* **Съхранение от тези, с които кореспондирате -** повечето хора и организации пазят всички мейли, които са изпратили и получили.

Ето защо почти всеки имейл, който изпратите и получите ще бъде съхранен поне на още едно място, независимо от практиките и процедурите, които следвате.

В добавка на личната машина на човека, на когото изпращате или от когото получавате съобщение, копията могат да бъдат направени от техния интернет доставчик или фирмен мейл или бекъп сървър. Трябва да вземете тези копия в предвид и ако заплашителният модел, който имате за комуникации с висока степен на поверителност включва противник, който може да получи достъп до тези копия, тогава трябва или да използвате PGP за криптиране на тези съобщения или да ги изпращате по някакъв начин, различен от имейла.

Осъзнайте, че дори да използвате PGP, тези, с които комуникирате биха могли да са обект на призовка или изискване от правоохраняването да декодират вашата кореспонденция.

* **„От край до край” имейл криптиране -** имейл криптирането е тема, която би могла да напълни книга и е: вижте книгата на Брус Шнайер „Сигурност на имейла: Как да запазите поверителността на електронните си съобщения”.

Книгата е до известна степен извън времето (тя отпраща към стари версии на софтуера), но представената концепция е важна.

## Защита от отказ и възстановяване/хардуерна защита/ - Хардуерните повреди могат да бъдат сериозна причина за загуба на информация, затова е необходимо вземането на определени мерки за защита и възстановяване на данните от сривове.

## Могат да се предприемат някои препоръчителни действия в тази насока:

* **Използване на аварийно захранване** за избягване на проблеми с електрозахранването. Често срещан вариант е включването на UPS устройства, които притежават батерии, съхраняващи определено количество заряд, осигуряващо време за работа на системата след прекъсване на основното захранване.
* **Архивиране на данните с помощта на програма за архивиране**, в случай на повреда на твърд диск или вирусен проблем. Необходимо е осигуряване на допълнително устройства, където да се съхраняват архивираните данни.
* **Хеш алгоритми** – това са алгоритми със загуба на информация, при които не се изисква възстановяването на оригиналната информация.

Те най-често се използват за цифрови подписи. Най-често използваните в съвременния свят са MD5 и SHA, като първият вече се счита за компрометиран, но въпреки това е все още широко използван.

Преди изпращането на съобщението източникът изработва подписа чрез избраната хеш функция и съдържанието на съобщението. Полученият цифров подпис представлява фиксиран по размер брой битове, който се долепя в края на съобщението.

Получателят приема съобщението и подписа, по същата функция от съдържанието на полученото съобщение изработва нов хеш и го сравнява с получения подпис.

Ако двете стойности са еднакви, то това е гаранция, че съобщението не е променяно след предаването си. Цифровите подписи не криптират самото съобщение, а само удостоверяват неговото съдържание.

## Мрежова сигурност - е основен проблем при използване на мрежова среда. Съществуват немалко случай, свързани с проникване в мрежи на правителствени и бизнес организации, както и сериозни атаки от компютърни вируси в широк мащаб. Терминът сигурност се обвързва с необходимите действия, които трябва да се предприемат за защита на един компютър и съдържащата се в него информация.

# II. ВТОРА ЧАСТ

# ИМПЛЕМЕНТАЦИЯ НА СИГУРЕН MAIL – SERVER ПОД LINUX

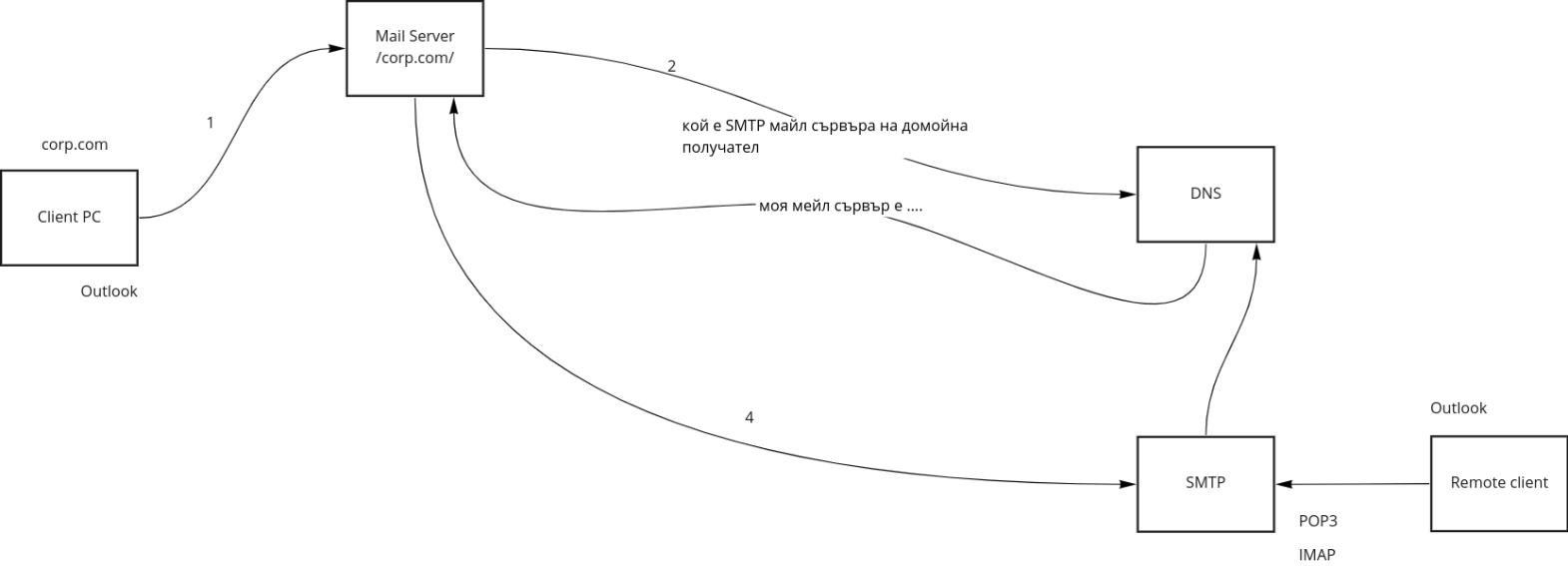
***1.Проектно предложение:***

На Laptop с характеристики : Intel Core i3- 3120M,2.5GHz; RAM-8GB; HDD-1TB; NVIDIA GeForce GT 635M е инсталиран Linux Ubunto и са виртуализирани две машини, на една от които е инсталиран сигурен mail – server. Postfix, основан от софтуерен инженер на Google, Wietse Venema работи не само с Linux, но и с AIX, BSD, HP-UX, IRIX, MacOS X, Solaris, Tru64 UNIX и други UNIX системи.

И поддържа MySQL, Memcache, SQLite, PostgreSQL, LDAP, CDB и Berkeley Database като съхранение на данни. Postfix може да бъде дефиниран като ефективен Linux пощенски сървър с отворен код със своите функции като контрол на нежелана поща, поддръжка на база данни и удобно управление на регистрационни файлове.

Той идва с филтър за съдържание, механизъм за контрол на достъпа, поддръжка на виртуален домейн, конфигурируеми известия за състоянието. Може да доставя над 300 имейла в секунда от един екземпляр на Postfix. Предоставяйки защитни механизми срещу злонамерен софтуер и спам ботове, той предлага сигурна услуга. Идеята от този сървър да се изпращат сигурни e- mail съобщения към определен брой потребители.

Схемата е :



***2.Техническо решение*** – стъпки при инплементиране на сигурен **MAIL – SERVER**

### Как да настроите пълен пощенски сървър (Postfix) с помощта на „Roundcube“ (Webmail) на Ubuntu/Debian?

### Създаването на пощенски сървър на машини, задвижвани от Linux, може да бъде едно от най-важните неща, които всеки системен администратор трябва да направи, докато конфигурира сървърите за първи път, ако не знаете какво означава това; просто е, ако имате уебсайт като „example.com“, можете да създадете имейл акаунт като „username@example.com“, за да го използвате за лесно изпращане/получаване на имейли, вместо да използвате услуги като Hotmail, Gmail, Yahoo Mail, и т.н.

### Как да го направим, като инсталираме пощенския сървър Postfix с приложението за уеб поща „Roundcube“ и неговите зависимости от версиите на Debian 10/9 и Ubuntu 20.04/18.04/16.04 LTS.On this page.

### Стъпка 1. Задайте име на хост и създайте DNS записи за домейн/

**Първо, задайте валидно име на хост FQDN (напълно квалифицирано име на домейн) за вашия сървър на Ubuntu, като използвате командата hostnamectl, както е показано.**

**/$ sudo hostnamectl set-hostname mail.tecmint.com/**

**Второ,** трябва да добавите записи MX и A за вашия домейн във вашия DNS контролен панел, който насочва други MTA, че вашият пощенски сървър mail.yourdomain.com домейн е отговорен за доставката на имейл.

MX record@ mail.tecmint.com mail.tecmint.com <IP-address>

### Стъпка 2: Инсталиране на Apache, MariaDB и PHP в Ubuntu/

* За да създадем работещ пощенски сървър с помощта на „Roundcube“, първо ще трябва да инсталираме пакетите Apache2, MariaDB и PHP, за да го изпълним$ sudo apt-get update -y

$ sudo apt-get upgrade -y

$ sudo apt install apache2 apache2-utils mariadb-server mariadb-client php7.4 libapache2-mod-php7.4 php7.4-mysql php-net-ldap2 php-net-ldap3 php-imagick php7.4-common php7.4-gd php7.4-imap php7.4-json php7.4-curl php7.4-zip php7.4-xml php7.4-mbstring php7.4-bz2 php7.4-intl php7.4-gmp php-net-smtp php-mail-mime php-net-idna2 mailutils

* На Debian 10/9 трябва да изтеглите и инсталирате SURY PHP PPA хранилище, за да инсталирате PHP 7.4 на Debian 10/9$ sudo apt -y install lsb-release apt-transport-https ca-certificates

$ sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg

$ echo "deb https://packages.sury.org/php/ $(lsb\_release -sc) main" | sudo tee /etc/apt/sources.list.d/php.list

$ sudo apt update

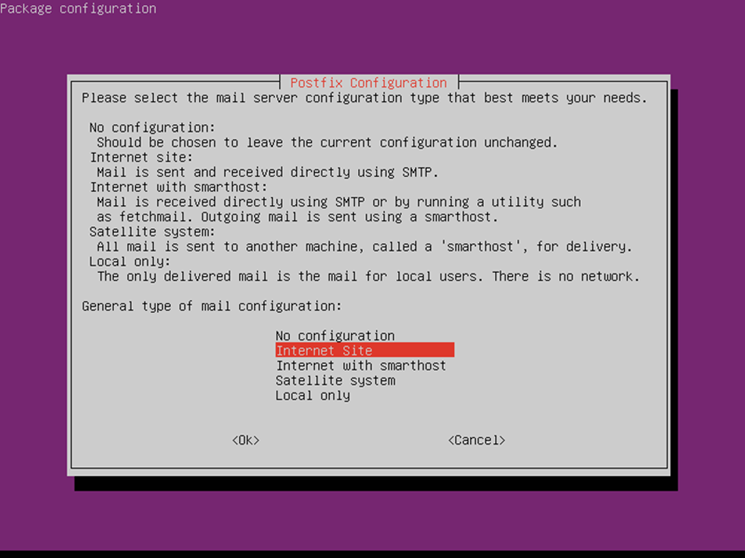
$ sudo apt install apache2 apache2-utils mariadb-server mariadb-client php7.4 libapache2-mod-php7.4 php7.4-mysql php-net-ldap2 php-net-ldap3 php-imagick php7.4-common php7.4-gd php7.4-imap php7.4-json php7.4-curl php7.4-zip php7.4-xml php7.4-mbstring php7.4-bz2 php7.4-intl php7.4-gmp php-net-smtp php-mail-mime php-net-idna2 mailutils

### Стъпка 3: Инсталиране на Postfix Mail Server в Ubuntu/

Postfix е агент за прехвърляне на поща (MTA), който е отговорният софтуер за доставка и получаване на имейли, това е от съществено значение, за да се създаде пълен сървър за електронна поща.

За да го инсталирате на Ubuntu/Debian или дори Mint, изпълнете:$ sudo apt-get install postfix

По време на инсталацията ще бъдете помолени да изберете типа конфигурация на пощата, изберет„Интернет сайт



*Install Postfix in Ubuntu*

* Сега въведете напълно квалифицираното име на домейн, което искате да използвате за изпращане и получаване на имейли.

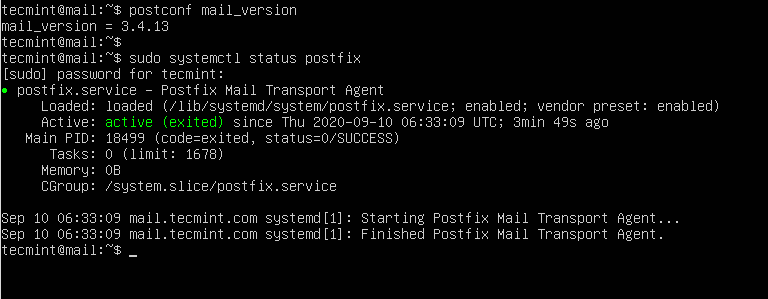
[[](https://www.tecmint.com/wp-content/uploads/2014/12/Set-Postfix-Mail-Domain.png)](https://www.tecmint.com/wp-content/uploads/2014/12/Set-Postfix-Mail-Domain.png)

*Set Postfix Mail Domain*

* След като Postfix бъде инсталиран, той автоматично ще стартира и ще създаде нов /etc/postfix/main.cf файл. Можете да проверите версията на Postfix и състоянието на услугата, като използвате следните команди.

$ postconf mail\_version

$ sudo systemctl status postfix

[[](https://www.tecmint.com/wp-content/uploads/2020/09/Check-Postfix-Version.png)](https://www.tecmint.com/wp-content/uploads/2020/09/Check-Postfix-Version.png)

*Check Postfix Version*

**Стъпка 4:** Тестване на Postfix Mail Server в Ubuntu /

* Сега опитайте да проверите дали вашият имейл сървър се свързва на порт 25, като използвате следната команда;

$ telnet gmail-smtp-in.l.google.com 25

Trying 74.125.200.27...

Connected to gmail-smtp-in.l.google.com.

Escape character is '^]'.

220 mx.google.com ESMTP k12si849250plk.430 - gsmtp

The above message indicates that the connection is successfully established. Type **quit** to close the connection.

* Можете също да използвате програма за електронна поща, за да изпращате и четете имейли, като използвате следната команда;

$ mail username@gmail.com

**Cc**:

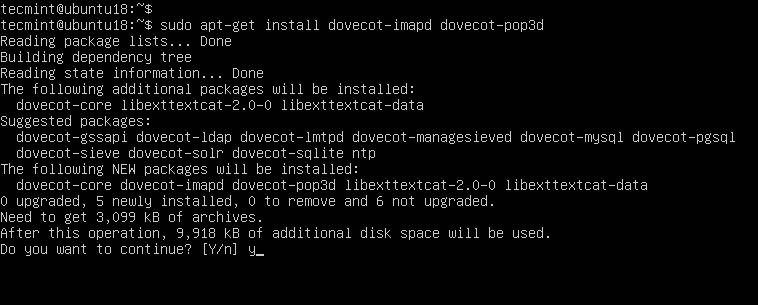
**Subject**: Testing My Postfix Mail Server

I'm sending this email using the postfix mail server from Ubuntu machine

**Стъпка 5:** Инсталиране на Dovecot IMAP и POP в Ubuntu /Инсталиране на Dovecot IMAP и POP в Ubuntu/

* **Dovecot** е агент за доставка на поща (MDA), той доставя имейлите от/до пощенския сървър, за да го инсталирате, изпълнете следната команда.

$ sudo apt-get install dovecot-imapd dovecot-pop3d

[[](https://www.tecmint.com/wp-content/uploads/2014/12/Install-Dovecot-in-Ubuntu.png)](https://www.tecmint.com/wp-content/uploads/2014/12/Install-Dovecot-in-Ubuntu.png)

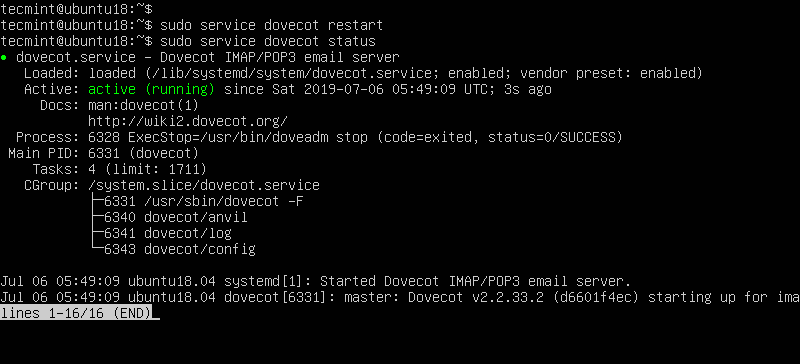
*Install Dovecot in Ubuntu*

* След това рестартирайте услугата Dovecot, като използвате следната команда.

$ sudo systemctl restart dovecot

или

$ sudo service dovecot restart

[[](https://www.tecmint.com/wp-content/uploads/2014/12/Start-Dovecot-in-Ubuntu.png)](https://www.tecmint.com/wp-content/uploads/2014/12/Start-Dovecot-in-Ubuntu.png)

*Start Dovecot in Ubuntu*

### Стъпка 6: Инсталиране на Roundcube Webmail в Ubuntu/

* **Roundcube е сървърът за уеб поща, който ще използвате за управление на имейли на вашия сървър, той има прост уеб интерфейс, за да върши работата, може да бъде персонализиран чрез инсталиране на повече модули и теми;**

$ wget https://github.com/roundcube/roundcubemail/releases/download/1.4.8/roundcubemail-1.4.8.tar.gz

$ tar -xvf roundcubemail-1.4.8.tar.gz

$ sudo mv roundcubemail-1.4.8 /var/www/html/roundcubemail

$ sudo chown -R www-data:www-data /var/www/html/roundcubemail/

$ sudo chmod 755 -R /var/www/html/roundcubemail/

* **След това трябва да създадете нова база данни и потребител за Roundcube и да предоставите всички разрешения на нов потребител да пише в базата данни;**

$ sudo mysql -u root

**MariaDB [(none)]>** CREATE DATABASE roundcube DEFAULT CHARACTER SET utf8 COLLATE utf8\_general\_ci;

**MariaDB [(none)]>** CREATE USER roundcubeuser@localhost IDENTIFIED BY 'password';

**MariaDB [(none)]>** GRANT ALL PRIVILEGES ON roundcube.\* TO roundcubeuser@localhost;

**MariaDB [(none)]>** flush privileges;

**MariaDB [(none)]>** quit;

* **След това импортирайте първоначалните таблици в базата данни Roundcube.**

$ sudo mysql roundcube < /var/www/html/roundcubemail/SQL/mysql.initial.sql

### Стъпка 7: Създайте виртуален хост на Apache за уеб поща на Roundcube

* **Създайте виртуален хост на apache за уеб поща на Roundcube;**

$ sudo nano /etc/apache2/sites-available/roundcube.conf

Add the following configuration in it.

<VirtualHost \*:80>

ServerName tecmint.com

DocumentRoot /var/www/html/roundcubemail/

ErrorLog ${APACHE\_LOG\_DIR}/roundcube\_error.log

CustomLog ${APACHE\_LOG\_DIR}/roundcube\_access.log combined

<Directory />

Options FollowSymLinks

AllowOverride All

</Directory>

<Directory /var/www/html/roundcubemail/>

Options FollowSymLinks MultiViews

AllowOverride All

Order allow,deny

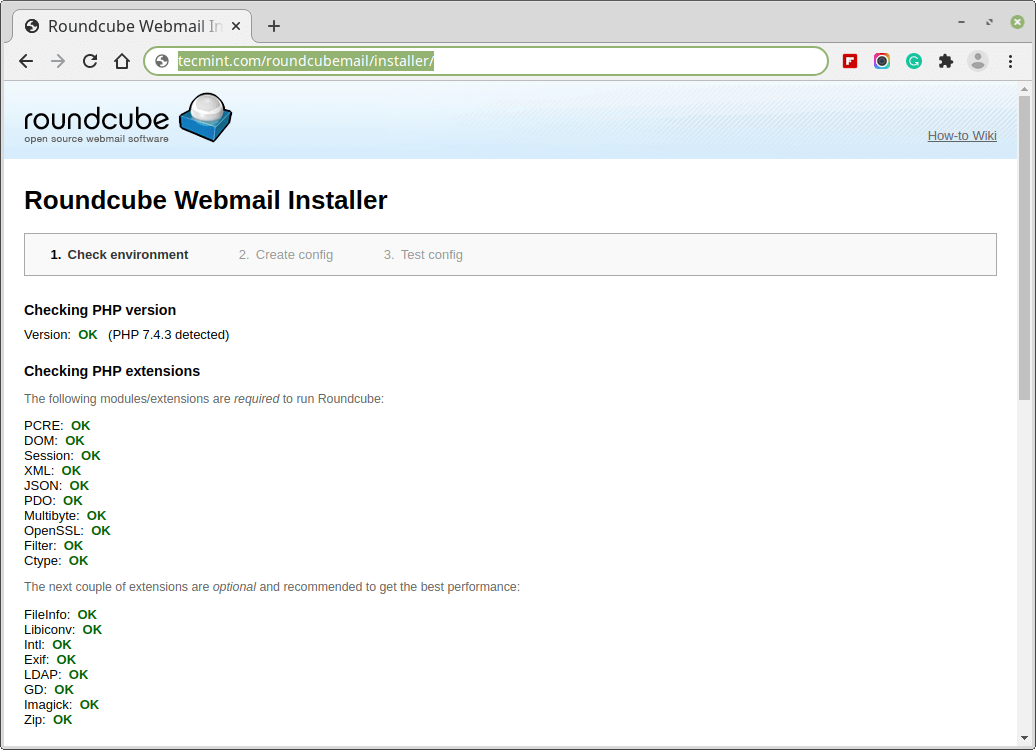
allow from all

</Directory>

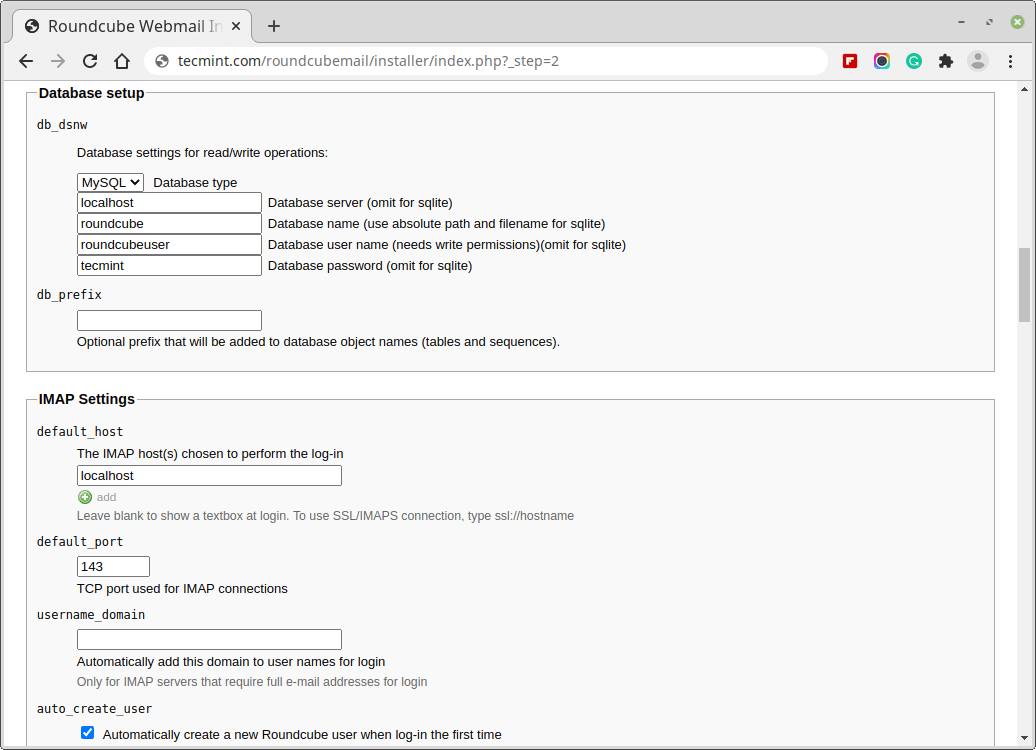
</VirtualHost>

$ sudo a2ensite roundcube.conf

$ sudo systemctl reload apache2

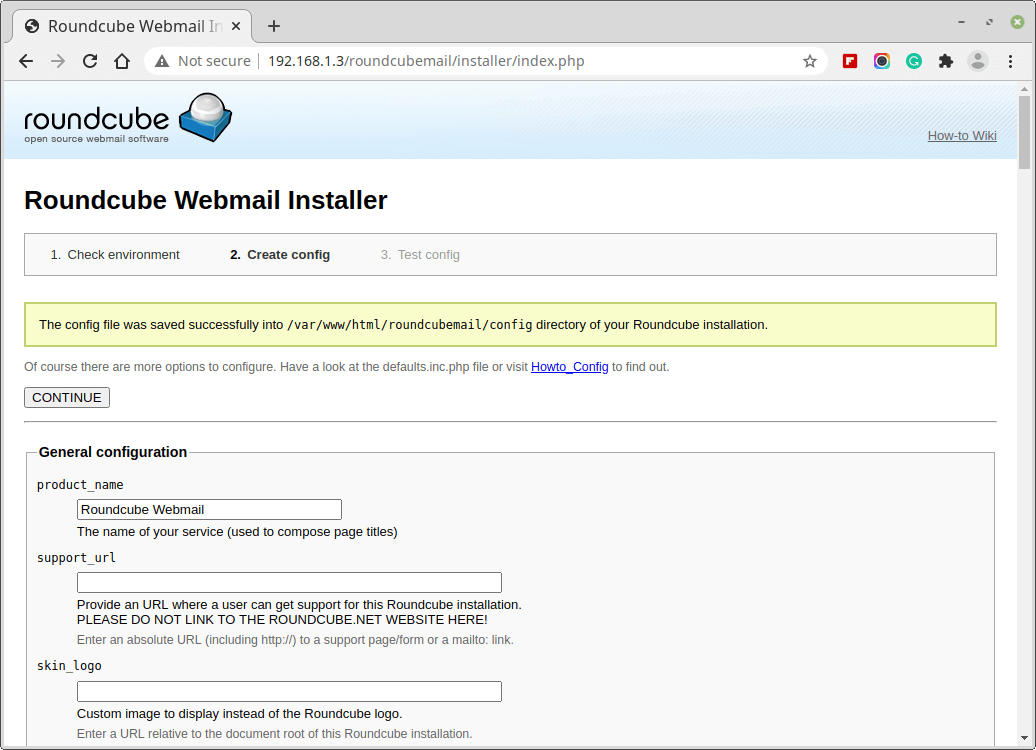
[](https://www.tecmint.com/wp-content/uploads/2020/09/Roundcube-Webmail-Installer.png)

* **След това отидете на настройките на базата данни и добавете данните за базата данни;**

[](https://www.tecmint.com/wp-content/uploads/2020/09/Roundcube-Webmail-Database-Settings.png)

*Roundcube Webmail Database Settings*

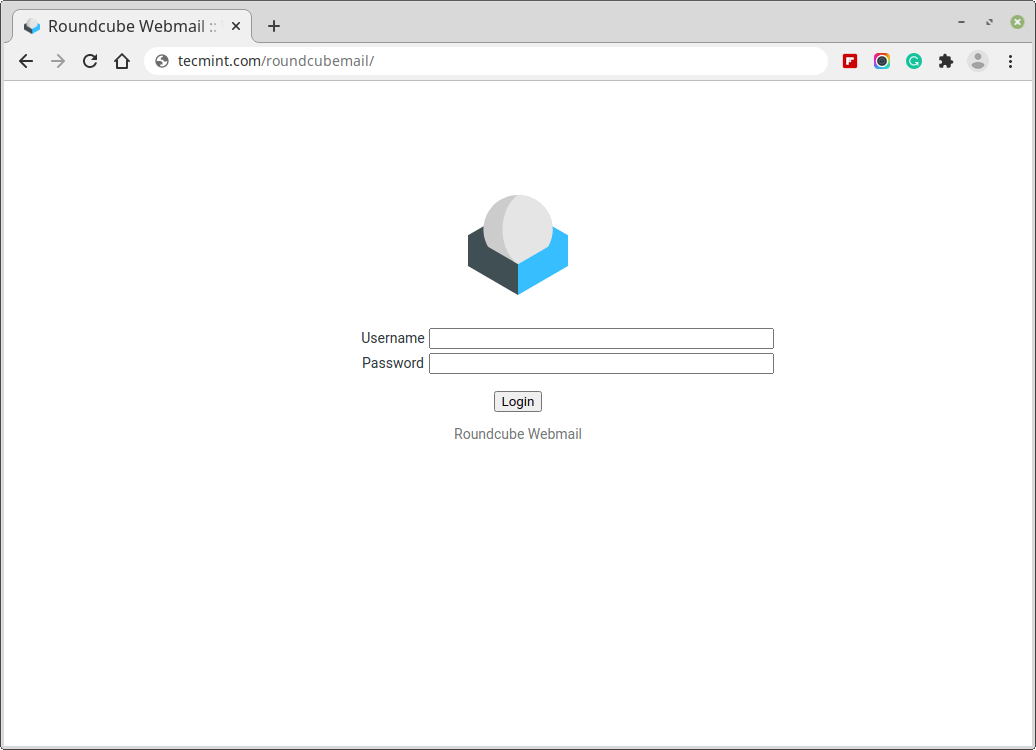
* **След като направите всички промени, създайте файл config.inc.php;**

[[](https://www.tecmint.com/wp-content/uploads/2020/09/Create-Roundcube-Configuration-File.png)](https://www.tecmint.com/wp-content/uploads/2020/09/Create-Roundcube-Configuration-File.png)

* **След приключване на инсталацията и финалните тестове, моля, изтрийте папката на инсталатора и се уверете, че опцията enable\_installer в config.inc.php е деактивирана;**

$ sudo rm /var/www/html/roundcubemail/installer/ -r

* **Сега отидете на страницата за вход и въведете потребителското име и паролата на потребителя;**

[[](https://www.tecmint.com/wp-content/uploads/2020/09/Roundcube-Webmail-Login.png)](https://www.tecmint.com/wp-content/uploads/2020/09/Roundcube-Webmail-Login.png)

**Стъпка 8**: Създаване на потребители на поща /Създаване на потребители на поща/

* За да започнете да използвате уеб пощата на Roundcube, ще трябва да създадете нов потребител, за да го направите, стартирайте:

$ sudo useradd myusername

Заменете „myusername“ с потребителското име, което искате, създайте парола за новия потребител, като стартирате.

$ sudo passwd myusername

* Сега се върнете на страницата за вход и въведете потребителското име и паролата на новосъздадения потребител.

**ИЗВОДИ, ОБОБЩЕНИЕ И ЗАКЛЮЧЕНИЕ**

**ИЗВОДИ:**

Пощенски сървър, известен още като имейл сървър, е приложение, което може да съхранява и прехвърля имейл. Когато се изпрати имейл, той преминава през различни пощенски сървъри, преди да достигне до своя получател.

Въпреки че в днешно време писмата се доставят почти мигновено, това е много сложен процес. Има много приложения за пощенски сървър, които работят на операционни системи Linux. Тези, които искат да управляват частен уеб сървър или искат да наемат такъв като част от цялостно хостинг решение чрез доставчик, често са изправвени пред една стара дилема – Linux или Windows?

Тези две операционни системи доминират уеб хостинг пазара от години, борейки се за цифрова хегемония, като Linux определено води в тази надпревара. Заради минималните различия при двете системи по отношение на функции и приложения, решението става още по-трудно.

Един задълбочен поглед към двете системи ще даде разяснения на потребителите относно предимствата и недостатъците на тези две системи.

Най-често това съперничество се свежда до въпрос на съвместимост на приложенията.

**Предимствата и недостатъците на на Linux като операционнна система**

В сравнение с Windows, основната философия на Linux се свежда до запазването на структурата на операционната система колкото може по-проста.

Всички компоненти, включително устройства и процеси, са файлове и настройки към ядрото на системата.

Съществуват много простио инструменти, които могат да помогнат с настройката и администрирането на системата. Това обикновено се случва чрез командната лента, но, при нужда, може да се направи и през графичният интерфейс (GUI), който е достъпен през почти всички приложения.

Само че с голямата свобода идва и голямата отговорност, които лесно могат да повалят неопитния потребител.

*Основни слабости и силни страни на Linux като сървърна операционна система.*

|  |  |
| --- | --- |
| **Предимства** | **Недостатъци** |
| Безплатна | Сложна за работа |
| Администраторите са облагодетелствани от свободите, които систеата предлага | Някои програми могат да бъдат инсталирани само от администратора |
| Подкрепя съдействената работа без нормални потребители да могат да нарушат или пренастроят ядрото на програмата | Изучаването на Linux системи не е на фокус при много хардуерни и софтуерни инженери |
| Рядко е обект на кибер престъпления | Процеса по обновяване на системата може да бъде много сложен процес понякога |
| Рядко има проблеми със сигурността, а ако се появят такива, лесно можем да се справим с тях | Не всички версии имат дългосрочна поддръжка |
| Малко хардуерни изисквания | Някои професионални програми не се поддържат от Linux |
| Интегрирана дистанционна функция за дистанционно адинистриране |  |

**Предимства и недостатъци на Windows** **като сървърна операционна система**

Фактът, че Linux, за разлика от Windows, има сложна структура, е главно заради фактът, че Windows винаги са се стремяли към простотата на операционната система.

Всички програми са достъпни и ясни, чрез интуитивен графичен интерфейс.

Това значи, че администрирането чрез командна лента не е необходимо, въпреки че технически все още е възможно.

По принцип потребителят има контрол над хардуерните ресурси, получава редовна информация за състоянието на системата и може да я накара сама да си инсталира софтуер. Това обаче крие и един друг потенциал – този на честите грешки.

Това се случва, когато системните настройки биват променени, ако потенциално опасни програми биват инсталирани.

*Основни слабости и силни страни на Windows като операционна система за сървъри.*

|  |  |
| --- | --- |
| **Предимства** | **Недостатъци** |
| Лесна за управление дори от начинаещи, благодарение на графичния потребителски интерфейс | Високи разходи за лицензиране, които се увеличават с всеки потребител |
| Драйверите за най-новия хардуер са лесно достъпни | Чести грешки по сигурността |
| Поддържа голям брой приложения на външни разработчици | Уязвима срещу зловреден софтуер |
| Ъпдейти, които се инсталират лесно и могат да бъдат автоматизирани по желание | Изразходва голям ресурс, заради графичния интерфейс |
| Техническите проблеми могат да се решат чрез системно рикавъри | Твърде много потребителски грешки |
| Гарантирана дългосрочна поддръжка | Не е подходяща за система с много потребители |
| Съвместима с най-популярните програми на Microsoft – Sharepoint или Exchange | Начинът, по който функционира патентованата система, не е напълно разкрит |

**ОБОБЩЕНИЕ:**

**Linux срещу Windows – сравнение**

Ето и най-важните критерии за сравнение на двете сървърни операционни системи:

|  |  |  |
| --- | --- | --- |
| **Windows** | | **Linux** |
| Цена | Лиценз за всеки потребител | Безплатен лиценз – цената за разпространение зависи от поддръжката |
| Опериране | Графичен интерфейс | Командна лента |
| Дистанционен достъп | Краен сървър/клиент трябва да бъде инсталиран и настроен | Интегрирано решение |
| Софтуер и функционалности | Поддържа популярни програми | Не е съвместим с всички програми. Въпреки това голям арсенал от приложения, включени в системата |
| Поддръжка на хардуера | Обикновено Windows системите вървят в комплект с нов хардуер | Обикновено трябва да се чака драйверите за Linux да излязат за новия хардуер |
| Сигурност | Уязвима към потребителски грешки. Интегрираният интерфейс се смята за потенциална начална точка за атака | Обикновените потребители нямат достъп до основните системни настройки; пробивите в сигурността се овладяват бързо |
| Документация | Дългосрочна поддръжка за всички версии | Офертата за поддръжка варира според разпространението и версията |

**ЗАКЛЮЧЕНИЕ:**

В крайна сметка няма как да се определи победител в битката между Linux и Windows. Двете операционни системи могат да бъдат ползвани като 2 различни средства за едно и също нещо.

Докато Windows предлага по - комплексни функции, за по - лесно структуриране на потоците данни за работа и комуникация, Linux бележи със статута си на предпочитана система за уеб приложения, като например системи за управление на съдържанието.

## Сравнение на сигурността на Linux и Windows

Докато говорим за сигурност, макар че Linux е с отворен код, обаче е много трудно да се пробие и следователно това е **изключително сигурна операционна** система в сравнение с другите операционни системи. Неговата високотехнологична сигурност е една от основните причини за популярността и огромното използване на Linux. Междувременно Linux е с отворен код и има **силна потребителска общност**. Тъй като цялата потребителска база има достъп до изходния код, те могат да следят за проблеми и има големи шансове **всяка уязвимост да бъде открита по-рано, отколкото хакерите са я насочили.**

Нещо повече, потребителите на Linux ще разследват и отстраняват проблема тогава и там, *тъй като е с отворен код. По този начин Linux получава страхотно ниво на поддръжка от* своята общност от разработчици.

За разлика от това, потребителите на Windows **не могат да решат проблема сами**, тъй като нямат разрешение да модифицират изходния код. Ако засекат някаква уязвимост в системата, ще трябва да я докладват на Microsoft и след това да изчакат да се поправи.

**Linux използва IP таблици за повишаване на сигурността на системата**. Iptables помагат за контролиране на мрежовия трафик, като конфигурират определени правила, налагани чрез защитната стена на ядрото на Linux. Това помага за създаването на по - сигурна среда за изпълнение на всяка команда или достъп до мрежата. Linux има **сегментирана работна среда**, която го предпазва от атаката на вируса. Операционната система Windows обаче не е много сегментирана и по този начин е по - уязвима към заплахи.

Друга важна причина Linux да бъде по-сигурен е, че Linux има **много малко потребители** в сравнение с Windows. Linux има близо 3% от пазара, докато Windows заема повече от 80% от пазара. По този начин хакерите винаги са по - заинтересовани от насочването към Windows, тъй като създаденият от тях вирус или злонамерен софтуер ще засегне голям сегмент от потребители. Това от своя страна поддържа потребителите на Linux по-безопасни.

Накратко можем да кажем, че Linux има някои функции, които го правят по-сигурен от Windows и другите операционни системи.

*Администраторът на системата се нарича****root****потребител.*

Той има всички права над всичко и всички. Останалите потребители имат ограничени права спрямо операционната система и пълни права във собствената си директория, която се намира в директорията **/home**. Това означава, че потребителят може да се разпорежда само със директориите и файловете в директорията на акаунта си **/home/потребител**, но не с файлове и директории на други потребители или в системните директории. Всички програми и услуги, стартирани от определен потребител, придобиват неговите права. Някои програми, предназначени за управление на операционната система, не могат да се стартират от обикновен потребител, а само от **root**. Всички директории и файлове са притежание на потребителите означени не само с име, но и със специални флагове, показващи няколко неща:

**1.** Файловете трябва да се указват дали са изпълними или не.   
**2.** Чия собственост е файла или директорията.   
**3.** Права за употреба на файловете и директориите. Тук имаме три варианта:   
**a)** права на собственика,   
**b)** права на потребителите от групата   
**c)** права на другите потребители

*Тези три пункта имат следните възможности:*  **a)** файла или директорията са забранени   
**b)** файла или директорията може да се отворят, но не и да се променят   
**c)** файла или директорията може да се отварят и променят.

Така изготвения дипломен проект може да бъде използван за учебни цели . Може да бъде полезно ръководство по теория и практика, както за ученици, така и за учители. Едно такова помагало може да бъде ползвано за професионална подготовка на учениците от специалностите Компютърна техника и технологии и компютърни мрежи. Може да се ползва по предмети като Компютърни мрежи, софтуер и операционни среди, Комплексна практика по специалността и др. Този дипломен проект може да се ползва стъпка, по стъпка за изграждане на сигурен mail – server, както от професионалисти така и от любители компютърни и мрежови „специалисти“.

# 

# ИЗТОЧНИЦИ

# ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Virtual Private Networking with Windows Server 2003: Overview, Microsoft Corporation, 2003г.

2. Linux as a VPN Client to FireWall-1, Ron Naken, Elie Bitton, 2000г.

3. Security and Cryptographer Refresher, Cisco Systems inc., 2000г.

4. Trivial Denial of Service Attack against TCP-based VPN, Alex Pankratov, Cipherica Labs, 2003г.

5. “Компютърни мрежи”, Дебра Шиндър, Софтпрес, София, 2003г.

1. Ръководство КМ на Делян Генков
2. **Компютърна сигурност и информационна защита на компютърни системи и мрежи**
3. Основни типове заплахи за компютърните системи и мрежи

Валентина Войноховска, Светлозар Цанков

**ЕЛЕКТРОННИ ИЗТОЧНИЦИ**

1. <https://uroci.net/urok/3169/Linux-Mail-Server-From-A-Z.html>
2. <https://bg.delachieve.com>
3. <https://bg.erch2014.com/kompyutery/62754-pochtovyy-server-na-linux-obzor-i-nastroyka.html>
4. <https://www.tecmint.com/setup-postfix-mail-server-in-ubuntu-debian/amp/>
5. https://help.superhosting.bg/mail-server-explained.html
6. https://help.superhosting.bg/differences-mail-server-mail-client.html
7. https://serversmtp.com/bg/bg\_smtp-mail-server-administrators/