ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТЕЛЕКОМУНИКАЦИИ – СОФИЯ

КОМПЮТЪРНИ МРЕЖИ

***ЗАДАНИЕ ЗА КУРСОВ ПРОЕКТ***

***ПРОЕКТИРАНЕ НА ЛОКАЛНА МРЕЖА***

*Ученик: Кирил Костадинов Стоичков Клас 11Д № 21*

*Да се проектира локална компютърна мрежа на фирма с 22 работни места.*

*Разположението на компютрите да бъде както следва:*

* *На първия етаж - 10 работни места в 2 отдела ;*
* *На втория етаж – 9 работни места в 3 отдела ;*
* *На всеки етаж – мрежов принтер за общо ползване ;*
* *В складове, отдалечени на 50 метра и видима връзка – 3 работни места ;*

*Проекта съдържа:*

* *Текстова част включваща: литературен преглед, анализ на необходимите мрежови услуги и капацитет на пренос, анализ и план за сигурност, избор на топология и обосновка, таблица на използваните адреси, маршрутна таблица за всеки рутер, таблица с обозначение /маркировка/ на мрежовите връзки, спецификация на активните устройства и пасивни компоненти, съдържание, използвана литература.*
* *Графичната част включва: физическа топология на мрежата, разположение на мрежовите устройства от първи, втори и трети слой на OSI модела.*

***Предаване на проекта за оценяване – до 11 юни 2017 г.***

*Дата на издаване: 27.03.2017 г. Дата на предаване:.................................*

*Проверил:...................................*

*Съдържание:*

*2 – 6 стр. – видове компютърни мрежи*

*6 – 9 стр. – план за сигурност*

*9 стр. – избор и обосновка на избраната топология*

*10 стр. – packet tracer*

*11 стр. – IP таблица*

*12 – 13 стр. – маршрутни таблици*

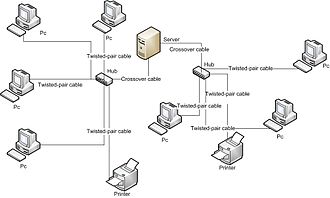
*14 стр. – чертеж на 2та етажа*

*15 стр. – таблица за окабеляване*

*16 стр. – таблица с активни и пасивни у-ва*

* 1. **Литературен преглед – схеми и анализ на видовете компютърни мрежи, технически данни.**

**Компютърната мрежа** (за по-накратко – **мрежа**) е съвкупност от хардуерни компоненти и компютри, свързани помежду си чрез преносна среда, която позволява обмен на информация помежду им . Устройствата участващи в мрежата, за да обменят данни трябва да бъдат свързани помежду си чрез технология на свързване. Най-разпространените връзки са *кабелната (коаксиален,* *усукана двойка или оптичен кабел)* и *безжичната (радиовълнова, сателитно предаване, лазерна или инфрачервена технология)*. Възможна е връзка чрез допълнително устройство – *рутер* (маршрутизатор). Най-известната мрежа е *Интернет*.



Компютърните мрежи биват:

* Локални мрежи (Local Area Network – LAN)
* Глобални мрежи (Wide Area Network – WAN)
* Градска мрежа (Metropolitan Area Networks – MAN)

***Локална мрежа (LAN)***

вид малка компютърна мрежа, обслужваща компютри и други устройства (напр. мрежови принтери или скенери), свързани помежду си. За разлика от големите (международни) WAN мрежи, локалната мрежа се разполага обикновено в една сграда. В днешно време най-разпространени са технологиите на свързване Ethernet или Wi-Fi, за разлика от миналото, когато са били използвани предимно [ARCNET](https://bg.wikipedia.org/w/index.php?title=ARCNET&action=edit&redlink=1), Token ring и др.

Видове локални мрежи:

**Според организацията**

Според организацията на управлението локалните мрежи са два основни вида:

* Мрежи с равноправен достъп (peer-to-peer)
* Мрежи клиент-сървър (client-server)

При мрежите клиент-сървър един от компютрите има централна роля и се нарича сървър, а останалите се наричат клиенти. Те ползват услугите, осигурени от сървъра.

При мрежите с равноправен достъп се позволява всеки компютър в мрежата да работи и като клиент, и като сървър. Този вид мрежи премахват нуждата от скъп сървър, но имат извести недостатъци. Споделените файлове са разпръснати из цялата мрежа, което затруднява тяхната защита.

**Според топологията**

[](https://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Intercpunetstar.png)

Мрежа тип „звезда“

Основните типове топологично структуриране са: звездовидно *(star)*, token ring *(токен ринг, букв. „маркеров кръг“)* и шина *(Bus)*. Топологичните деления се различават по начина на пренос на данни:

* Най-разпространената мрежова структура която се използва днес е тип „звезда“. При нея всеки един компютър се свързва чрез кабел директно към комутатора – суич или рутер.

[](https://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Intercpunetring.png)

Мрежа тип „token ring“

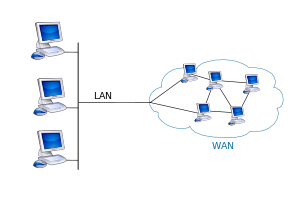
* При структурата token ring всеки компютър е свързан само с двата съседни, като така се получава затворен кръг. Информацията може да се движи само в една посока, като се задава централно, кой компютър може да предава данни в даден момент. Това се извършва чрез маркера *(token)*, който представлява 3 битов сигнал и циркулира по кръга.
* Най-старият вид е топологията тип – шина. При нея всички компютри са свързани с един кабел. Тъй като мрежата има начало и край, трябва да се добави [терминатор](https://bg.wikipedia.org/w/index.php?title=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D1%82%D0%BE%D1%80_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)&action=edit&redlink=1) в двата края на мрежата. Терминаторът предпазва линията от т.нар. „отскачане на сигнала“.
* **Според йерархията**

Йерархичното деление е основно на два типа: работна група (Workgroup) и домейн (Domain). При работната група всички компютри са равнопоставени, докато в домейна йерархичната структура е пирамидална.

***Глобална мрежа (WAN)***

[Компютърна 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) с голям обхват. Те могат да бъдат разположени на различни места в света като връзката често минава през спътник. На практика всяка мрежа, чиито връзки преминават през границите на различни организации, области или държави може да се счита за **WAN** мрежа. За разлика от тях [персоналните мрежи](https://bg.wikipedia.org/w/index.php?title=PAN&action=edit&redlink=1) (PAN), [локалните мрежи](https://bg.wikipedia.org/wiki/LAN) (LAN) и [кампусните мрежи](https://bg.wikipedia.org/w/index.php?title=CAN&action=edit&redlink=1) (CAN) или [метро мрежите](https://bg.wikipedia.org/w/index.php?title=%D0%9C%D0%B5%D1%82%D1%80%D0%BE_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0&action=edit&redlink=1) (MAN) обикновено са разположени в една стая, сграда или град съответно.

WAN мрежите се използват за да свързват много LAN и други видове мрежи, така че потребителите и устройствата разположени в една от тези мрежи да могат да достъпват, да обменят информация и да използват ресурси от отдалечените мрежи.



***Градска мрежа (MAN)***

[Компютърна 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) на територията на един град, чрез която всеки две точки в зоната на покритие могат да се свържат една с друга чрез [оптичен кабел](https://bg.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D0%BD_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB), без да е нужно кабелът да е прекалено дълъг от едната точка до другата. По своя обхват MAN мрежата се намира по средата между [WAN](https://bg.wikipedia.org/wiki/WAN) (Wide area network) мрежата като [Интернет](https://bg.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) и [LAN](https://bg.wikipedia.org/wiki/LAN) ([локална мрежа](https://bg.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D0%BD%D0%B0_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0)), които осъществяват достъпа на крайните абонати.

## **Мрежови модели**

Целта на моделите е да се представи една абстрактна концепция визуално, за да се създаде представа за дадена струткура, процес или релационна връзка.

**Моделът OSI**

Моделът OSI (*Interconnection*) e разработен от Международната организация за стандартизация **(ISO)**.

Моделът OSI е изграден от седем слоя, всеки от които представлява една стъпка в процеса на мрежовите комуникации. Седемте слоя на OSI:

* *Приложен (Application)*
* *Представителен (Presentation)*
* *Сесиен (Session)*
* *Транспортен (Transport)*
* *Мрежов (Network)*
* *Канален (Data link)*
* *Физически (Physical)*

**Моделът DоD**

*(наричан*[*TCP/IP модел*](https://bg.wikipedia.org/wiki/TCP/IP)*)*

Моделът на DoD (Department of Defense) – разработен 10 години по рано от OSI модела, през 70-те.

Разработен със сътрудничество със TCP/IP - част от проекта ARPAnet. Той е по-прост модел, състоящ се само от четири слоя, които могат да бъдат приблизително асоциирани със седемте слоя на OSI модела.

Слоеве:

* *Приложение/процес (application/process layer)*
* *Хост до хост(транспортен слой) (host to host)*
* *Интермрежа (internetworking layer)*
* *Мрежов интерфейс (network interface layer*)
  1. ***Проучване и анализ на необходимите мрежови услуги и капацитет на преносна среда, анализ и план за сигурност***
  2. **Нива на сигурност на операционната система**

За всеки потребител се задават:

• права за достъп до системата и нейните ресурси;

• време за влизане;

• потребителска директория;

• дата на изтичане. Важен момент при задаването на тези настройки е дефинирането за всеки акаунт на достъпа до ресурсите на системата! Операционната система предлага ключови потребителски акаунти, които автоматично се активират по време на инсталацията. Administrator – първоначален акаунт. Той е с пълни права в мрежата и може да:

• стартира мрежата;

• инсталира файлове и програми на операционната система;

• настройва първоначалните параметри на системата за сигурност;

• създава други потребителски акаунти;

• поделя директории и принтери. Guest – посетителски акаунт. Дава временен достъп до мрежата на някой, който няма акаунт. Мрежовите операционни системи могат да поддържат хиляди акаунти. Мрежовият администратор ще бъде затруднен, ако реши да извърши някакви настройки върху всички акаунти или дори само върху част от тях. Почти във всяка мрежова операционна система различни потребителски акаунти се обединяват в един общ акаунт, наречен група. Групата е акаунт, съдържащ други акаунти. Основната причина за въвеждането на групите е улесняване на администрирането. Групата дава възможност на администратора да третира голям брой потребители като един-единствен акаунт. Правата за достъп се настройват за групата и всичките й членове автоматично ще по- лучат и наследят тези права. Правата за достъп за различните групи могат да бъдат различни. Така например за потребителите в Group\_1 може да бъде разрешен пълен достъп до file1.doc - да могат да четат, променят и съхраняват файла, но за потребителите от Group\_2 – само да четат този файл.

* 1. **Сигурност на паролите**

• Паролата не трябва да съдържа имена на роднини, рождени дати, адреси, телефони;

• Да не се използват смислени думи, които се съдържат в речниците. Комбинацията между букви и цифри е добър вариант;

• В паролата да има включени главни и малки букви на случайни позиции (например DoYspGO);

• Паролата трябва да бъде лесна за запомняне от потребителя. В противен случай тя ще бъде записана на хартия, което не е желателно;

• Да се използват дълги пароли (поне 8 символа);

• Периодично потребителите трябва да сменят паролите си;

• Съвременните операционните системи притежават възможности за задаване на правила при въвеждане на потребителските пароли – минимална дължина, история, срокове за изтичане на паролата, както и изисквания към символите, които са включени в паролата.

• Хеша на всички пароли да бива проверяван в hash и rainbow таблици постоянно за да се знае кога вече паролата е много уязвима. Също така тя не трябва да съществува в никой от известните wordlist-ове или dictionary-та за bruteforce на пароли.

* 1. **Криптиране и подписване на файлове /електронни документи/** Политиката за сигурност на данните във фирмата включва засекретяване /криптиране/ и подписване на данните чрез използване на криптографски методи. - Криптиране - процес на преобразуване на данните във форма, трудна за разбиране от другите. При криптиране на файловете в една компютърна система единствено техният създател ще има достъп до тях. Криптирането използва код или ключ за разбъркване (шифриране) на данните и след това за тяхното подреждане (дешифриране). Разработени са програмни продукти за криптиране на информацията (писма, документи, бази от данни и др.). Те се базират на следните основни криптографски методи: криптиране с публичен ключ, криптиране със секретен ключ и др.

Препоръчва се използването на асиметрични алгоритми за криптиране.

* 1. **Сигурност на данните и мрежовите услуги**

• Authentication Header (AH) – осъществява проверка на самоличността на изпращащия IPsec.

• Encapsulating Security Payload (ESP) – гарантира конфиденциалност на самите данни. SSL (Secure Sockets Layer) е друго средство за гарантиране на сигурността на данните. Той използва криптиране с публичен и частен ключ. Работи в приложния слой на OSI модела. Програми за защита на електронната поща При изпращането на писма по електронната поща не се гарантира конфиденциалност. Писмата по време на своето пътуване до получателя преминават през различни сървъри. На всеки от тези сървъри може да бъде направено копие от тях. Затова са разработени програми за защита на електронната поща:

• Pretty Good Privacy

• Kerberos

• Baltimore Mail Secure и др. Защитни стени и проксита Важен момент от защитата на една локална мрежа е използването на защитна стена (firewall). Защитната стена се поставя между вътрешната мрежа и външния свят. Firewall се използва срещу злонамерени атаки от отдалечени компютри. Също така тя позволява да се регламентира и ограничи достъпа на програмите и потребителите в локалната мрежа до Интернет услуги

* 1. **Физическа сигурност**:

• всяко устройство да се маркира с инвентарен номер;

• да се изисква легитимиране на външните посетители, преди да бъдат допуснати до оборудването;

• работните станции и сървърите да се държат в заключващи се помещения;

• там където това не е възможно, да се въведе софтуерна защита. Използване на технически средства за защита

• система за видеонаблюдение;

• алармена система (СОТ);

• кодови брави;

• система с персонални магнитни карти.

* 1. **Защита от външи атаки**

• постоянен мониторинг на мрежата

• мониторинг на firewall-a

• седмично сканиране на мрежата с Nmap, Nessus, OpenVas

• проверяване в exploit-db.com дали за някоя от версиите на софтуера, който се използва в мрежата има exploit, какъв е шанса да успее този exploit и колко неща може да направи.

• Wi-fi рутери колкото се може по-малко да има

• забрана на всички протоколи, които не се използват всеки ден

Извод: като цяло редовно да се сканира мрежата за технологични пропуски. Има какви ли не инструменти и скриптове за тестване на мрежи така, че не е необходимо да сте pen tester за да подържате добра сигурност на мрежата.

* 1. **Защита от вътрeшни атаки:**

• много внимателно с уволняването на служители, задължително backup на всичко до което има достъп преди да бъде уволнен

• секретарките и счетоводителките може да бъдат много опасни – ако с някаква магия успеят да обедят системнияt администратор да им даде да си работят с лаптопа от вкъщи се правят няколко неща:

* 1. пуска се VPN
  2. задължително се слага парола на BIOS-а на лаптопа на колежката
  3. хард диска се криптира
  4. задължително UEFI
  5. устройството се сканира и се прави опит с всички познати техники да бъде открадната информация от него
  6. ако е с Windows OS задължително се тества с PcUnlocker Enterprise Edition, ако успее да мине през паролата на Windows се забранява да се ползва лаптопа от вкъщи. (напоследък сме свидетели как програма за 45$ бърка в MBR partition на BIOS и маха паролата на Windows)

Заключение: всички това е в случай, че някой успее да открадне лаптопа и се добере до заплатите на цялата фирма.

• в никакъв случай не се уволнява системен администратор, може да струва много скъпо на фирмата, решението на проблема е да му предложите по-хубава работа някъде другаде

• никой не трябва да има достъп до каквито и да било мрежови у-ва освен системния администратор и хората, които отговарят за тях

Извод: Колкото и защитена да е една мрежа тя винаги ще бъде уязвима. Както е казано в War-games – “няма 100% сигурно компютърна с-ма“. Светът е свидетел на това даже как в мрежа без достъп до Интернет бива съсипана (за Stuxnet говоря).

Напоследък са модерни криптовирусите съответно те са с цел само изкарване на пари и винаги ще засягат операционните системи с най-много потребители (какъвто беше случая с WannaCry) така, че по далеч от Windows. По-добре всичко живо да си ползва Linux.

***1.3 Избор на топология и обосновка:***

- избрах топология - звезда. Според мен е най-добре тя да бъде използвана заради предимствата си:

- лесно се откриват повреди в съобщителната среда;

- лесно се добавят нови компютри;

- лесно се отстраняват съществуващи компютри;

- работоспособността на мрежата не зависи от отделните компютри;