

# Тармоқ хавфсизлиги

---

1-маъруза. Тармоқ хавфсизлиги тушунчаси ва унинг  
МОХИЯТИ



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

# Мақсад ва вазифалар



МАҚСАД

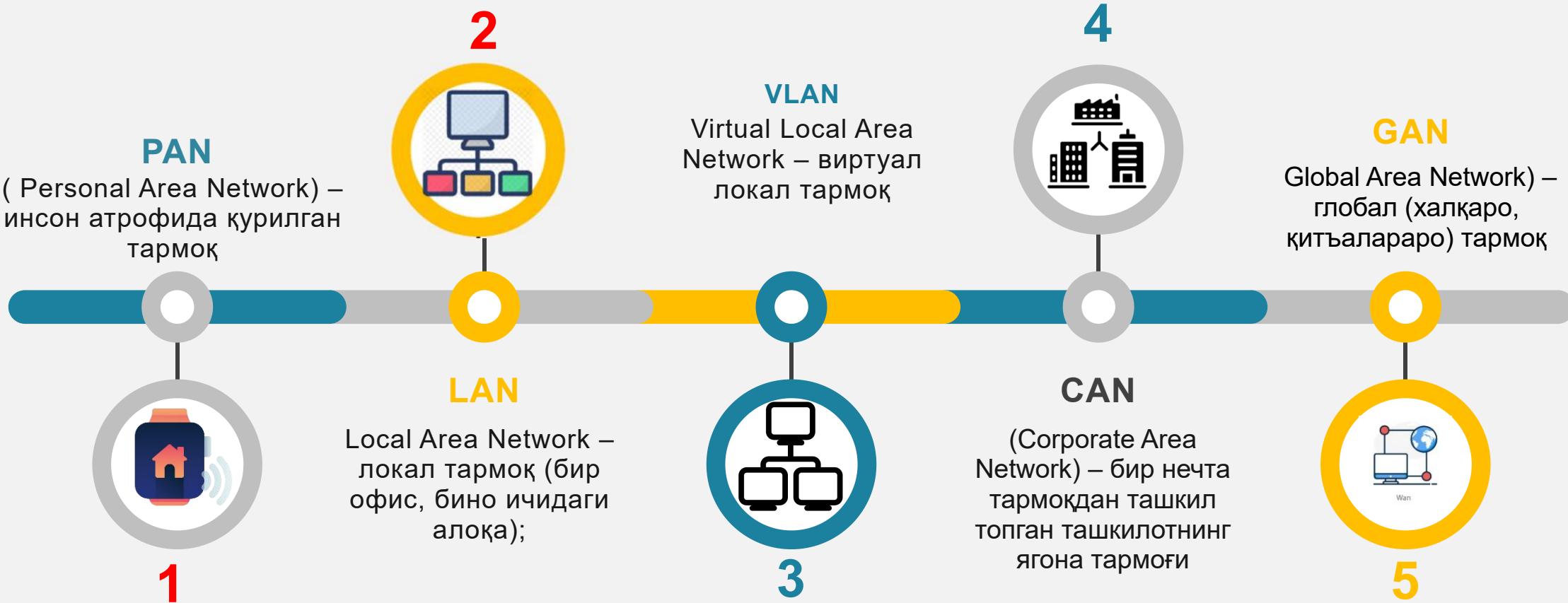
Талабаларга тармоқ хавфсизлигини таъминлаш соҳасидаги ҳалқаро ва миллий меъёрий, назарий ва амалий изланишлар натижалари билан таништириш билан бир қаторда тармоқ хавфсизлигини таъминлашда фойдаланиладиган усувлар, аппарат ва дастурий воситалар ва улардан фойдаланиш, тармоқ хавфсизлигини таъминлашда ҳимоя қурилмалари ва воситаларини қўллашга доир билимлар ва уқувлар ҳосил қилишдан иборат



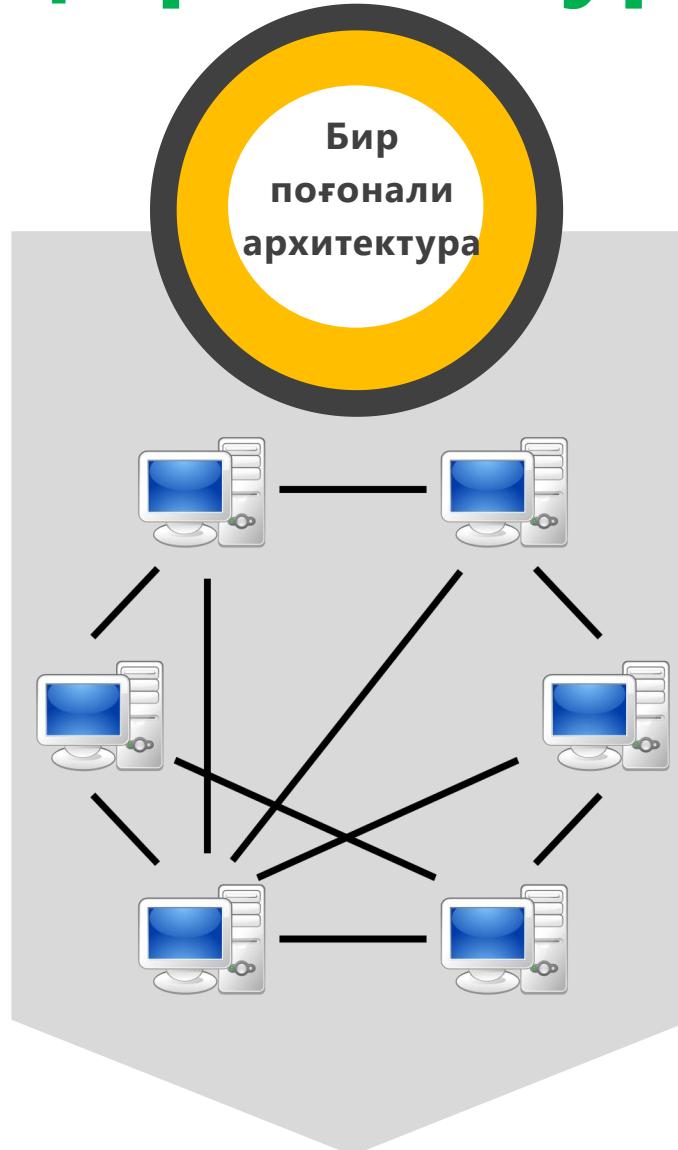
ВАЗИФА

Талабаларга назарий билимлар, амалий кўникмалар бериш, ҳамда тармоқ хавфсизлигининг асосий тушунчалари, тармоқ турлари ва тармоқ хавфсизлигига замонавий таҳдидлар, тармоқ хавфсизлиги стандартлари, тармоқ хавфсизлигини таъминлашда фойдаланиладиган воситаларнинг аҳамиятини очиб бериш

**Компьютер тармоғи** - фойдаланувчиларни алоқа каналлари ва коммутация воситаларини құллаган ҳолда үзаро маълумот алмашишлари, тармоқдаги техник, дастурий, ахборот ресурсларидан фойдаланышлари учун ягона тизимга уланган компьютерлар түпламидир.



# Тармоқ архитектураси



# Тармоқ топологияси

жисмоний

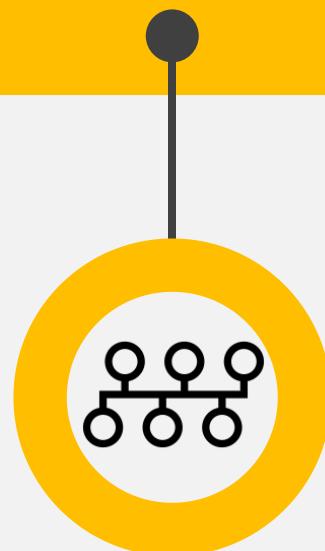
тармоқ тугуларининг алоқаси ёки жойлашишини акс эттиради

ахборотли

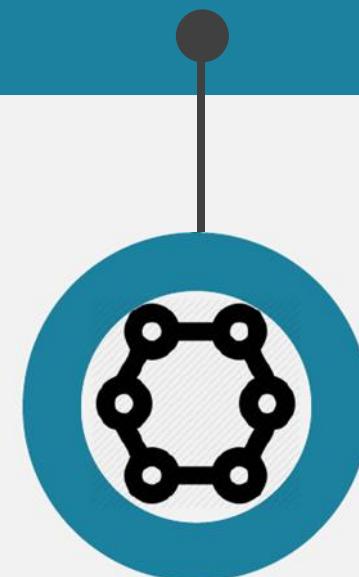
тармоқ бўйлаб узатилаётган ахборот оқимини акс эттиради

мантиқий

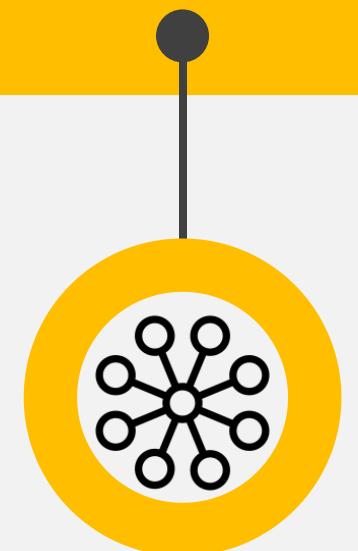
жисмоний топология доирасида сигналларнинг «ҳаракати»ни  
акс эттиради



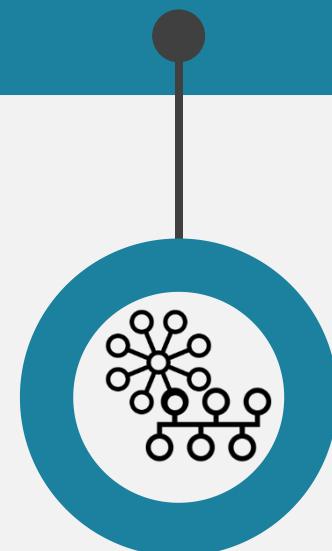
**Шина (автобус)  
топологияси**



**Халқа топологияси**



**Юлдуз топологияси**



**Гибрид топология**

# Тармоқ қурилмалари

Концентратор  
hub



алоқани ташкил этиш учун тармоқдаги қурилмаларни боғловчи, OSI моделининг 1-қатламида (яғни, жисмоний (физик) қатlam) ишлай олувчи тармоқ қурилмаси.

Свитч



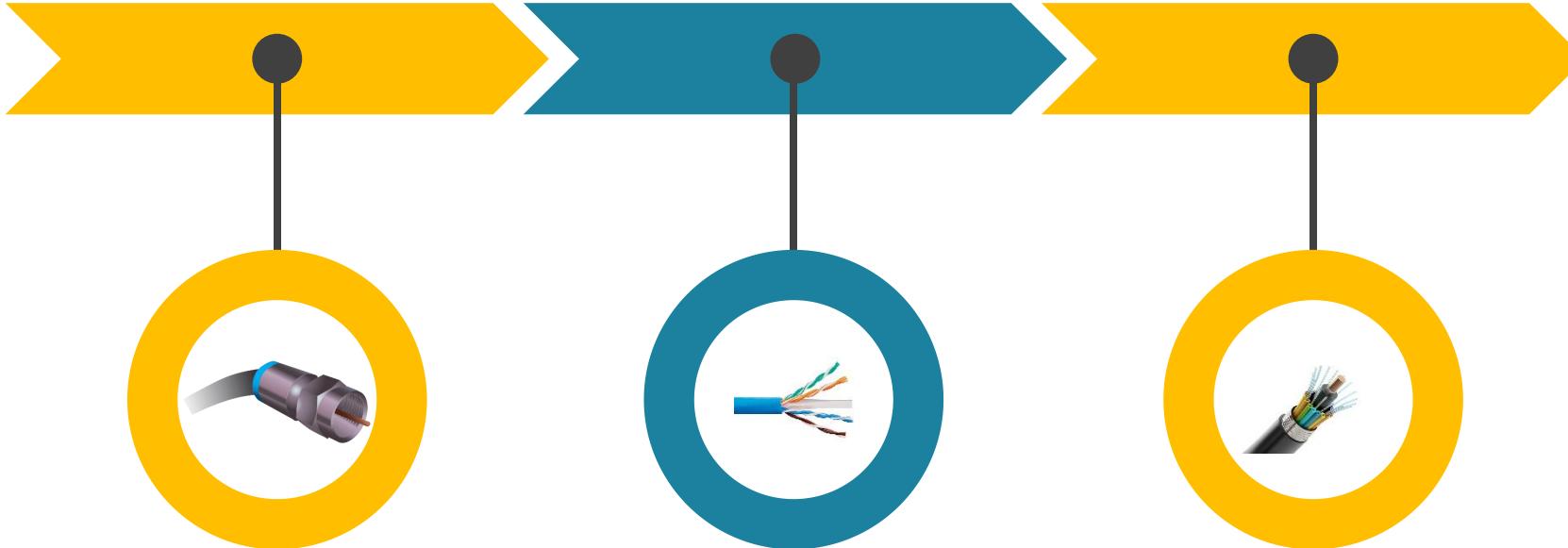
түгунлар коммуникациянинг OSI моделидаги 2 қатламда ишловчи тармоқ қурилмалари. Свитч «ақпли хаб» деб ҳам юритилади.

Роутер



OSI моделининг 3-қатламида ишловчи қурилма бўлиб, бир-биридан мустақил бўлган 2 ёки ундан ортиқ тармоқлар ўртасидаги алоқани ташкил этади.

# Тармоқ кабеллари



коаксиаль кабель

ўрама жуфт кабель

оптик толали  
кабель

# Коаксиаль кабель турлари



Қаттиқ  
линиялы  
(hardline)



Радиацион  
(radiating,  
“leaky”)



Эгизак үқли  
(twinaxial)



Уч үқли  
(triaxial)



Қаттиқ  
(rigid line)



Ярим қаттиқ  
(semi-rigid)



RG-6

# Ўрама жуфт кабель

UTP кабелларнинг категория бўйича техник тавсифи

Кабель категорияси	Частота кенглиги, МГцча	Маълумот алмашиш тезлиги, Мбит/секунд	Тавсифи
CAT1	0.1	-	Телефон, ISDN
CAT2	1	4	TokenRing, ҳ. қўлланилмайди
CAT3	16	10/100	телефон, 10BASE-T Ethernet
CAT4	20	16 (1ж)	100 метр, ҳ. қўлланилмайди
CAT5	100	100 (2ж), 1000 (4ж)	Ethernet
CAT5e	125	100 (2ж)	100 Mbps TPDDI, 155 Mbps ATM, Gigabit Ethernet
CAT6	250	1000 (4ж), 10 000 (50м)	Gigabit Ethernet
CAT6a	500	40 000	Gigabit Ethernet
CAT7	700	50 000	Gigabit Ethernet

# Оптик толали кабель

GOF

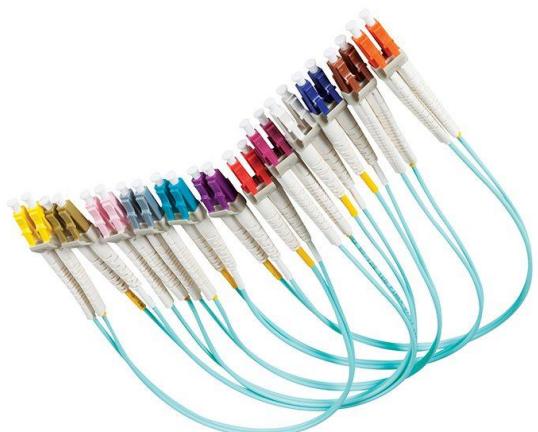


glass optic fiber cable

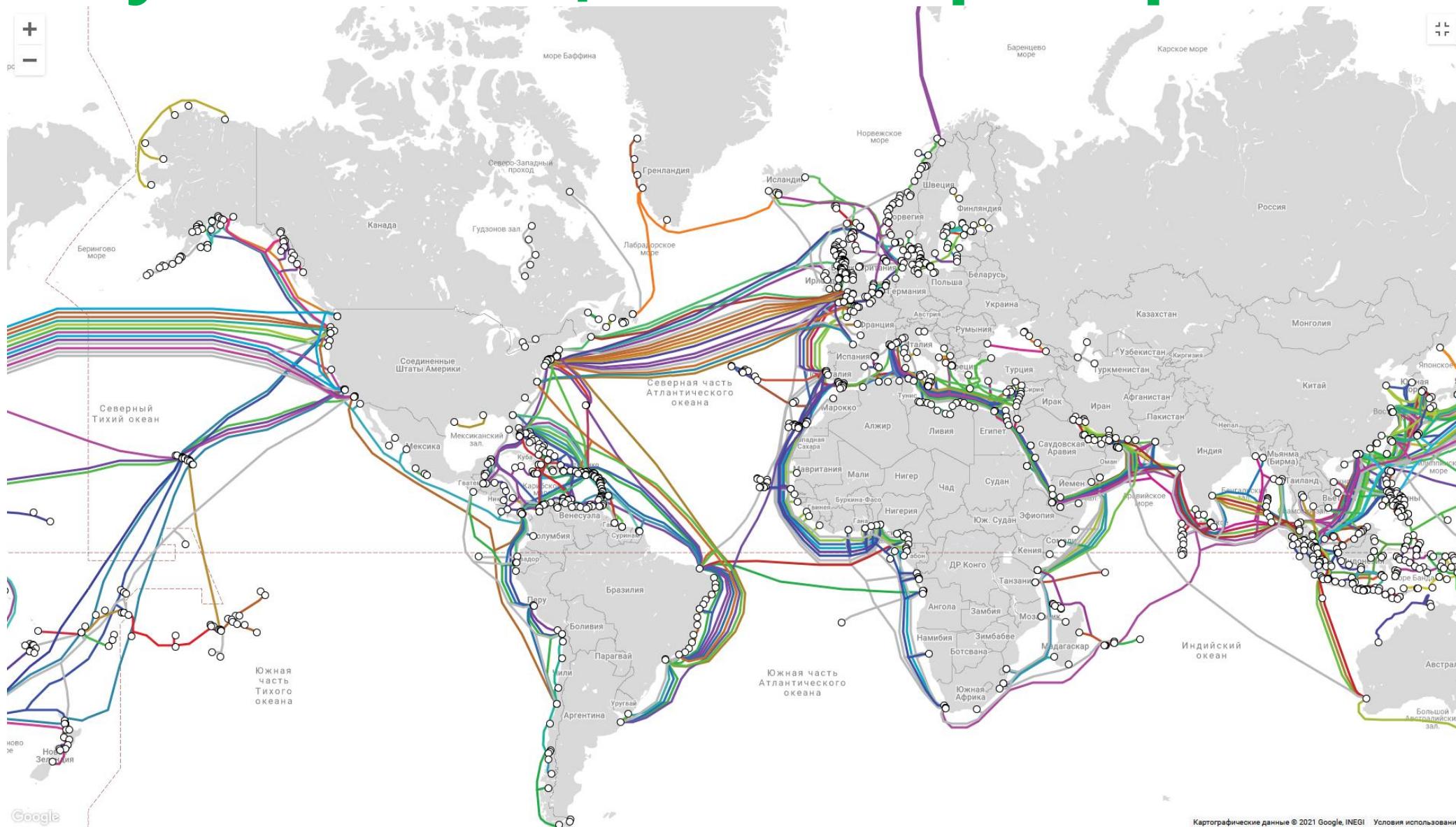
POF



plastic optic fiber cable



# Сув ости алоқа кабеллари харитаси



# Сув ости алока кабеллари



# Тармоқ манзиллари

IP манзил

IPv4  
IPv6

IPv4  
Құлланилиши: 1981  
Үлчами: 32 бит  
Формат: 192.168.100.13  
Префикс: 192.168.100.0/24  
Миқдори:  $2^{32} = 4.294.967.296$

IPv6  
Құлланилиши: 1999  
Үлчами: 128 бит  
Формат: fe80:20:f8ff:fe21:ab9::67cf  
Префикс: fe80:20:f8ff:fe21::/64  
Миқдори:  $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$

DNS

**DNS** ёки Domain Name System - IP-манзилларда ёки TCP/IP тармоқларида доменларнинг белгили номларини ташкил этиш имкониятини берадиган домен номи хизмати

ДОМЕН

Чексиз интернет уммонаидаги серверлардан бирида жойлашган қайсиdir сайтга олиб борадиган манзил ҳисобланади

[www.state.gov](http://www.state.gov)

.aero ҳаво-транспорт саноати

.coop кооператив ассоциациялар

[www.pm.gov.uz](http://www.pm.gov.uz)

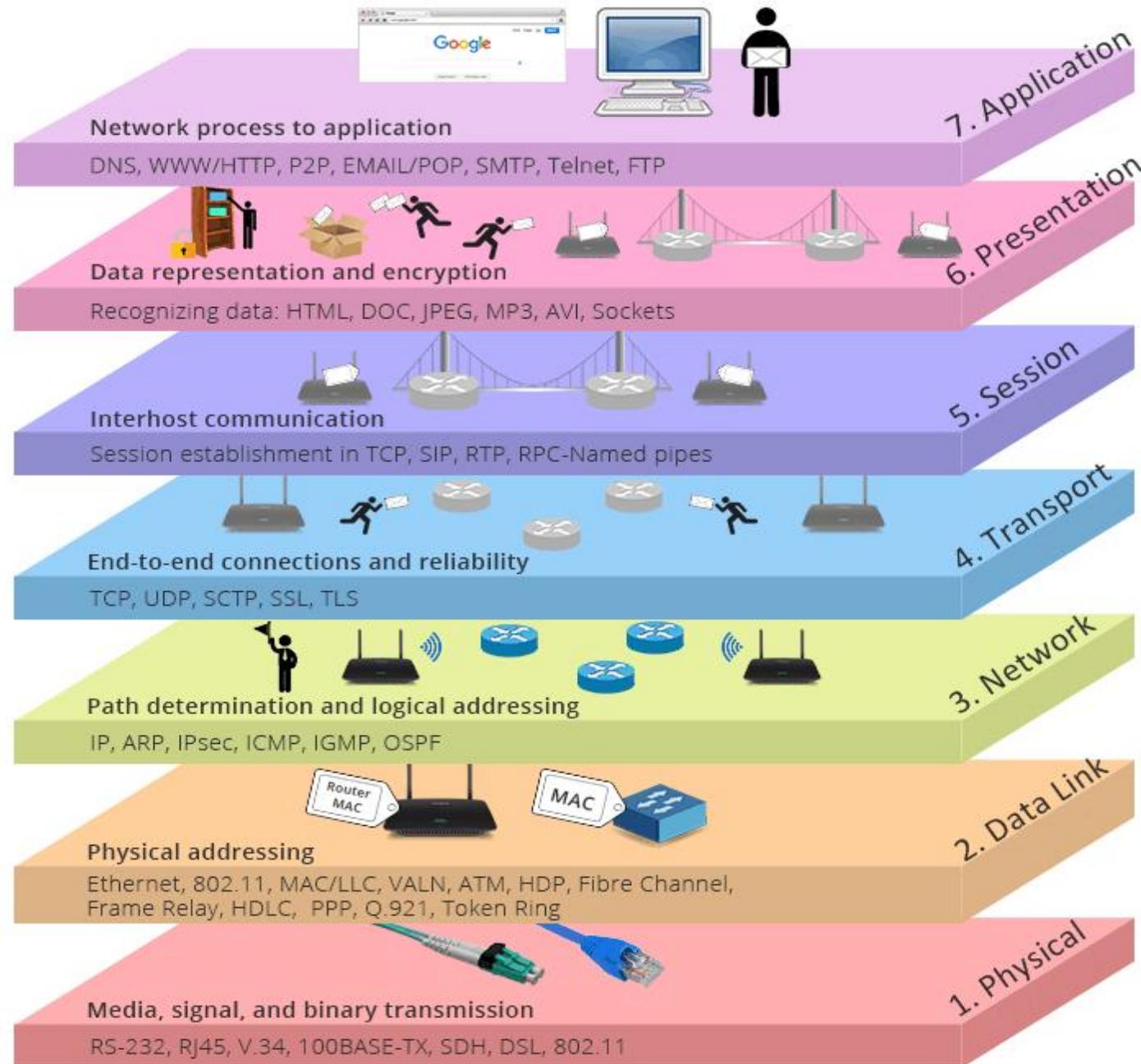
.us АҚШ

.uz Ўзбекистон

Регистратор

Рўйхатдан ўтказилган домен номлари ҳақида маълумотларга эга бўлган маълумотлар базаси ягона домен реестри деб номланади. Реестрни масъул органлар бошқаради, - мисол учун .UZ домени администратори. Хизматларни рўйхатдан ўрказиш учун администратор томонидан аккредитацияга эга бўлган жисмоний шахс Регистратор деб аталади.

# OSI модели



# Тармоқ протоколларининг TCP/IP модели сатҳларида қўлланиши

ИЛОВА



Telnet, SMTP, FTP, NNTP,  
HTTP, SNMP, DNS, SSH.

ТРАНСПОРТ



TCP, UDP

ИНТЕРНЕТ



IP, ICMP, ARP, DHCP

ТАРМОҚҚА КИРИШ



Ethernet, PPP, ADSL

# Тармоқ хавфсизлигининг асосий мақсадлари



## Конфиденциаллик

- Тизим маълумоти ва ахборотига фақат ваколатга эга субъектлар фойдаланиши мумкинлигини таъминловчи қоидалар.
- Мазкур қоидалар ахборотни фақат қонуний фойдаланувчилар томонидан “ўқилишини” таъминлайди



## Яхлитлик (бутунлик)

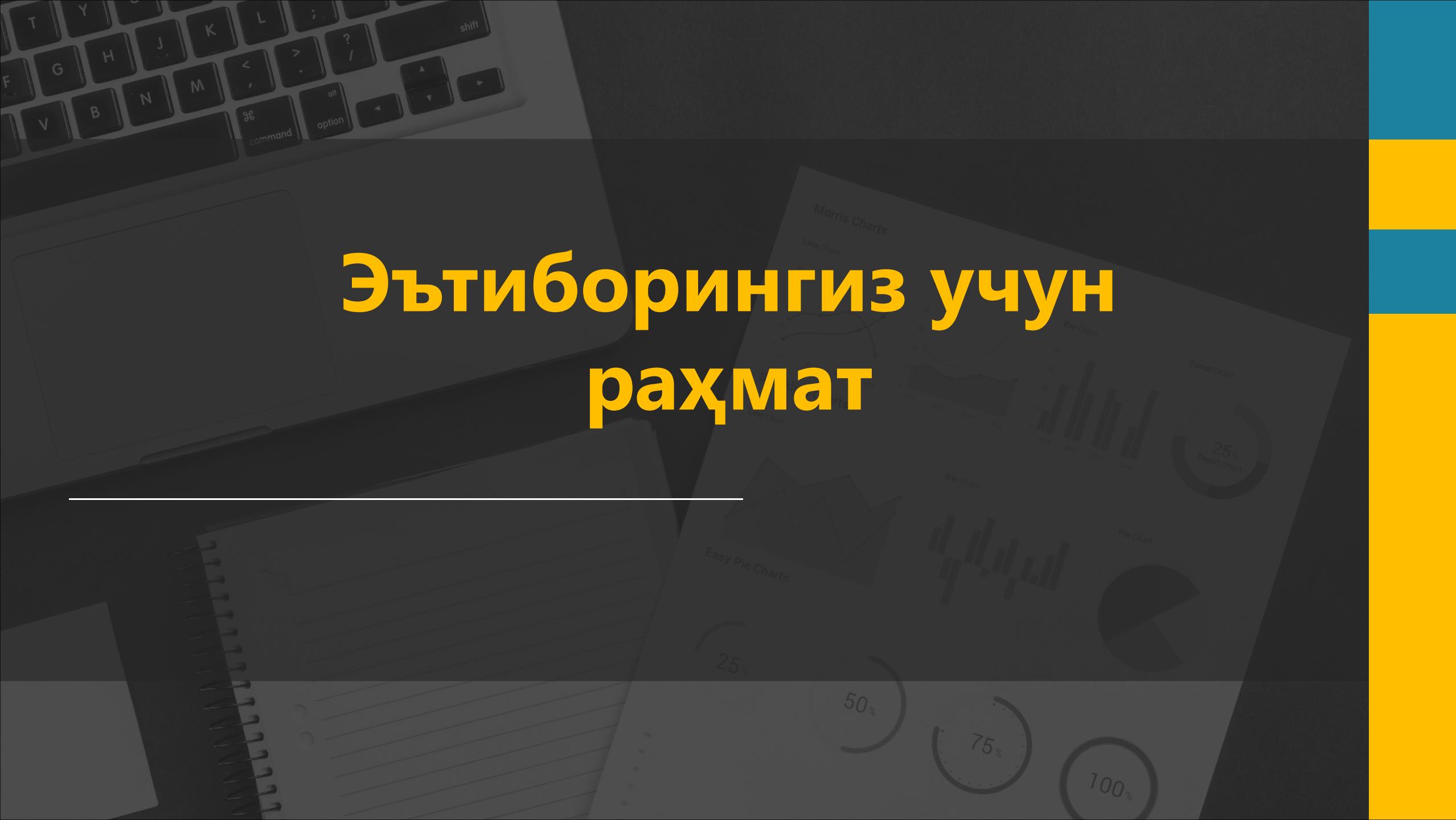
- Маълумотни аниқ ва ишончли эканлигига ишонч ҳосил қилиш.
- Яъни, ахборотни рухсат этилмаган ўзгартиришдан ёки “ёзиш” дан ҳимоялаш.



## Фойдаланувчанлик

- Маълумот, ахборот ва тизимдан фойдаланишнинг мумкинлиги.
- Яъни, рухсат этилмаган “бажариш” дан ҳимоялаш

# Эътиборингиз учун раҳмат



# Тармоқ хавфсизлиги

---

2-маъруза · Тармоқ хавфсизлигига замонавий  
таҳдидлар ·

---



+998 71 238 6525



@tarmoq\_xavfsizligi



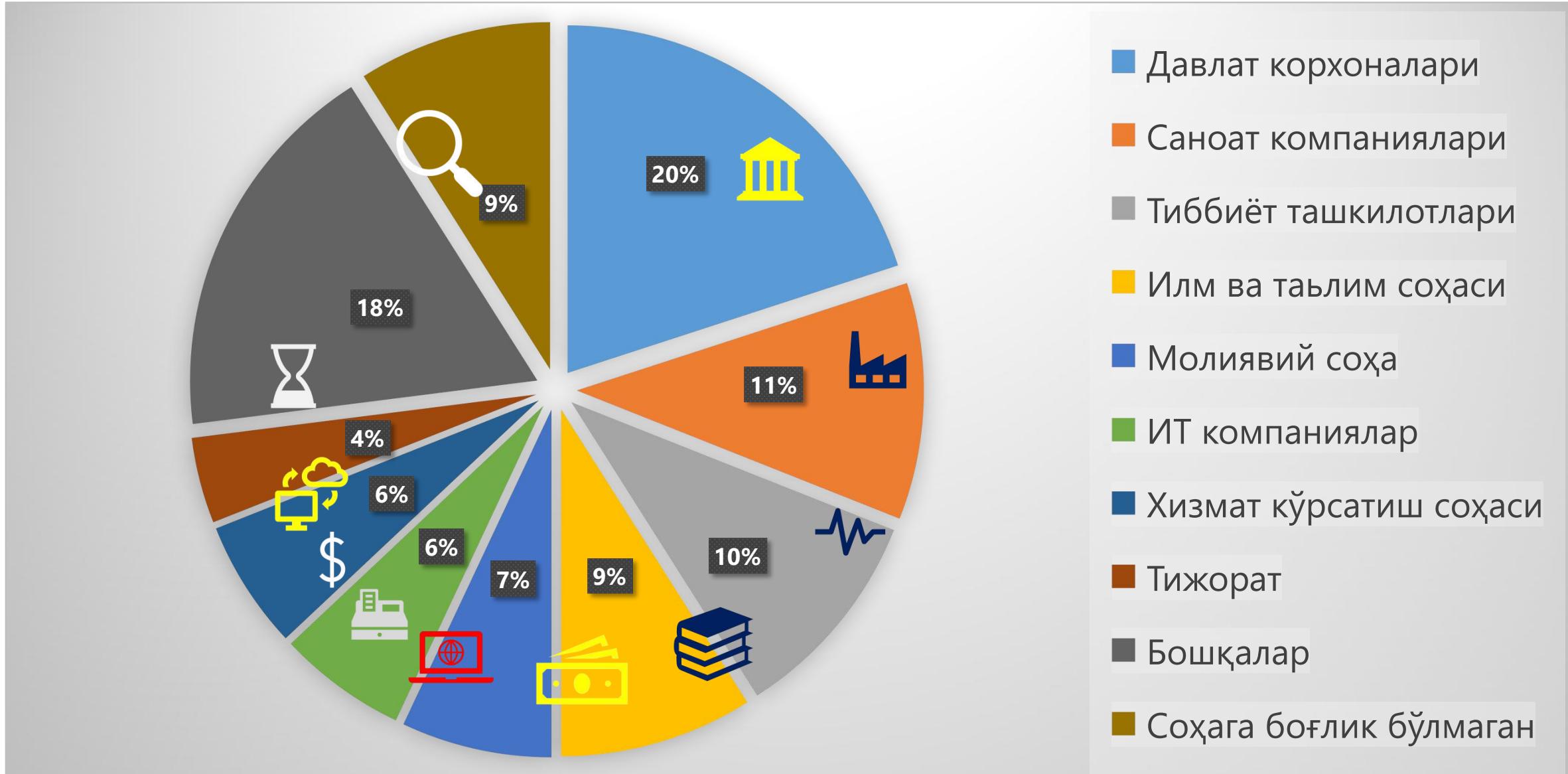
[www.tuit.uz](http://www.tuit.uz)



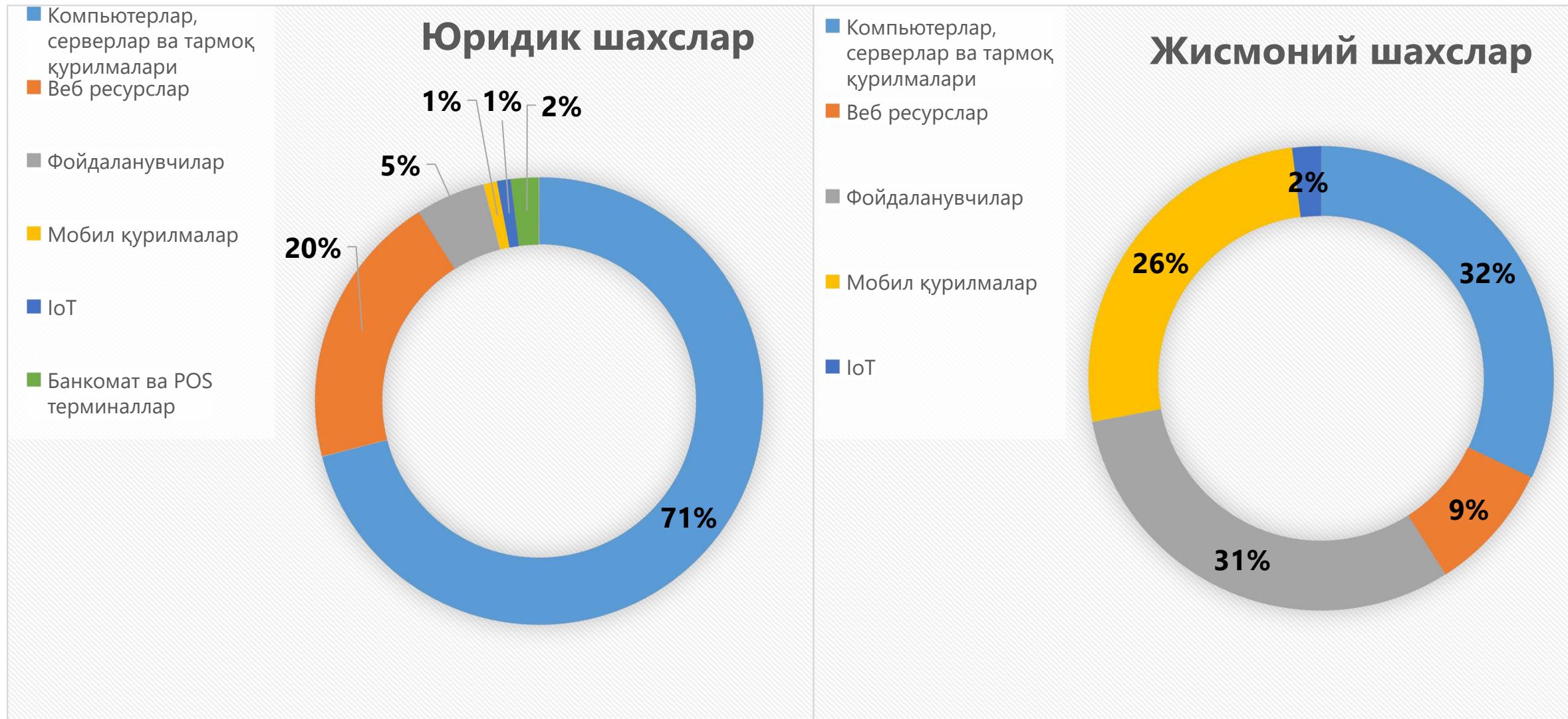
108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

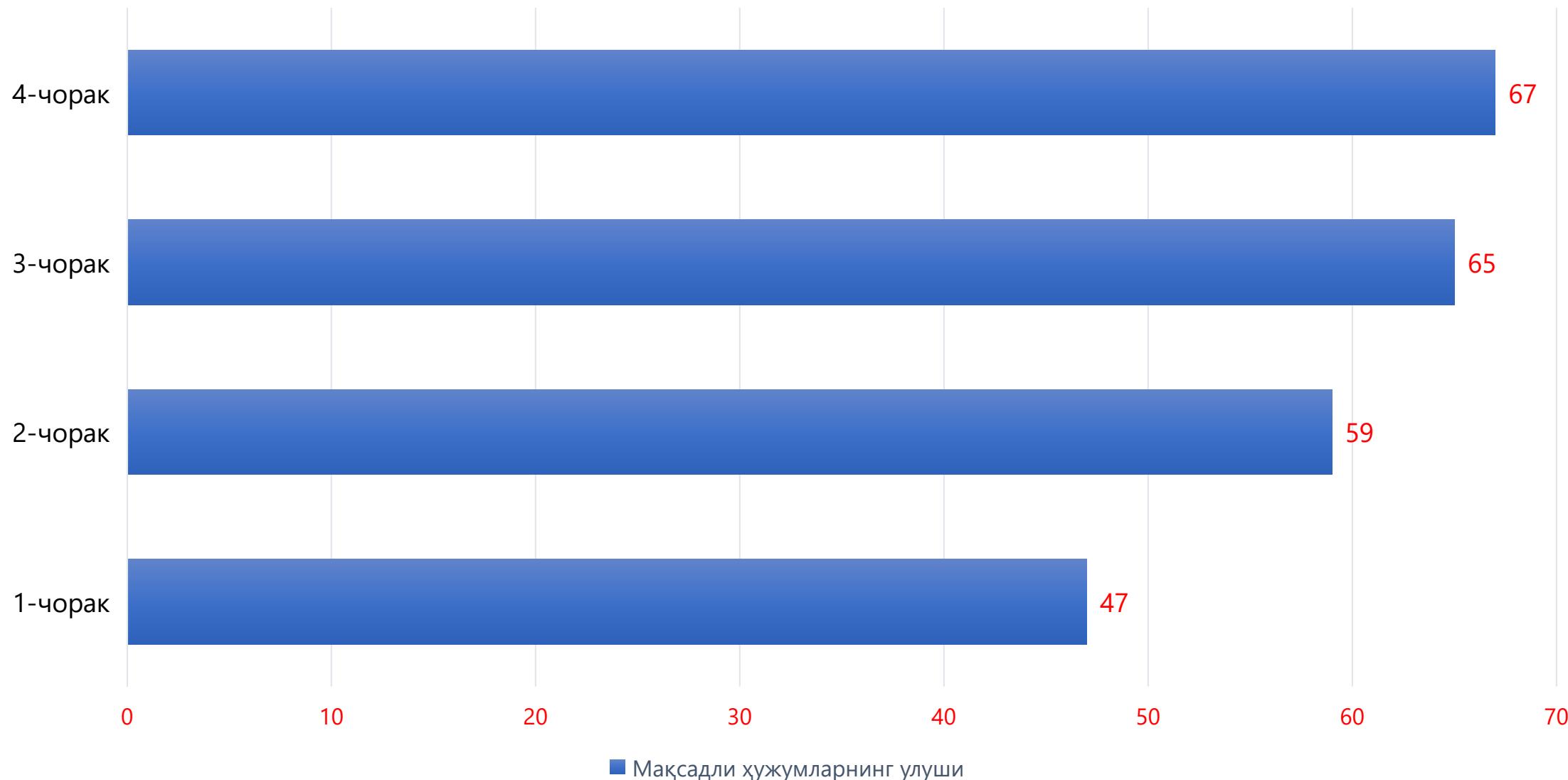
# Зарарланган юридик шахслар категорияси



# Хужум объектлари



## Мақсадли ҳужумларнинг улуши %



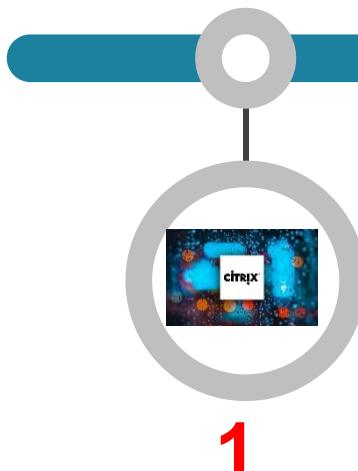
# Хужум усуллари



# Хавфли заифликлар

## Кнопка «Взломат интернет»

Идентификатор: CVE-2019-19781  
Құлланилиш: 2019 йил декабр  
Заиф ДТ: Citrix Application Delivery Controller (NetScaler ADC) и Citrix Gateway (NetScaler Gateway)  
Риск даражаси: критик  
Экспloit: мавжуд



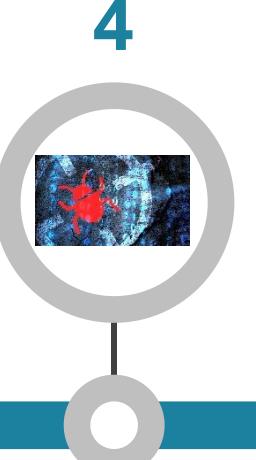
## Next day, NextCry

Идентификатор: CVE-2019-11043  
Құлланилиш: 2019 йил откябр  
Заиф ДТ: PHP-FPM  
Риск даражаси: критик  
Экспloit: мавжуд



## BlueKeep

Идентификатор: CVE-2019-0708 (BlueKeep)  
Құлланилиш: 2019 йил май  
Заиф ДТ: Microsoft Windows Remote Desktop Services  
Риск даражаси: критик  
Экспloit: мавжуд, ҳаттоқи Metasploit учун бир неча күринишда



## Держа руку на Pulse

Идентификатор: CVE-2019-11510  
Құлланилиш: 2019 йил апрел  
Заиф ДТ: Pulse Secure Pulse Connect Secure (PCS) Desktop Services  
Риск даражаси: критик  
Экспloit: мавжуд



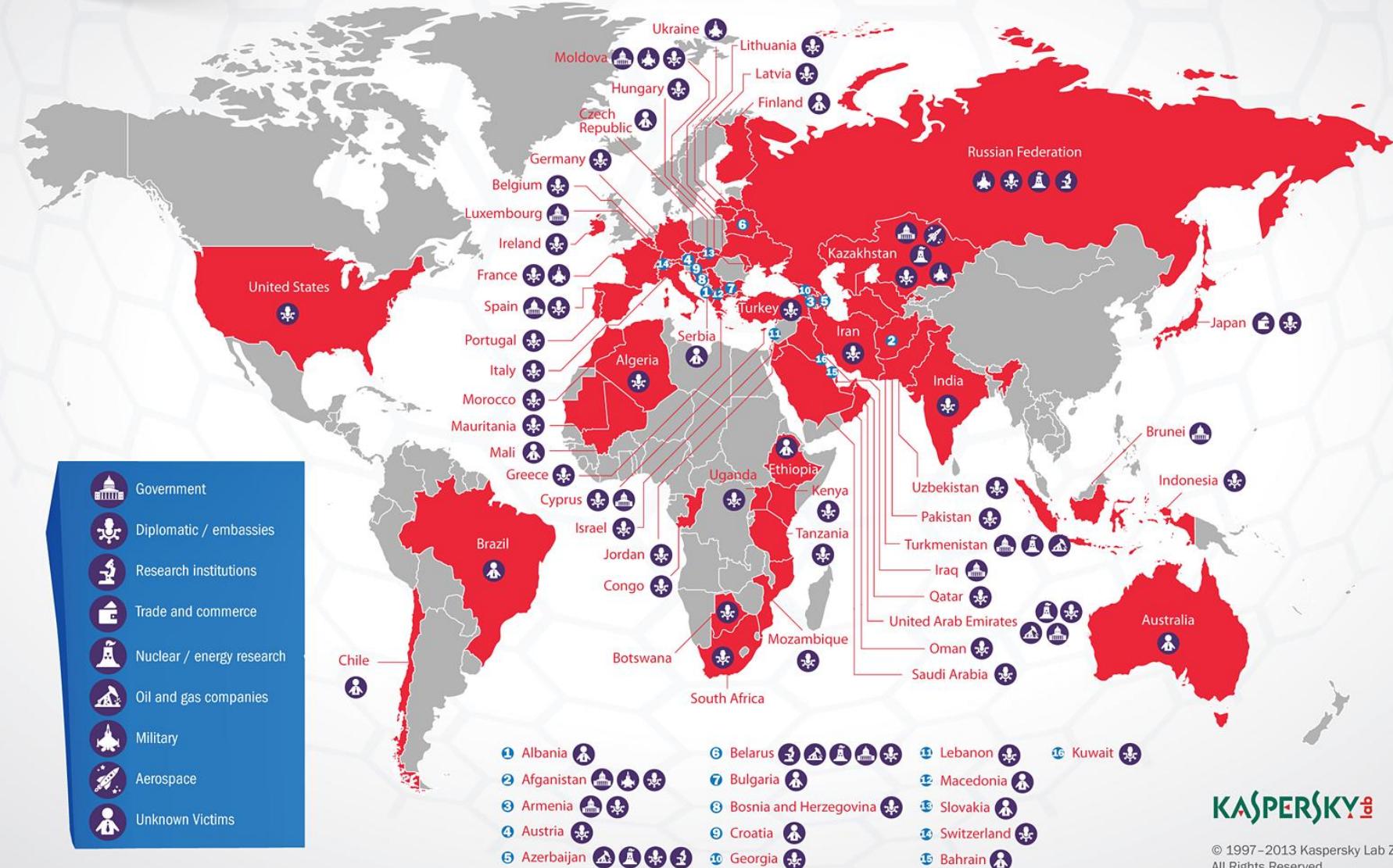
## Эпидемия MageCart

JavaScript-снифферлари, supply chain ұжуми, 600 дан ортиқ доменлар

# Operation “Red October”

Victims of advanced cyber-espionage network

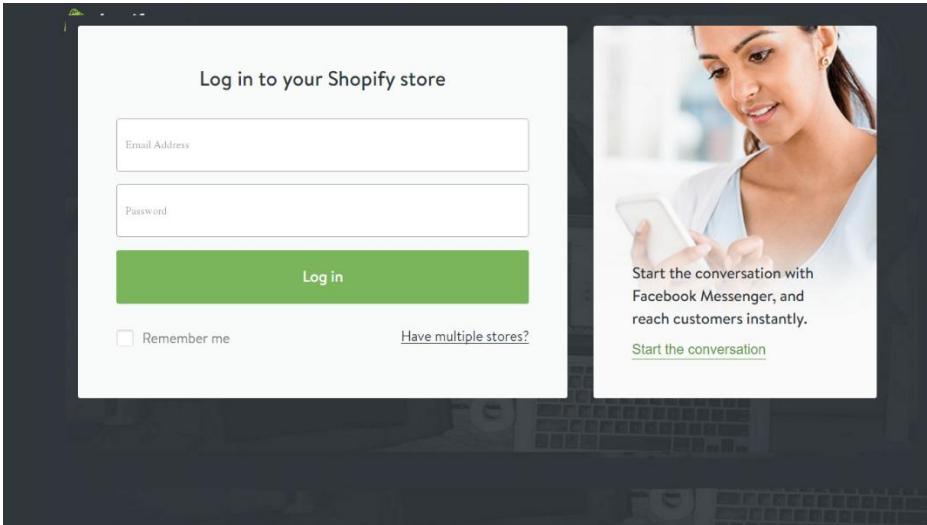
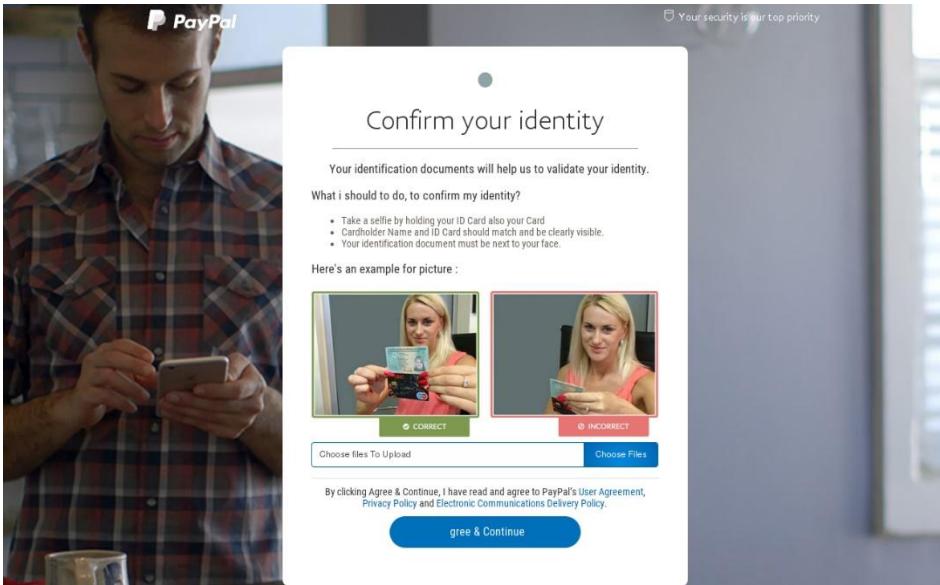
RED ОКТОВЕР  
операцияси



KASPERSKY

© 1997–2013 Kaspersky Lab ZAO.  
All Rights Reserved.

# Фишинг ҳужуми сценарийси



## Visa Home



### VISA HOME PARA SOCIOS

- Información sobre el estado de cuentas de sus tarjetas Visa. Últimos movimientos, liquidaciones y resúmenes de cuenta.
- Realice el pago puntual o adhiera al débito automático sus facturas de servicios e impuestos a través del Servicio de Pagos Visa.
- Abone en cuotas fijas el saldo del resumen de cuenta o los consumos realizados en un pago.

Tipo de Documento  
Documento Nacional de Identidad

Número

Sexo  
Masculino

Contraseña

Usuario

INGRESAR

Los datos que se proporcionan a Prisma Medios de Pago S.A. podrán utilizarse para procesar sus pedidos, solicitudes, denuncias, reclamos, para la relación comercial y fines publicitarios. Disposición DNPDP 10/2008: "El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 de la Ley N° 25.326" y "La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Organismo de Control de la Ley N° 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales."



## Log in

Continue to your store

Store address  
myshop.myshopify.com

Password      [Forgot password?](#)

Email Address  
Email Address registered with your account.

Email Password  
Email Password

[Sign In](#)

New to Shopify? Get started

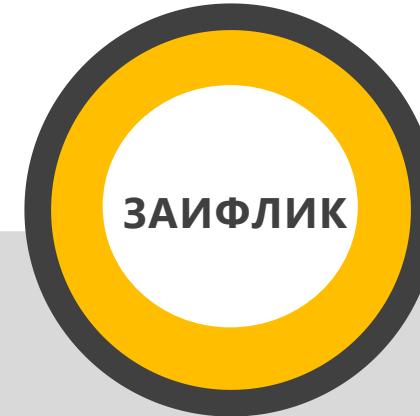
Help   Privacy   Terms

# АКТИВ & ЗАИФЛИК



Ташкилот активларини идентификациялаш үзоқ ва мураккаб жараён бўлиши мумкин. Ушбу жараён заифликларни баҳолашда энг муҳим қадамлардан биридир.

**АГАР ТАШКИЛОТ НИМАНИ  
ҲИМОЯЛАШИНИ БИЛМАСА, ҚАНДАЙ  
ҚИЛИБ ҲИМОЯНИ ТАШКИЛ ЭТИШ  
МУМКИН???**



Заифликни баҳолаш – активларга бузғунчилар, табият кучлари ёки ҳар қандай хавф туғдириши мумкин бўлган обьектлардан этиши мумкин бўлган заарнинг тизимли ва услубий баҳоси. Заифликни баҳолаш нимани ҳимоялаш зарур (активларни идентификациялаш), қанчалик таъсир этиши (таҳдидларни баҳолаш), жорий ҳимоя қанчалик заиф (заифликларни баҳолаш), таҳдид натижасида қандай заарар этиши мумкин (riskни баҳолаш) ва қандай чора кўриш зарур (risk даражасини пасайтириш).

# Асосий таҳдид манбалари

Таҳдид тури	Мисоллар
Табиий оғатлар	Ёнғин, тошқин ёки зилзила маълумотларни йўқ қиласди
Интеллектуал мулкни обрўсизлантирилиши	Дастурий маҳсулот лицензияланмаган ёки авторлик ҳуқуқи бузилган
Шпионаж	Маҳсулот ишлаб чиқариш жадвалини ўғирлаш
Товламачилик	Почта ходимининг хатларни ноқонуний ўқиши
Аппарат воситаларининг бузилиши ёки ишлашидаги хатоликлар	Firewall бутун тармоқ трафигини блоклаб қўйиши
Инсон хатоликлари	Ходим ташкилот ноутбукини авторургоҳда тўсатдан тушириб юбориши
Саботаж ёки бузғунчилик	Хужумчи файлларни ўчириб юборадиган қуртни ўрнатади
Дастурий ҳужумлар	Вирус, қурт ёки DOS ҳужуми дастурий ёки аппарат таъминотни бузади
Дастурнинг бузилиши ёки ундаги хатоликлар	Хатолик дастурнинг юкланишига тўсқинлик қиласди
Техник талаблар жиҳатидан эскириш	Дастур операцион тизимнинг янги версияси билан ишлай олмайди
Ўғирлик	Ходим компьютерининг ўғирланиши
Электр тармоғининг узилиши	Электр токининг ўчиши

# Заифликларнинг таъсир доираси

Таъсир	Тавсиф	Мисоллар
Таъсири йўқ (No impact)	Ушбу заифлик ташкилот фаолиятига таъсир қилмайди	Иш столидан сичқончанинг ўғирланиши ташкилот фаолиятига таъсир қилмайди
Кичик таъсир (Small impact)	Кичик таъсирили заифликлар ноқулайликларни ва иш жараёнларининг қисман ўзгаришига олиб келиши мумкин	Маълум бир турдаги қаттиқ диск қурилмаларининг ишлаши учун қўшимча дисклар ёки тестлаш талаб этилиши мумкин
Ўрта (Significant)	Иш фаолиятнинг тўхтаб қолиши оқибатида ходимларнинг иш унумдорлигини пасайишига олиб келувчи таҳдидлар	Тармоқса ўрнатилган заарли дастурий таъминот
Муҳим (Major)	Ташкилот даромадига сезиларли даражада таъсир кўрсатувчи заифликлар	Backdoorglar орқали ташкилот маҳсулотларини ишлаб чиқиш технологияси ва илмий асосларини ўғирлаш
Ўта муҳим (Catastrophic)	Ташкилотнинг иш фаолиятининг тўхтаб қолишиган ёки сезиларли даражада бузилишига сабаб бўлувчи ўта муҳим турига кирувчи заифликлар	Талабаларнинг мисоллари!!!

# ПОРТ & ПОРТ РА҆АМЛАРИ

## Порт

IP манзиллари TCP/IP тармоғидаги манзилни идентификациялашнинг асосий шакли бўлиб, ҳар бир тармоқ мосламасини ноёб идентификациялаш учун ишлатилади.

TCP/IP ушбу тизимдаги дастурлар ва хизматларнинг идентификатори сифатида рақамли қийматдан фойдаланади. Улар порт рақами сифатида танилган. Ҳар бир пакет манба ва манзил IP-манзилларини, шунингдек маҳаллий тизимдаги бошланғич хизматни ва масофавий тизимдаги тегишли хизматни белгилайдиган манба порти ва манзил портини ўз ичига олади.

## Порт-рақамлари

Порт рақамлари узунлиги 16 бит бўлгандиги сабабли улар 0 дан 65 535 гача ўнлик қийматига ега бўлиши мумкин. TCP/IP порт рақамларини учта тоифага ажратади:

- Машҳур порт рақамлари (0–1023). Энг универсал дастурлар учун ажратилган
- Рўйхатдан ўтган порт рақамлари (1 0 2 4 – 4 9 1 5 1). У қадар кенг қўлланилмайдиган бошқа дастурлар
- Динамик ва хусусий порт рақамлари (49152 - 65535). Иловаларда исталган киши фойдаланиши мумкин

# Стандарт тармоқ портлари

File Transfer Protocol (FTP)  
Secure Shell (SSH), Secure Shell File Transfer Protocol (SFTP),  
Secure Copy (SCP)



20 (data) and 21 (control)  
22

Telnet  
Trivial File Transfer Protocol (TFTP)



23  
69

Hypertext Transfer Protocol (HTTP)



80  
139

NetBIOS



Hypertext Transfer Protocol Secure (HTTPS)  
FTP Secure (FTPS)



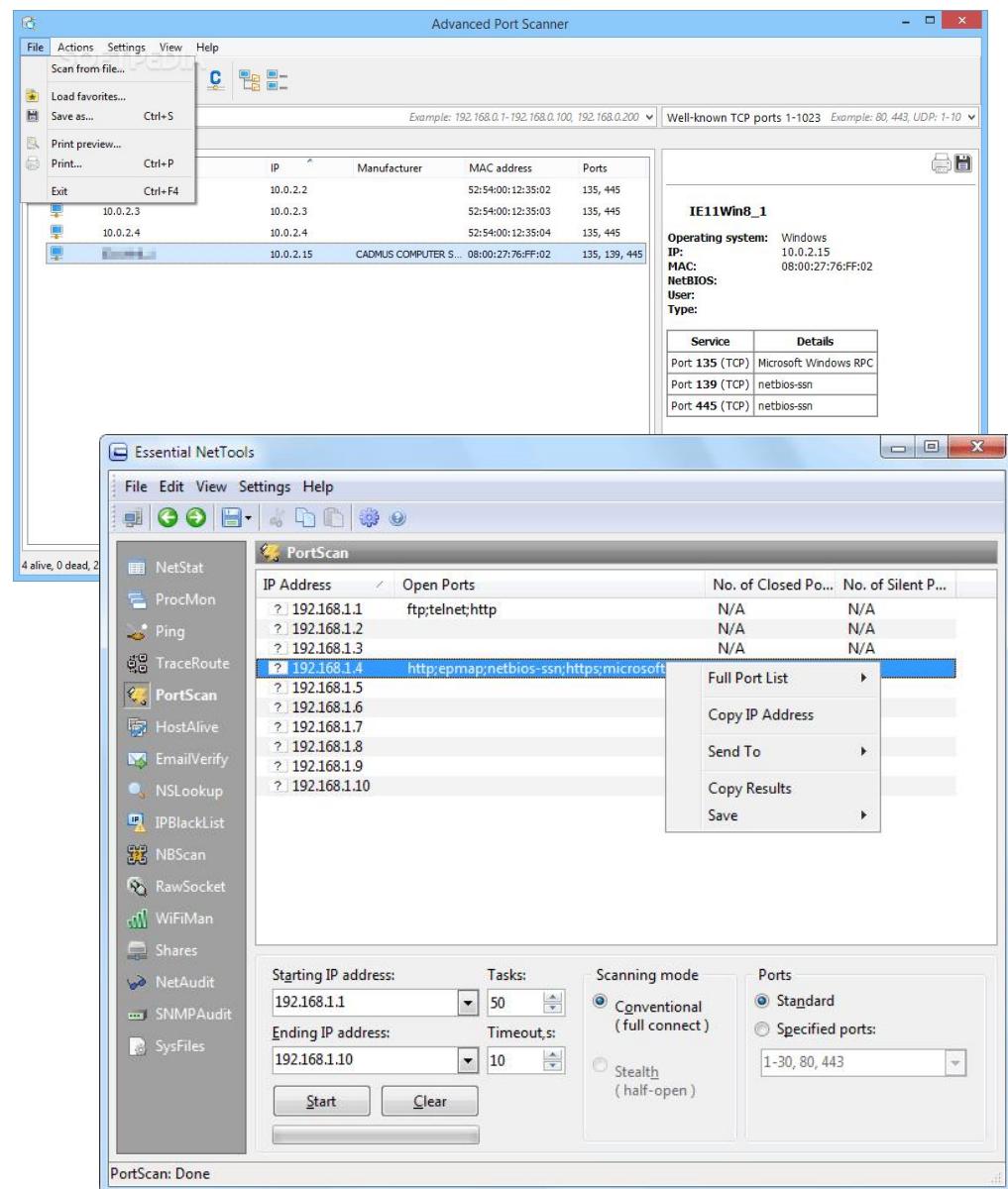
443  
989 (data) and 990 (control)

# Порт ишлаш ҳолатлари

Порт рақамлари хизматлар билан боғланганлиги сабабли, агар бузғунчи маълум бир портга кириш мумкинлигини билса, бу қандай хизматлардан фойдаланилаётганини кўрсатиши мумкин. Масалан, агар 20 порт мавжуд бўлса, бузғунчи тармоқда FTP ишлатилаётганини тахмин қилиши мумкин. Оқибатда у ўз ҳужумларини ушбу хизматга йўналтириши мумкин.



# Порт сканнерлари



**PortScan & Stuff [1.36]**

Scan Ports Search Devices Ping Devices Speed Test About

Internet2.edu NDT Server perfSONAR-PS : MCNC : UNC-CH at UNC Chapel Hill in UNC-CH

Firewall Your computer can't be connected from the internet

Upload Speed 46.6 kByte/sec

Download Speed 951.2 kByte/sec

SpeedTest.net Server Great Britain - London - Namesco

Response Time 36.4 ms

Upload Speed 53.4 kByte/sec

Download Speed 1013.8 kByte/sec

Microsoft Download Server 1035.1 kByte/sec

HiNet.net Server 655.3 kByte/sec

**PortScan & Stuff [1.26]**

Scan Ports Search Devices Ping Devices About

Start IP Address or Server Name: testmachine5

End IP Address: 192.168.1.255

Scan Only Most Common Ports

Check SMB Shares

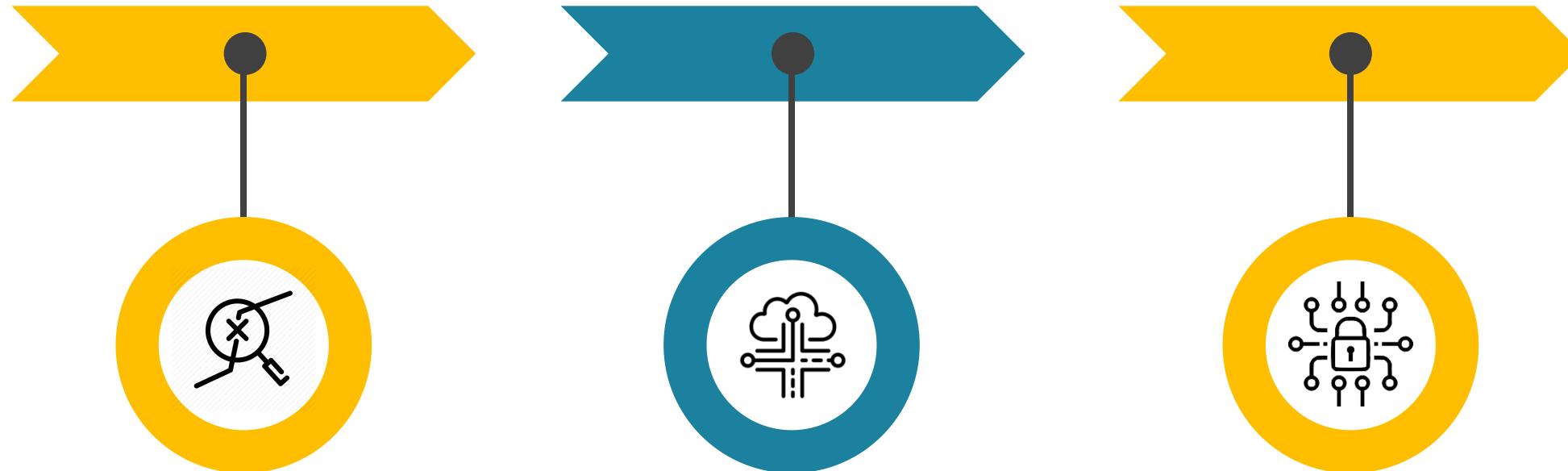
Host: 192.168.1.32 - TM1  
Host: 192.168.1.35 - NETBOOK  
Host: 192.168.1.5 - testmachine5  
MAC Address: 00-  
Hostname: testmachine5  
Open Port: Shared Network Folder [139]  
Open Port: Remote Procedure Call (RPC) [1025]  
Open Port: 1027  
Open Port: Epmap [135]  
Open Port: Shared Network Folder [445]  
Share: \\192.168.1.5\storage  
Share: \\192.168.1.5\Users  
Share: \\192.168.1.5\VM\_shared

# Портларни сканерлаш

Номи	Қидириш жараёни	Тавсиф
TCP connect scanning	Ушбу сканерлаш ҳар бир мавжуд портга уланишга ҳаракат қиласи. Агар порт очиқ бўлса, операцион тизим TCP билан уч томонлама "қўл сиқиши" ни якунлайди ва порт сканери уланишни ёпади; акс ҳолда хато коди қайтарилади	Бу тур сканерлаш учун маҳсус рухсат талаб этилмайди; у секин ишлаганлиги боис сканерни аниқлаш мумкин
TCP SYN scanning	Сканер операцион тизим функцияларидан фойдаланиш ўрнига, ўзи IP-пакетларни генерациялайди ва жавобларни кузатади. Сканер SYN-пакетни генерациялайди ва агар кўзланган порт очиқ бўлса, ушбу порт SYN + ACK пакети орқали жавоб қайтаради, ундан сўнг сканер хости "қўл сиқиши" жараёни тугагунча алоқани узади	SYN-сканерлаш - TCP-сканерлашнинг энг оммабоп тури бўлиб, аксарият сайклар ушбу ҳаракатларни рўйхатдан ўтказмайди; ушбу сканерлаш «яrimочиқ сканерлаш» деб ҳам аталади, чунки бунда ҳеч қачон тўлиқ TCP-уланиш очилмайди
TCP FIN scanning	Сканер бошланиш пакети SYNни юбормасдан, тугалланиш пакети (FIN)ни юборади; ёпиқ порт жавоб беради, лекин очиқ порт пакетни қабул қиласи	FIN пакети оддий келишиш жараёни қисми сифатида брандмауердан ўтиб кетиши ва аниқланмаслиги мумкин
Stealth scans	Яширин сканерлашда аниқланмаслик учун турли хил усуллардан фойдаланилади. Портни сканерлаш маълумотсиз кирувчи уланиш бўлгани учун, одатда хато сифатида қайд етилади; яширинча сканерлаш қайд этиш хизматларини "алдашга" ҳаракат қиласи	Биринчи усул – аниқлашдан қочиш учун, бир неча кун давомида (секин) сканерлаш; иккинчи усул – сканерлаш мақсадини бошқача кўрсатиб, умуман бошқа реал манзилдан сканерлашни амалга ошириш
Xmas Tree port scan	Xmas tree пакети – ишлатилаётган ҳар қандай протокол учун барча параметрлар активлаштирилган пакет. Xmas tree TCP-пакети сарлавҳасини сканерлаши учун тугатиш байроғи (FIN), муҳимлик (URG) ва туртки (PSH) активлаштирилади;	Пакет сарлавҳасидаги барча битлар тўлдирилганлигидан «Пакет янги йил арчаси» каби безатилган дейиш мумкин

# Протокол анализаторлари

Тармоқ трафигини анализатори қурилмаси ёки дастури үрнатилған компьютер ёрдамида күриш мүмкін. Протокол анализатори (шунингдек, сниффер деб ҳам аталади) тармоқ пакетларини декодлаш ва таҳлил қилиш имкониятига эга пакетларни тутиб қолувчи аппарат ёки дастурий таъминот. Протокол анализаторлари дастур сатқининг тармоқ протоколлари, HTTP ёки FTP-ни түлиқ декодлаши мүмкін.



## Network troubleshooting.

Протокол анализаторлари манзиллашдаги ва протоколни созлашдаги хатоликларни топиши мүмкін

## Network traffic characterization

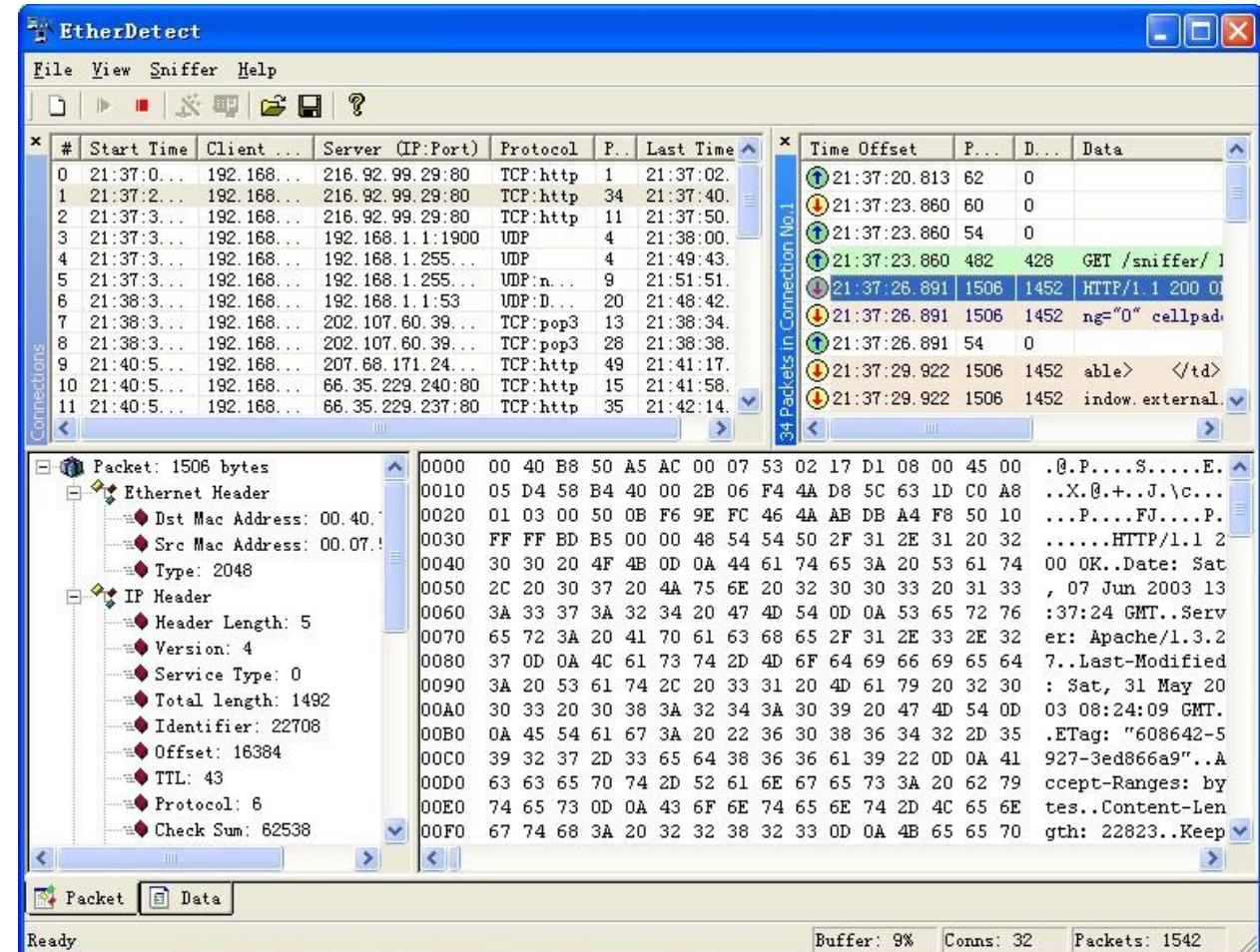
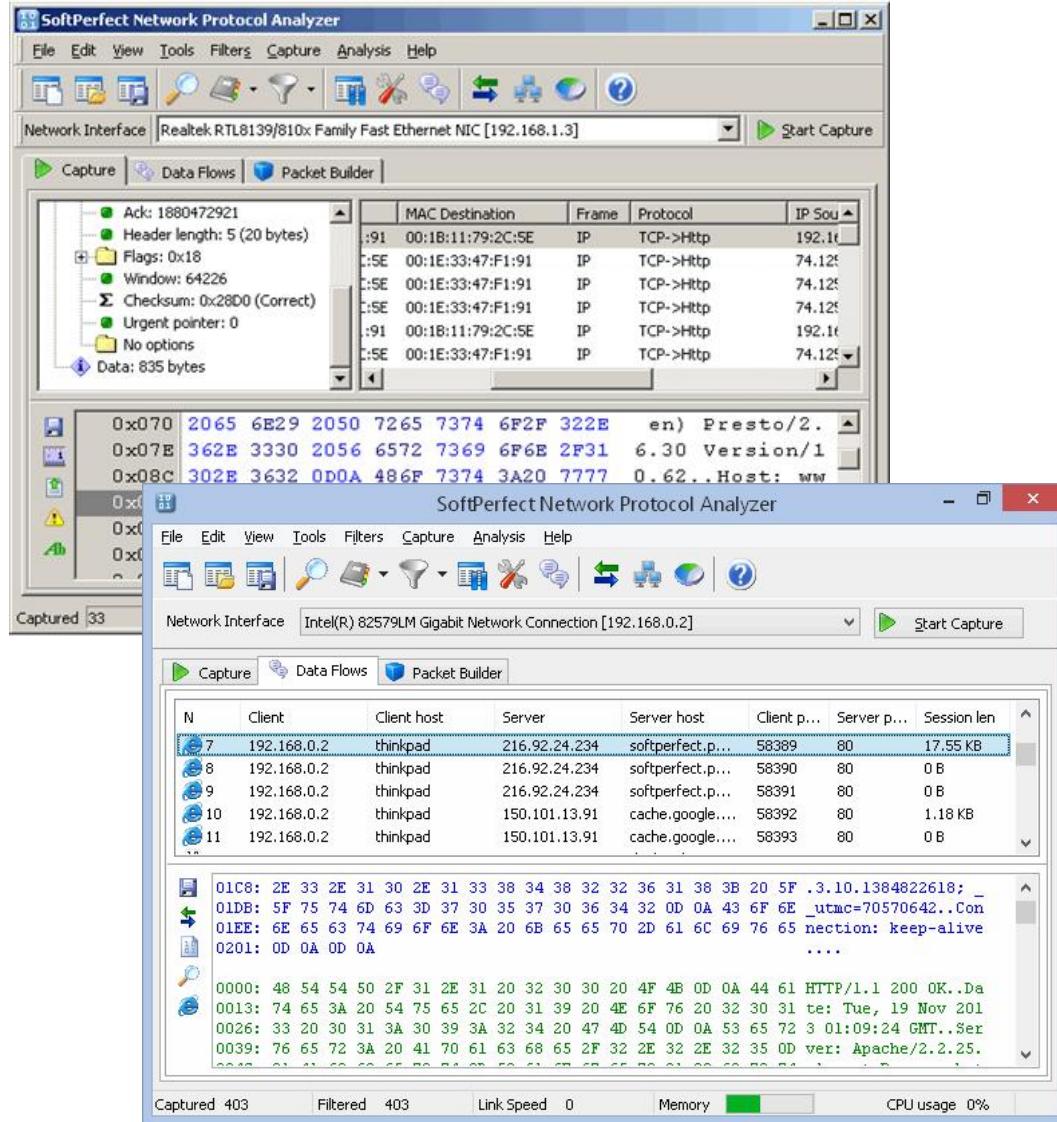
Протокол анализаторлари ёрдамида тармоқ турлари ва топологиясини тасвирлаш мүмкін. Бу фойдаланувчиларга енг юқори даражадаги хизматни күрсатиш учун тармоқни аниқ созлаш ва ўтказиш қобилиятини бошқариш учун ёрдам беради.

## Security analysis.

Тармоқ трафигини таҳлиллаш орқали хизмат күрсатишдан воз кечиш ва бошқа турдаги эксплойтларни аниқлаш мүмкін.

# Протокол анализаторлари

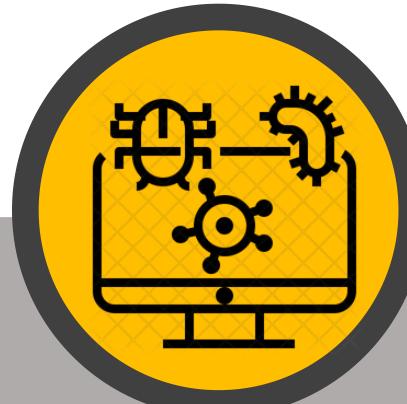
Main capture window showing data flow through a network card and decoded packet headers



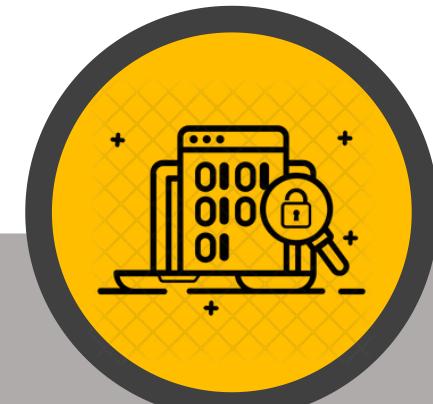
# Заифликлар сканери



Заифлик сканерлари ташкилот тармоғидаги заифликларни аниқлаш ва улар ҳақида тизим маъмурларини огоҳлантириш учун мўлжалланган. Аксарият сканерлар заифликлар базасини қўллаб қувватлайди.

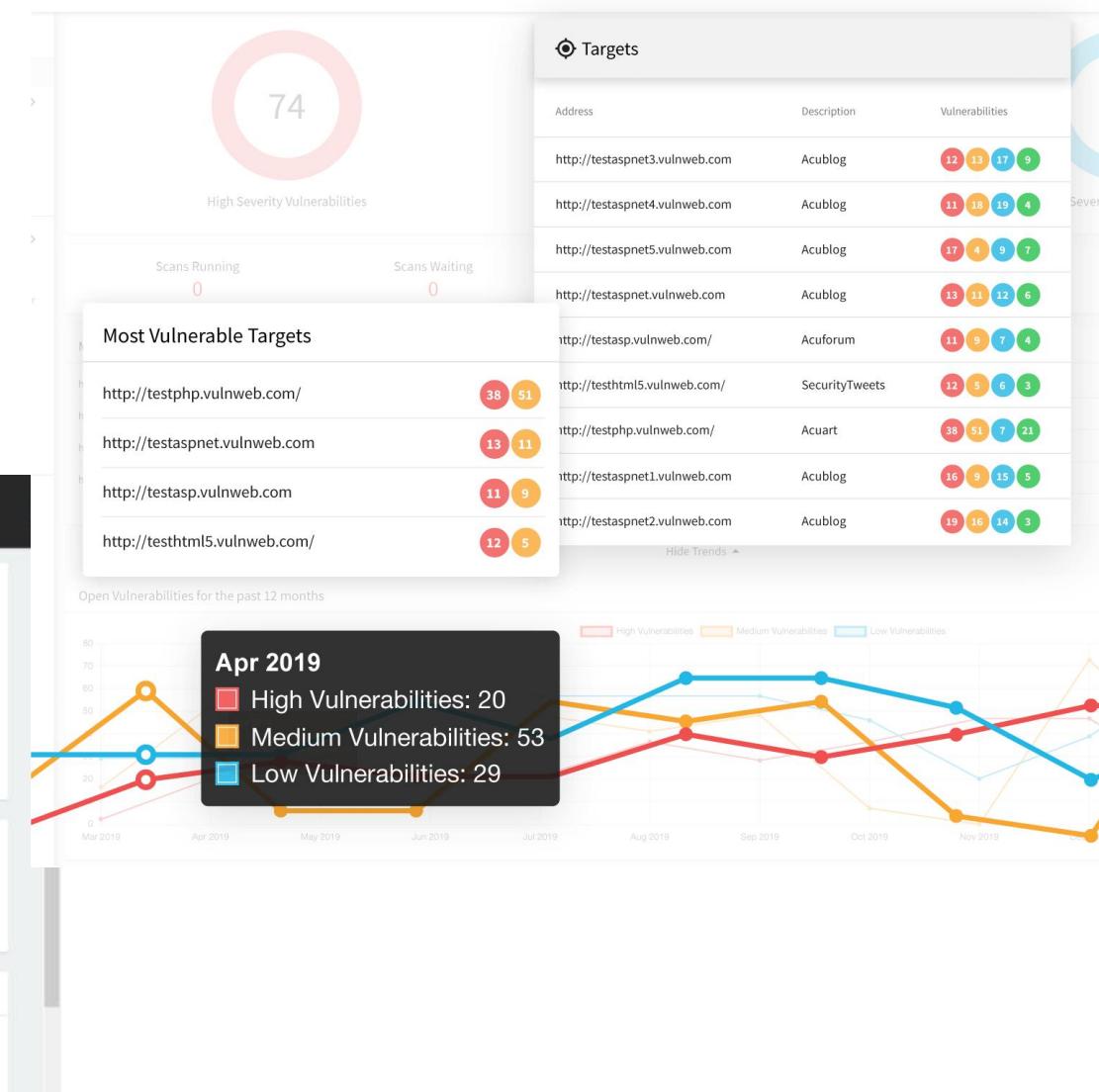
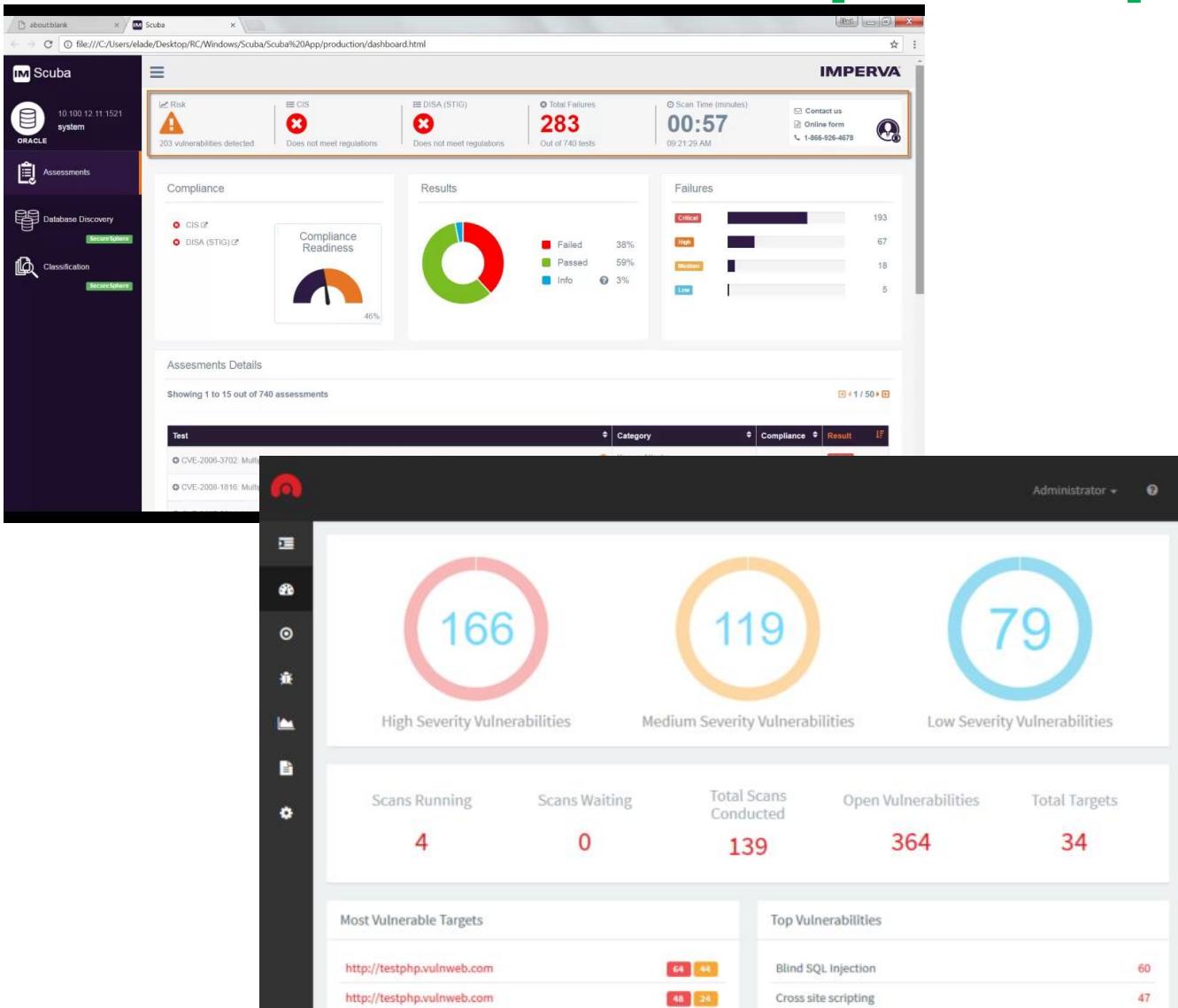


- Тармоққа янги элементлар кўшилгани ҳақида огоҳлантириш;
- Иловаларни бузилишини аниқлаш;
- Ички тармоқ ресурслари ташқи тармоқни сканерлаш жараёнини аниқлаш;
- Алоҳида ҳар бир тизим учун қайси портлар хизмат кўрсатаётгани ва қайси портлар кузатилаётганини аниқлаш;
- Қайси илова ва серверлар конфиденциал маълумот узатаётганини аниқлаш;



- Барча интерактив тармоқ сеансларининг журналини юритиш;
- Барча фаол тизимларнинг оперцион тизими турини пассив шаклда аниқлаш
- Барча мижоз ва сервер иловалари ининг заифликларини кузатиб бориш.

# Зайфликлар сканери



# Penetration Testing

Заифликларни сканерлашдан фарқли равища суқилиб киришга тестлаш (пентест деб ҳам юритилади) тизимдаги ҳар қандай заиф нуқталардан фойдаланишга мўлжалланган. Суқилиб киришга тестлашда жараён автоматлашган дастурӣ воситалар ўрнига тестловчи мутахассиснинг билим, қўникма ва уддабуронлигига асосланади.

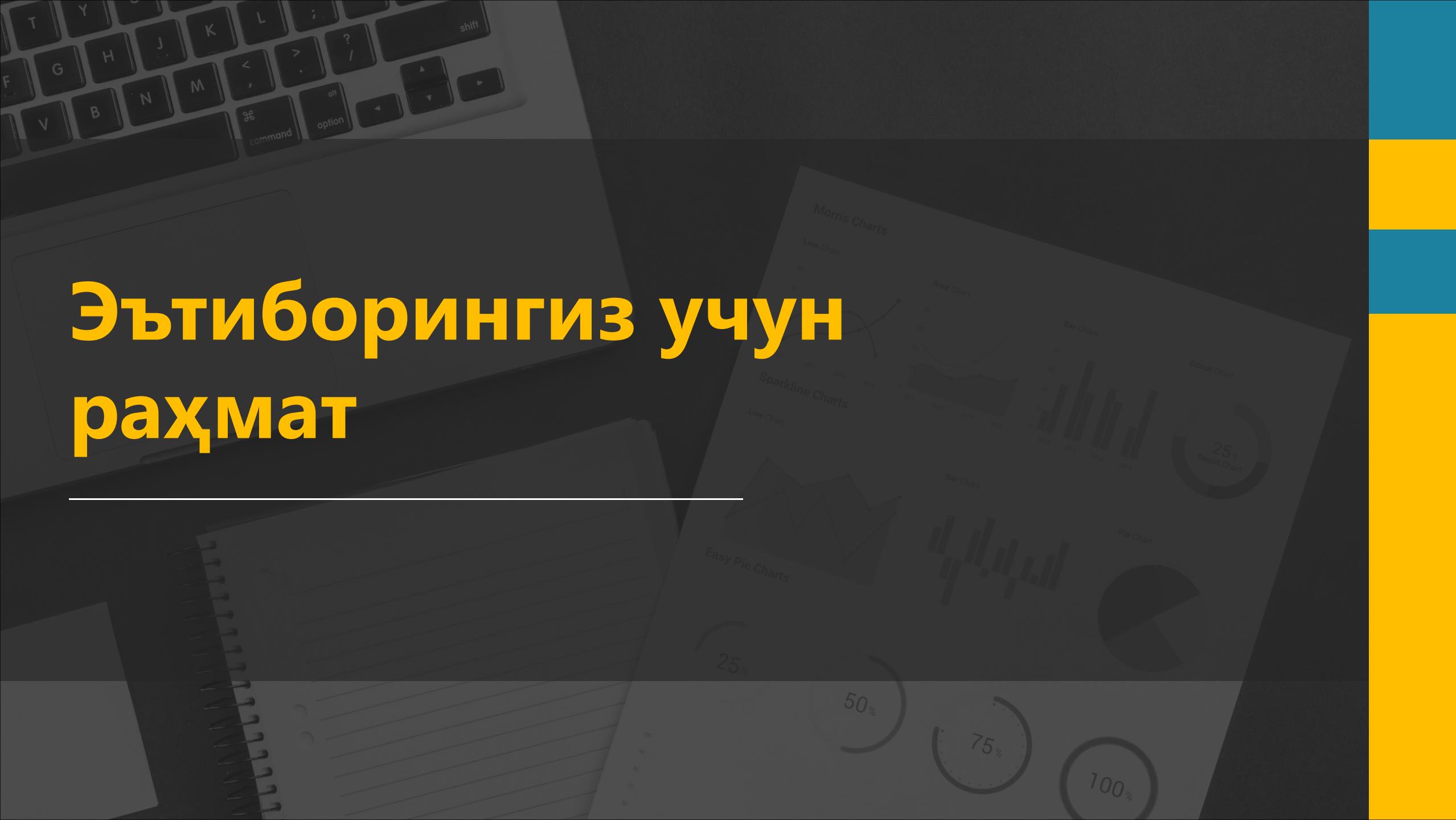


## Сүқилиб киришга тестлаш ва заифликлар сканери имкониятлари

Имконият	Заифликлар сканери	Сүқилиб киришга тестлаш
Частота	Янги қурилмалар ўрнатилганда ва ундан кейин камидა ойига бир марта	Йилда бир марта
Мақсад	Мавжуд ва янги заифликларни аниқлаш	Бизнес жараёнига таъсир этувчи ноъмалум омилларни аниқлаш
Тестер	Ички ходим	Ташқи мустақил тестловчи
Локация	Ички томондан ишлатилади	Ташқи томондан ишлатилади
Бузилиш	Хатоликларсиз пассив баҳолаш	Потенциал бузилишлар орқали актив ҳужум
Инструмент	Автоматлашган дастурий воситалар	Тестловчининг билим ва кўникмалари
Нарх	Арzon (ходимлар маоши билан 1500 \$ атрофида)	Қиммат (12500 \$ атрофида)
Ҳисобот	Жорий заифликни мавжуд заифликлар билан солиштириш	Ҳужумни амалга оширилиш ва келтирилган зарар ҳақида қисқа таҳлил
Қиймат	Дастурий ва аппарат воситаларнинг заиф нуқталарини аниқлайди	Бизнес жараёни таъсирларни камайтириш учун профилактик чора тадбирлар

# Эътиборингиз учун раҳмат

---



# Тармоқ хавфсизлиги

З-маъруза· Компьютер тизимлари ва  
тармоқларида хавфсизлик сиёсати ва

моделлари·



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

- 20

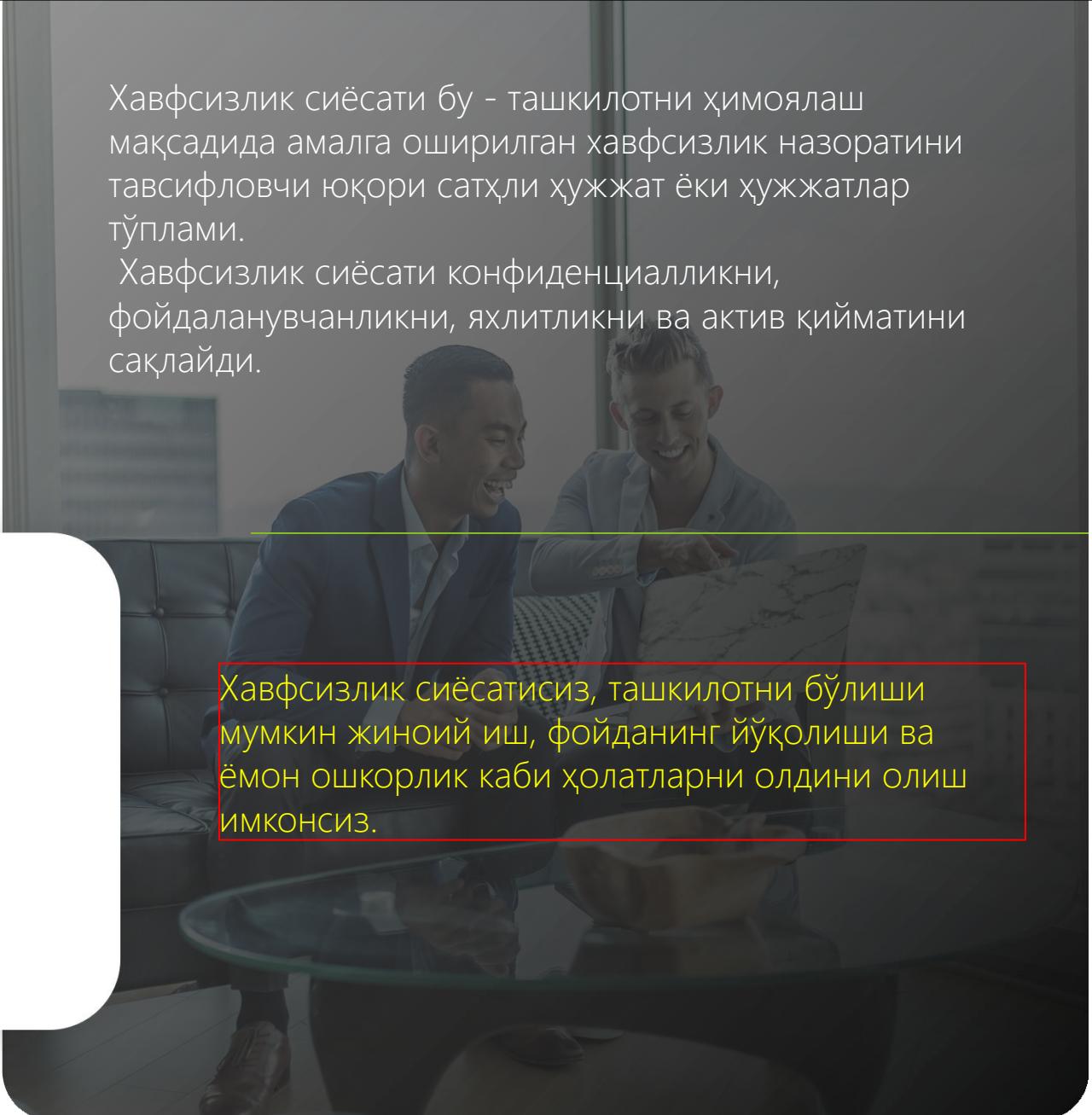


## Хавфсизлик сиёсати нима?

Хавфсизлик сиёсати бу - ташкилотни ҳимоялаш мақсадида амалга оширилган хавфсизлик назоратини тавсифловчи юқори сатхли ҳужжат ёки ҳужжатлар түплами.

Хавфсизлик сиёсати конфиденциалликни, фойдаланувчанликни, яхлитликни ва актив қийматини сақлады.

Хавфсизлик сиёсатисиз, ташкилотни бўлиши мумкин жиной иш, фойданинг йўқолиши ва ёмон ошкорлик каби ҳолатларни олдини олиш имкониз.



# Хавфизлик сиёсати нимага керак?



Турли заифликлар натижасида ҳосил бўлган хавфизлик таҳдидларига қарши курашиш ва уни ахборотни йўқолишидан ҳимоялаш учун;



Ташкилотнинг барча функцияларини хавфисиз тарзда амалга оширилиши учун;



Ташқи ахборот таҳдидларига компаниянинг дучор бўлишини камайтириш учун;



Хавфизлик сиёсалари таҳдидларни содир бўлишидан олдин башоратлаш ва заифликларни аниқлаш орқали хавфизлик бузилишлари ҳолати эҳтимолини камайтиради;



Кучайтирилган маълумот ва тармоқ хавфизлиги  
Рискларни камайтириш



Қурилмалардан фойдаланиш ва маълумотлар трансферининг мониторингланиши ва назоратланиши



Тармоқни юқори унумдорлиги  
Мұаммоларга тезкор жавоб бериш ва ҳаракатсиз вақтнинг камлиги



Бошқарувдаги стресс даражасини камайиши  
Харажатларни камайиши

## Хавфизлик сиёсаларининг афзалликлари

# Хавфсизлик сиёсатининг иерархияси

• 20



# Хавфизлик сиёсатининг контенти



## Хавфизлик талаблари

- Интизом хавфизлиги талаблари
- Қўриқлаш хавфизлиги талаблари
- Муолажавий хавфизлик талаблари
- Кафолат хавфизлиги талаблари



## Сиёсат тавсифи

Мазкур қисмда асосий эътибор хавфизлик тартибига, қўриқлаш, муолажалар, амалларнинг боғлиқлиги ва хужжатлаштиришга қаратилади.



## Амалнинг хавфизлик тушунчаси

Ушбу тушунчалар хавфизлик сиёсатининг ролларини, жавобгарликлари ва функцияларини аниқлайди.



## Элементлар жойлашувининг архитектураси

Ушбу сиёсат дастурдаги ҳар бир тизим учун компьютер тизимлари архитектурасини жойлашувини таъминлайди.

# Сиёсатнинг типик мазмуни



**Мақсад**

**1**

Сиёсат нима учун тузилганлигин батафсил тушунтириш

**Ҳаракат соҳаси**

**2**

Кимни ва нимани қамраб олиш ҳақидага ахборотни ўз ичига олади

**Қоидалар ва жавобгарликлар**

**3**

Ходимлар ва бошқарув учун аниқланади

**Санкциялар ва бузилишлар**

**4**

Мижозлар ва фойдаланувчилар риоя қилиши керак бўлган рухсат бериш/ рад этиш жараёнини белгилайди

**Контакт маълумотлари**

**5**

Сиёсат санкциялари ва / ёки бузилишлари йуз берганда ким билан боғлиниш кераклиги ҳақидаги ахборот

# Тармоқ хавфсизлиги сиёсатини яратиш ва амалга ошириш

- 20 йылдан кийинде 24



# Тармоқ хавфсизлиги сиёсатини яратишнинг 5 итератив қадами



**Хавфсизлик сиёсати - бу ташкилотнинг технологиялари ва ахборот активларига кириш ҳуқуқига ега бўлган фойдаланувчилар амал қилиши керак бўлган қоидаларнинг расмий баёнидир**

**1**

Нимани ҳимоялашни аниқлаш

**2**

Нимадан ҳимоялашни аниқлаш

**3**

Таҳдидларнинг содир бўлиш эҳтимолини аниқлаш

**4**

Ташкилот активларини рентабел усулда ҳимоялаш чораларини кўриш

**5**

Иш жараёнини доим кузатиб бориш ва заиф нуқта аниқланганда ҳар сафар тизимни яхшилаш

# Тармоқ хавфсизлиги сиёсатини қоидаларига риоя этишни таьминлаш

Any employee found to have violated any of these policies might be subject to disciplinary action, up to and including termination of employment!!!

## Тармоқ хавфсизлиги сиёсати

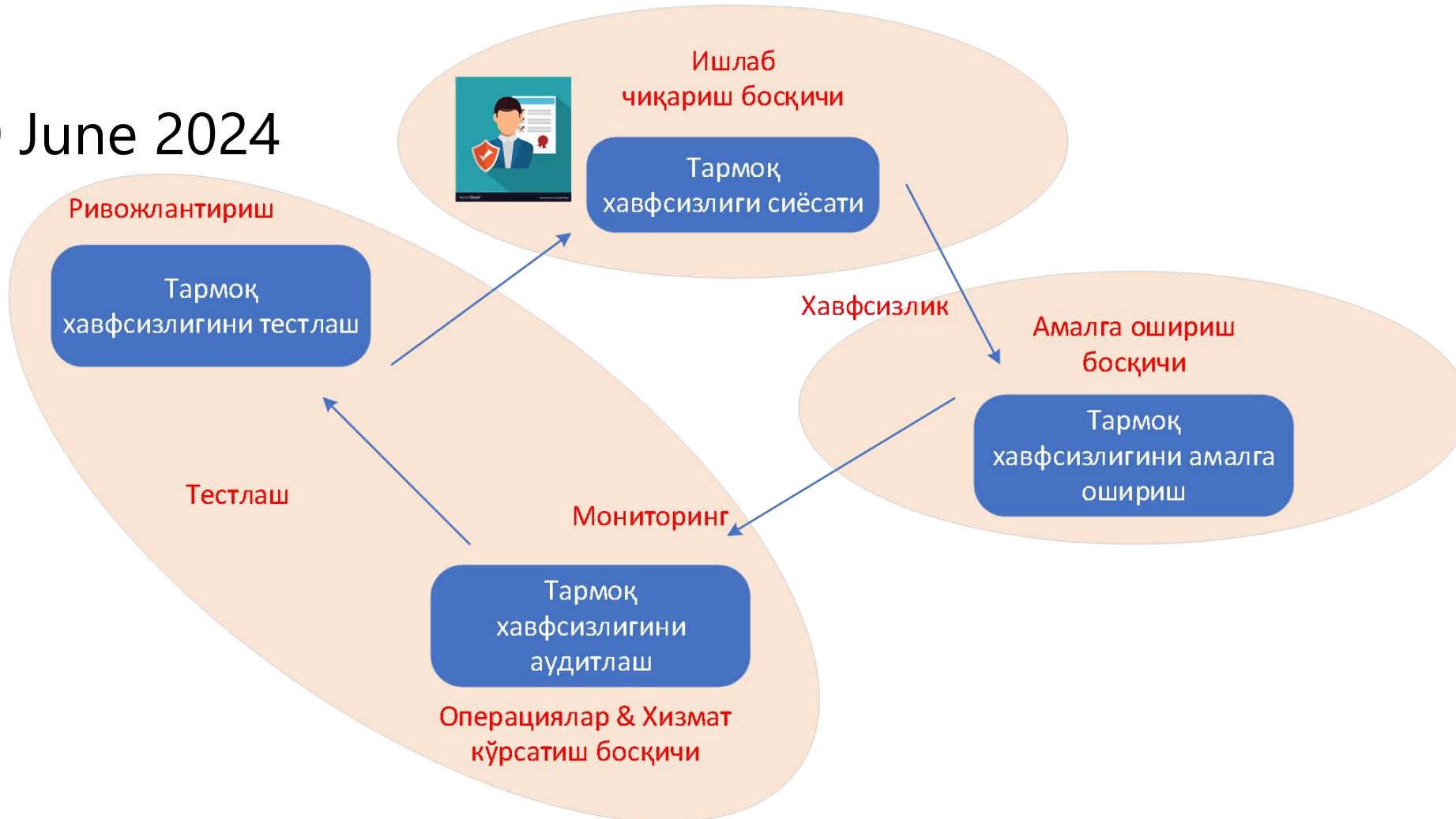


Бошқарувчи кўрсатмалар

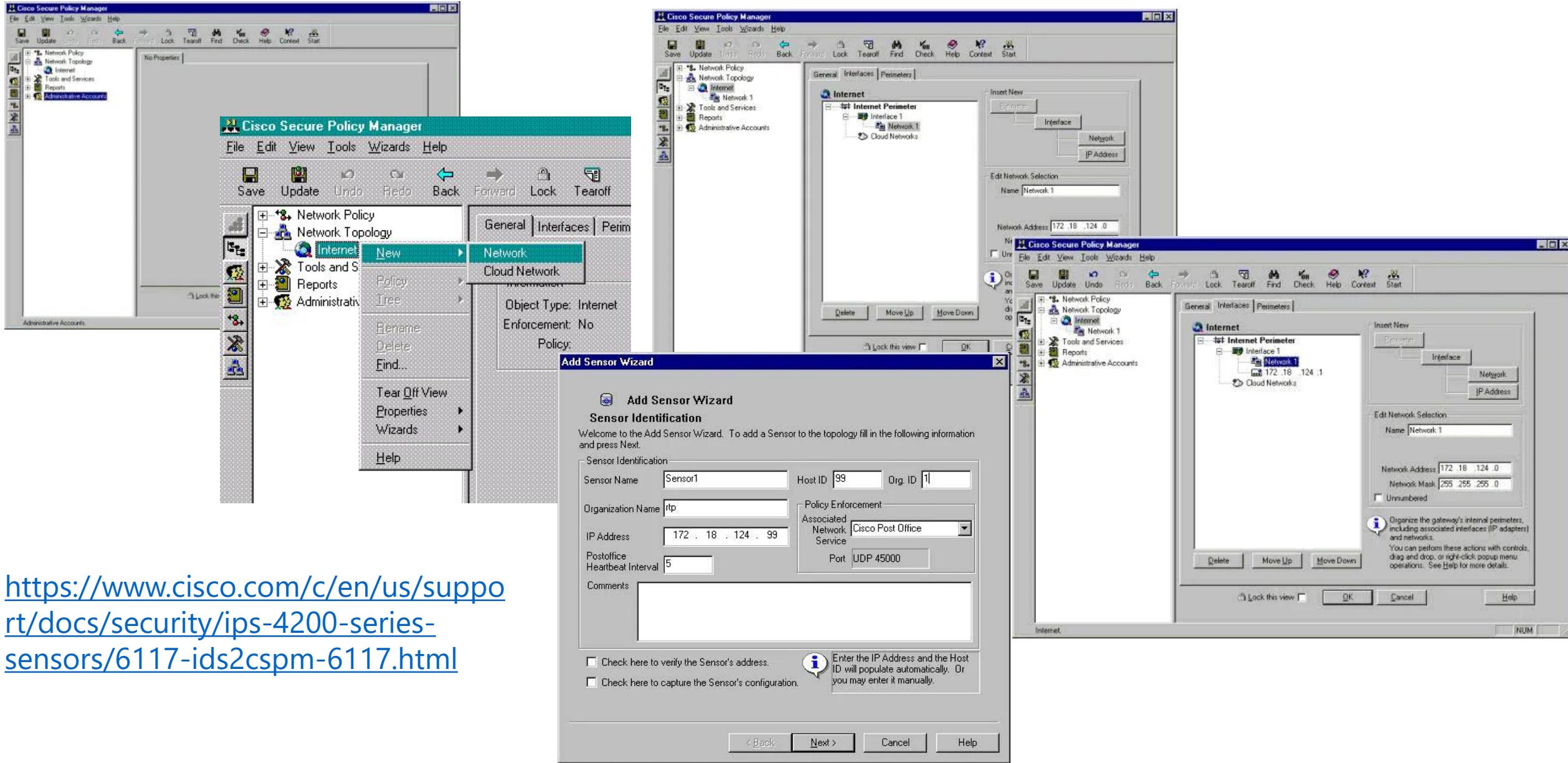
Процедуралар

# Тизимнинг ҳаётий цикли

- 20 June 2024

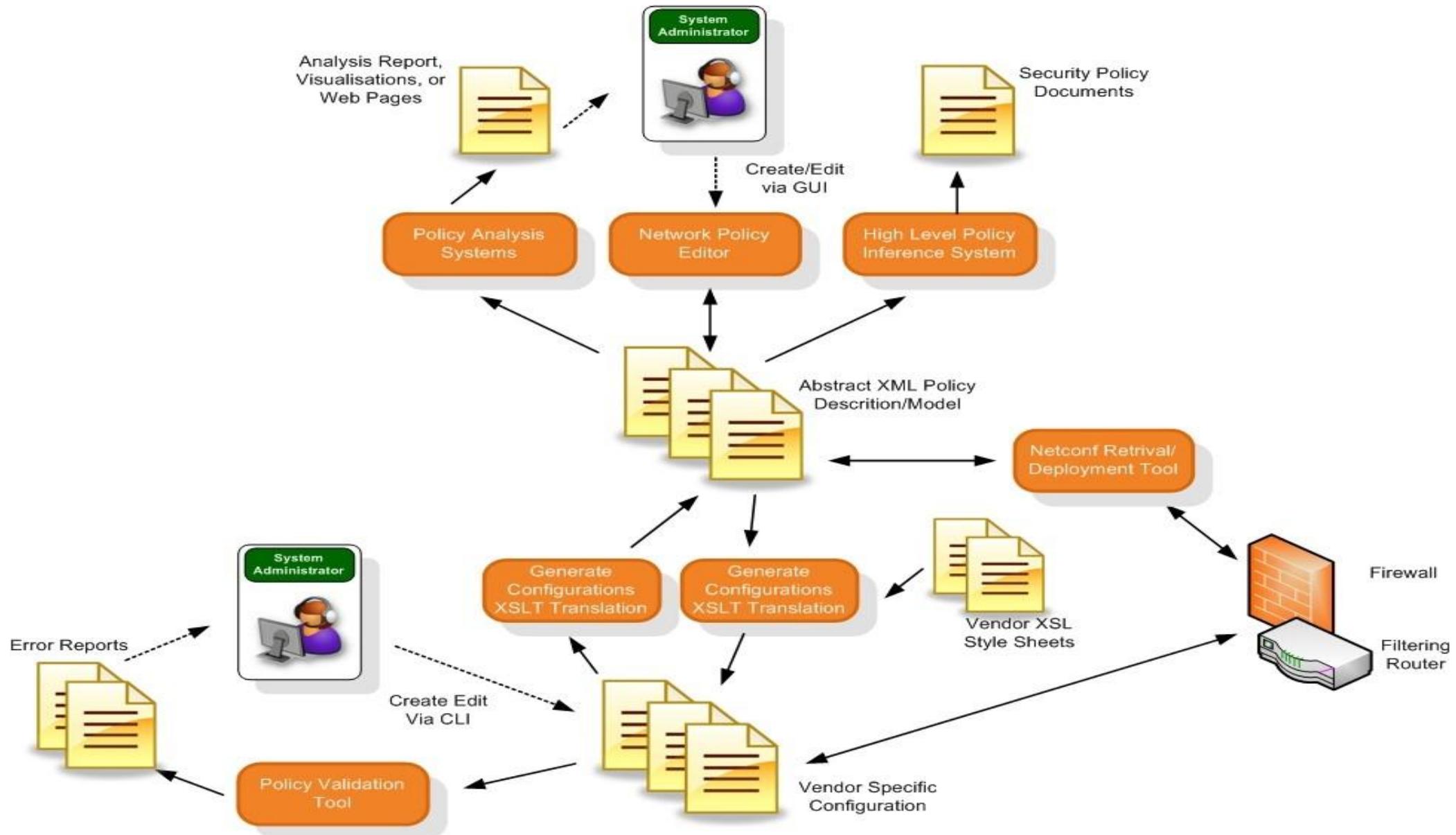


# Cisco Security Policy Manager GUI



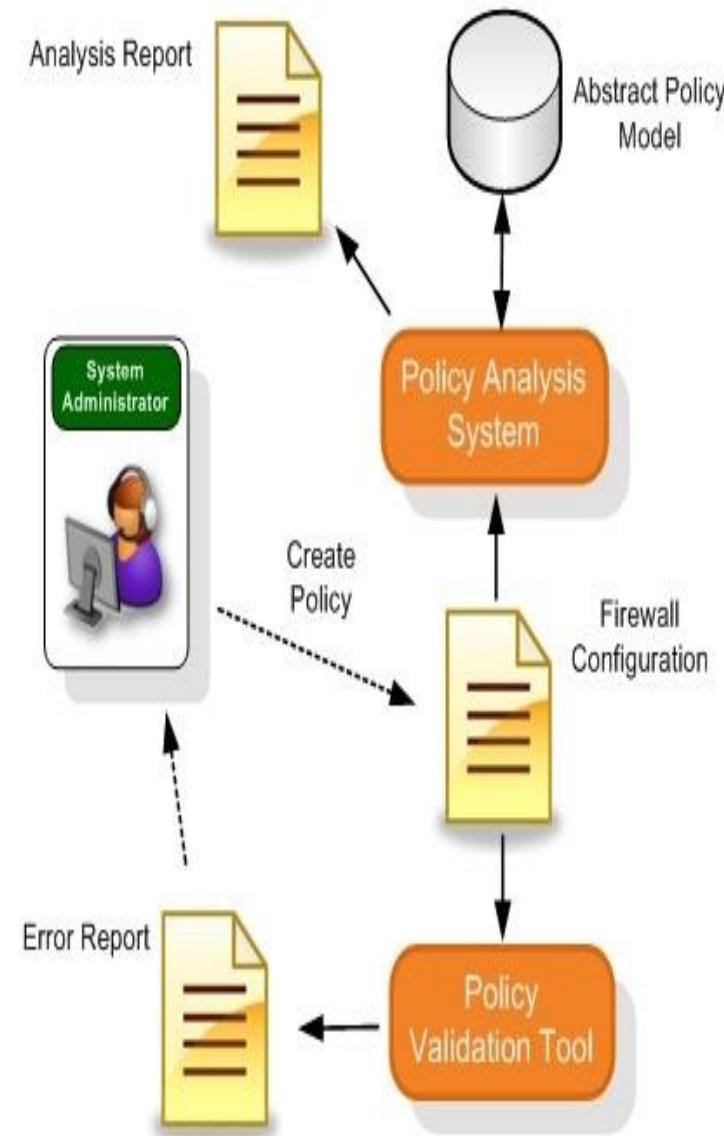
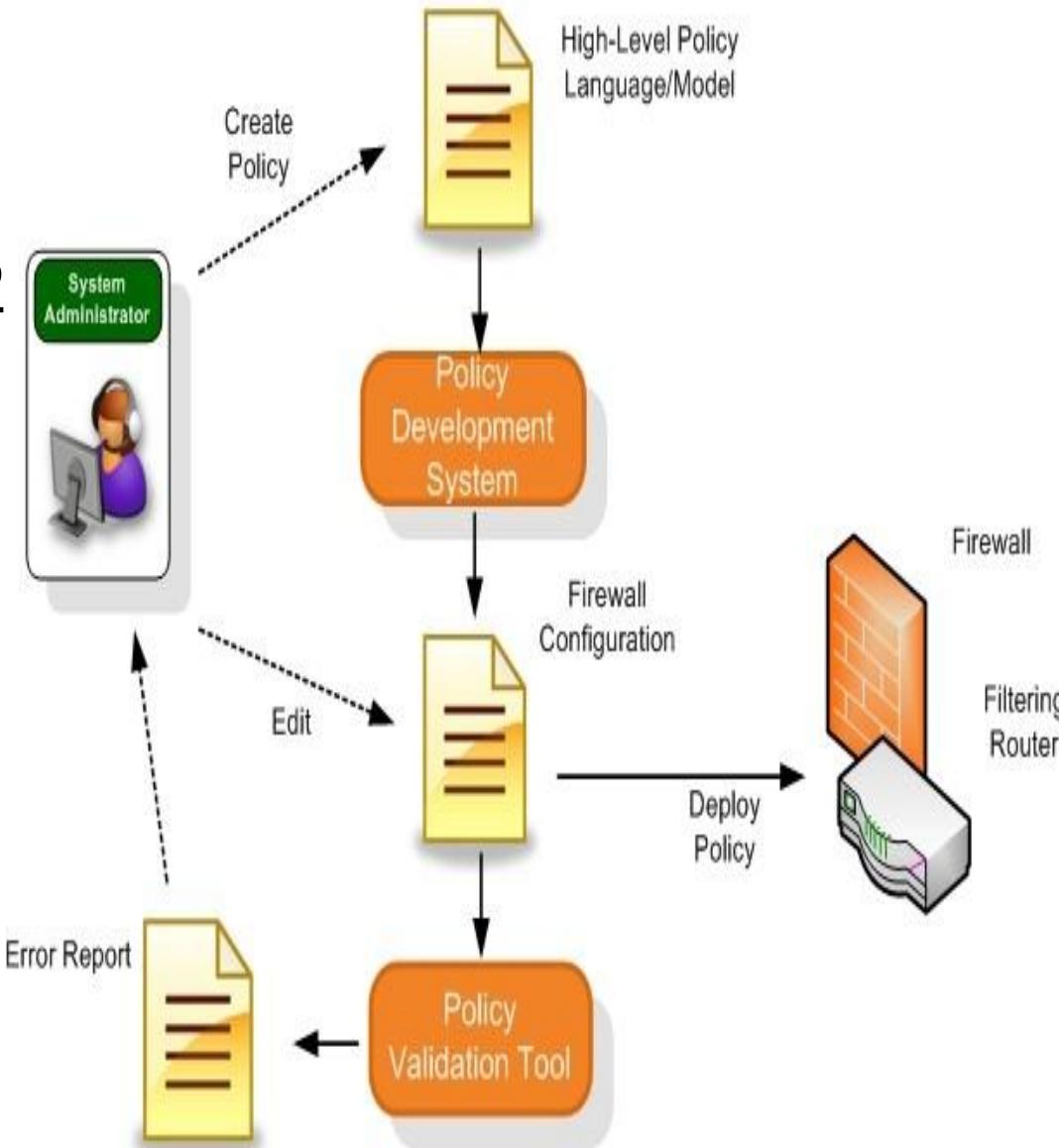
<https://www.cisco.com/c/en/us/support/docs/security/ips-4200-series-sensors/6117-ids2cspm-6117.html>

# Тармоқ хавфсизлиги сиёсатини бошқариш фреймворки



## Мавжуд тизимлар билан интеграциялашган сиёсатни текшириш инструменти

- 2



# Фойдаланишни чеклаш ва таъқиқлаш

## • 1. Акция 2024

Бошқа бирорни таҳдид қилиши, безовта қилиши, қўрқитиши ёки безовта қилишимумкин бўлган материалларни яратиш ёки узатиш.

Туҳмат қилувчи материални яратиш ёки узатиш

«Фойда олиш» учун бизнес фаолиятини юритиш ёки унда қатнашиш

Иш билан боғлиқ тергов мақсадлари учун ва бўлим бошлиғи томонидан тасдиқланган ҳолатлардан ташқари ҳар қандай "катталар учун мўлжалланган кўнгил очиш", порнографик ёки одобсиз материалларга кириш, кўриш ёки олиш

Қайси серверда жойлашишидан қаътий назар ташкилот фаолияти билан боғлиқ шахсий веб саҳифаларни очиш ва юритиш

Иш фаолиятига тегишли бўлмаган ҳужжатларни чоп этиш

Иш фаолияти билан боғлиқ бўлмаган ҳолатларда интернетдан фойдаланиш, кўшимча қурилмалардан фойдаланиш

Қонунларни ёки ташкилотнинг ички меъёрий ҳужжатларида келтирилган талабларга амал қиласли

# Интернет контентини фильтрлаш



- 1. Ходимларнинг Интернетдан фойдаланишига сарфланган вақтини камайтириш.
- 2. Ходимларнинг вазиятларни текширишда интернетга сарфланадиган вақтини қисқартириш.
- 3. Ишга алоқадор бўлмаган ҳолатларда Интернетбраузерлар учун ишлатиладиган тармоқ ўтказувчанлиги ҳажмини минималлаштириш.

## Фойдаланувчиларнинг логин ва пароллари



Хар бир мижоз ўз номи билан боғлик бўлган ноёб фойдаланувчи идентификаторидан фойдаланиши шарт. Умумий / умумий фойдаланувчи идентификаторларига рухсат берилмайди.

Тармоқдан фойдаланувчиларнинг идентификаторлари ташкилот нормаларидан берилган талабларга мос келиши шарт

Иловалар серверларда сақланадиган фойдаланувчилар идентификатор ва паролларини LDAP протоколи орқали текшириши лозим

Фойдаланувчиларга тизим ва унинг элементларидан ҳамда ташкилот фаолияти билан боғлик иловалардан фойдаланишда ягона идентификатор ва паролдан фойдаланишларига рухсат берилади

1. Камида 8 ва 14 белгидан ошмаслиги керак.
2. Кетма-кет 3 та белгига (яъни, ааа) рухсат берилмаслиги керак ва 5 та бир хил белгиларга рухсат берилмайди (яъни, 1аабаа).
3. Ҳар 60 кунда муддати тугаши керак.
4. Олдинги саккизта паролни қайта ишлатмайди.
5. Эгасининг электрон почта манзили ёки тўлиқ исмининг бирон бир қисми бўлиши мумкин емас.
6. "Умумий" сўз бўлиши мумкин эмас (масалан, луғатдаги ёки умумий фойдаланишдаги сўз бўлмаслиги керак).
7. Ҳеч қандай тилдаги сўзларни ўз ичига олмаслиги керак

# Тармоқ инфратузилмаси



▶ Routers and Switches



▶ Internet DMZ Equipment



▶ Virtual Private Network (VPN)

▶ Wireless Communication

▶ Servers



▶ Workstations



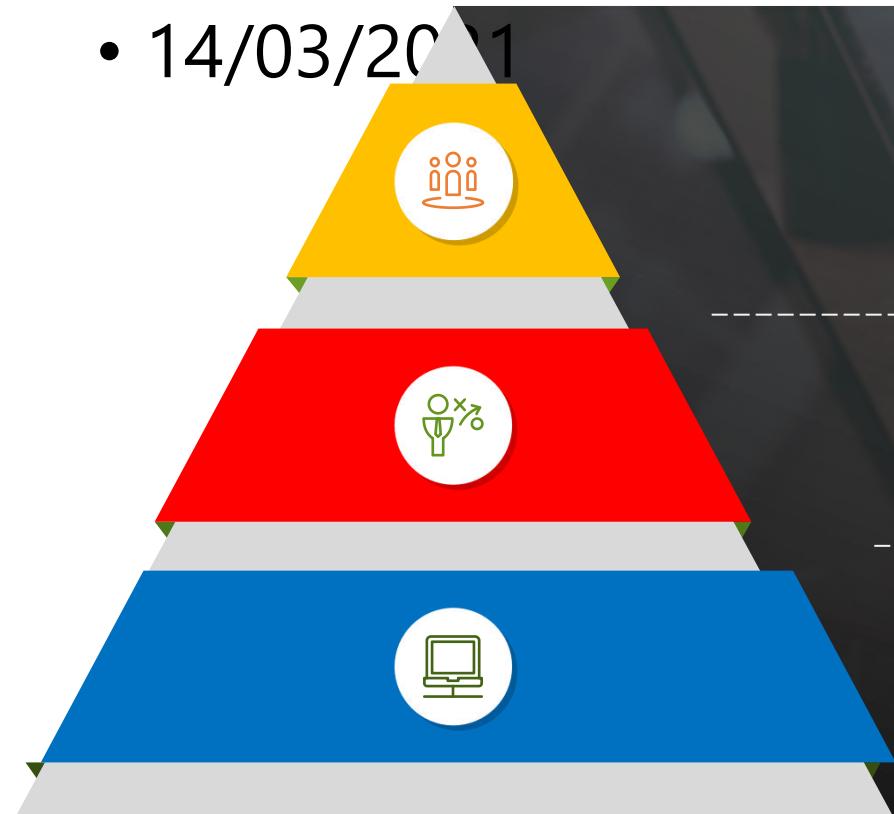
▶ Portable Computing Devices



▶ Network Storage

# Routers and Switches

- 14/03/2021



Курилмаларда локал фойдаланувчиларнинг идентификаторлари созланмаган бўлиши лозим.

Курилмалар фойдаланувчиларни аутентификациялашда TACACS + дан фойдаланиши шарт.

Курилмани ишга тушириш пароли шифрланган ҳолатда сакланиши лозим.

IP трансляция

Рухсат берилмаган IP манзиллардан кирувчи пакетлар  
TCP ва UDP хизматлари

Барча манбаларни маршрутизациялаш

Ушбу қурилмага рухсатсиз кириш қаътиян тақиқланади!!!

Эътиборингиз  
учун раҳмат



# Тармоқ хавфсизлиги

---

4 маъруза. Тармоқларниң ахборот хавфсизлиги  
стандартлари.

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,

Tashkent, Uzbekistan

100200

# Тармоқ хавфсизлиги стандартлари



O'z DSt ISO/IEC 27033-1:2016

O'z DSt ISO/IEC 27033-2:2016

O'z DSt ISO/IEC 27033-3:2016

O'z DSt ISO/IEC 27033-4:2016

O'z DSt ISO/IEC 27033-5:2016

1

2

3

4

5

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ.  
ТАРМОҚ ХАВФСИЗЛИГИ. 1-ҚИСМ.  
ШАРҲ ВА КОНЦЕПЦИЯЛАР

ТАРМОҚ ХАВФСИЗЛИГИНИ  
ЛОЙИХАЛАШТИРИШ ВА ЖОРИЙ  
ЭТИШ БҮЙИЧА РАХБАРИЙ КҮРСАТМАЛАР

ЭТАЛОН ТАРМОҚ СЦЕНАРИЙЛАРИ. ТАҲДИДЛАР,  
ЛОЙИХАЛАШТИРИШ УСУЛЛАРИ ВА БОШҚАРУВ  
МАСАЛАЛАРИ

ХАВФСИЗЛИК ШЛЮЗЛАРИНИ ҚЎЛЛАГАН ҲОЛДА  
ТАРМОҚЛАРАРО ХАВФСИЗЛИКНИ ТАЪМИНЛАШ  
УЧУН КОММУНИКАЦИЯЛАР

ВИРТУАЛ ҲУСУСИЙ ТАРМОҚЛАРНИ ҚЎЛЛАГАН  
ҲОЛДА ТАРМОҚЛАРАРО ХАВФСИЗЛИКНИ  
ТАЪМИНЛАШ УЧУН КОММУНИКАЦИЯЛАР



## O'z DSt ISO/IEC 27033 ?

O'z DSt ISO/IEC 27033 бошқарув хавфсизлиги, ахборот тизимлари тармоқларининг ишилаши ва фойдаланилиши ҳамда уларнинг уланиши аспектлари бўйича батафсил тавсияномаларни ўзида мужассам этган. Ташкилотда ахборот хавфсизлигини умуман ва тармоқ хавфсизлигини қисман таъминлашга масъул шахслар ушбу стандартда келтирилган материалларни ўзининг конкрет талабларига мувофиқлаштириш имкониятига эга бўлиши керак.

Қайд этиш лозимки, O'z DSt ISO/IEC 27033 тармоқ хавфсизлигини бошқариш воситаларини амалга ошириш бўйича O'z DSt ISO/IEC 27002 асосий стандартида келтирилган таърифларга қўшимча равишда батафсил келтирилган тавсияларни ўзида мужассам этади.

# Норматив ҳаволалар



O'z DSt ISO/IEC 7498-1:2009 Ахборот технологияси. Очиқ тизимларнинг ўзаро боғлиқлиги. Асосий этalon модель. 1-қисм. Асосий модель



O'z DSt ISO 7498-2:2011 Ахборот технологияси. Очиқ тизимларнинг ўзаро боғлиқлиги. Асосий этalon модель. 2-қисм. Хавфсизлик архитектураси



O'z DSt ISO/IEC 27000:2014 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқариш тизимлари. Шарҳ ва луғат



O'z DSt ISO/IEC 27001:2009 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқариш тизимлари. Талаблар



O'z DSt ISO/IEC 27002:2016 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари



O'z DSt ISO/IEC 27004:2014 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқариш тизими самарадорлигини ўлчаш

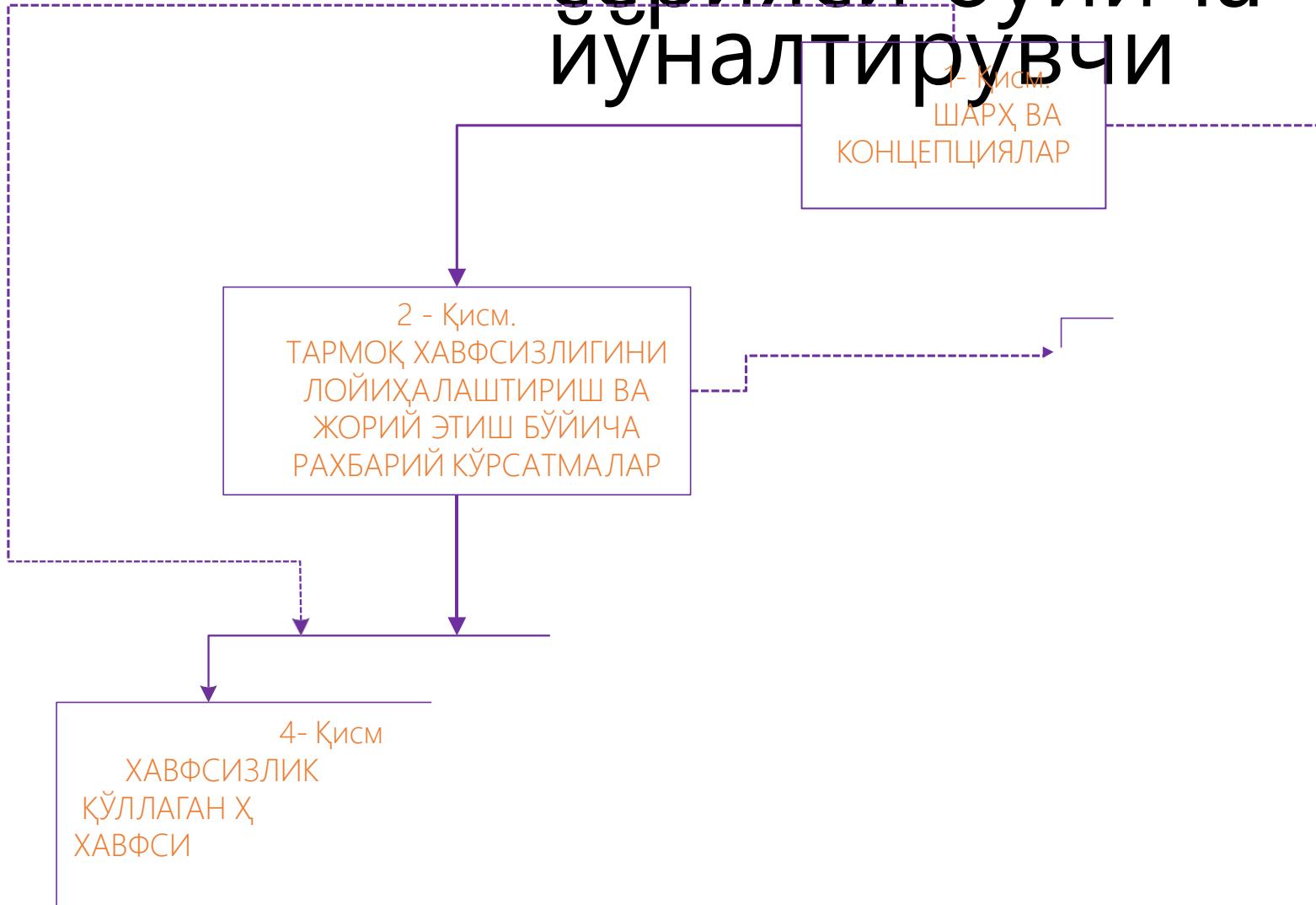


O'z DSt ISO/IEC 27005:2013 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлиги рискларини бошқариш



O'z DSt ISO/IEC 27035:2015 Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлиги инцидентларини бошқариш

# О'з DSt ISO/IEC 27033 стандартлари серияси буйича иуналтирувчи



# Тармоқ хавфсизлигини режалаштириш ва

бс

Шунингдек қаранг  
О'з DSt ISO/IEC 27001,  
О'з DSt ISO/IEC 27002  
О'з DSt ISO/IEC 27003  
О'з DSt ISO/IEC 27004  
О'з DSt ISO/IEC 27005

Риск доира  
контекстини аниқлаш  
ва кейнги баҳолаш

Бошқарув  
воситаларини  
кўлловчи  
идентификация

Хавфсизлик ва  
бошқарувнинг талаб  
етиладиган маҳсус  
архитектураси  
идентификацияси

Ишлаб чиқиш амалга  
ошириш ва тестлаш,  
шуningдек,  
експлуатация,  
мониторинг ва  
текширув

Тармоқлар билан боғлиқ рискларни идентификациялаш ва хавфсизликни  
бошқариш воситаларини идентификацияга тайёрлаш:

- а) жорий ва (ёки) режалаштирилган тармоқ мухити тўғрисидаги  
ахборотларни йигиши:  
1) ахборот хавфсизлиги корпаратив сиёсатини текшириш;  
2) тармоқ архитектураси, иловалари ва сервисларини текшириш;  
3) тармоқ уланишлари кўринишлари идентификацияси;  
4) бошқа тармоқ характеристикаларини кўриб чиқиш;  
5) бизнесга потенциал салбий таъсирни, бизнес таҳдидларини ва  
заифликларни баҳолаш имкониятини олиш учун ахборотни йигиши;  
б) ахборот хавфсизлиги ва бошқарув воситалари потенциал доираси  
рискларини идентификациялаш:  
1) хавфсизлик ва раҳбарият томонидан ўтказиладиган текширув рискларни  
баҳолашни амалга ошириш (шуningдек О'з DSt ISO/IEC 27002, О'з DSt  
ISO/IEC 27005 га қаранг) - зарур бўлган ҳолларда талаб етиладиган тармоқ  
сенирийлари "технология" сўрвлари билан боғлиқ риск тўғрисидаги  
ахборотлардан фойдаланиш (10- ва 11- бўлимларни қаранг) - Хавфсизлик  
талабларини аниқлаш (7- бўлимни қаранг)

Кўлланувчи бошқарув воситалари идентификацияси:

- нотехник;
- фақатгина тармоқларда қўлланилмайдиган техник(8-бўлимга қаранг);

Хавфсизлик маҳсус архитектура/лойиха вариантларини текшириш  
тармоқ сенирийларини кўриб чиқиш ва тармоқ "технологиялари"  
масалалари, хавфсизликнинг маҳсус афзал бўлган  
архитектура/лойиҳалари ва улар билан боғлиқ бошқарув  
воситаларини танлаш ва хужжатлаштириш(9-11-бўлимiga қаранг)

Хавфсизлик таъминлаш бўйича йечимларни ишлаб чиқиш, амалга  
ошириш ва тестлаш (12-бўлимг ақаранг)

Хавфсизлик таъминлашни амалга ошириш (13-бўлимг ақаранг)

Амалга оширишни мониторинг қилиш ва текшириш (14-бўлимга  
қаранг)

вақт вақти билан ва  
сезиларли ўзгаришлар  
бўлган ҳолларда  
ўтказиладиган  
текширишлар (бизнес,  
технология,  
хавфсизликни  
таъминлаш бо;йича  
йечимлар ва ҳ.к. талаб  
бўлганда)

# Тармоқ хавфсизлиги рисклари доираси үз дели

Ҳакиқийлик. Рухсат этилган ва рухсат этилмаган фойдаланиш ва тармоқ ресурслари эксплуатациясини назорат қилиш. Испоттаб бўлмаслик. Ҳисобдорлик. Сакланувчи маълумотларнинг конфиденциалитиги ва ҳ.к.

Конфиденциаллик, бутунлик, фойдалана олишилилик ва ишончлилик

Ҳакиқийлик. Рухсат этилган ва рухсат этилмаган фойдаланиш ва тармоқ ресурслари эксплуатациясини назорат қилиш. Испоттаб бўлмаслик. Ҳисобдорлик. Сакланувчи маълумотларнинг конфиденциалитиги ва ҳ.к.



# ХАВФСИЗИТИ БАҲОЛАШ БОШҚАРИШ

РИСКИНИ  
ва  
ЖАРАЁНЛАРИ



11

12

13

14



Тармоқ хавфсизлиги маҳсус архитектурасининг юқори сифатига қандай эришиш йўллари, шунингдек, типик тармоқ сценарийлари ва тармоқ «технологиялари» (O'z DSt ISO/IEC 27033 нинг кейинги қисмларида батафсил кўриб чиқилади) доиралари билан боғлиқ риск, лойиҳалаштириш, бошқарув воситалари аспектлари билан таниширади, ва тармоқ хавфсизлиги бошқарув воситаларини амалга ошириш ва ишлаши, доимий мониторинг ва уларни амалга оширилишини текшириш билан боғлиқ масалаларни қисқача кўриб чиқилишини ўзида мужассам этган.



«Технологиялар» аспектлари –  
рисклар, лойиҳалаштириш усуллари  
ва бошқариш воситаларига  
тегишли масалалар

- локал ҳисоблаш тармоқлари;
- глобал ҳисоблаш тармоқлари;
- симсиз тармоқлар;
- радио тармоқлар;
- кенг полосали тармоқлар;
- хавфсизлик шлюзлари;
- виртуал хусусий тармоқлар



Хавфсизликни таъминлаш бўйича  
аппарат-дастурий воситалар ва  
хизматлар комплексини ишлаб  
чиқиш ва тестилаш

- хавфсизлик маҳсус архитектураси;
- тармоқ хавфсизлиги сиёсати;
- SecOPs билан боғлиқ хужжатлар;
- шлюз хавфсизлиги  
хизматларидан фойдаланиш  
(хавфсизлик) сиёсати;
- фаолиятузлуксизлигини  
таъминлаш режаси(лари);
- уланишхавфсизлигини  
таъминлаш шартлари (зарур  
бўлганда).



Хавфсизликни таъминлаш бўйича  
аппарат-дастурий воситалар ва  
хизматлар комплексини амалга  
oshiриш

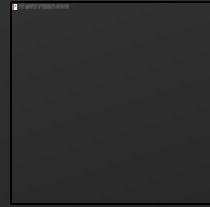
- «Амалга ошириш» тушунчаси  
хавфсизликни таъминлаш бўйича  
аппарат-дастурий воситалар ва  
хизматлар келишилган  
комплексини, ўтказилган  
хавфсизликни тестилаш натижалари  
ва улар билан боғлиқ олдиндан  
бажарилган зарур ҳаракатларининг  
кўлланилиши билан амалдаги  
тармоқнинг (кундалик) ишлашини  
англатади.



Аппарат-дастурий воситалар  
ва хизматлар комплекси  
мониторинг ва таҳлили  
эксплуатацияси

- Эксплуатация бошланғандан сўнг  
давлат стандартлари, ташкилот  
стандартлари (давлат стандартлари  
мавжуд бўлмаганда) талабларигага  
жорий мониторинг ватаждилл  
мувофиқлиги ҳаракатлари  
ўтказилиши керак.

# Қўллаб-қувватловчи бошқариш воситалари



- Кириш
- Тармоқ хавфсизлигини бошқариш
- Техник заифликларни бошқариш  
Идентификация ва аутентификация
- Назорат журналларини юритиш ва тармоқ мониторинги
- Бостириб киришни аниқлаш ва олдини олиш
- Заарловчи дастурлардан ҳимоя
- Криптографияга асосланган хизматлар
- Бизнес узлуксизлигини бошқариш

## Тармоқ хавфсизлигини бошқариш фаолияти



Кириш



Тармоқ хавфсизлиги сиёсати



Тармоқ хавфсизлиги операцион жараёнлари



Тармоқ хавфсизлиги талабларига мувофиқликни текшириш



Тармоқ хавфсизлиги талабларига мувофиқликни текшириш



Кўпгина ташкилотлар билан тармоқ уланиши хавфсизлигини таъминлаш шартлари



Масофавий тармоқ фойдаланувчилари учун хавфсизликни таъминлашнинг хўжжатлаштирилган шартлари  
Тармоқ хавфсизлиги инцидентларини бошқариш



Тармоқ хавфсизлигини таъминлаш билан боғлиқ вазифалар ва мажбуриятлар

# Типик тармоқ сценарийлари – рисклар, лойиҳалаштириш усуллари ва бошқариш воситаларига тегишли масалалар



## Кириш



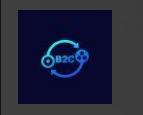
Ходимлар учун Интернетдан фойдаланиш хизмати



Ҳамкорликдаги ишларнинг кенгайтирилган хизматлари



«Бизнес - бизнес» хизматлари



«Бизнес - мижоз» хизматлари



## Аутсорсинг хизматлари



Тармоқ сегментацияси



Мобил алоқа



Сафарларда бўлган фойдаланувчиларнининг тармоқ томонидан қўллаб-қувватланиши



Уй оғислари ва кичик корхоналар оғисларининг тармоқ томонидан қўллаб-қувватланиши

# Тармоқ сценарийларини тартибта

## Социалдык тармоқтар

		Фойдаланувчилар		
		Ички	Ташкилотдан ташқарида ишловчи ходимлар	Ташқи
<b>Ахборот ресурсларидан фойдалана олишлик</b>	Очиқ	<ul style="list-style-type: none"> <li>-ходимлар учун Интернетдан фойдаланиш хизматлари;</li> <li>- бизнес-бизнес хизматлари</li> </ul>		<ul style="list-style-type: none"> <li>- бизнес-мижоз хизматлари</li> </ul>
	Чегараланган	<ul style="list-style-type: none"> <li>- биргаликда фойдаланиш учун хизматларни кенг татбиқ этиш;</li> <li>- бизнес-бизнес хизматлари;</li> <li>- тармоқ сегментацияси;</li> <li>- уйда ёки кичик корхоналарда ишловчиларни тармоқ орқали қўллаб-қувватлаш</li> </ul>	<ul style="list-style-type: none"> <li>- мобил алоқа;</li> <li>- мобил фойдаланувчиларни тармоқ орқали қўллаб-қувватлаш</li> </ul>	<ul style="list-style-type: none"> <li>- биргаликда фойдаланиш учун хизматларни кенг татбиқ этиш;</li> <li>-бизнес-бизнес хизматлари;</li> <li>-бизнес-мижоз хизматлари</li> </ul>
	Ташқи	<ul style="list-style-type: none"> <li>- аутсорсинг хизматлари</li> </ul>		<ul style="list-style-type: none"> <li>- аутсорсинг хизматлари</li> </ul>

# Стандартдаги сценарийлар тартиби



Ходимлар учун Интернетдан  
фойдаланиш хизматлари  
(7-бўлим)



Бизнес-бизнес хизматлари  
(8-бўлим)



Бизнес-мижоз (9-бўлим)



Биргаликда фойдаланиш учун  
хизматларни кенг татбиқ этиш  
(10-бўлим)

Тармоқ сегментацияси (11-бўлим)  
Уйда ёки кичик корхоналарда  
ишловчиларни тармоқ орқали  
қўллаб-кувватлаш (12-бўлим)



Мобил алоқа (13-бўлим)



Мобил фойдаланувчиларни  
тармоқ орқали қўллаб-  
кувватлаш (14-бўлим)



Аутсорсинг хизматлари  
(15-бўлим)



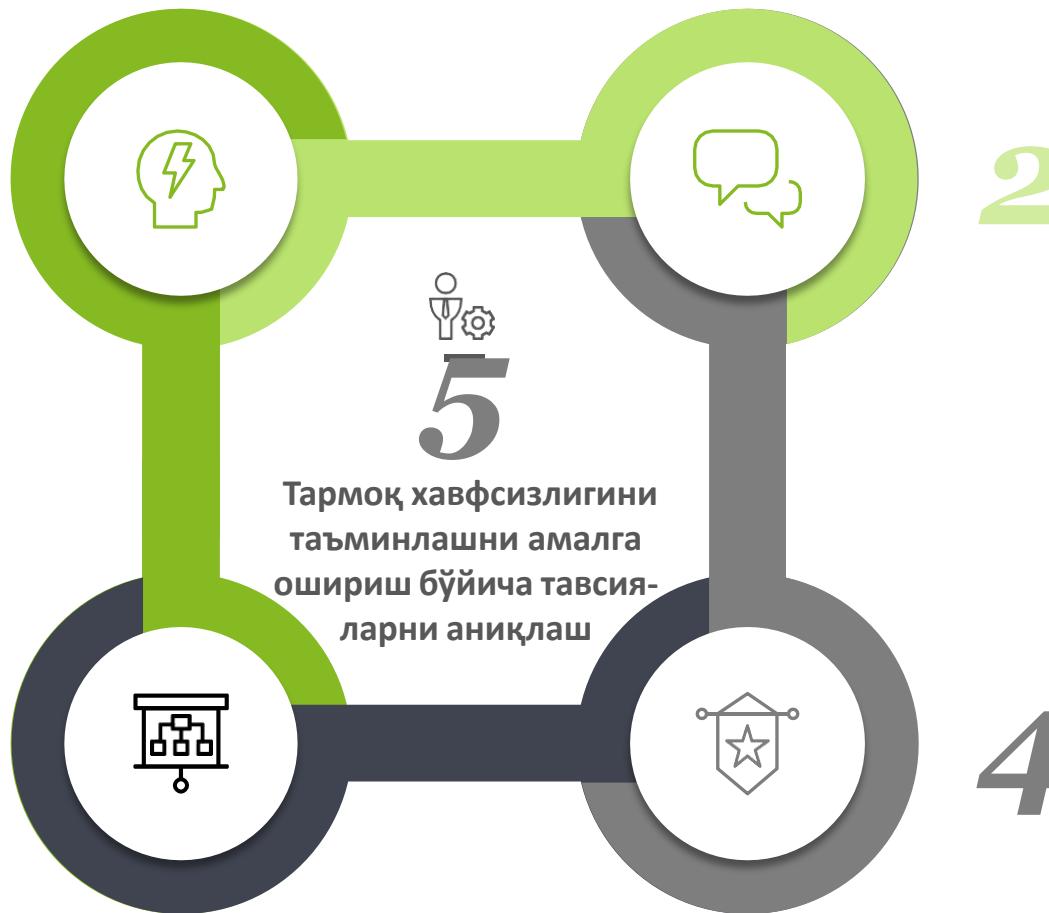
# ЁНДАШУВЛАР

Сценарийнинг киравчи  
ахборотлари ва  
чегараларини текшириш

1

3

Аниқланган  
заифликларга нисбатан  
risk таҳлилини ўтказиш



Сценарийга мос келувчи  
таҳдидларнинг тавсифи

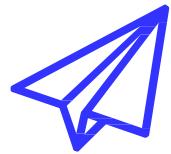
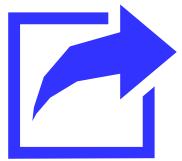
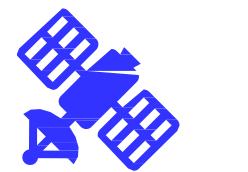
2

4

Кўриб чиқилаётган  
заифликларнинг  
бизнесга таъсирини  
таҳлил қилиш

# Тармоқ хавфсизлигини таъминлаш усулларига мисоллар

Хавфсизлик бўйича талаблар	Хавфсизликни таъминлаш механизмлари/усуллари
Фойдалана олишлиликни бошқариш	 Кириш учун рухсатномалар тизими (идентификация карточкалари), ACL, мажбуриятларни тақсимланиши
Аутентификация қилиш	 Тизимга киришни соддалаштирилган рўйхатдан ўтказиш/пароль, рақамли сертификатлар, электрон рақамли имзо, TLS нинг 1.2 версияси, SSO, CHAP
Фойдалана олишлилик	 Керагидан кўплик ва резерв нусҳа олиш, тармоқлараро экранлар, IDS/IPS (DoS ҳужумларини блокировка қилиш учун), бизнеснинг узлуксизлиги, тармоқ бошқаруви ва SLA билан хизматларни бошқариш
Алоқа хавфсизлиги	 IPSec/L2TP, хусусий алоқа линиялари, мослаштирилган тармоқлар
Конфиденциаллик	 Шифрлаш (3DES, AES, шунингдек O'z DSt 1105 да келтирилган шифрлаш алгоритмлари), фойдалана олишлиликни бошқариш рўйхати, файллардан фойдалана олишилик ҳуқуқи
Яхлитлик	 IPSec HMAC (мисол учун, SHA-256), даврий керагидан кўп назорат, антивирус дастурларий таъминоти
Рад этмаслик	 Ҳодисаларни рўйхатга олиш, роллар асосида фойдалана олишлиликни бошқариш ва электрон рақамли имзолар
Хиралик	 IP-сарлавҳаларни шифрлаш (мисол учун, IPSec, NAT (4-версиядаги IP учун) туннеллаш режимили VPN



# Ходимлар учун Интернетдан фойдалана олиш хизматлари



Интернетдан фойдаланиш бизнес  
эҳтиёжларидан келиб чиқиб тақдим  
этилган

агар Интернетдан фойдалана олиш ҳуқуки  
(чегараланган тарзда) шахсий эҳтиёжларидан  
келиб чиқиб берилган бўлса, у ҳолда қандай  
хизматлардан фойдаланишга рухсат берилган

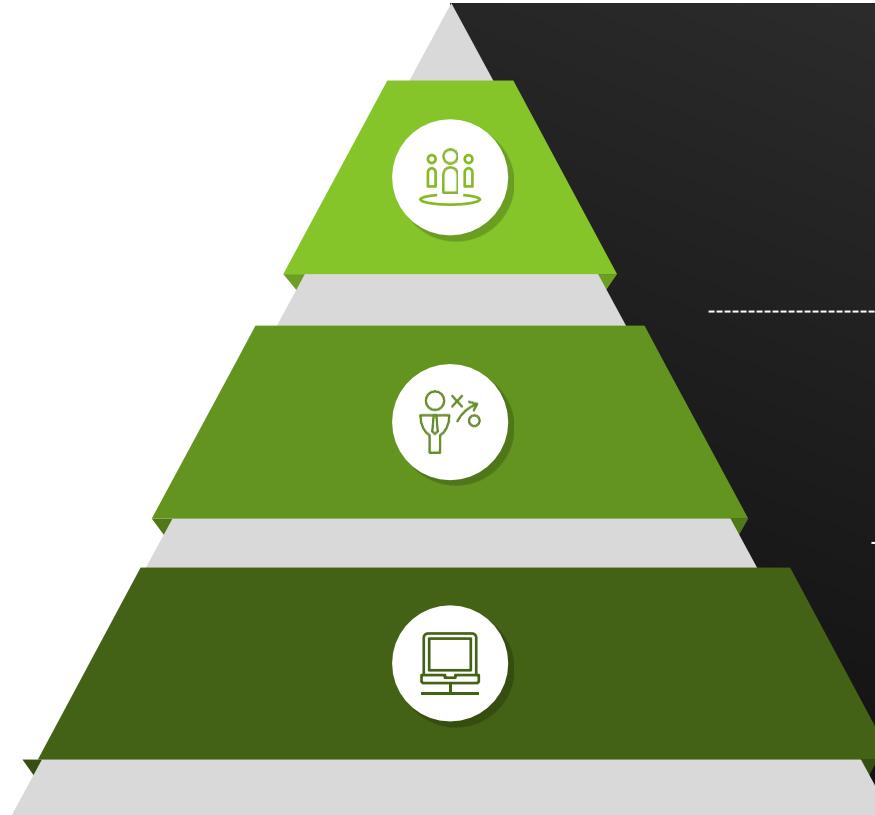
биргаликда фойдаланиш учун хизматларни  
кенг татбиқ этиш рухсат этилганми

ходимларга чатларда, форумларда ва ҳак.  
қатнашишга рухсат берилганми



*Гарчи, кўп ҳолларда, ёзилган сиёсат  
Интернетдан номақбул фойдаланишида муҳим  
тўхтатиб турувчи фактор сифатида рол  
ўйнасада, ташкилот хануз катта ахборот  
хавфсизлиги рискларига йўлиқиб туради*

# Ахборот хавфсизлиги талабларыга боғлиқ талаблар



- конфиденциаллик билан  
(айниңса электрон банк хизматларини күрсатишига нисбатан)

- аутентификация қилиш билан  
яхлитлик билан

- фойдалана олишлик билан

# Бизнес-мижоз хизматлари билан боғлиқ хавфсизлик таҳдидлари

Вирус ҳужумлар ва заарловчи дастурларни жорий этиш

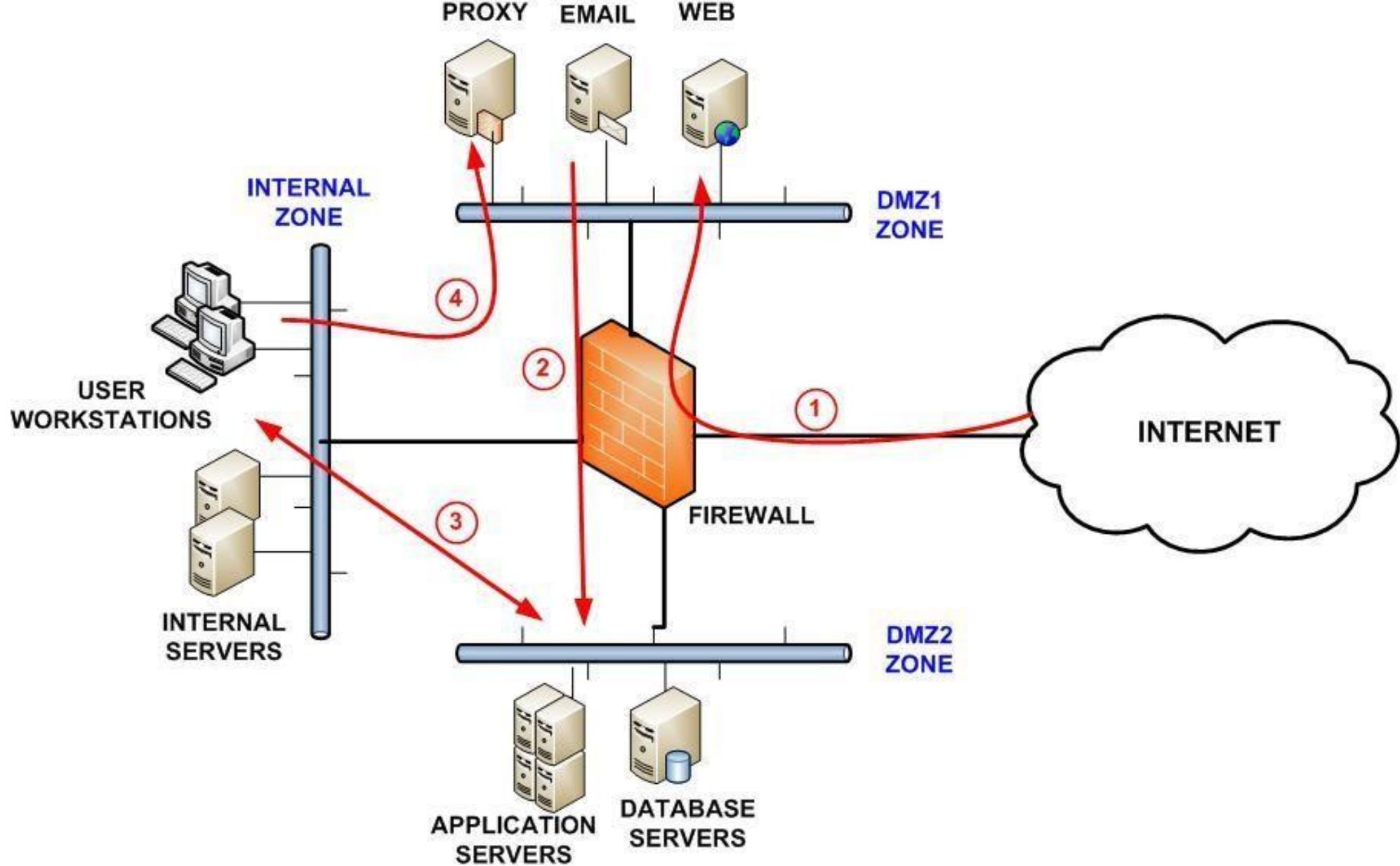
«Хизмат кўрсатишда рад этиш» ҳужумлари

Муаллифлаштирилмаган фойдалана олиш

Транзакцияларни ахборот билан тўлдиришни қалбакилаштириш (хабарлар олувчигача етиб бормайди ёки ахборотлар узатиш вақтида ўзгартирилади)



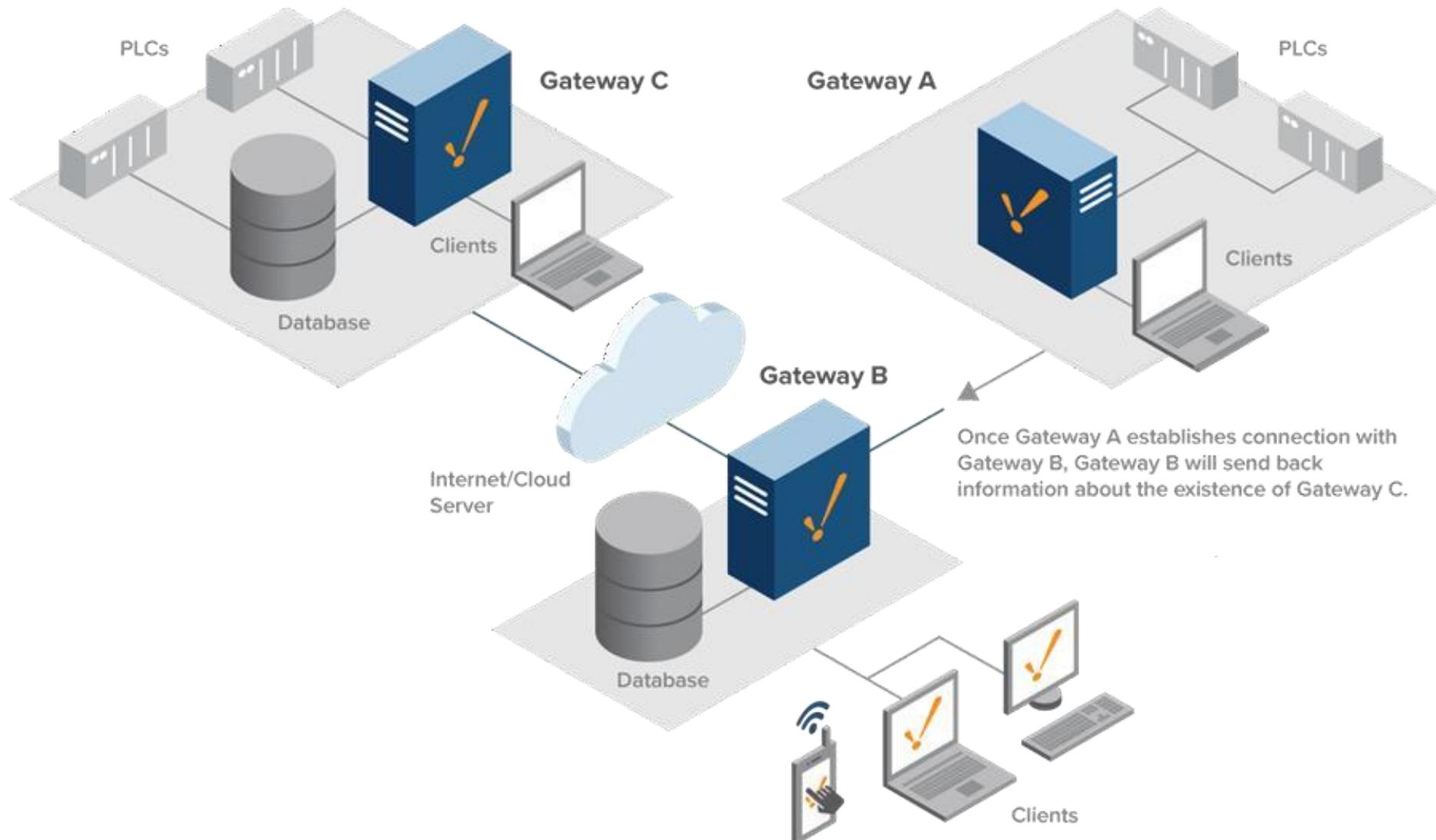
# Тармок мұхити намұнаси



# Таҳдидлар ва хавфсизлик бўйича талаблар ўртасидаги ўзаро алоқа

ТАҲДИДЛАР	ТАЛАБЛАР						
	Логик тармоқ сегмента циясини таъминлаш	Логик тармоқла р орқали ўтувчи трафикни чеклаш ва таҳлил қилиш	Танланган иловаларда уланишни текширишда ёки прокси-сервер операцияларида ташкилот тармоғига киришни ва тармоқдан чиқишни назорат қилиш	Ташкилот тармоқ хавфсизли ги сиёсатини бажариш	Кейинги аудит учун трафикни қайд этиш	Иловаларнинг ички тармоғи, хости ва архитектурасини яшириш/маскировкалаш	Тармоқни бошқариш функцияларини енгиллаштириш имкониятларини таъминлаш
Ваколатли фойдаланувчиларга хизмат кўрсатиша рад этиш			X		X		X
Маълумотларнинг рухсатсиз модификацияси	X		X	X	X		X
Маълумотларнинг рухсатсиз ошкора этилиши	X		X	X	X		X
Тизимли конфигурациянинг рухсатсиз ўзгарилиши				X	X		X X
Ташкилот тармоқ ресурслари ва активларидан рухсатсиз фойдаланиш	X		X	X	X		X X
Рухсат этилмаган контент	X		X	X	X		X X
Виртуализациянинг бузилиши	X		X	X	X		X
Хавфсизлик шлюзларига DoS-ва DDoS-хужумлари			X		X		X

# Шлюзни икки томонлама улаш



# Тармоқ қурилмалари хавфсизлик конфигурацияси үчүн тавсиялар



- DMZ га мувофиқ көлувчи ҳимояланган тармоқ архитектураси үчүн коммутацияланадиган тармоқ бўлиши керак
- маршрутизатор(лар) ва хавфсизлик шлюзи ўртасида статистик маршрутизация бўлиши керак
- маршрутизация манбааси ахбороти қабул қилинган бўлиши керак
- фақатгина «ҳимояланган платформа» ишлаши учун керакли бўладиган дастурий таъминотни хавфсизлик шлюзига ўрнатиш керак
- портлар рухсатсиз фойдаланилмаслигига ишонч ҳосил қилиш
- агар бостириб киришларни аниқлаш тизимидан фойдаланиш талаб этилмаса, SPA- портлар рухсатсиз фойдаланилмаслигига ишонч ҳосил қилиш
- қурилма интерфейсларида пароллар ўрнатилганига ишонч ҳосил қилиш
- RIP протоколи «берилган тугунлар орқали маршрутизация» хабарини рад этиш зарур

# Хавфсизлик воситалари ва параметрлари

**ТАЛАБАЛАР учун  
ТОПШИРИК !!!**

- 1** Тармоқлараро экран-илова камида, қуидагиларни таъминлаши керак
- 2** Пакетлар фильтрацияси қурилмаси энг камида қуидагиларни қўллаб-куватлаш имкониятига эга бўлиши керак
- 3** Пакетлар фильтрацияси ва ҳолатини сақлаган ҳолда фильтрация қурилмаси энг камида қуидагиларни қўллаб-куватлаш имкониятига эга бўлишлари керак
- 4** Қўшимча равишда, ҳолатини сақлаган ҳолда фильтрация қурилмаси энг камида қуидагиларни қўллаб-куватлаш имкониятига эга бўлиши керак
- 5** Бошқа турли функцияларни ёки созлашларни текшириш талаб этилади, масалан:

Этиборингиз  
учун раҳмат

---

# Tarmoq xavfsizligi

---

OSI va TCP/IP modellari

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100084

# OSI va uning vazifalari



1980-yillar boshida Xalqaro standartlashtirish tashkilotlari – ISO va xalqaro elektraloqa ittifoqi -ITU-T tomonidan tarmoq rivojlanishida muhim o'rin tutgan model ishlab chiqdilar.

Ushbu model ochiq tizimlarning o'zaro ishlashi modeli (Open System Interconnection, OSI) yoki OSI deb ataldi.



OSI modeli tizimlarning turli pog'onalarda o'zaro ishlashini, ularga standart nom berish va qaysi sath qanday vazifalarni bajarishini aniqlaydi.

Har bir sath tarmoq qurilmalari o'zaro ishlashining malum bir jihatni bilan bog'liq bo'ladi.

# OSI – tarmoq modeli etaloni

## OSI modeli:

- Ochiq tizimlarning o'zaro bog'lanish modeli (Open Systems Interconnection, OSI);

- Xalqaro standartlashtirish tashkiloti (ISO) 1983 yilda standart sifatida qabul qilingan.

## OSI modeli quyidagilarni tavsiflaydi:

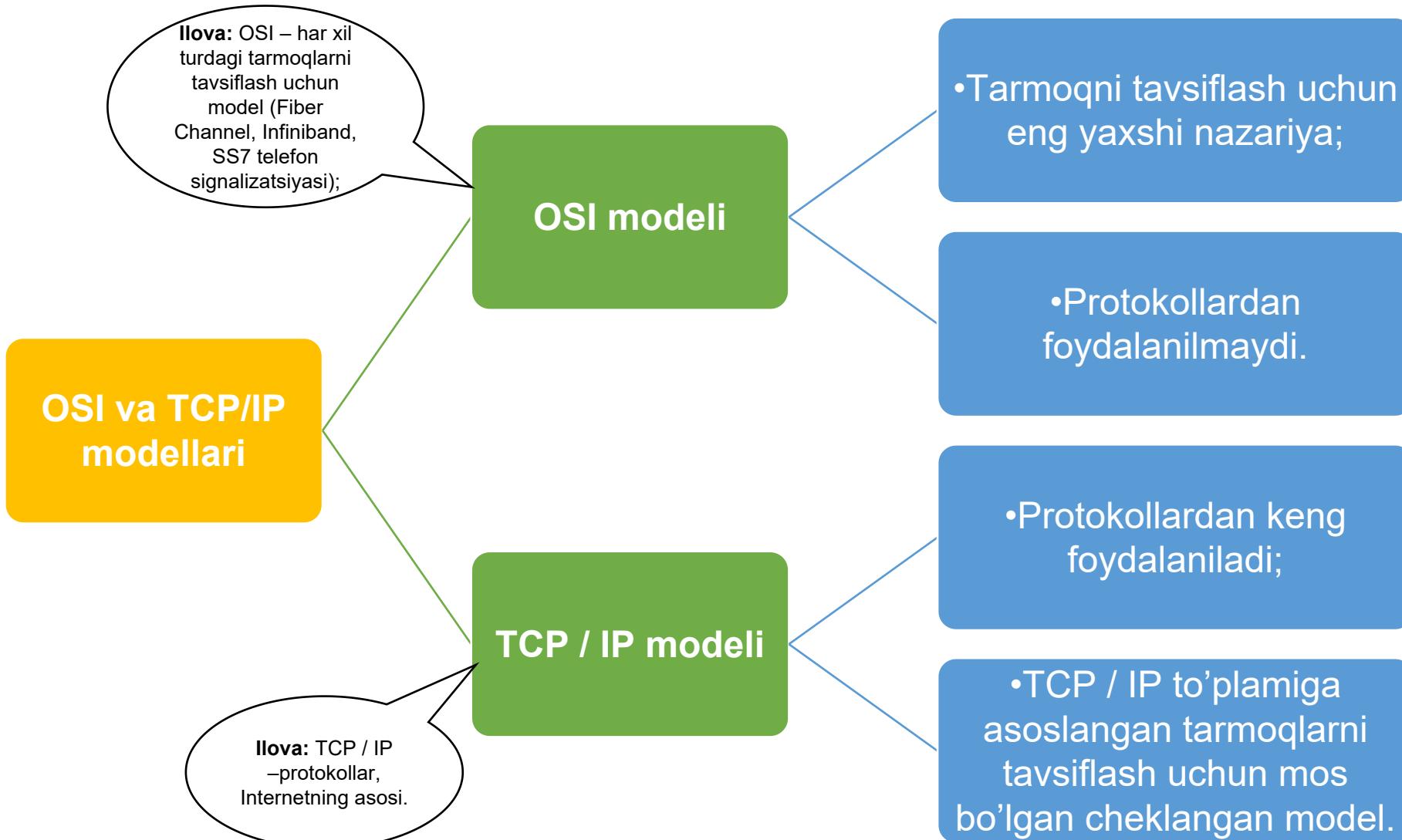
- Yetti darajadan tashkil topgan;

- Har bir darajadanning maqsadi mavjud.

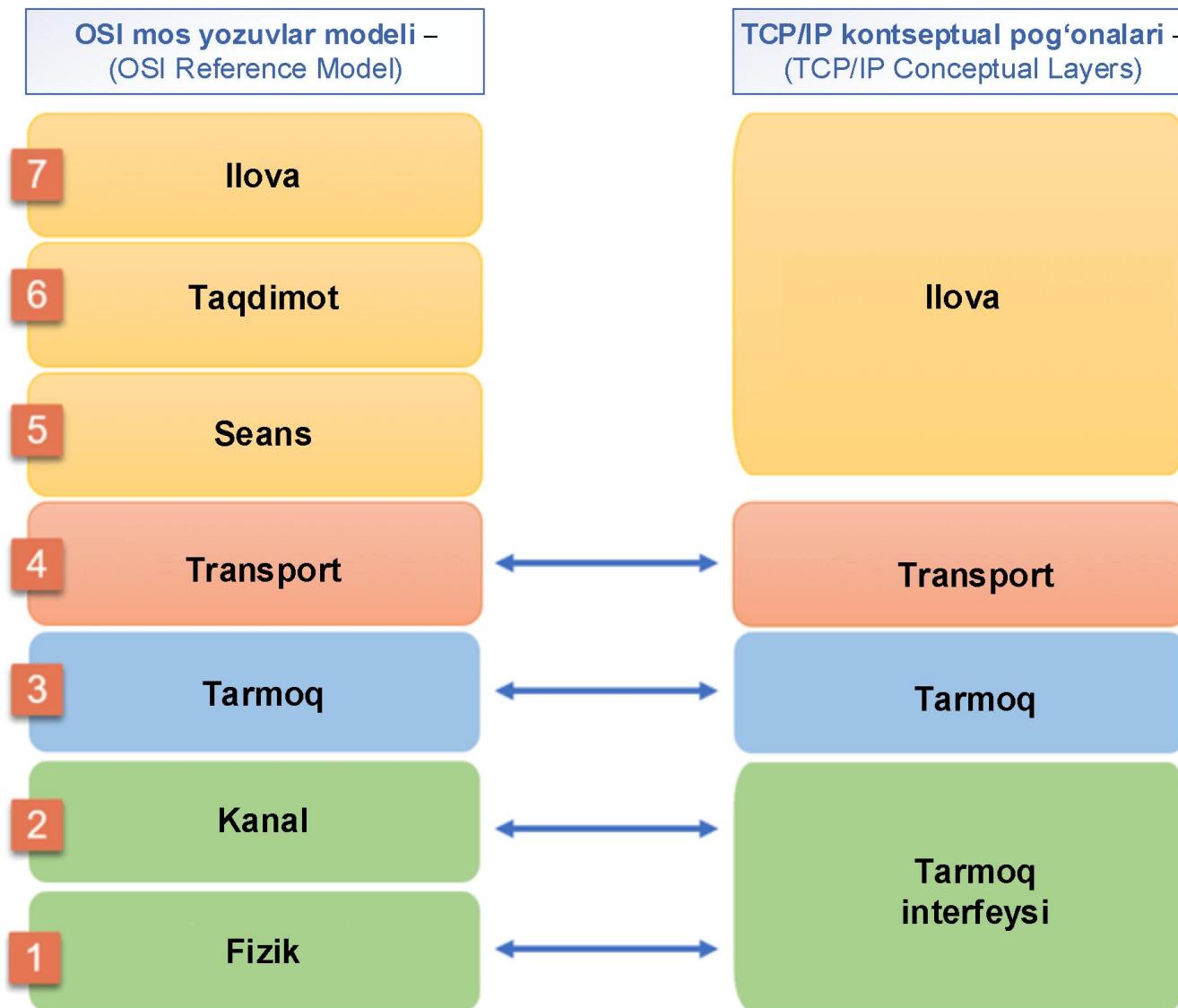
- **Tarmoq arxitekturasi emas!**

- **OSI modeli turli xil tarmoqlarni tavsiflash uchun «umumiyl til» sifatida ishlataladi.**

# OSI va TCP/IP modellari



# OSI va TCP/IP modellarini taqqoslash

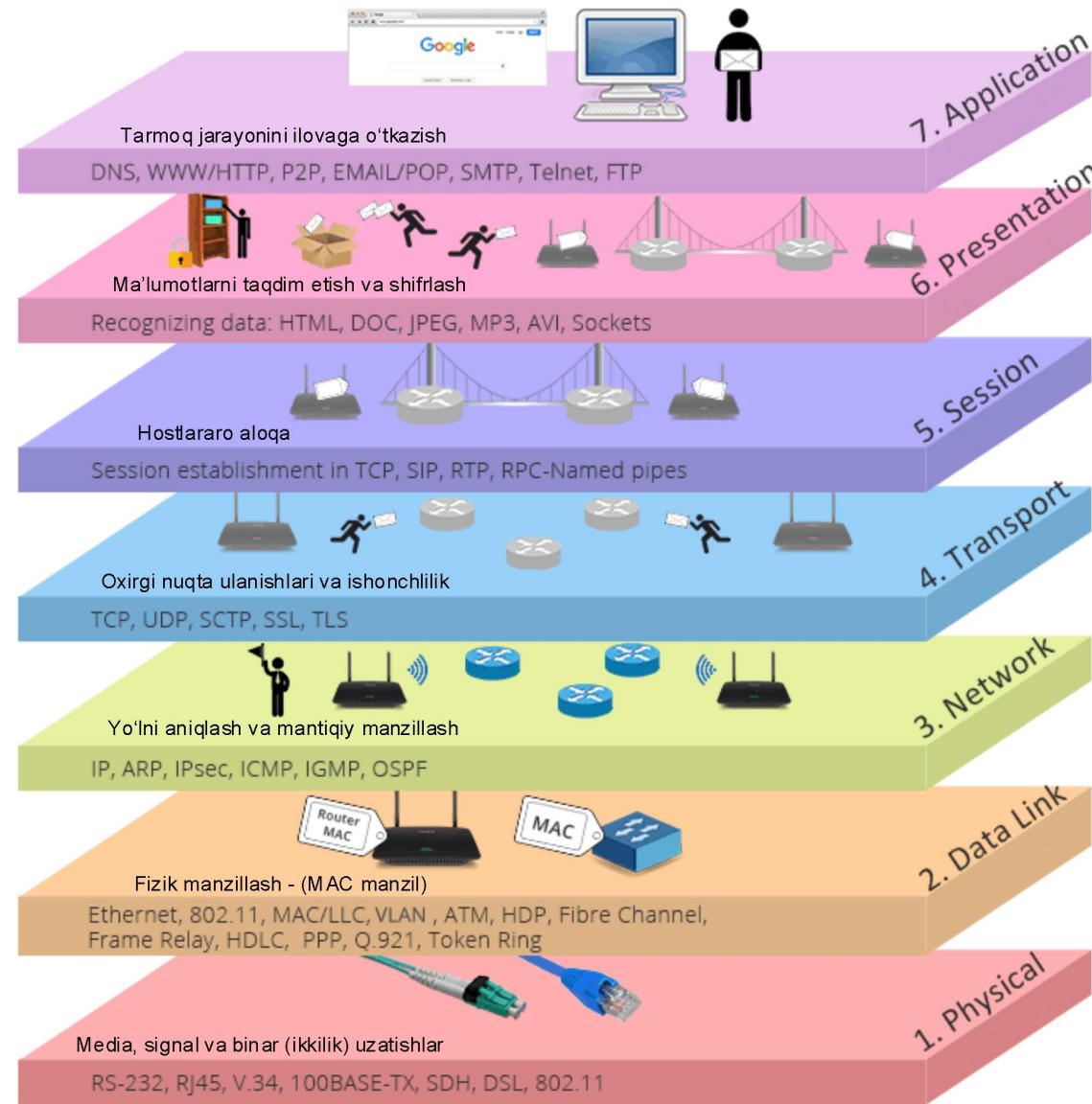


# OSI modeli xususiyatlari

## OSI modeli xususiyatlari

- Tarmoq bo‘ylab amalga oshirilgan aloqani oson tushunilishini ta’minlaydi;
- Dasturlar va qurilmalar ishlashini ko’rsatadi;
- Foydalanuvchilarga yangi topologiyani tushunishga yordam beradi;
- Turli tarmoqlar orasidagi funksional boq’liqliklarni oson solishtirish imkoniyatiga ega.

# OSI modelining 7 ta pog'onasining xususiyati



# OSI modelining 7 ta pog'onasing xususiyati

7-llova pog'onasi

tomondan amaiga  
oshiriladi. Ushbu

6-Taqdimot  
pog'onasi

pog'ona  
foydaluvchiga  
tarmoqqa kirishga

5-Seans  
pog'onasi

imkon beradi. Tarmoq  
orqali uzatilishi kerak  
b<sup>o</sup>lg'almotlarning

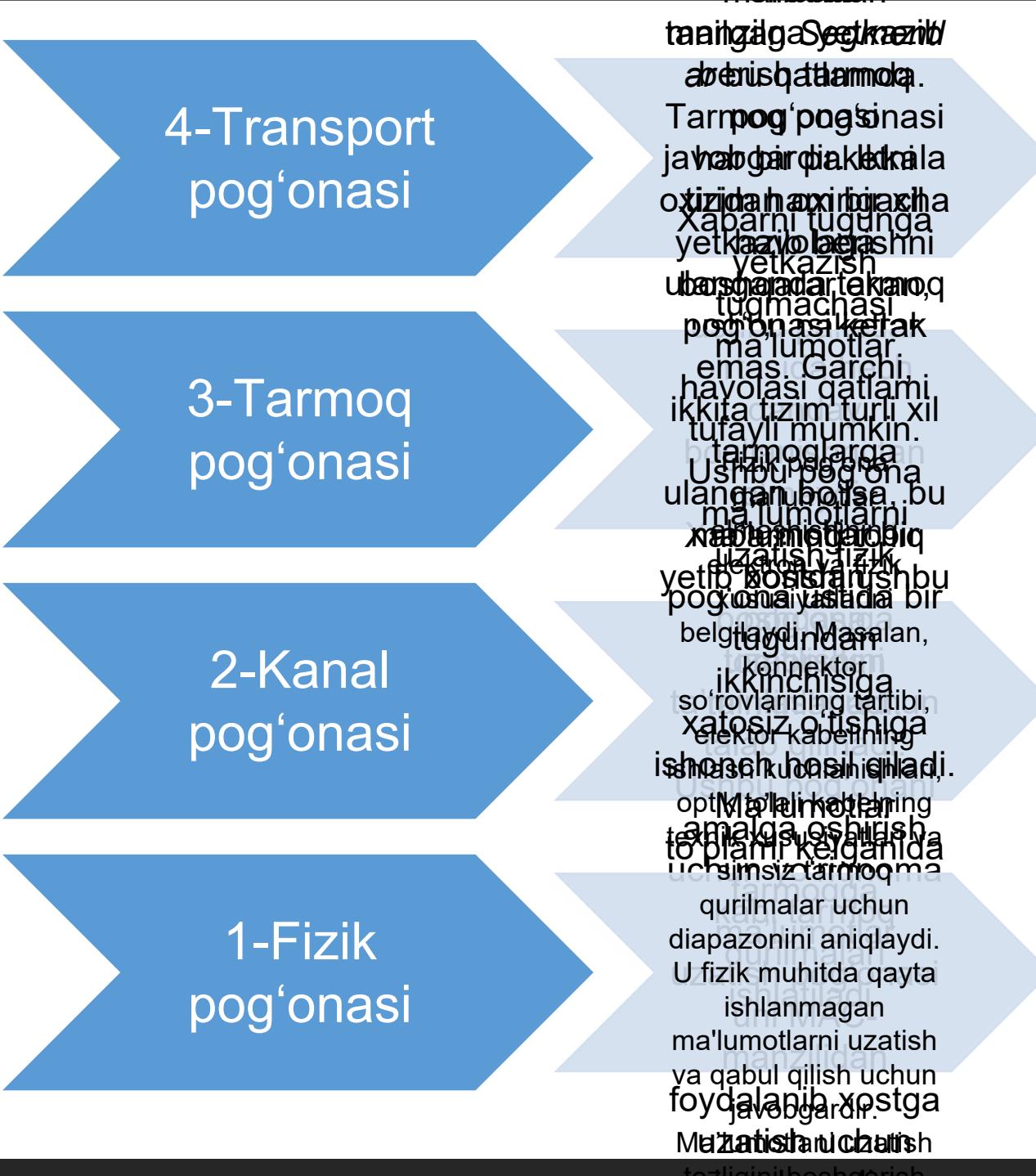
ushbu dastur  
mashinalardan ishlash<sup>ga</sup> r<sup>i</sup>  
ishlashtirish qila不得已り

Faydaluvchilar  
totarfa qanday

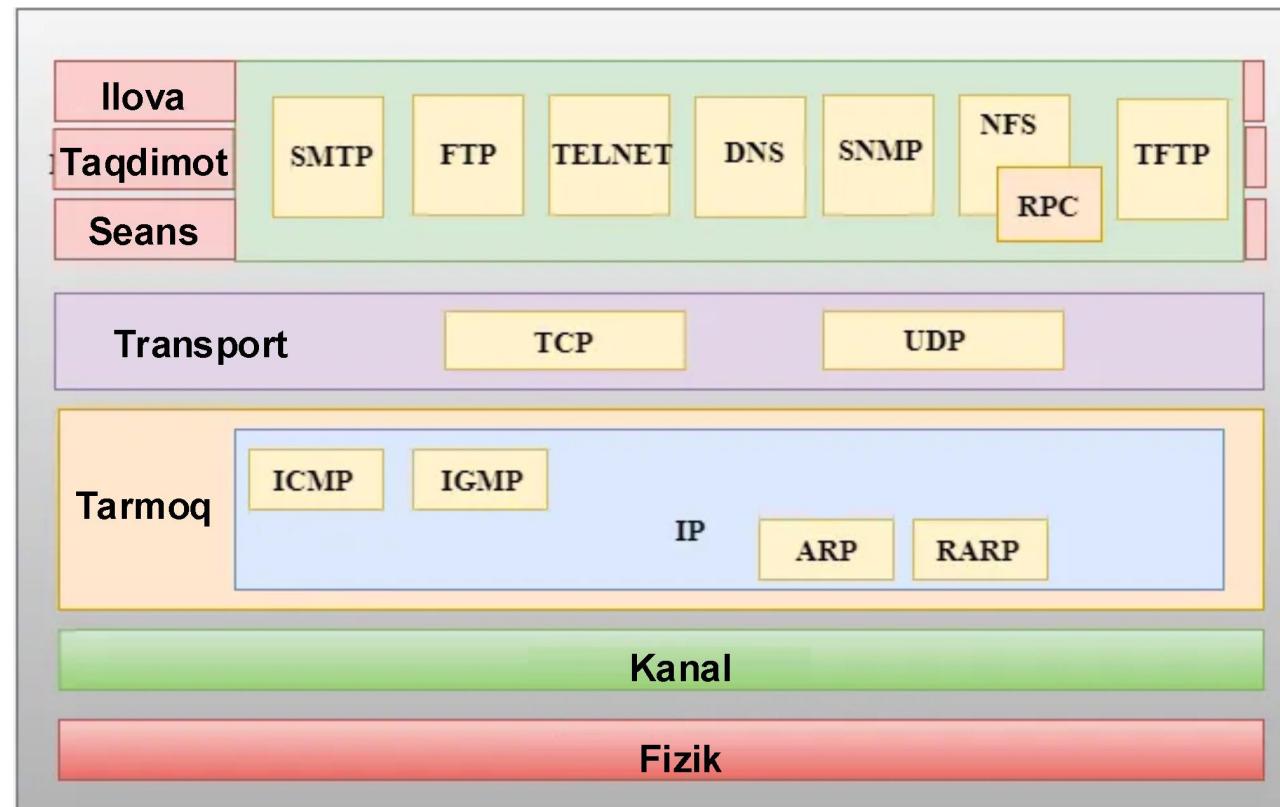
ma'lumotlar tushunarli  
bo'lishi kerak va bu  
pog'ona shu uchun  
javobgardir. Agart

almashtirish bo'lganligi  
pog'ona shuningdek  
amaiga o'shilasib

sinxronizatsiya va  
ulanishni to'xtatish  
ushbu pog'ona uchun  
javobgardir. Ushbu  
pog'ona shuningdek  
ulanish va  
autentifikatsiya  
xavfsizligini



# TCP/IP qatlamlarining funksiyalari:

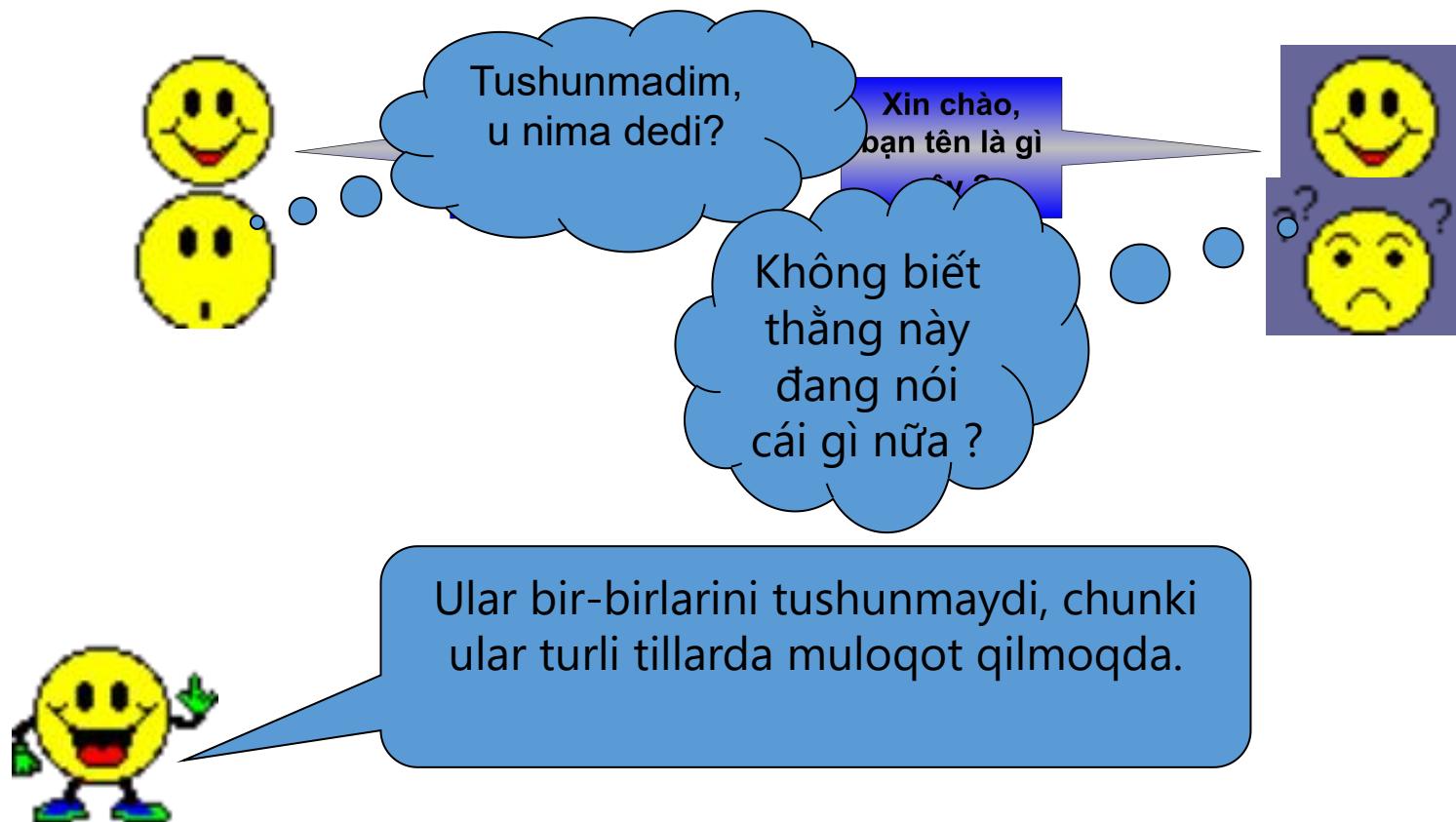


# Tarmoqqa kirish pog'onasi

- Tarmoq pog'onasi TCP/IP modelining eng quyi pog'onasidir.
- Tarmoq pog'onasi OSI modelida belgilangan fizik va kanal pog'onalarining birikmasidir.
- Tarmoq pog'onasi ma'lumotlarning tarmoq orqali fizik ravishda qanday yuborilishi kerakligini belgilaydi.
- Ushbu pog'ona asosan bitta tarmoqdagi ikkita qurilma o'rtasida ma'lumotlarni uzatish uchun javobgardir.
- Ushbu pog'ona tomonidan bajariladigan funksiyalar IP-datagrammani tarmoq orqali uzatiladigan kadrlarga o'zgartirish va IP-manzillarni MAC-manzillarga joylashtirishdir.
- Ushbu pog'ona tomonidan ishlataladigan protokollar Ethernet, token ring, FDDI, X.25, kadr o'rni.

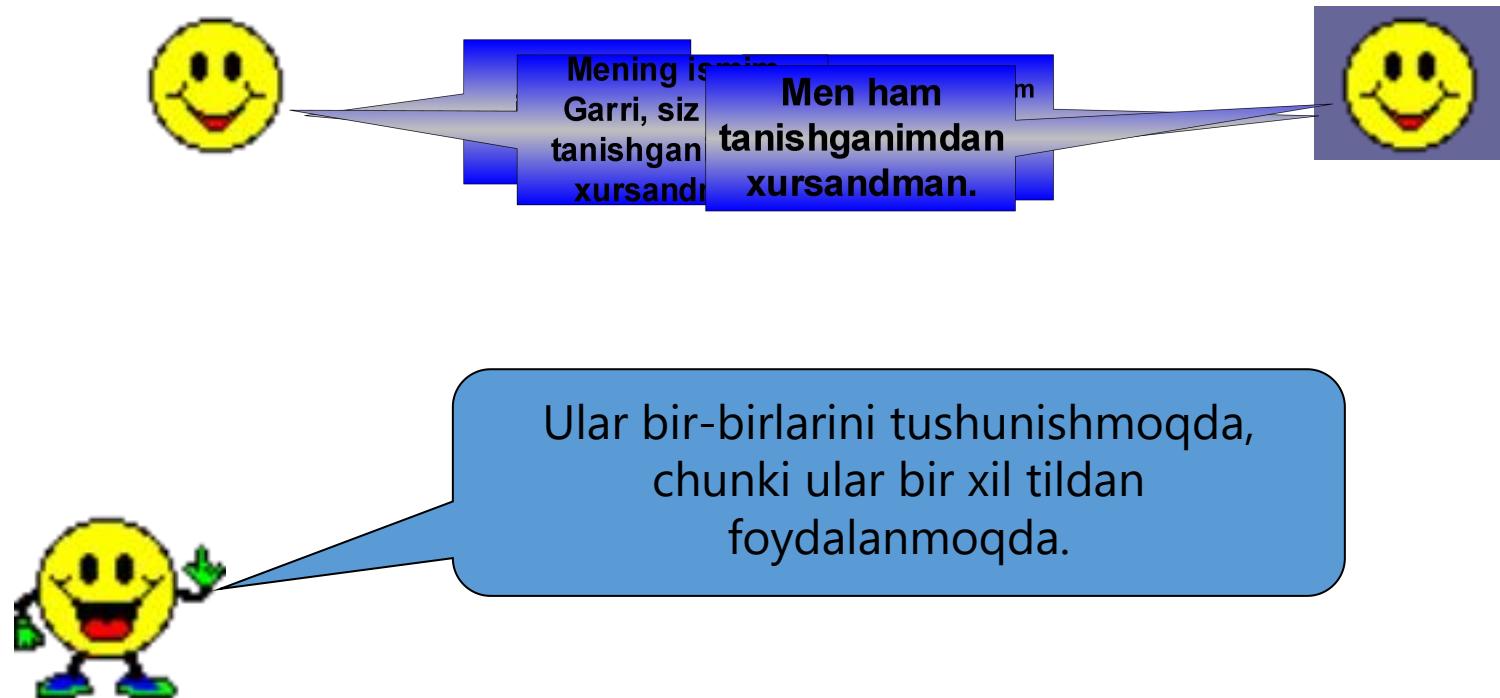
# PROTOKOL NIMA?????

- **Nima sodir bo'lishini kuzatib turing:**



# PROTOKOL NIMA?????

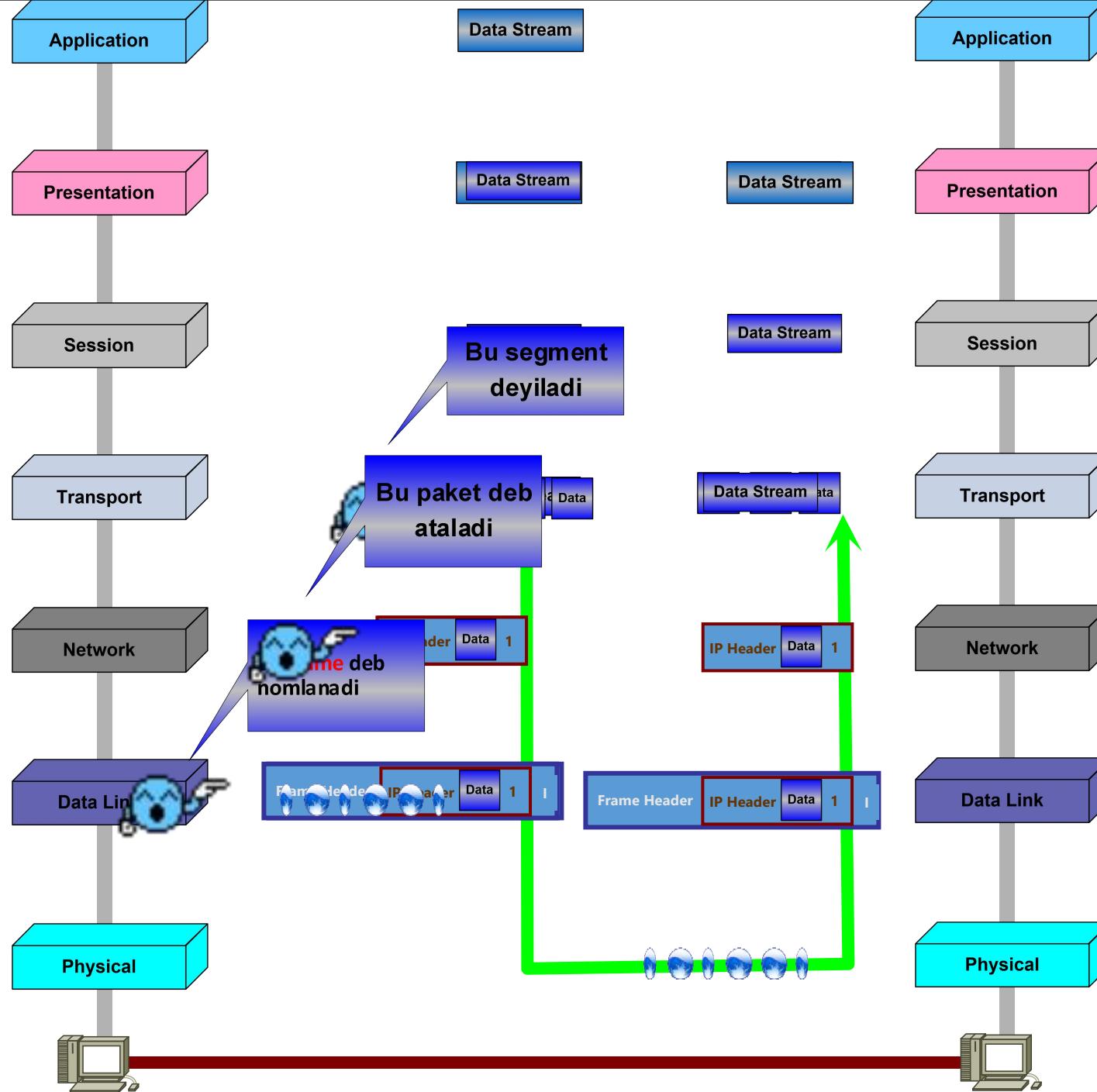
Davomida nima sodir bo'lishini kuzatib turing:



# PROTOKOL NIMA?????



## OSI modelining ishlash sxemasi



# ILOVA POG'ONASI

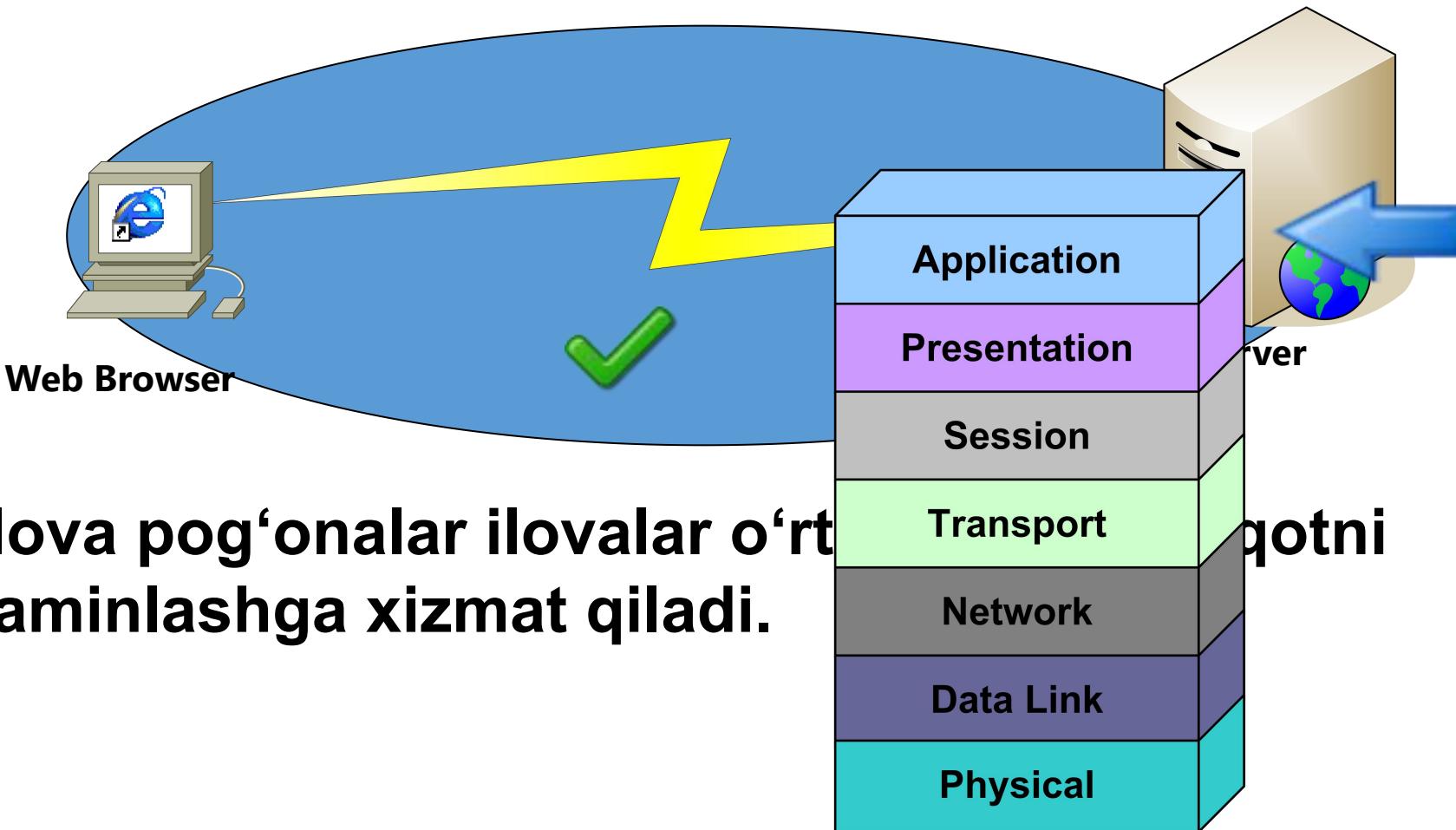


Siz Websayt manzilini kiritdingiz...

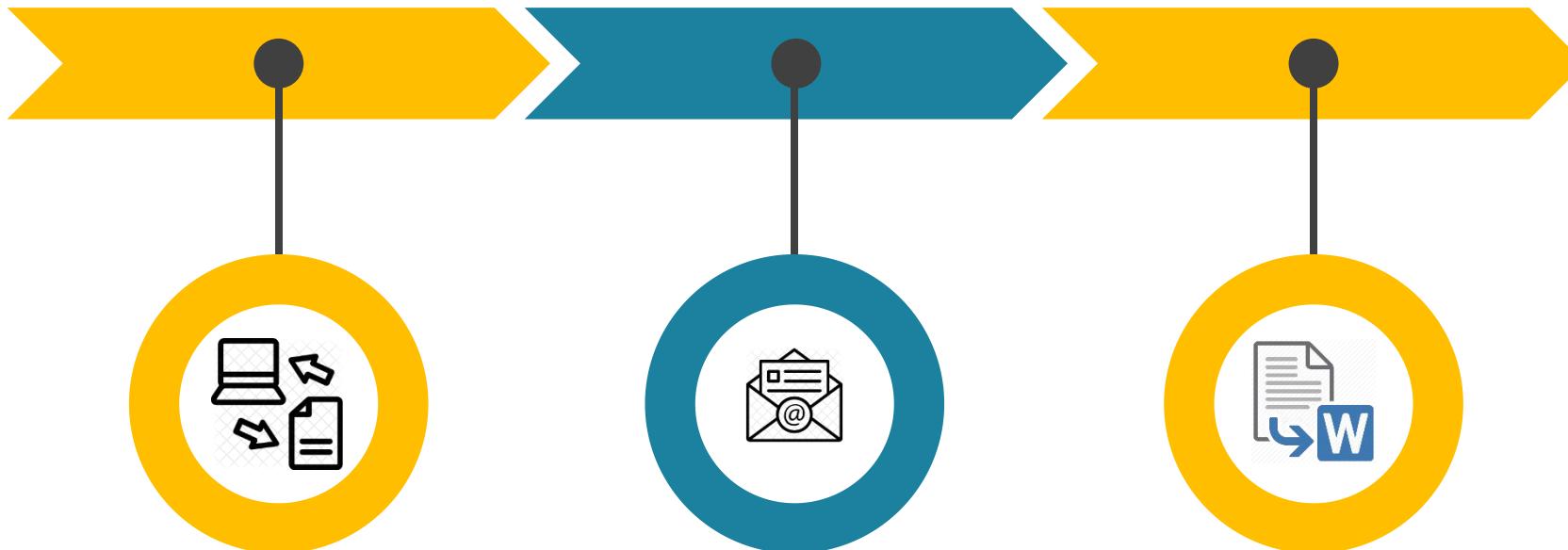


# ILOVA POG'ONASI

- Ilova pog'onasi eng yuqori pog'ona hisoblanadi



# ILOVA POG'ONASI IMKONIYATLARI



## File transfer

Kompyuter fayllarini uzatish - bu ikki kompyuter o'ttasida masofaviy aloqa o'rnatish uchun dastur.

Dastur ikkita ulanishga ega: to'g'ridan-to'g'ri va foydalanuvchi (account) ulanishlari.

## Electronic mail

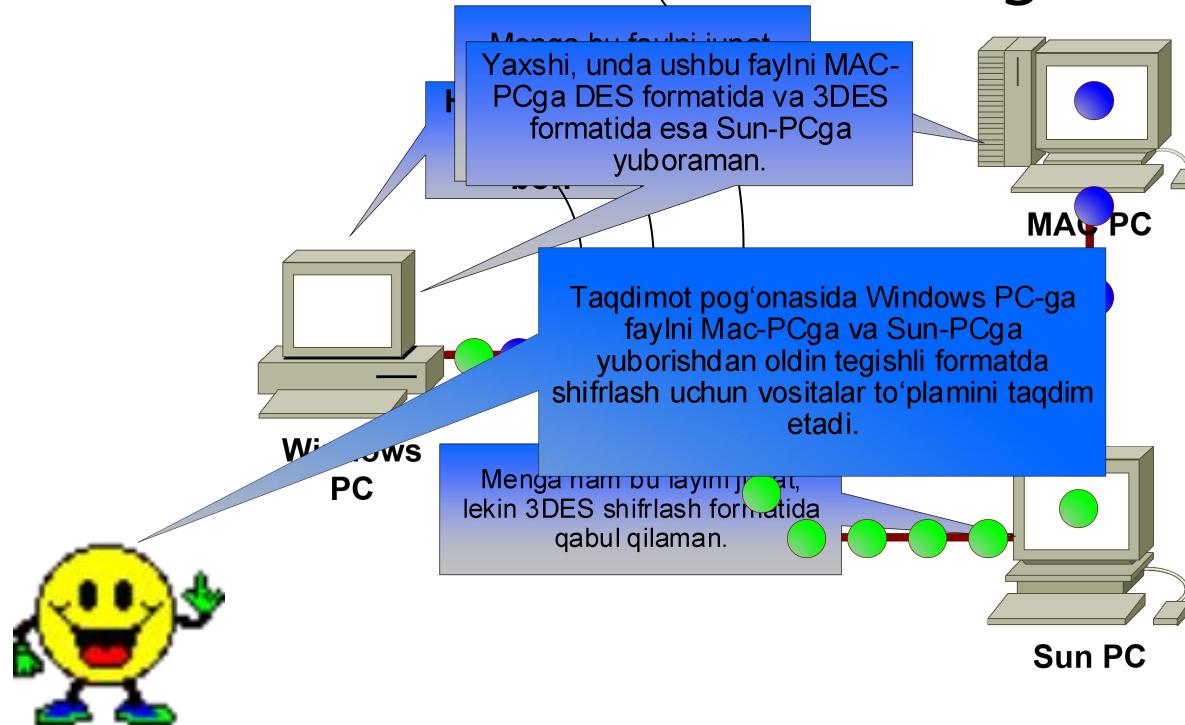
Elektron pochta — ma'lumotlarni uzatish tarmog'i orqali axborotlarni bir foydalanuvchi elektron qutisidan boshqasinkiga jo'natish, qabul qilish va ma'lum vaqtlargacha saqlanishini ta'minlovchi dasturiy-texnik vositalar to'plami.

## Terminal access Word processing Web Browser

Terminalga kirish boshqaruvchisi odatda dial-up liniyalaridan terminal ulanishlarini qabul qiluvchi va foydalanuvchiga Telnet kabi Internetga masofadan kirish tartib-qoidalarini chaqirish imkonini beruvchi asosiy kompyuterdir.

# TAQDIMOT POG'ONASI

Nima sodir bo'l shini kuzatib turing:



# TAQDIMOT POG'ONASI

Pog'onaning  
faoliyati:



Ma'lumot formati, ma'lumot strukturasi,  
ma'lumotni o'zgartirish, ma'lumotni  
siqish va shifrlash.

Pog'ona bo'yicha  
misollar:

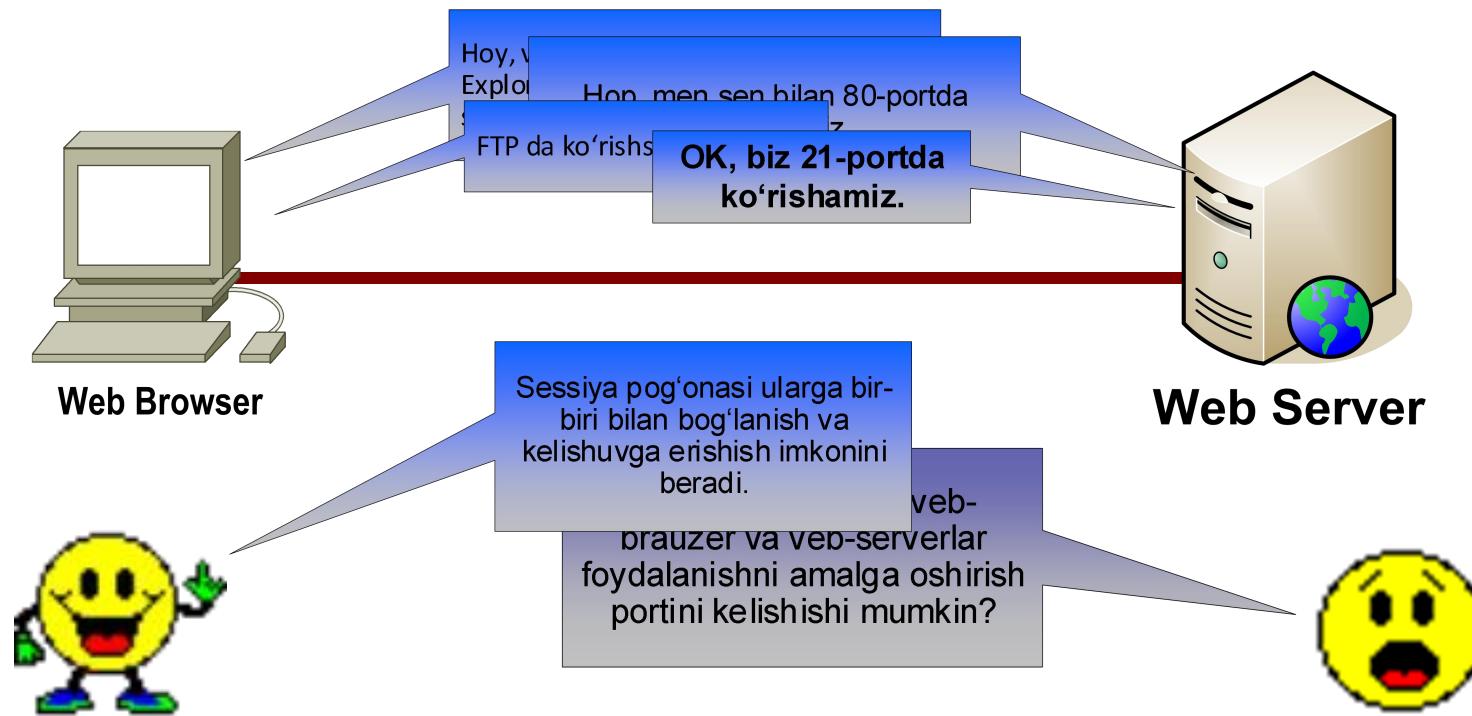


PICT, MIDI, MPEG, RTF



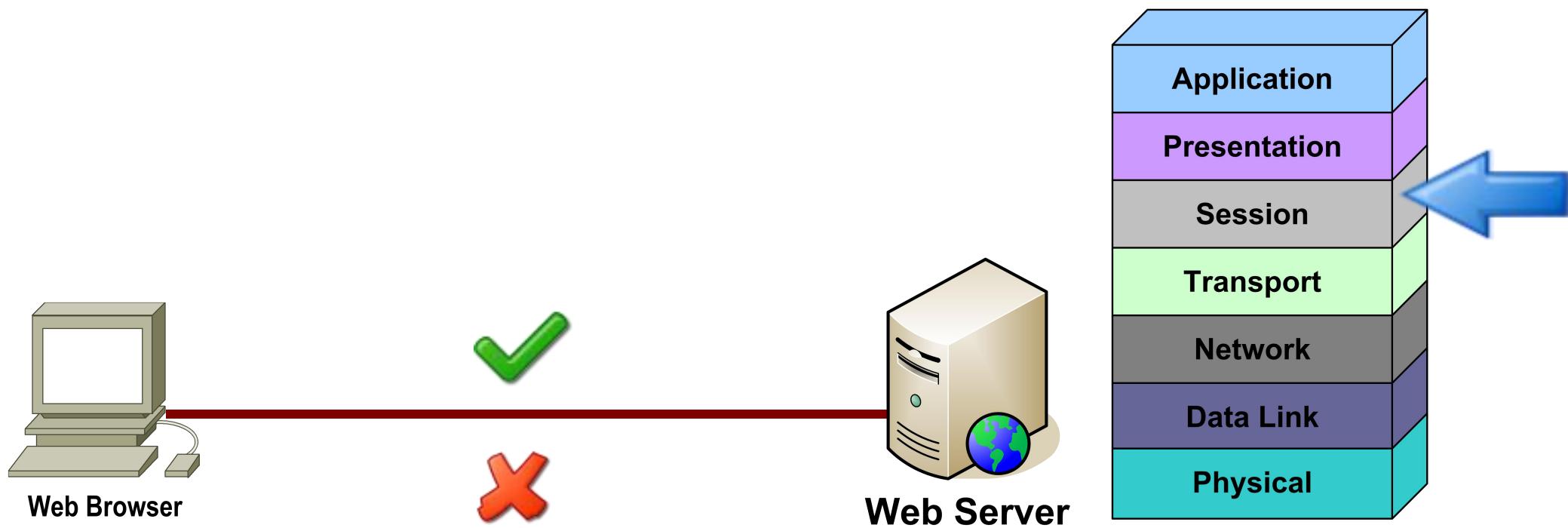
# SEANS POG'ONASI

- Nima sodir bo'lishini kuzatib turing:



# SEANS POG'ONASI

Seans pog'onasi ikkita o'zaro ishlovchi xostlar o'rtasida aloqani  
o'rnatish, boshqarish va yakunlash vazifasini bajaradi



# SEANS POG'ONASI

Pog'onaning  
faoliyati:



Seans, muloqot, dialog, ma'lumotni  
almashish.

Pog'ona bo'yicha  
misollar:



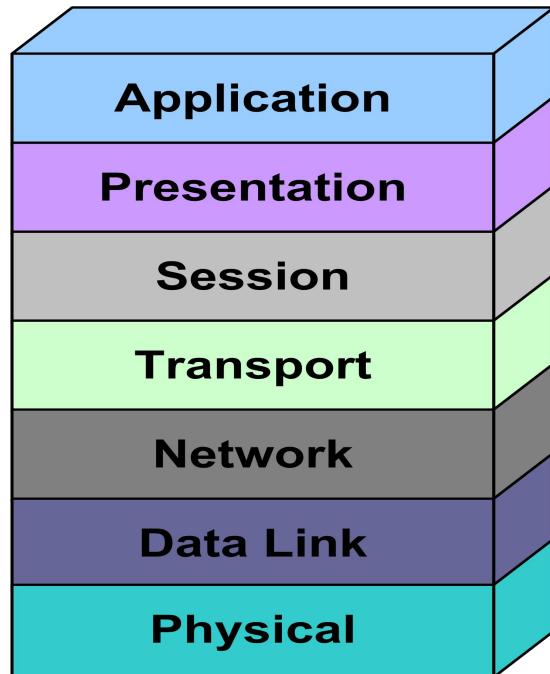
Network File System (NFS)  
AppleTalk Session Protocol (ASP)

ASP  
is an acronym for  
AppleTalk Session  
Protocol  
by [allacronyms.com](http://www.acronyms.com)

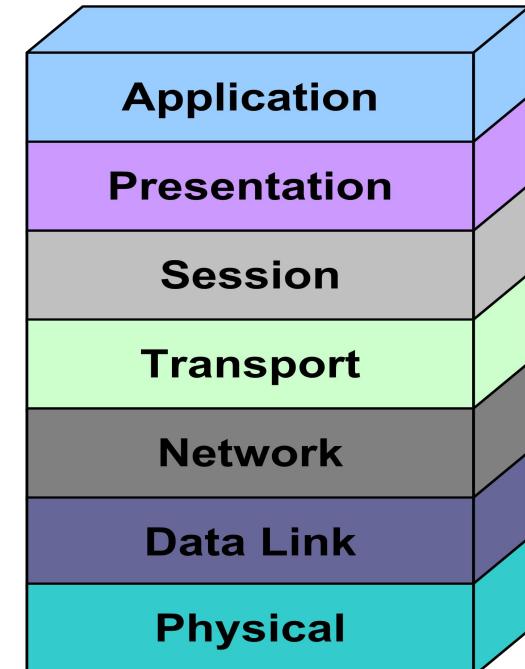


# TRANSPORT POG'ONASI

Transport pog'onasi paketlarni qabul qilishga kafolat beradi.

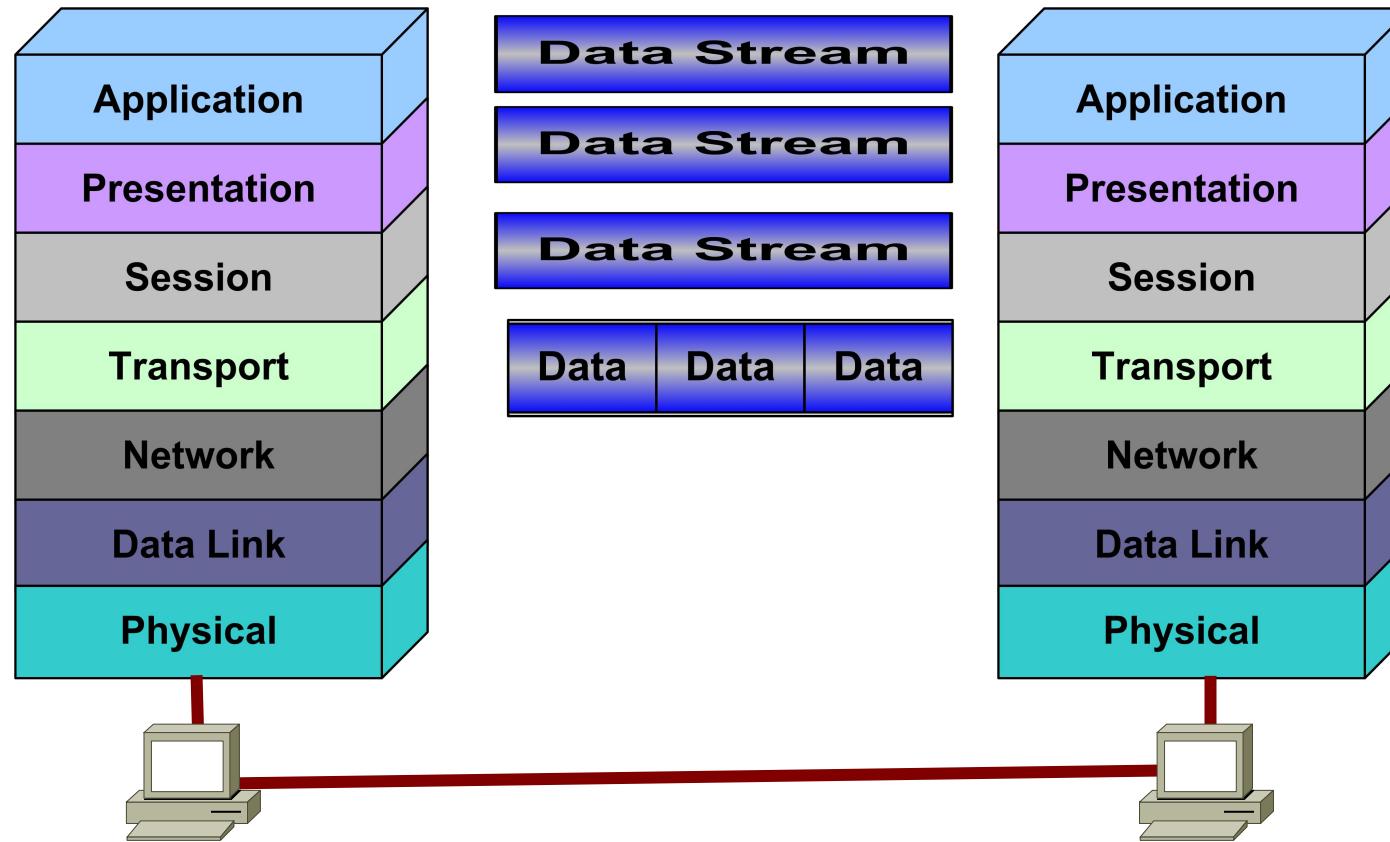


Bu jarayonda murojaat qilinadi sessiya pog'onasiga, yaniy sessiya pog'onasidan ma'lumotlarni transport pog'onasiga berilishini, ushbu ma'lumotlarni transport to'g'ri manzilga yuborilishini ta'minlaydi

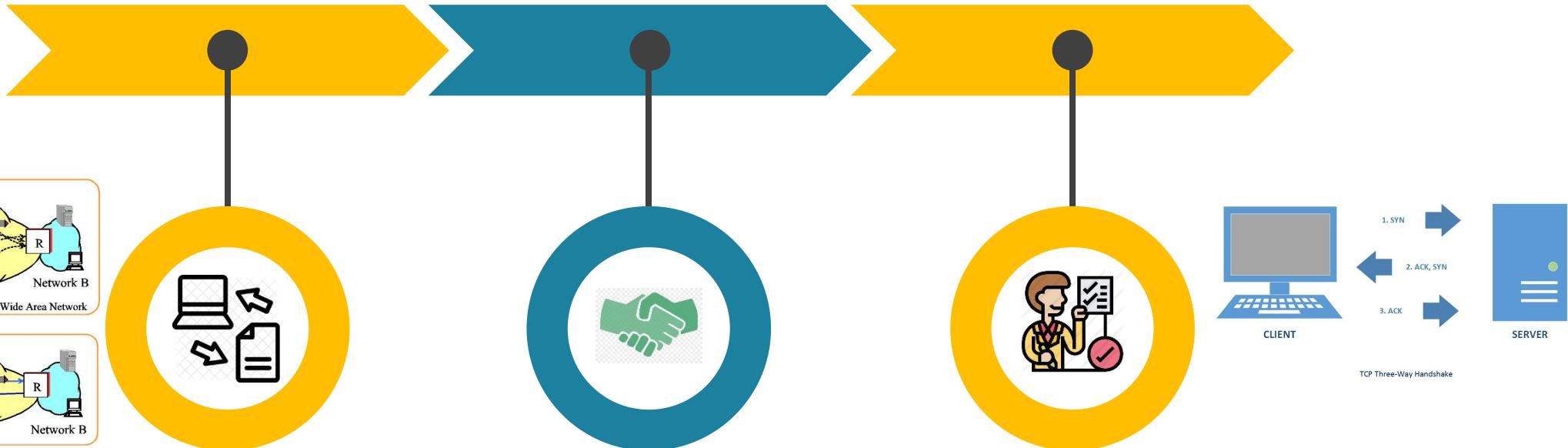


# TRANSPORT POG'ONASI

Transport pog'onasi ma'lumotlar potokidagi ma'lumotlarni segmentlash va qayta yig'ish vazifasini bajaradi.



# Transport pog'onasi imkoniyatlari



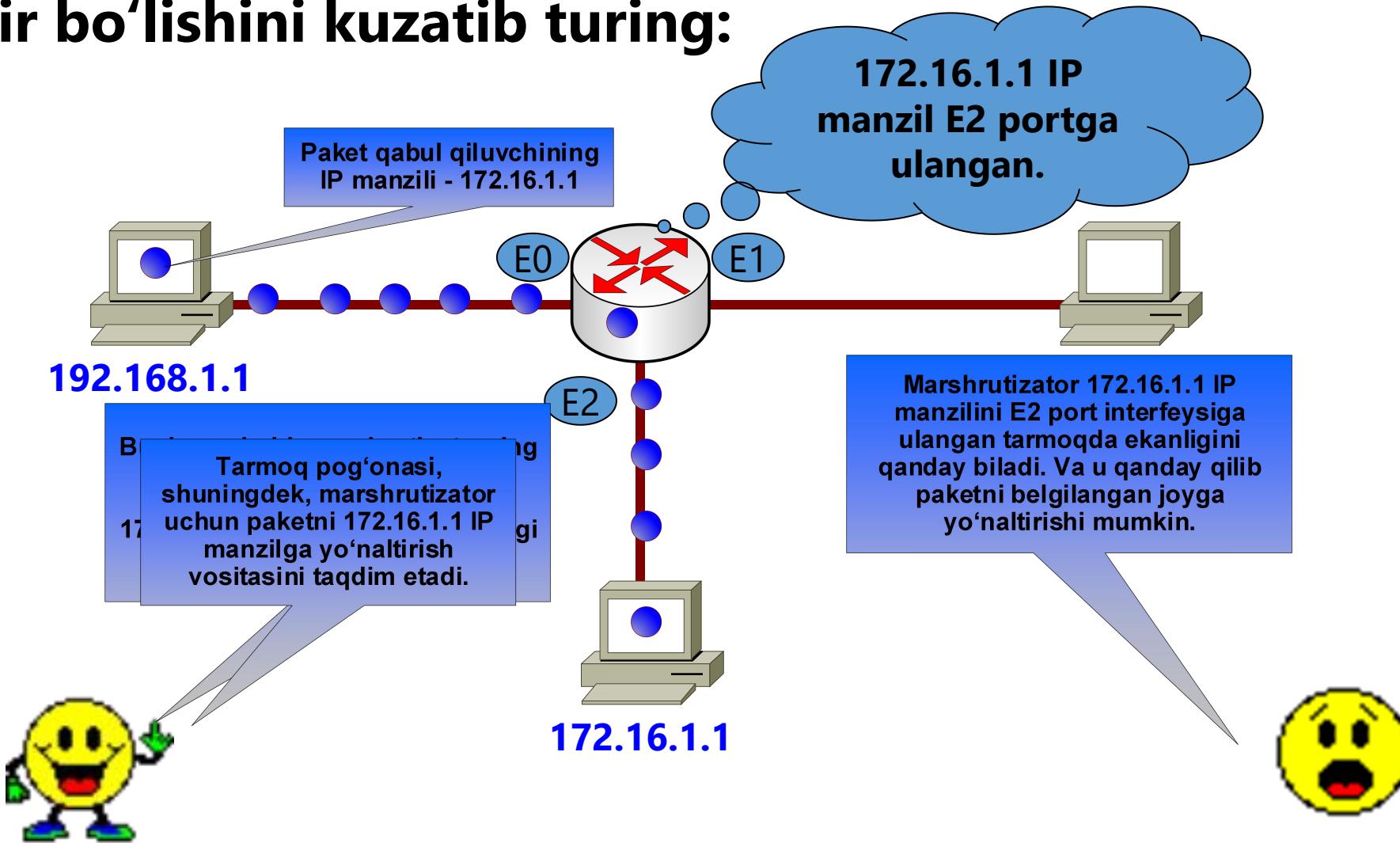
**Ulanishsiz uzatish**  
**Ulanib uzatish**

**Uch tomonlama qo'l siqish**  
**Potokni boshqarish**

**Tasdiqlash**  
**Windowing**

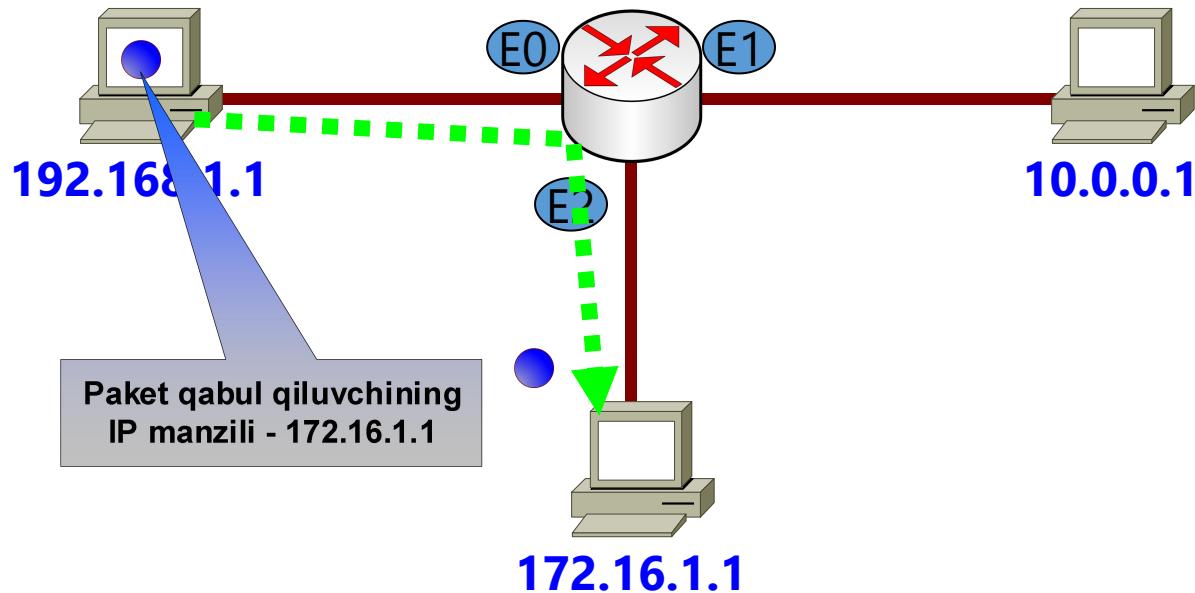
# TARMOQ POG'ONASI

- Nima sodir bo'lishini kuzatib turing:



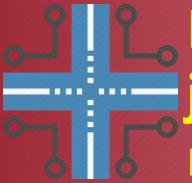
# TARMOQ POG'ONASI

- Tarmoq pog'onasi paketning mantiqiy manzili asosida uning marshrutizatsiyasiga javob beradi



# TARMOQ POG'ONASI

Tarmoq pog'onasining  
faoliyati:



Paketlar, marshrutlash, marshrutlar  
jadvali, marshrutlash protokoli,  
mantiqiy manzil, fragmentatsiya

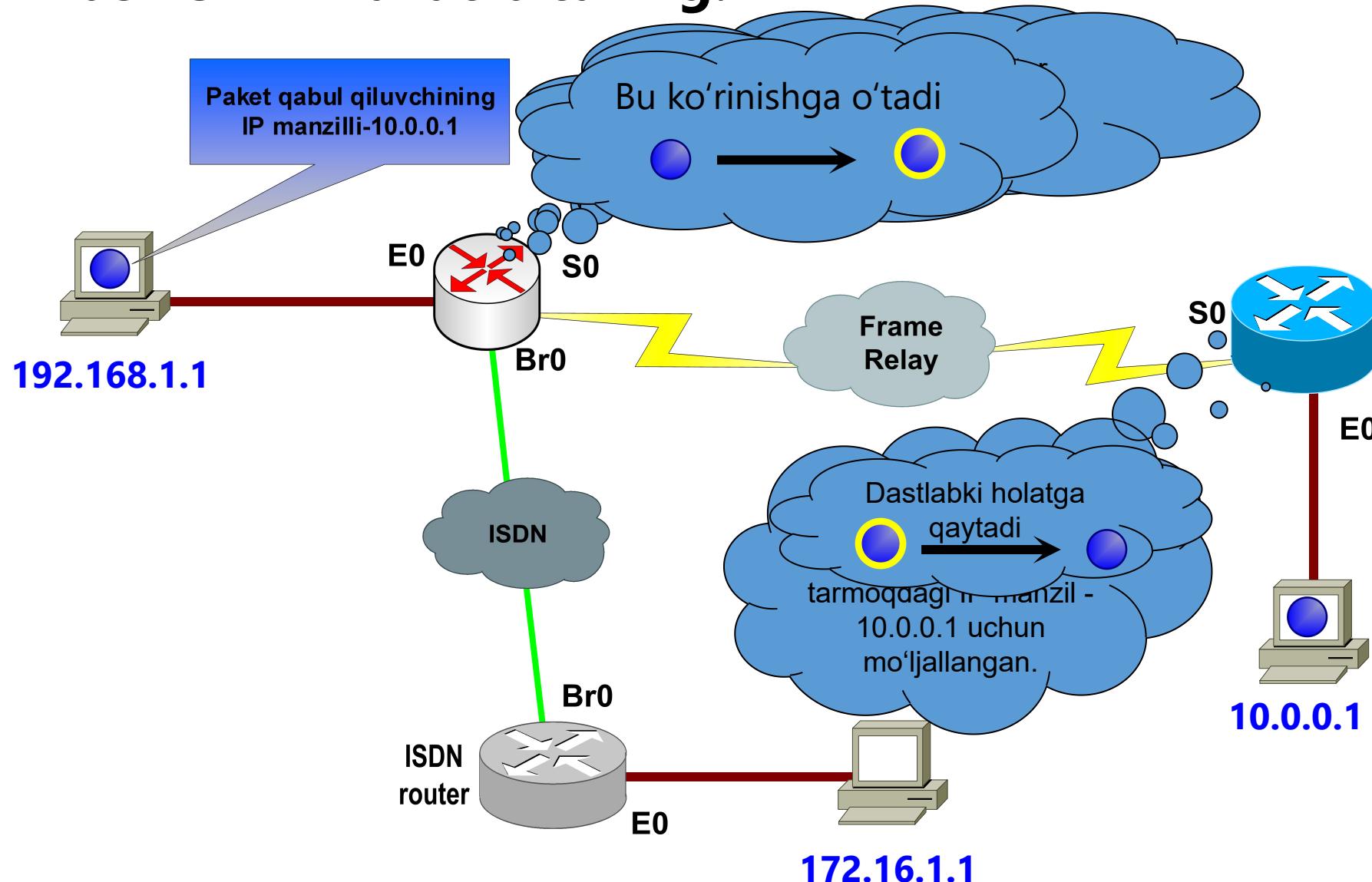
Pog'ona bo'yicha  
misollar:



Internet Protocol (IP)  
Internetwork Packet Exchange (IPX)

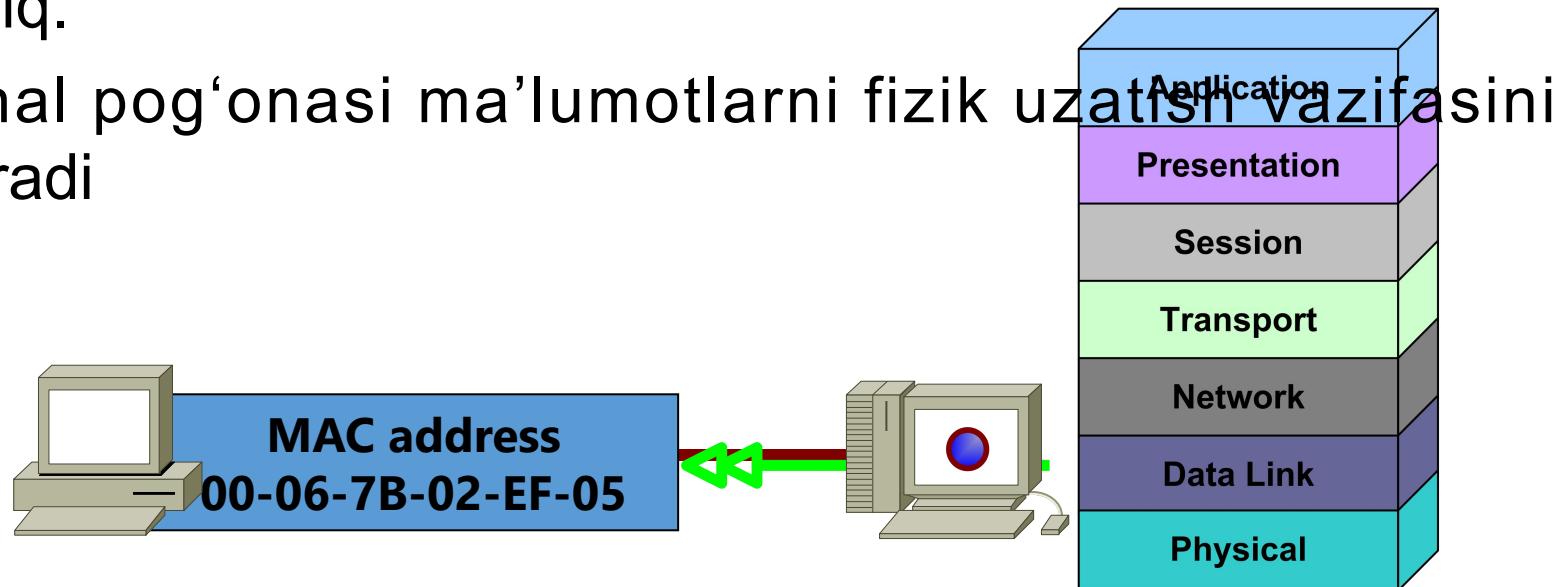
# KANAL POG'ONASI

- Nima sodir bo'lishini kuzatib turing:



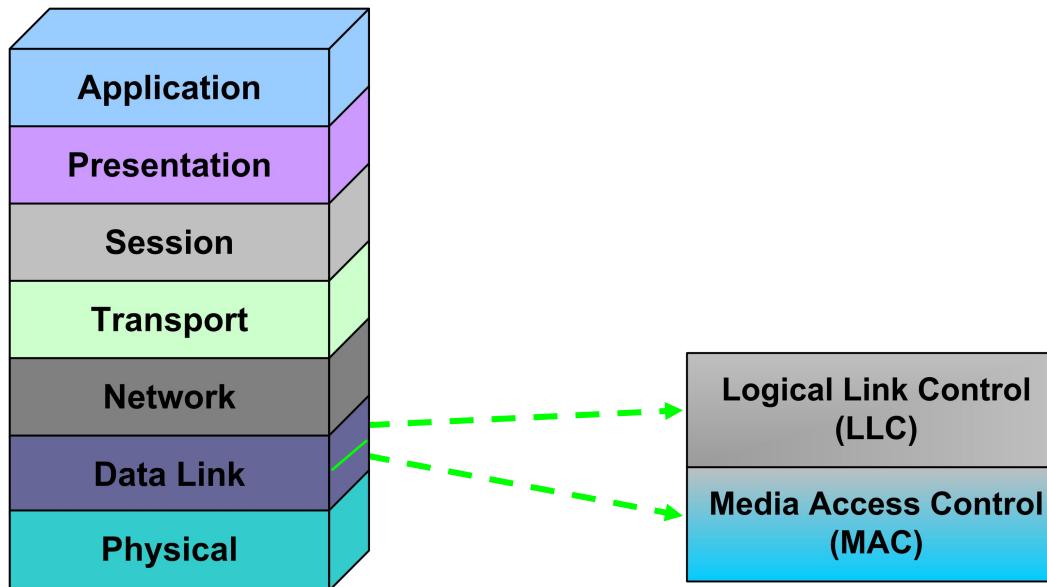
# KANAL POG'ONASI

- Kanal pog'onasi tarmoq pog'onasidan pastda joylashgan.
  - Kanal pog'onasi ma'lumotlarni yuborishi fizik manzilga bog'liq.
  - Kanal pog'onasi ma'lumotlarni fizik uzatish vazifasini bajaradi



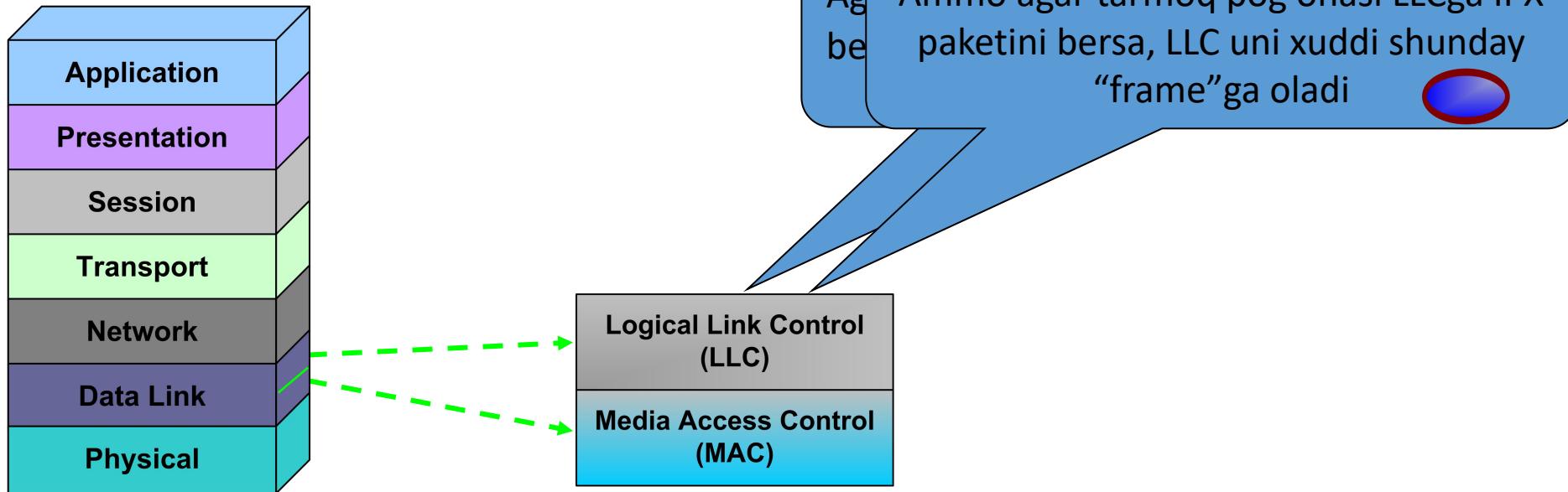
# KANAL POG'ONASI

- Kanal pog'onasi ikkita qism pog'onasidan tashkil topgan:
  - The Logical Link Control (LLC) sublayer.
  - The Media Access Control (MAC) sublayer



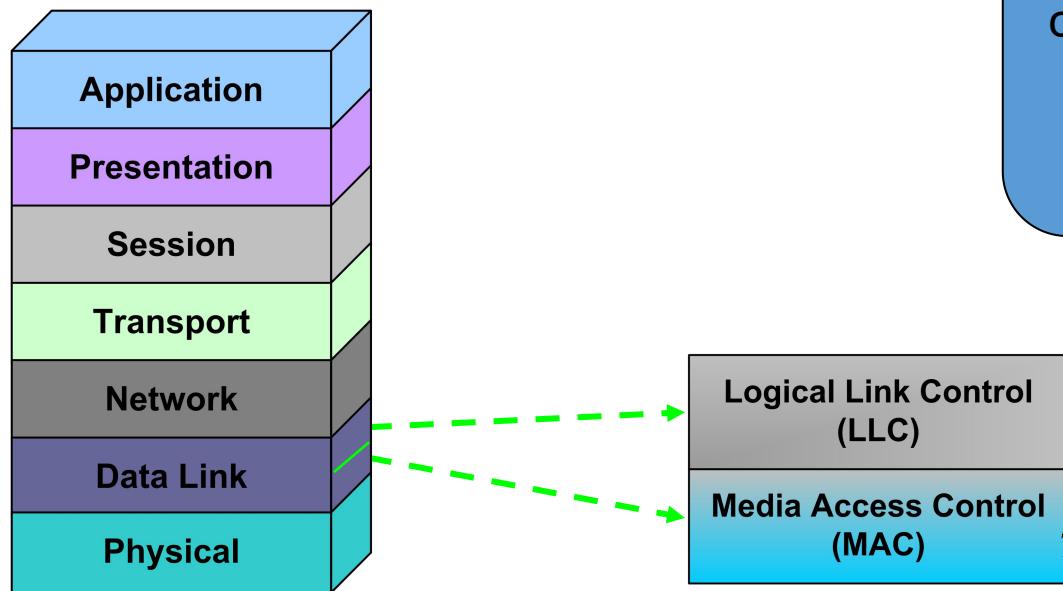
# KANAL POG'ONASI

**Logical Link Control (LLC) qismi pog'onasi tarmoq pog'ona protokollarini identifikatsiyalashga va keyinchalik kadrlarga enkapsulyatsiyalashga xizmat qiladi.**



# KANAL POG'ONASI

- Media Access Control (MAC) qism pog'onasi paketlarni tashuvchilarga qanday joylanishini aniqlaydi



Agar tarmoq interfeysi kartasi (TIK) RJ45 portiga ega bo'lsa va crossover (UTP) kabeliga ulangan bo'lsa. MAC "Frame"ni 2-pinga o'

Lekin, agar tarmoq interfeysi kartasi (TIK) BNC portiga ega bo'lsa, MAC "Frame"ni boshqa yo'l bilan uzatadi.

# FIZIK POG'ONA

Pog'onaning  
faoliyati:

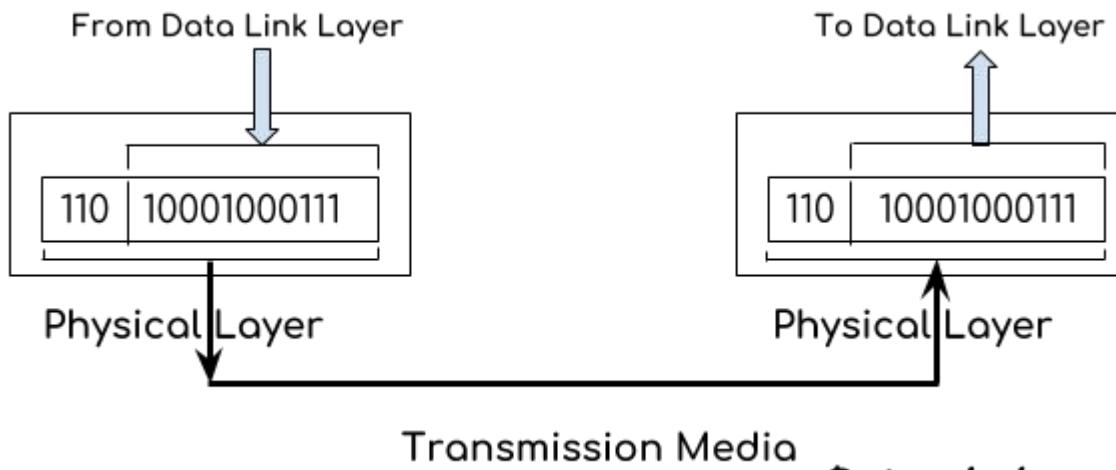


Oxirgi tizimlar o'rtasida fizik kanal orqali  
strukturlanmagan bitlar potokini uzatadi.

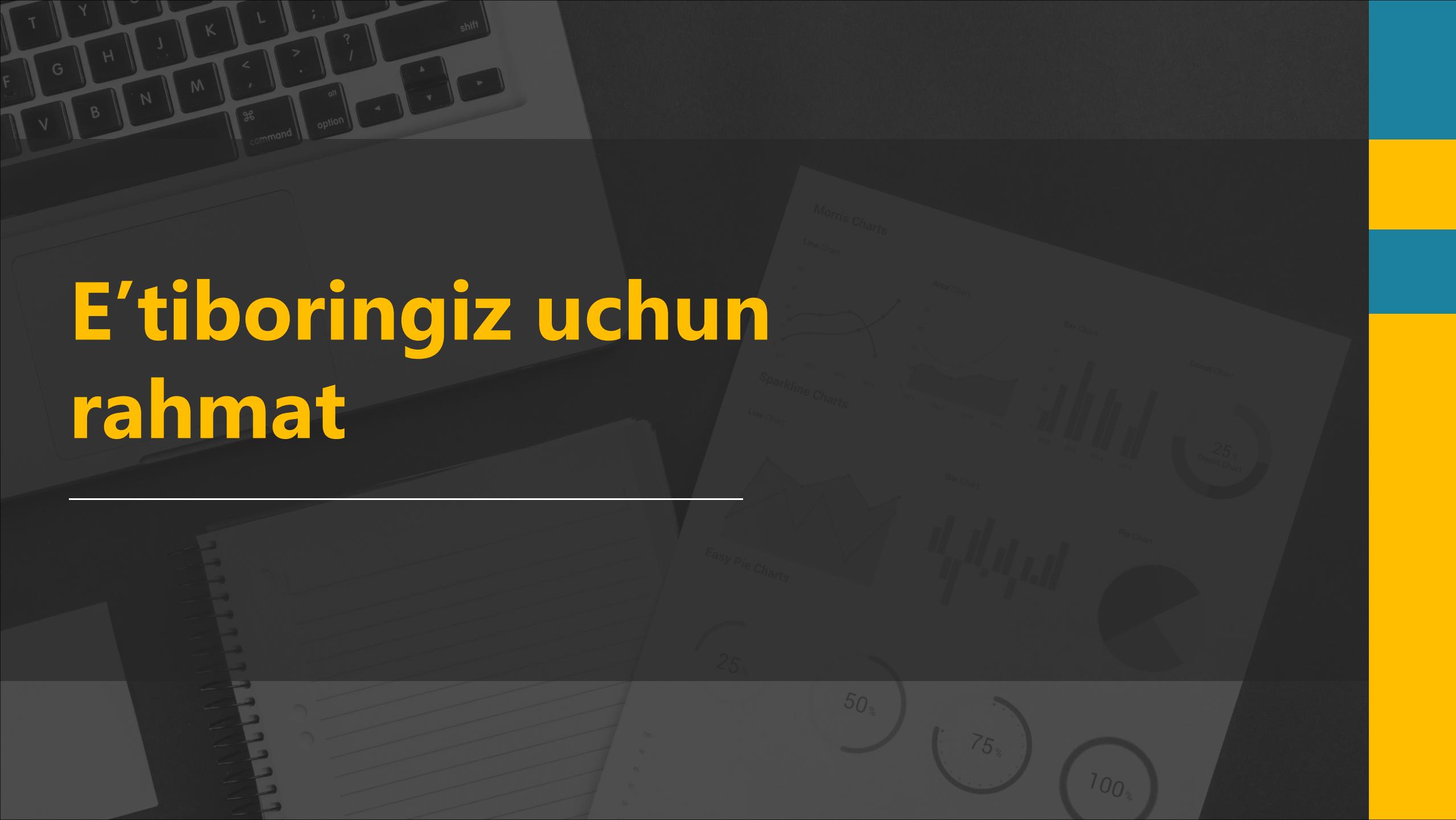
Pog'ona bo'yicha  
misollar:



UTP, STP, coaxial, Fiber cable  
RJ45, RJ11 connector  
DB9, DB25 connector  
10base2, 10base5, 100baseT, 1000baseTx



E'tiboringiz uchun  
rahmat



# Тармоқ хавфсизлиги

6-маъруза · Илова ва тақдимот сатҳлари ·



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

# Илова сатҳи – Инсон ва маълумотларни узатиш тармоқлари орасидаги алоқа



Илова сатҳи

Илова сатҳи OSI модели бўйича маълумотларни тармоққа узатишнинг дастлабки қадамларини бажаради. Илова сатҳи аниқ иловалар учун тармоқ вазифасини таъминлаб беради ва фойдаланувчилар даражасидаги дастурий воситалар билан бирга ишлайди. Бошқа сатҳлардан фарқли равишда ишлаш учун аниқ талабларни шакллантирмайди.



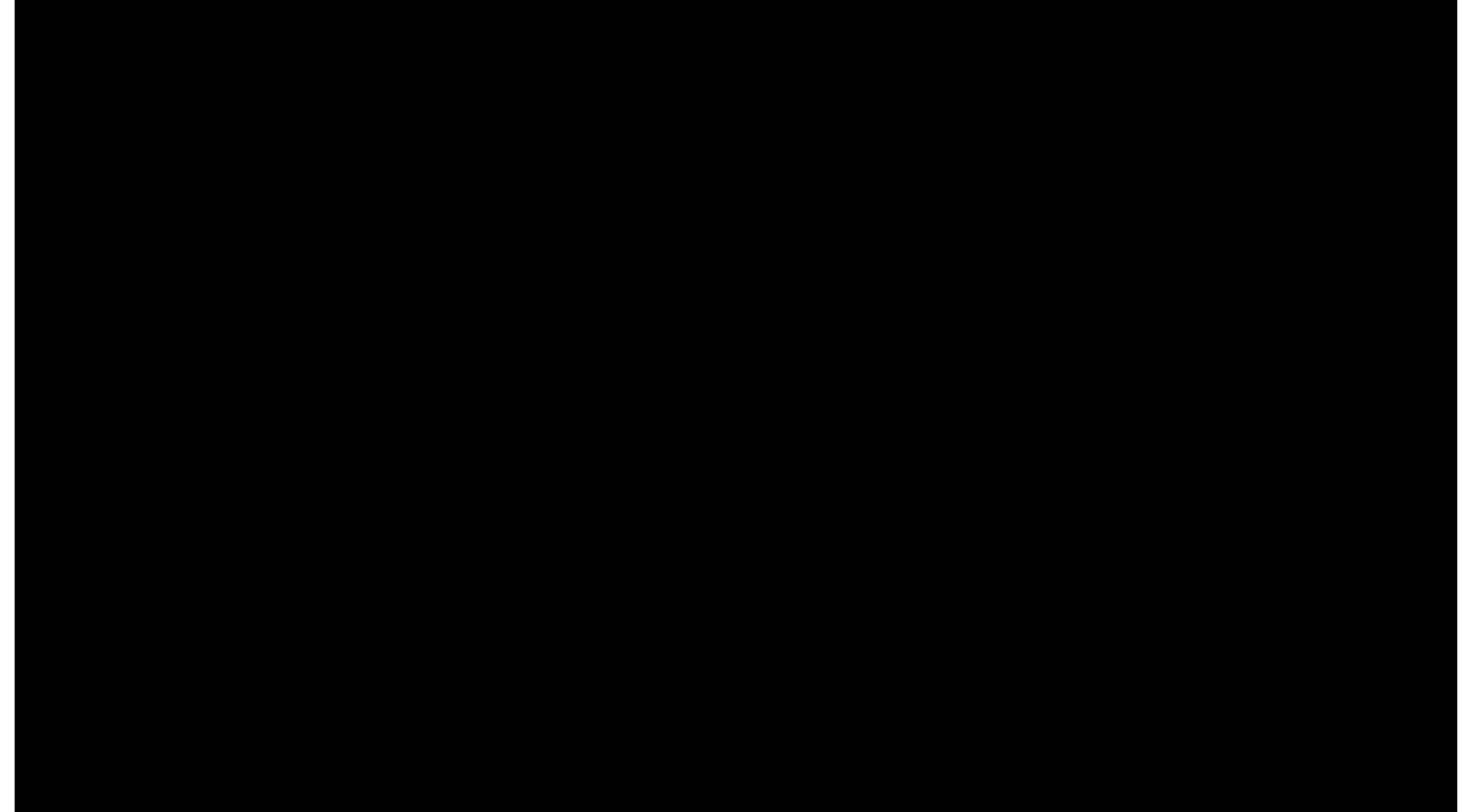
Илова дастурлари

Илова – фойдаланувчилар учун тармоқда алоқа имкониятини берувчи дастурлар. HTTP, FTP, электрон почта ва бошқалар илова дастурий воситалари ҳисобланади ва тармоқлар орасидаги тушунмовчиликларни ҳал этиш учун хизмат қиласди.

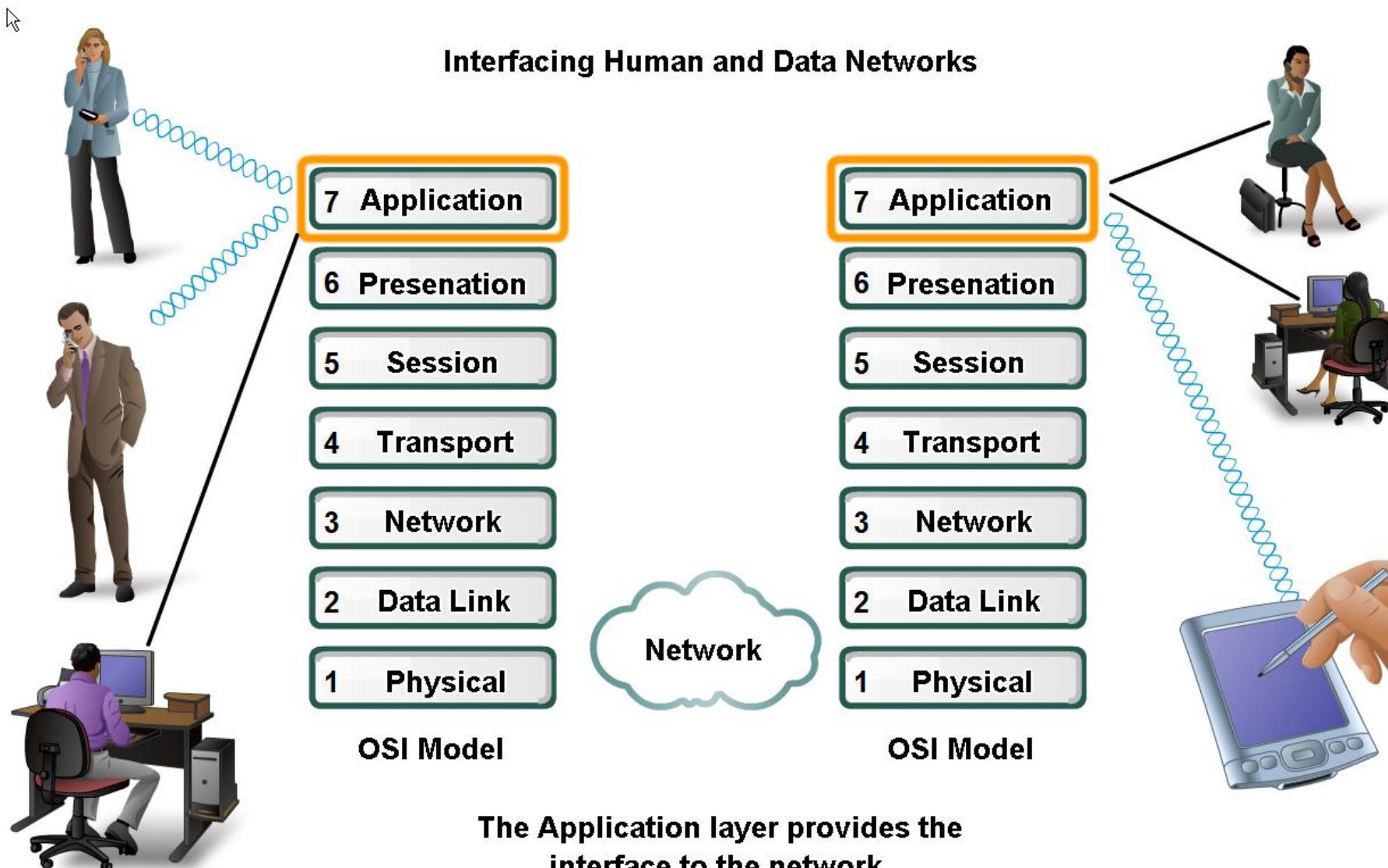
- 7 - Application - A
- 6 - Presentation - Person
- 5 - Session - Sent
- 4 - Transport - Through
- 3 - Network - Network
- 2 - Data Link - Data
- 1 - Physical - Packets

- Physical - Please
- Data Link - Do
- Network - Not
- Transport - Throw
- Session - Sausage
- Presentation - Pizza
- Application - Away

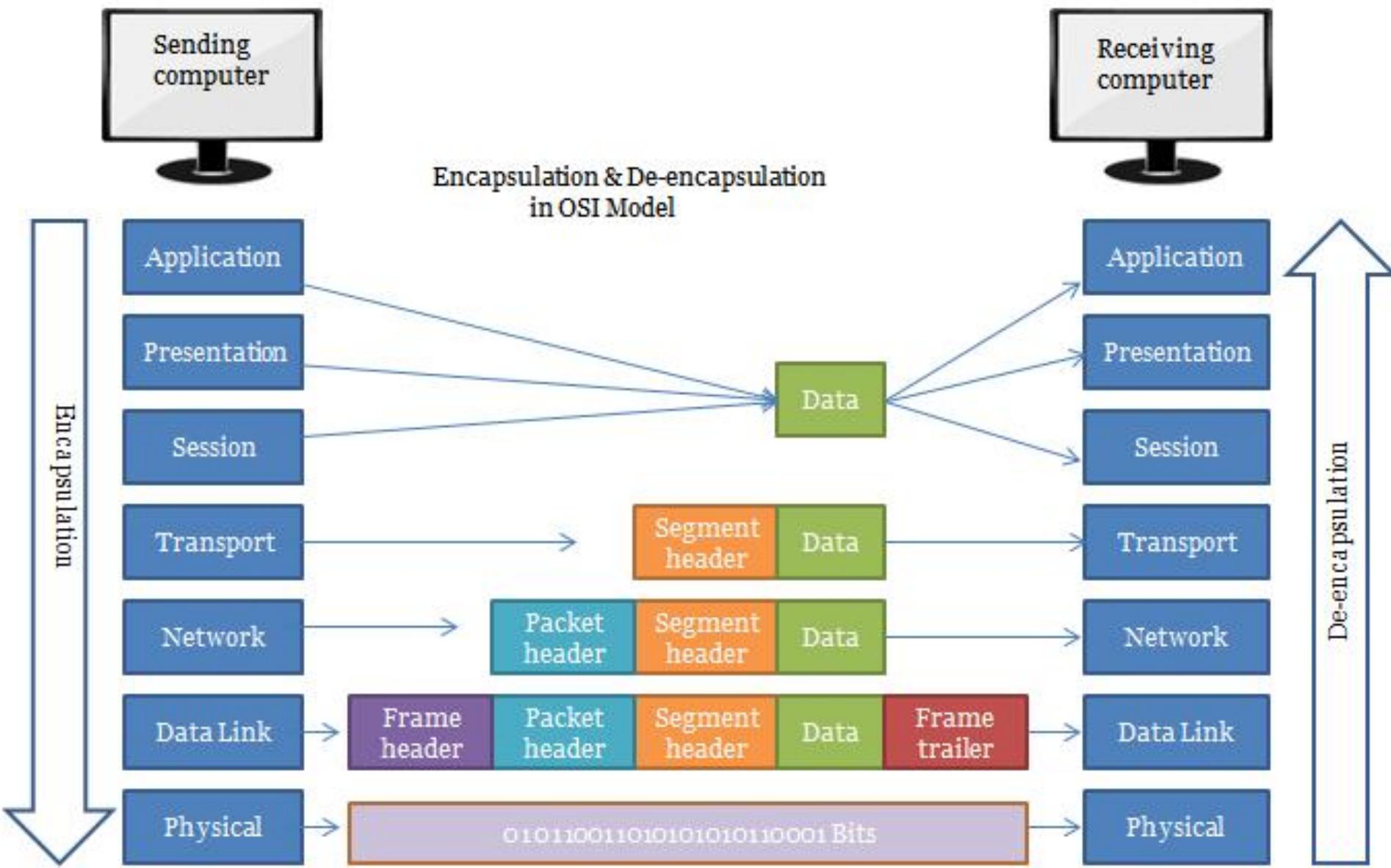
# The OSI Model Animation



# Илова сатҳи – Инсон ва маълумотларни узатиш тармоқлари орасидаги алоқа



# Энкапсулация & Деинкапсулация



# Илова сатҳи – Инсон ва маълумотларни узатиш тармоқлари орасидаги алоқа

Илова сатҳи протоколлари узатувчи ва қабул қилувчи хостларда ишловчи дастурлар ўртасида маълумот алмашиш учун ишлатилади

Веб браузер ёки электрон почта каби аксарият иловалар OSI модели 5,6,7 сатҳларининг функционал имкониятларини ўз ичига олади.



OSI Model

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Application Layers

Data Flow Layers

TCP/IP Model

Application

Transport

Internet

Network Access

Domain Name System

Hypertext Transfer Protocol

Simple Mail Transfer Protocol

Post Office Protocol

Dynamic Host Configuration Protocol

# Кенг фойдаланиладиган илова сатҳи протоколлари

Тармоқ диагностикаси

Маълумотларни узатиш ва қабул  
қилиши

Тизим конфигурацияси  
Масофадан буйруқларни  
бошқариш

Иш столига масофадан  
рухсат олиш  
График ва аудио

Аутентификация

SNMP, RSTAT, RWHO

NFS, SMB, FTP, TFTP, HTTP, LPD

NTP, DHCP, BOOTP

RLOGIN, REXEC, RSH, Telnet, SSH

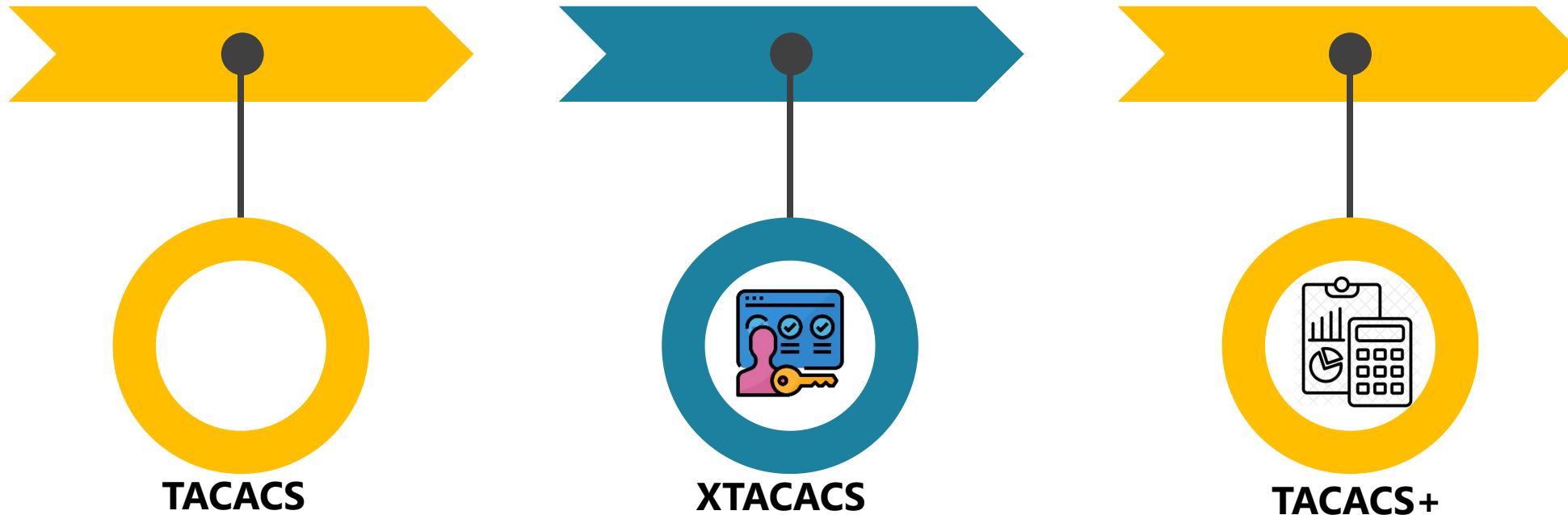
VNC, RDP

X-Windows, RTP, RTSP, VoIP

TACACS

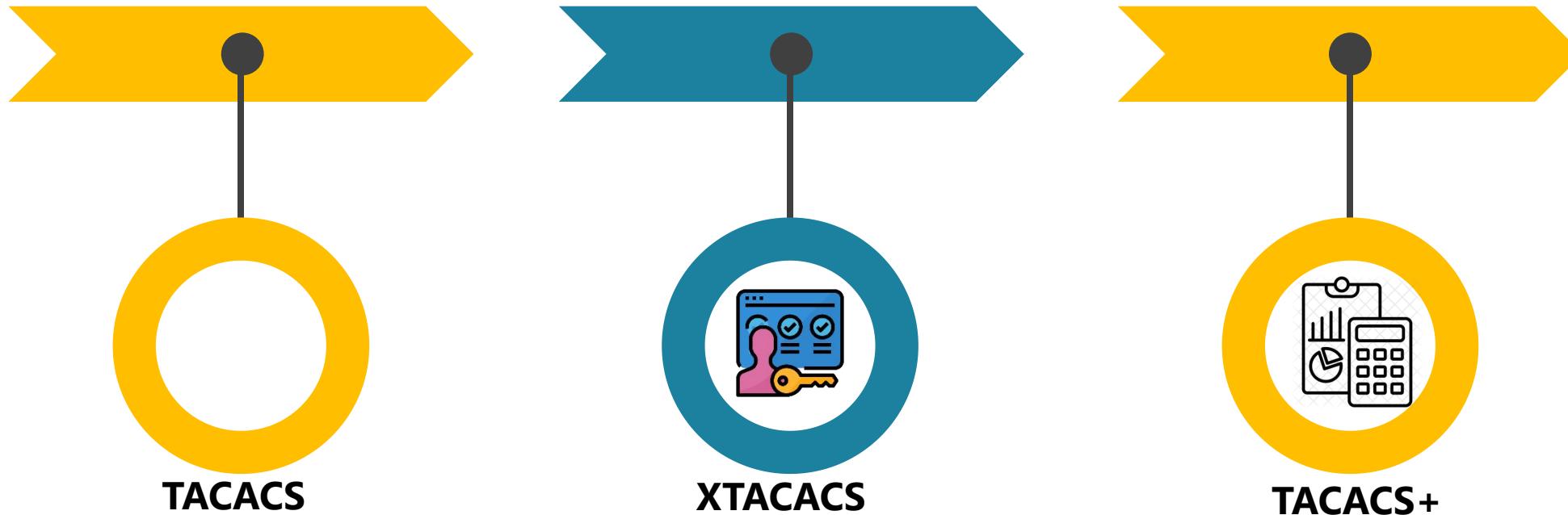
# TACACS

TACACS (*Terminal Access Controller Access Control System*) илова сатҳи протоколи бўлиб, аутентификация, авторизация ва ҳисобга олиш имкониятларини беради. Терминал серверлари ва тармоқ қурилмалари яратилган TACACS мижози фойдаланувчи номи ва паролини серверга юборади ва ҳисобга олиш маълумотлари [RFC1492] билан боғлиқ авторизация асосида асосида унга рухсат берилади. Мижоз мувафақиятли аутентификациядан сўнг терминал сервердан фойдаланишга рухсат олиши ёки SLIP боғланишини сўраши мумкин.



# TACACS

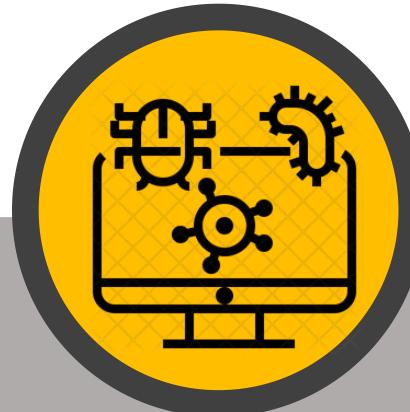
TACACS (*Terminal Access Controller Access Control System*) илова сатҳи протоколи бўлиб, аутентификация, авторизация ва ҳисобга олиш имкониятларини беради. Терминал серверлари ва тармоқ қурилмалари яратилган TACACS мижози фойдаланувчи номи ва паролини серверга юборади ва ҳисобга олиш маълумотлари [RFC1492] билан боғлиқ авторизация асосида асосида унга рухсат берилади. Мижоз мувафақиятли аутентификациядан сўнг терминал сервердан фойдаланишга рухсат олиши ёки SLIP боғланишини сўраши мумкин.



# Умумий рисклар



**Мерос заифликлар**  
Secure Lower Layer Protocols;  
Application Encryption;  
Nonstandard Application



**Аутентификация муаммолари**  
Илова сатҳи протоколларининг  
аксарият қисми ҳар қандай турдаги  
аутентификацияни қўллаб  
қўвватламайди. HTTP ҳам, SMTP  
ҳам аутентификацияланмаган  
м и ж о з л а р г а  
аутентификацияланмаган  
серверларга уланишга имкон  
беради.



**Тизимга тўғридан тўғри  
уланиш**

Илова сатҳи протоколлари  
операциян тизимдаги  
иловалар билан тўғридан  
тўғри ишлайди. Аксарият  
иловалар дисклар, файллар ва  
буйруқларни бажаришга  
рухсатлари бор ва бу  
имкониятлар тармоқда ҳам  
мавжуд.

# Буфер тўлиб тошиши ҳужумларида масофавий эксплойтларнинг нисбати

Йил	Масофавий эксплойтларнинг сони	Буфер тўлиб тошиши фоизи %
1997	56	22
1998	73	30
1999	194	21
2000	278	27
2001	643	38
2002	795	41
2003	512	41
2004	1209	52

```
... char buf[64], in[MAX_SIZE]; printf("Enter buffer contents:\n");
read(0, in, MAX_SIZE-1); printf("Bytes to copy:\n"); scanf("%d",
&bytes); memcpy(buf, in, bytes); ...

char *lccopy(const char *str) { char buf[BUFSIZE]; char *p; strcpy(buf, str); for (p = buf; *p;
p++) { if (isupper(*p)) { *p = tolower(*p); } } return strdup(buf); }

if (!(png_ptr->mode & PNG_HAVE_PLTE)) { /* Should be an error, but we can cope with it */
/ png_warning(png_ptr, "Missing PLTE before tRNS"); } else if (length > (png_uint_32)png_ptr->num_palette) { png_warning(png_ptr, "Incorrect tRNS chunk length"); png_crc_finish(png_ptr, length); return; } ... png_crc_read(png_ptr, readbuf, (png_size_t)length);

void getUserInfo(char *username, struct _USER_INFO_2 info){ WCHAR unicodeUser[UNLEN+1];
MultiByteToWideChar(CP_ACP, 0, username, -1, unicodeUser, sizeof(unicodeUser));
NetUserGetInfo(NULL, unicodeUser, 2, (LPBYTE *)&info); }
```

Feed a Cold, Starve a Fever

Most viruses spread through user-level functionality. The network transports the hostile code, but the user's application permits the execution. Computer viruses such as Sobig, Blaster, and Sasser were spread by the network but required user-level functionality to initiate the infection.

In contrast, most network worms exploit the application layer. The various Zotob worms, for example, scanned the network for vulnerable hosts. When one was found, a remote network connection was established to transfer the worm. A remote overflow in the server's application layer permitted execution. These worms self-propagated by exploiting vulnerable application layer implementations.

# SMTP протоколи

SMTP хавфсизликни таъмнилаш мақсадида эмас балки, хабарларни ишончли ва ўз вақтида етиб боришини таъминлаш учун ишлаб чиқилган. Протокол дастлабки ишлаб чиқилган вақтларда ишончлилик хавфсизликка қараганда муҳимроқ муаммо бўлган. Мана шу қарашиб МUA ва MTA нинг амалга оширилишига боғлиқ бўлмаган бир қатор хавфсизлик рискларини келтириб чиқарган.

**MUA мълумоти билан келтирилган SMTP-сеансига мисол (қорайтирилган шрифтда ажратилган).**

% telnet rudolf 25 Trying...

Connected to rudolf.npole.org. Escape character is '^]'.

220 rudolf.npole.org ESMTP Sendmail 8.8.6 (PHNE\_17135)/8.7.3 SMKit7.1.1  
hp hp; Thu, 25 Apr 2002 09:17:17 -0600 (MDT) **helo ranch.npole.org**

250 rudolf.npole.org Hello ranch.npole.org [10.2.241.27], pleased to meet  
you **mail from: santa@npole.org**

250 santa@npole.org... Sender ok **rcpt to: grinch@xmas.mil**

250 grinch@xmas.mil... Recipient ok **data**

354 Enter mail, end with "." on a line by itself

**Subject: Ho ho ho**

**I know you've been a bad boy.**

250 JAA19237 Message accepted for delivery **quit**

**SMTP-сеансидан электрон почта хабарига мисол**

Received: from exchange2.npole.org ([10.8.16.2]) by exchange.npole.org with  
SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2653.13) id  
J2DYC3G1; Thu, 25 Apr 2002 08:19:32 -0700

Received: from rudolf.npole.org (rudolf.npole.org [10.2.23.20]) by  
exchange2.npole.org (Postfix) with ESMTP id 97BB3C0093F for  
<grinch@xmas.mil>; Thu, 25 Apr 2002 08:19:32 -0700 (PDT)

Received: from **ranch.npole.org** (IDENT:santa@npole.org [10.2.241.27]) by  
rudolf.npole.org with SMTP (8.8.6 (PHNE\_17135)/8.7.3 SMKit7.1.1 hp hp) id  
JAA19237 for grinch@xmas.mil; Thu, 25 Apr 2002 09:17:31 -0600 (MDT)

Date: Thu, 25 Apr 2002 09:17:31 -0600 (MDT)

From: **santa@npole.org**

Subject: **Ho ho ho**

Message-ID: <200204251517.JAA19237@rudolf.npole.org>

To: **grinch@xmas.mil**

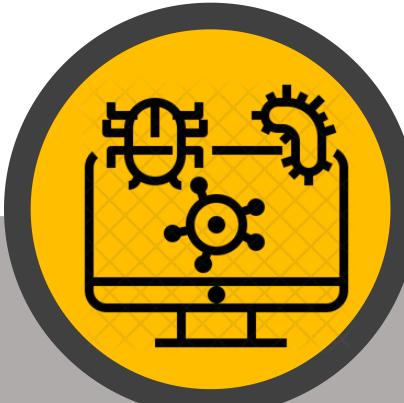
**I know you've been a bad boy.**

# SMTP протоколи рисклари Қалбаки сарлавҳа ва спамлар



## Қалбаки электрон почта хабари

Қалбаки email хабари жуда хавфли муаммоларни келтириб чиқариши мумкин. Бунга мисол сифатида ташкилот менежерининг ташкилот ходимини илавозимидан озод этиш ҳақидаги хабарини келтириш мумкин.



## СПАМ

Ёкимсиз почта хабари (спам) қалбаки электрон хабарлардан ғарзли мақсадларда фойдаланишга мисол бўла олади. Бир қарашда хабар қонуний шахс томонилан юборилгандек кўринса ҳам, аслида умуман бошқа шахс томонидан юборилган бўлади.



## MAIL логлари

Электрон почтани қалбакилаштиришда ёлғон сарлавҳаларда келтирилган серверлар журналларда сақланмайди, қалбаки хабарни юборган тизимлар эса ҳақиқий қабул қилувчи учун аккаунтлар ҳақида маълумотни ўзида сақлаши мумкин.

# Қалбаки сарлавҳали спам хабар

Received: from 25EECCEB (unknown[216.133.219.154] (misconfigured sender))  
by rwcrmxc21.comcast.net (rwcrmxc21) with SMTP  
id <20060115230410r2100f5ccie>; Sun, 15 Jan 2006 23:05:04 +0000  
Received: from 61.166.141.14 (unknown [61.166.141.14])  
by 204.127.202.26 with SMTP id allocate67074;  
Sun, 15 Jan 2006 15:00:55 -0800  
Message-ID: <24916.704613bery16943@eon.net.au>  
MIME-Version: 1.0  
Date: Sun, 15 Jan 2006 15:00:55 -0800  
From: "Jerrod Basil " <Gilbertk\_Whitfeld60@collahuasi.cl>  
To: homeuser145@comcast.net  
Subject: The findings support an earlier review by the U.S.

Have you ever stopped to wonder how much an average man pays for his medicines? Painkillers, drugs to improve the quality of life, weight reducing tablets, and many more. What's worse, the same medicine costs a lot more if it is branded.

We have over 172 Meds ready to order and be shipped

So why should you pay more especially when you can get the same drugs at a much cheaper cost? At Health Suite, we bring you the same drugs, the generic version - the same quality, the same formula at a very reasonable price.

Viagra low as 67.28

Cialis low as 93.73

<http://Beaverq<AC6>0x.isearc0fa.com>

Thank you  
Harry

6/20/2024

Reply Reply All Forward IM

Thu 3/31/2016

Invalid SPF <invalid.spf@iwlit.com>

Test Message - Invalid SPF

To Joseph Palarchio

**WARNING:** The sender of this email could not be validated and may not match the person in the "From" field.

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This is a test message.

## Imperative

1/23/19

K Kemail  
ipad@kemail.me

**Caution!** Inky Phish Fence thinks this message is potentially suspicious.  
(From: from@example.com, External)

### Potential Sender Forgery

The sender (First Last <from@example.com>) may be trying to trick you into thinking this message is from a major brand, a known contact, or a coworker.

[Report This Email](#) [FAQ](#) [Protection by Inky](#)

I need you to complete a task for me as soon as possible....  
P.S: I am in a meeting now and can't talk, so just reply back.

Regards.  
Sent from my iPad.

132

# HTTP протоколи

HTTP реал вақтда маълумотларни узатишнинг мослашувчан протоколи сифатида ишлаб чиқилган. HTTP 1.0 версиясининг дастлабки спецификацияси RFC1945-да аниқланган. Одатда HTTP HTML-ни узатиш учун ишлатилишига қарамай (ХМЛ асосидаги таркиб ва форматлаш спецификацияси), протокол узатилаётган таркибга боғлиқ емас. HTTP матн ёки иккилик файлларни ва ҳужжатларни ёки расмларни осонгина узата олади.

## GET / HTTP/1.0

Host: [www.hackerfactor.com](http://www.hackerfactor.com)

HTTP/1.1 200 OK

Date: Sat, 21 Jan 2006 16:49:12 GMT Server: Apache/1.3.34  
(Unix) mod\_pointer/0.8 PHP/4.4.1

X-Powered-By: PHP/4.4.1 Connection: close

Content-Type: text/html

<html>

<head><title>Hacker Factor Solutions</title></head> ...

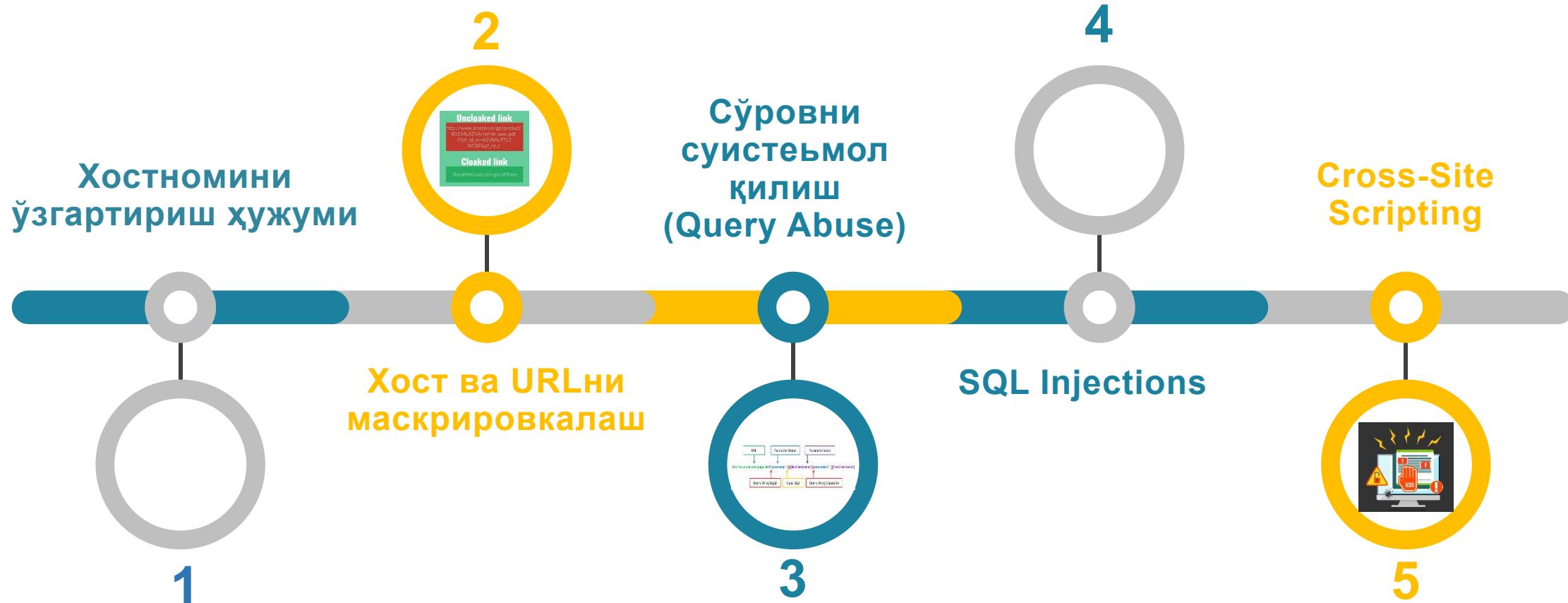
</html>

[www.hackerfactor.com](http://www.hackerfactor.com) сайтига HTTP сўров (қора шрифтда)  
ва унга жавоб

## HTTP жавоб қайтариш кодлари классификацияси

Code	Purpose
1xx	<i>Informational.</i> (Generally unused; not supported by HTTP 1.0.)
2xx	<i>Successful.</i> The request was received without processing errors.
3xx	<i>Redirection.</i> The reply indicates relocation information.
4xx	<i>Client Error.</i> The request could not be processed due to an error in the request.
5xx	<i>Server Error.</i> The request could not be processed due to a server problem.

# URL EXPLOITATION (Ишлатиш/Фойдаланиш)



# HTTPнинг асосий рисклари

## Аутентификациланмаган клиент ва сервер

HTTP серверда HTTP - мижозни аутентификациялаш учун кўп имкониятларни тақдим этмайди. Одатда ҳақиқийликни тасдиқлаш кенг тарқалган бўлсада, тармоқда узатилаётган фойдаланувчи шахсий маълумотларини маҳфийлигини таъминлай олмайди. Маълумотларни узатиш очиқ матн кўринишида бўлгани сабабли, оддий Оддий матнли маълумотлар узатилиши сабабли, ҳақиқийликни тасдиқлаш telnet и FTPдаги каби хавфли. SSH ну telnet и FTPнинг ўрнида ишлатиш мумкин бўлсада, SSH даги секин уланиш даражаси HTTPнинг ўрнига ишлатишга имкон бермайди





Тармоқقا уланган компьютерлар ўртасидаги алоқани таъминлаш учун илова маълумотларини машиналар учун тушунарли тилга ўзгаририш лозим. OSI нинг тақдимот сатҳи ушбу ўзгариришларнинг функциональ имкониятларини аниқлаб беради..

## Тақдимот сатҳи



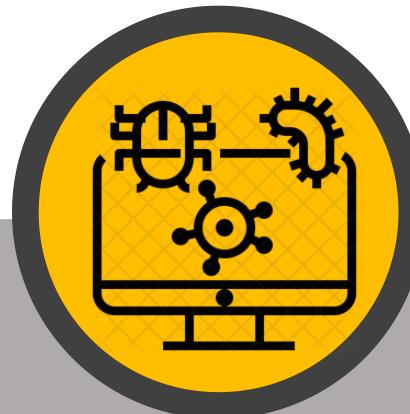
Ушбу сатҳ синтаксисларни келишиш ва маълумотларни ўзгариришни бошқаради. Бундан ташқари тақдимот сатҳи, сеанс сўровларини яратиш ва якунлаш орқали сеанс сатҳини ҳам бошқаради.

## Тақдимот сатҳи



### Кодлаш

Қалбаки email хабари жуда хавфли муаммоларни келтириб чиқариши мумкин.. Бунга мисол сифатида ташкилот менежерининг ташкилот ходимиини лавозимиidan озод этиш ҳақидаги хабарини келтириш мумкин.



### Сирқиш

Ёкимсиз почта хабари (спам) қалбаки электрон хабарлардан ғаразли мақсадларда фойдаланишга мисол бўла олади. Бир қараашда хабар қонуний шахс томонилан юборилгандек кўринса ҳам, аслида умуман бошқа шахс томонидан юборилган бўлади.

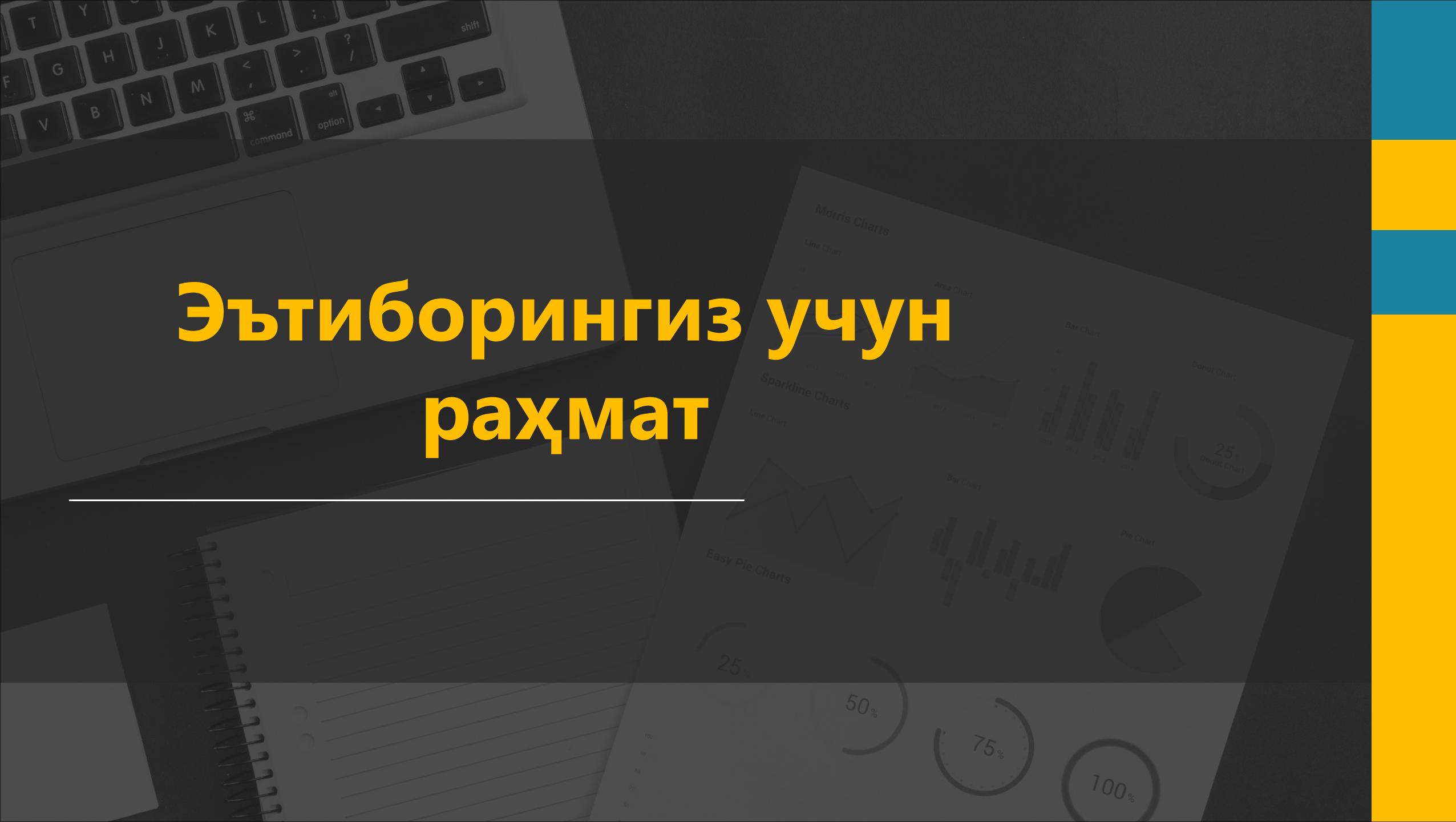


### Шифрлаш

Электрон почтани қалбакилаштиришда ёлғон сарлавҳаларда келтирилган серверлар журналларда сақланмайди, қалбаки хабарни юборган тизимлар эса ҳақиқий қабул қилувчи учун аккаунтлар ҳақида маълумотни ўзида сақлаши мумкин.

# Эътиборингиз учун раҳмат

---



# Тармоқ хавфсизлиги

---

7-маъруза. Канал ва сеанс сатҳларида  
ҳимояланган каналларни шакллантириш  
протоколлари.

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

## Канал сатҳи



ISO OSI моделининг 2-қатлами канал сатҳи қатламидир. Ушбу қатлам маълумотни рамкалаштиради, маълумотларни синхронлашни бошқаради, маълумотларни қабул қилувчиларни аниқлайди ва физик сатҳни бошқаради. Хавфсизлик муаммолари маълумотлар тузилиши ва қабул қилувчиларнинг манзилига тегишли бўлади.

- 7 - Application - A
- 6 - Presentation - Person
- 5 - Session - Sent
- 4 - Transport - Through
- 3 - Network - Network
- 2 - Data Link - Data
- 1 - Physical - Packets

6/20/2024

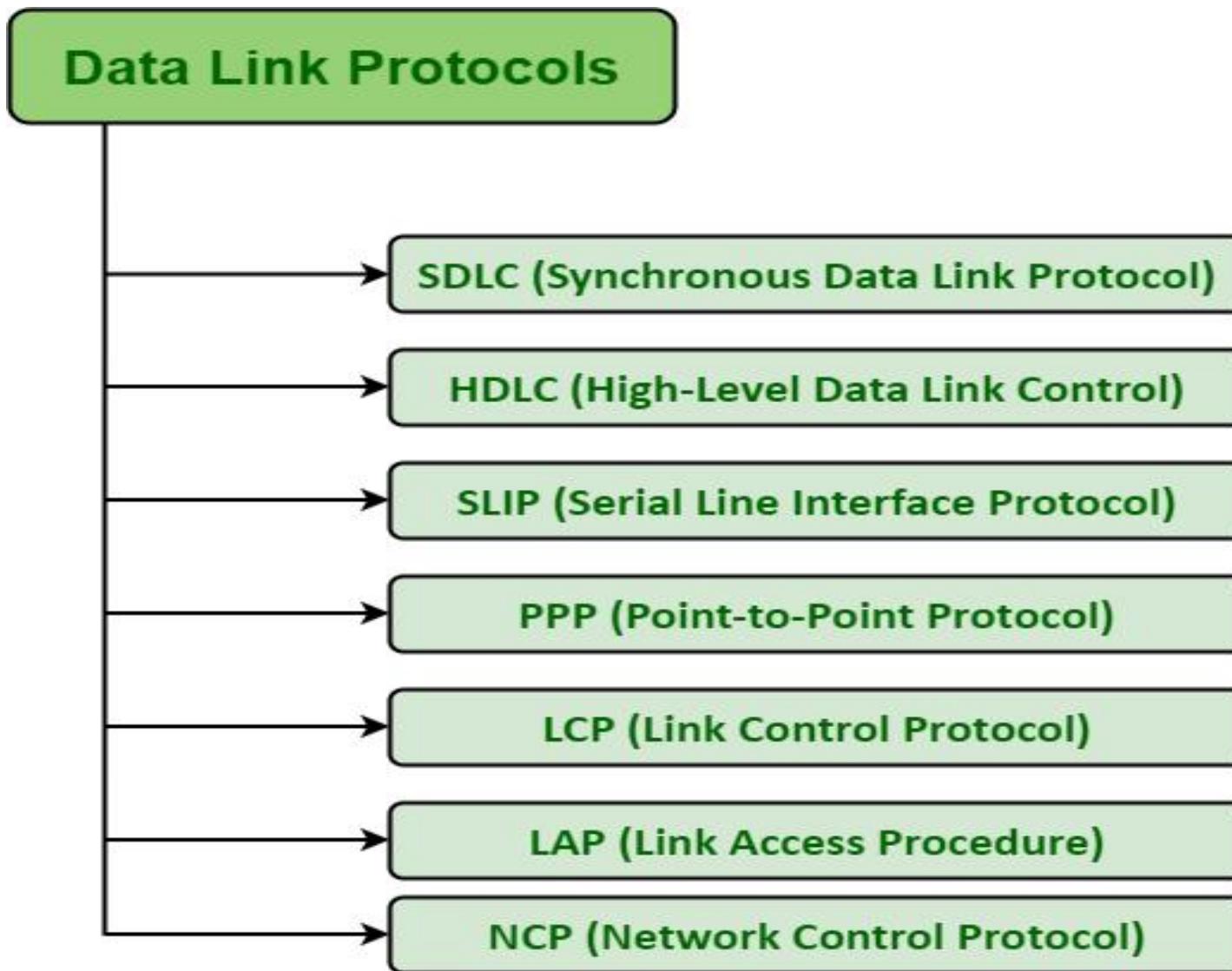


Ушбу сатҳнинг иккита мисоли - бу нуқта-нуқта тармоқ протоколлари (SLIP ва PPP) ва кўп кодли манзил протоколлари (MAC ва ARP).

- Physical - Please
- Data Link - Do
- Network - Not
- Transport - Throw
- Session - Sausage
- Presentation - Pizza
- Application - Away

140

# Канал сатхи – протоколлари



# Канал сатҳида маълумотлар оқими

Канал сатҳи орқали умумий маълумотлар оқими маълумотларни узатиш ва қабул қилишнинг тўрт босқичли жараёни сифатида намоён бўлади.

Маълумотларни  
узатиш

Канал сатҳи тармоқ бўйлаб узатиш учун тармоқ сатҳидан (OSI 3 сатҳи) маълумотларни олади. Тугун маълумотни тармоқ узатиш тезлигидан тезроқ ишлаб чиқариши мумкинлиги сабабли, Канал сатҳи маълумотларни узатиш учун кешлаши мумкин. Агар узатиш кеши тўлдирилган бўлса, у ҳолда Канал сатҳи тармоқ сатҳига маълумотлар узатилмаганлиги тўғрисида хабар беради.

Маълумотларни  
қабул қилиш

Физик сатҳдан маълумотларни қабул қилиш маълумотлар узатишга ўхшаш тўрт босқичли жараённи амалга оширади. Биринчидан, маълумотлар Физик сатҳдан олинади. Физик сатҳ маълумотлар оқимини ҳосил қиласи, шунинг учун сеанс сатҳи хабарларнинг рамкасини аниқлаш орқали маълумотларнинг бошланишини аниқлайди. Хабар доирасидан ташқаридаги маълумотлар битлари шовқин деб ҳисобланади.

# Умумий фойдаланиш

Канал сатҳи тармоқдаги қўшни тугунлар ўртасида ишончли маълумотларни узатишни таъминлайди. Ушбу қатлам алоҳида тармоқни улашга ҳаракат қилмайди ёки турли хил жисмоний тармоқ воситаларини қамраб олади. Канал сатҳи протоколлари учун энг кенг тарқалган фойдаланишга қуидагилар киради:

## Point-to-Point Networks

Point-to-Point Protocol (PPP) ва Serial Link Internet Protocol (SLIP)

## Multihost Networks

*unicast  
multicast  
broadcast*

## Frame Relay

ISDN, F-T1

## Switches

Parallel traffic  
Multiple addresses

## Bridges

10Base-2  
100Base-T

## Киришни чеклаш

SP

# Канал сатҳи протоколлари даражалари

Нуқтадан нуқта тармоқлар учун SLIP сингари маълумотлар сатҳининг ягона протоколи барча керакли функцияларни бажариши мумкин; аммо, бир нечта Канал сатҳи протоколлари бутун қатламни қамраб олади. Бунинг ўрнига, Канал сатҳи одатда бир нечта протоколларни ўз ичига олади, улар биргаликда тўлиқ маълумотлар ҳаволаси функсиясини таъминлайди. Пастки протоколлар жисмоний қатлам алоқаларини бошқаради. Ўрта қават протоколлари маршрутлаш ва манзиллашни бошқаради, юқори қават протоколлари эса тармоқ кашфиётини бошқаради.

**Low-Level  
Protocols**

FDDI, LAPF, PPP, Carrier Sense Multiple Access/Collision Detection

**Middle-Level  
Protocols**

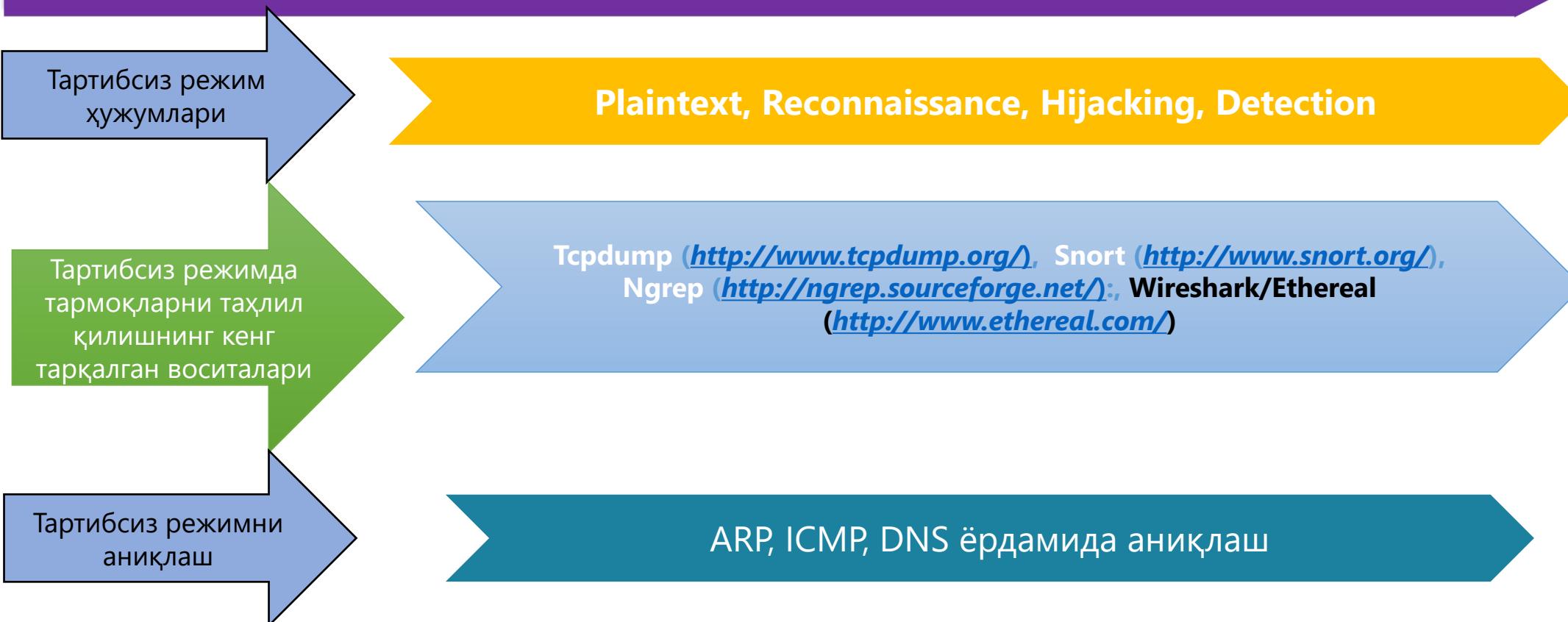
MAC ва LLC

**High-Level  
Protocols**

AppleTalk Address Resolution Protocol (AARP) ва the multilink protocol (MP)

# Ноодатий фойдаланиш

Канал сатҳи одатда физик сатҳга интерфейсни тақдим этади ва тармоқдаги иккита тугун ўртасида маълумотлар хавфсиз узатилишини таъминлайди; аммо, бу канал сатҳи учун ягона фойдаланиш эмас. Ноёб фойдаланиш ҳужумга учраган тармоқни кўрсатиши мумкин. Улар орасида тармоқни кузатиб боришга, тармоқнинг юкланишига, манзилга, кадрдан ташқари маълумотларга ва яширин каналларга асосланган ҳужумлар мавжуд.



# Ҳұжумларни амалға ошириш

Манзил  
ҳұжумлари

Күпгина манзиллар схемалари самарали тармоқ манзилини ўзgartиришга имкон беради. Агар иккита түгун битта манзил учун тузилған бўлса, иккаласи ҳам тармоқ трафигига жавоб беради. Натижада, одатда иккала түгун ҳам тармоқ уланишларини рад этади.

Out-of-Frame  
Data

Умуман олганда, хабар доирасига киритилмаган маълумотлар бекор қилинади. Маълумот физик қатлам бўйлаб узатилиши мумкин ва хабар доирасига киритилмайди. Ушбу кадрдан ташқари маълумотлар тармоқ ўтказувчанлигини истеъмол қилиши ёки маълумотни ностандарт (яширин) тарзда етказиши мумкин.

Covert Channels

Ҳұжумчилар канал сатҳи протоколлари сифатида қўринадиган орқа эшикларни ва масофадан бошқариш протоколларини яратишлари мумкин. Бунга қўйидагилар киради: Out-of-Frame Data, Addressing Information, Invalid Frames, Frame Size, Protocol Specific

Physical Layer  
Risks

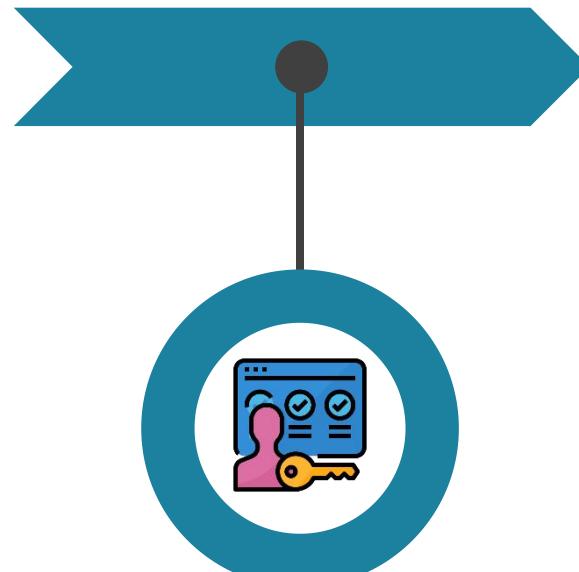
Физик сатҳ тажовузкори канал сатҳи хабарлари рамкаларига тўғридан-тўғри кириш хуқуқига эга.  
Физик сатҳга тажовузкор маълумотлар узатиш трафигини тинглаши мумкин.  
Физик сатҳга тажовузкор маълумотлар ҳаволаси трафигини ёзиши ва тақрорлаши мумкин. Қайта ижро этилған маълумотлар канал сатҳи учун мақбул бўлади.

# PPP

PPP хабар доираси рамка ичидаги маълумотлар ҳажмини ва фреймни қабул қилиши керак бўлган тармоқ хизмати турини белгилайдиган сарлавҳани ўз ичига олади. PPP шунингдек IP манзиллари, МТУ ва асосий аутентификация бўйича музокаралар учун маълумотлар ҳаволасини бошқариш протоколини ўз ичига олади. Бундан ташқари, PPP ҳавола сифатини қўллаб-қувватлайди, масалан, бошқа томоннинг ҳали ҳам уланганилигини аниқлаш учун эcho бошқарув рамкаси. Афсуски, PPP аутентификация маълумотларини ҳимоя қилиш, узатиш хатоларини аниқлаш ёки такрорий ҳужумларни тўхтатиш воситаларини тақдим этмайди.



**Authentication**



**Transmission Error Detection**



**Replay Attack  
Transmission**

# SLIP

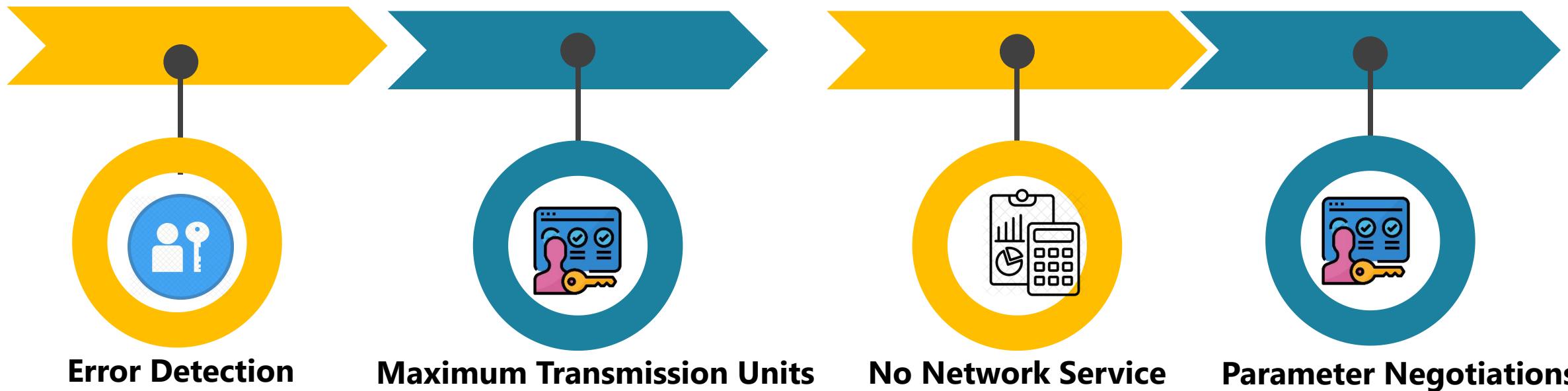
**Serial Line Internet Protocol (SLIP)** РФС1055 томонидан белгиланади. Ушбу оддий протокол дастлаб кетма-кет уланиш учун мүлжалланган эди. SLIP дастлабки сарлавҳаларни тақдим этмайди ва фақат бир нечта аниқланган байтларни таклиф қиласи:

**END** : 0xC0 байт рамканинг охирини билдиради.

**ESC** : 0xDB байти қочиш белгисини билдиради.

**Encoded END** : Агар маълумотлар оқимида ЕНД байти (0xC0) бўлса, у ҳолда SLIP белгини 0xDB 0xDC сифатида қайта кодлайди.

**Encoded ESC** : Агар маълумотлар оқимида ЕСС байт (0xDB) бўлса, у ҳолда SLIP белгини 0xDB 0xDD сифатида қайта кодлайди.

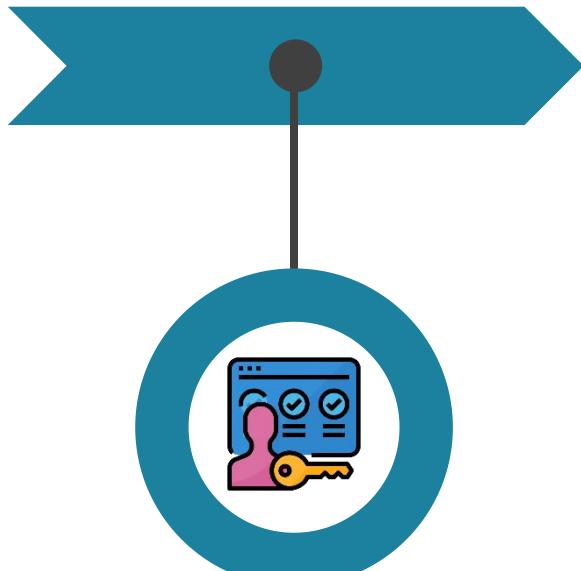


# SLIP ва PPP заифликлари

PPP ва SLIPнинг энг катта хатарлари аутентификация, икки томонлама алоқа ва фойдаланувчи таълимига тегишли. Гарчи тинглаш, такрорлаш ва қўшиб юбориш ҳужумлари мумкин бўлса-да, бу ҳужумлар физик сатҳга киришни талаб қиласди. Нуқтадан-Нуқта тармоқдаги фақат иккита тугунни ўз ичига олганлиги сабабли, канал сатҳига нисбатан жисмоний даражадаги таҳдидлар одатда муҳим аҳамиятга эга эмас.



**Authentication**



**Bidirectional Communication**



**User Education**

# MAC

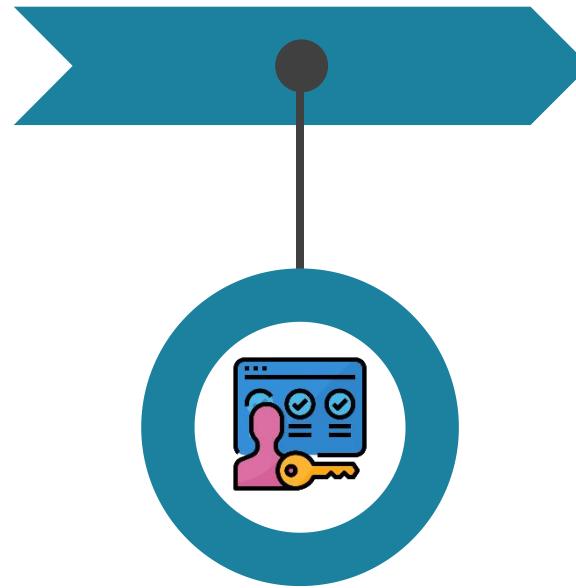
*Media access control* (MAC) пастки қатлами иккита асосий функцияни таъминлайди: узатишни бошқариш ва тармоқ манзилини бошқариш.

## Transmission Control:

**Network Addressing:** Тармоқдаги ҳар бир тугун ўзига хос манзилни талаб қиласди. Ушбу аппарат манзили қабул қилувчининг тугуни томонидан битта ва кўп тармоқли пакетларни қайта ишлашга имкон беради. Ҳар бир пакет қабул қилинганда, белгиланган аппарат манзили маҳаллий аппарат манзили билан таққосланади. Агар манзиллар мос келадиган бўлса, у ҳолда пакет қайта ишланади.



**Authentication**



**Transmission Error Detection**



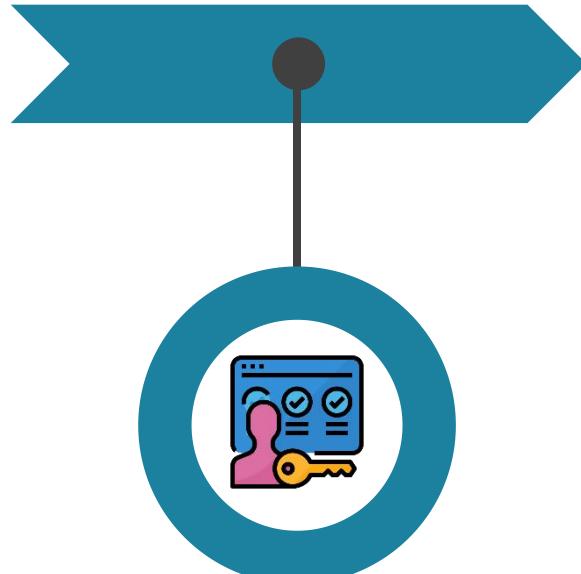
**Replay Attack  
Transmission**

# МАС заифликлари

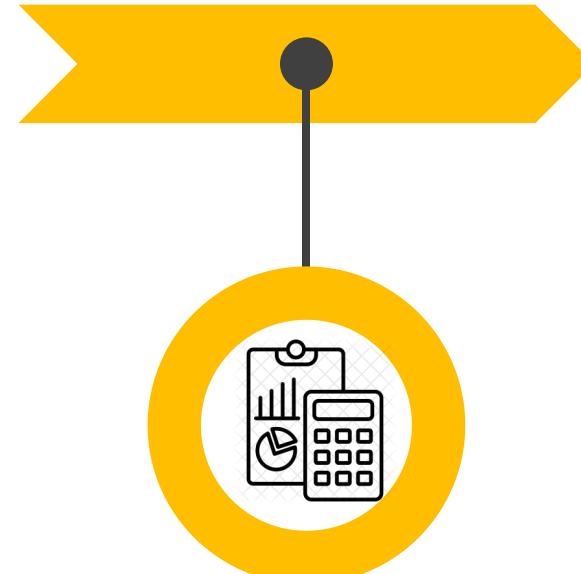
МАС тармоқдаги хостлар ўртасида маълумот алмасиш воситаларини тақдим этади, қўшимча потенциал ҳужум векторларини ҳам тақдим этади. Ҳужумчилар МАС маълумотларини разведка, ўзини тақлид қилиш ёки юкга асосланган ҳужумлар учун ишлатишлари мумкин.



Ускуна профилининг  
ҳужумлари



Ўзини тақлид қилиш учун  
ҳужумлар



Load Attacks

**Address Resolution Protocol (ARP)** хизматга кириш протоколининг намунасиdir. РФС826-да белгиланган ARP, IP-манзилларни аппарат манзиллариغا айлантириш орқали тармоқ сатҳига (OSI қатлами 3) ёрдам беради. **Reverse Address Resolution Protocol (RARP)** аппарат манзилини IP-манзилга ўзгартиради.

# Заифликлар

## ARP Poisoning

ARP пакетлари фақат янги IP-манзил (ёки MAC-манзил) қидиришни амалга ошириш зарур бўлганда талаб қилинади. Аммо, ушбу кешланган ёзувлар тизимни ARP заҳарланишига очиб беради, бу ерда жадвални тўлдириш учун яроқсиз ёки қасдан нотўғри ёзув ишлатилади.

## ARP Poisoning хужумлари

Resource Attack, Denial of Service (DoS), Man-in-the-Middle (MitM)

## ARP Poisoning хужумини камайтириш

ARP жадвалларини қаттиқ кодлаш, ARP ёзувлари муддат қўйиш, ARP жавобларини филтрлаш

## ARP жадвалларини қулфлаш

ARP жадваллари вақтинча блокланиши мумкин. Бундай ҳолатда, ўрнатилган уланиш (масалан, IP-уланиш) ARP жадвали ёзувини қисқа вақт ичida блоклайди. Шу вақт ичida янги ARP жавоблари блокировка қилинган жадвал ёзувини ёзиб бўлмайди - бу ўрнатилган уланишнинг ўрнатилиши ва MitM хужумларини юмшатиш пайтида уни ўзгартириш мумкин эмаслигини таъминлайди.

# ТАРМОҚ ЙЎЛЛАРИ

Свитчлар ва кўприклар каби тармоқ қурилмалари одатда ARP пакетларидан фойдаланадилар. Хусусан, ушбу қурилмалар ARP жавобларига эътибор беради. Афсуски, ушбу тизимлар ARP ҳужумларига сезгир, масалан, switch poisoning ва switch flooding.

1

## Switch Poisoning Attacks

Коммутаторлар трафикни йўналтириш учун ARP жадвалини маҳсус жисмоний тармоқ портларига ўтказади. ARP заҳарланиш ҳужуми ARP жадвалини бузиши мумкин. Заҳарланиш ARP жавоби бошқа тугуннинг МАС манзилини бошқа порт билан боғлаши мумкин. Бу жабрланувчининг тугунини тармоқдан самарали равища узиб қўяди ва жабрланувчи учун мўлжалланган барча трафикни тажовузкор порти орқали юборади. Свитч заҳарланиши тармоқ трафигини йўналтиргани сабабли, ушбу ҳужум уланишини ўғирлашга имкон беради.

2

## Switch Flooding Attacks

Бузук режимда ишлайдиган тугунлар бевосита маҳаллий тармоқдан ташқарида бирон бир тармоқ трафигини қабул қила олмайди. Свитчлар ва кўприклар одатда тугунлар фақат маҳаллий жисмоний тармоқ учун мўлжалланган трафикни қабул қилишни таъминлайди. ARP заҳарланишидан фойдаланган ҳолда тажовузкор калитнинг ARP жадвалини босиши мумкин. Коммутаторлар пакетларни ташлашга қодир эмаслиги сабабли, калитларнинг кўпи ARP жадвали тўлдирилганда тугмачанинг ҳолатига қайтади. Бундай ҳолатда барча тугунлар барча трафикни қабул қиласди; бузук режимда ишлайдиган тугун Свитч орқали ўтадиган барча тармоқ трафигини қабул қилишни бошлаши мумкин.

## Сэанс сатҳи



### Сеанс сатҳи

Сеанс фойдаланувчиси ва сеанс провайдери ўртасида сессиялар деб номланган узоқ муддатли диалогларни бошқариш учун мўлжалланган. Ушбу юқори даражадаги уланишлар қуи катламли транспорт, тармоқ ёки

маълумотлар алоқаси

уланишларига қараганда анча узоқ давом этади.



Тармоқ файл тизими (NFS), X-WINDOWS тизими ва AppleTalk Session Protocol (ASP)

- 7 - Application - A
- 6 - Presentation - Person
- 5 - Session - Sent
- 4 - Transport - Through
- 3 - Network - Network
- 2 - Data Link - Data
- 1 - Physical - Packets

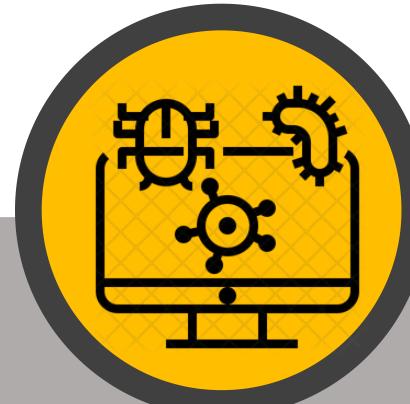
- Physical - Please
- Data Link - Do
- Network - Not
- Transport - Throw
- Session - Sausage
- Presentation - Pizza
- Application - Away

# Умумий рисклар



## Authentication and Authorization

DNS; NFS; SMB



## Session Hijacking

Сеанс қатлами протоколлари сессияни идентификатори орқали ҳолатини сақлайди ва идентификаторлар одатда узоқ муддат амал қиласди. Агар сессия идентификатори кодланмаган бўлса, тажовузкор Сеанс идентификаторини сотиб олиши ва сессияни ўғирлаши мумкин.



## Blind Session Attacks

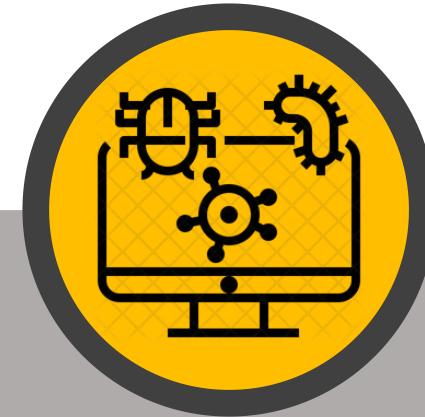
Сеанс идентификаторининг узунлиги протоколга хосдир. Масалан, DNS ва SMB 16-битли идентификаторлардан фойдаланади. Агар сессия уланмасдан транспорт хизматидан фойдаланса, у ҳолда кўр-кўронга сеанс ҳужумига қарши ҳимоясиз бўлади.

# Умумий рисклар- давоми



## Man-in-the-Middle (MitM)

Сеанс сатҳи протоколлари MitM ҳужумларига қарши ҳимоясиз. Ҳужумлар сеанс сатҳидан ёки ундан пастроқдан келиб чиқиши мумкин. MitM ҳужумлари сеанси учун тажовузкор сервердан олдин аутентификация қилишдан олдин тармоқ сўровини тўхтатиши керак. Кейин MitM мижоз ва ҳақиқий сервер билан мустақил равишда аутентификация қиласи ва мижоз ва сервер ўртасида сўровларни узатади.



## Information Leakage and Privacy

Сеанс сатҳи стандартлари сессия ва ҳолатни сақлашни белгиласа ҳам, улар аутентификация ёки маҳфийликни қўллаб-қувватламайди. Кўпгина ҳолларда, сеанс сатҳи протоколлари заиф аутентификациядан фойдаланади ва шифрланмайди. Мижоздан серверга йўналиш бўйлаб ҳар қандай тажовузкор тармоқ трафигини сифферлаши ва бутун сеансни қўриши мумкин. Масалан, DNS, NFS ва (эски) SMB маълумотлар шифрлашни амалга оширмайди. Тармоқ трафигини сифферлайдиган тажовузкор барча сессияни кузатиши мумкин.

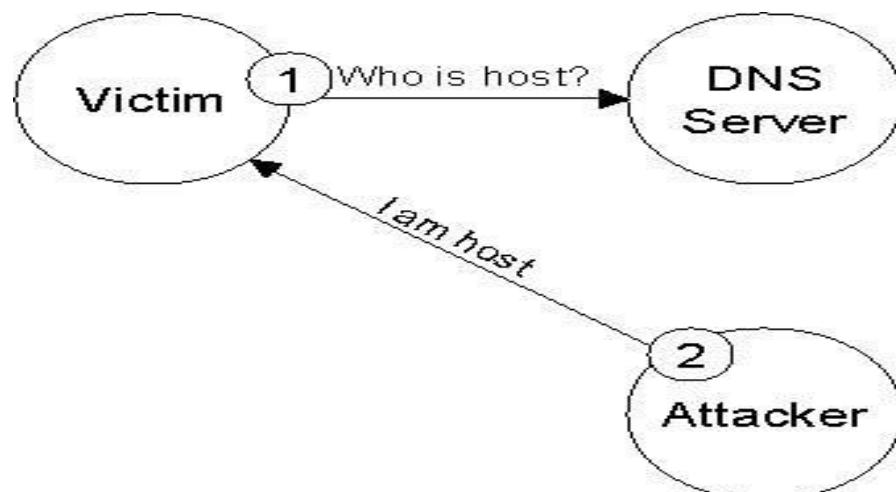
# DNS протоколи

Домен номлари тизими (DNS) кенгайтирилган, тарқатиладиган маълумотларни бошқариш тизими [РФС1034]. Бу динамик янгиланишларни, хост номини ва тармоқ манзилларини хариталашни ва хостлар ва доменлар ҳақида қўшимча маълумотларни қўллаб-қувватлади. DNS жуда катта тармоқлар учун ишлаб чиқилган. Амалдаги DNS тизими иш юкини осонгина тарқатади ва Интернетдаги миллионлаб компьютерларни қўллаб-қувватлади. DNS жисмоний шахсларга ва компанияларга DNS таркибини керак бўлганда ўзгартириш имкониятини беради.

## Тўғридан-тўғри хавф-хатарлар

Тасдиқланмаган  
жавоблар

Сўровларни жавоблар билан мослаштириш учун DNS сессия идентификаторидан фойдаланади, аммо сессия идентификатори аутентификацияни таъминламайди. DNS сўрувини кузатган тажовузкор DNS жавобини сохталаштириши мумкин.



# DNS протоколи рисклари



## DNS Poisoning

DNS ишончига ассоланган ҳужумларда ARP заҳарланишига ўхшаш усул қўлланилади ва IP ни ICMP йўналтириш орқали амалга оширилади



## DNS Cache Poisoning

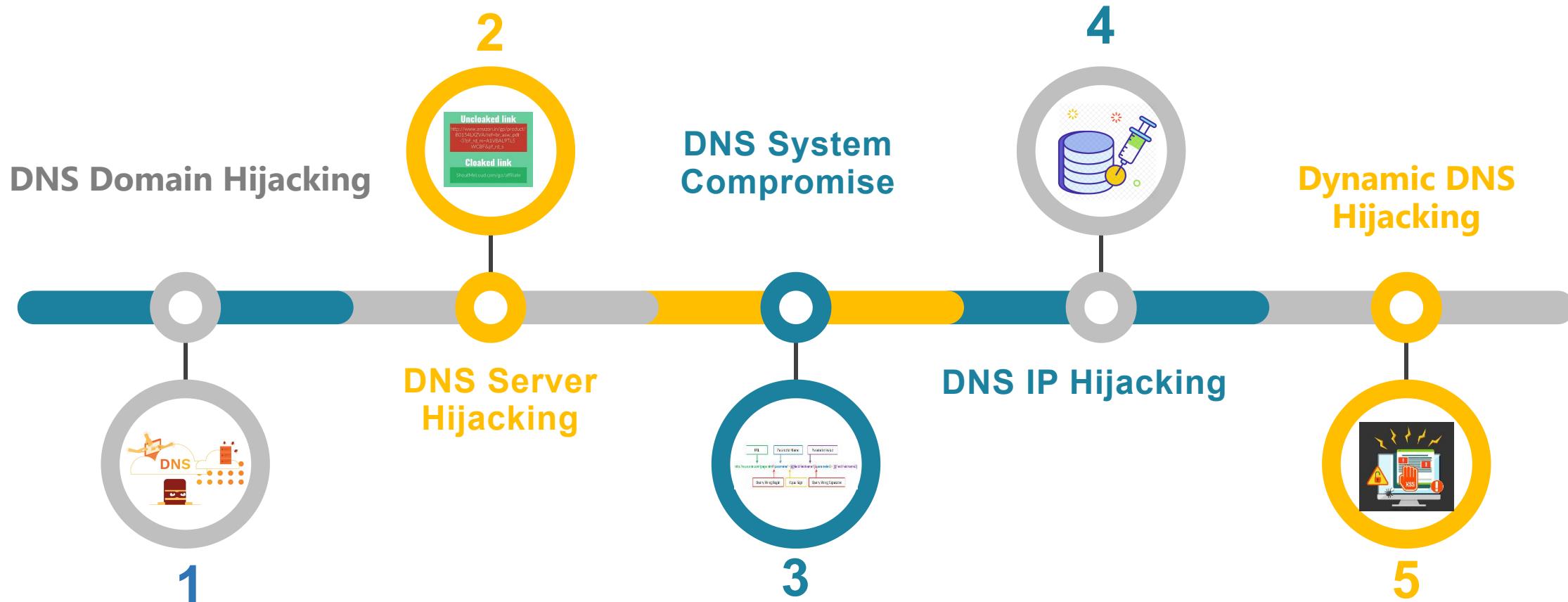
Тасдиқланмаган жавоблар сўров берувчига қаратилган бўлса, DNS кеш билан заҳарланиш ҳар қандай кешлаш DNS серверини мақсад қиласди. Тажовузкор DNS сўровни кузатади ва DNSга соxта жавоб беради. Жавоб ваколатли бўлиб кўринади ва кешнинг узоқ вақт кутиш қийматини ўз ичига олади.



## Blind ID Attack

Тасдиқланмаган жавоблар ва кеш билан заҳарланиш одатда тажовузкордан DNS сўрови ва сессия идентификаторини кузатишни талаб қиласди. Аммо сўровни бажариш ҳар доим ҳам муҳим емас. Тажовузкор умумий домен номини танлаши ва хост номи тугаши билан пайдо бўлганда ҳужумни бошлиши мумкин..

# Техник хавф-хатарлар



# Ижтимоий хавф-хатарлар

DNS Интернет учун ҳал қилувчи рол ўйнайди. Хост номини бузиш ёки ўғирлаш қобилияти тўғридан-тўғри DoS, MitM ва бошқа тизим ҳужумларига олиб келади. DNS-серверларда тўғридан-тўғри хатарлар ва техник ҳужумлар мавжуд, аммо хост ёки доменни бузиш учун бошқа усуллар мавжуд. Ушбу хатарлар инсон омилига қаратилган. DNS учун ижтимоий хавф-хатарларга ўхшаш хост номлари, автоматик номларни тўлдириш, ижтимоий муҳандислик ва доменни янгилаш киради.



# Таҳдидларни камайтириш

## Тўғридан-тўғри таҳдидни камайтириш

## Техник таҳдидни камайтириш

## Разведка таҳдидни камайтириш

## Ижтимоий таҳдидни камайтириш

Patch, ички ва ташқи доменларни ажратиш, Чекланган ҳудуд ўтказмаларини ҳосил қилиш, Ўтказиш ҳудудини аутентификациялаш, Кешнинг давомийлигини чеклаш, Нотўғри жавобларни рад этиш

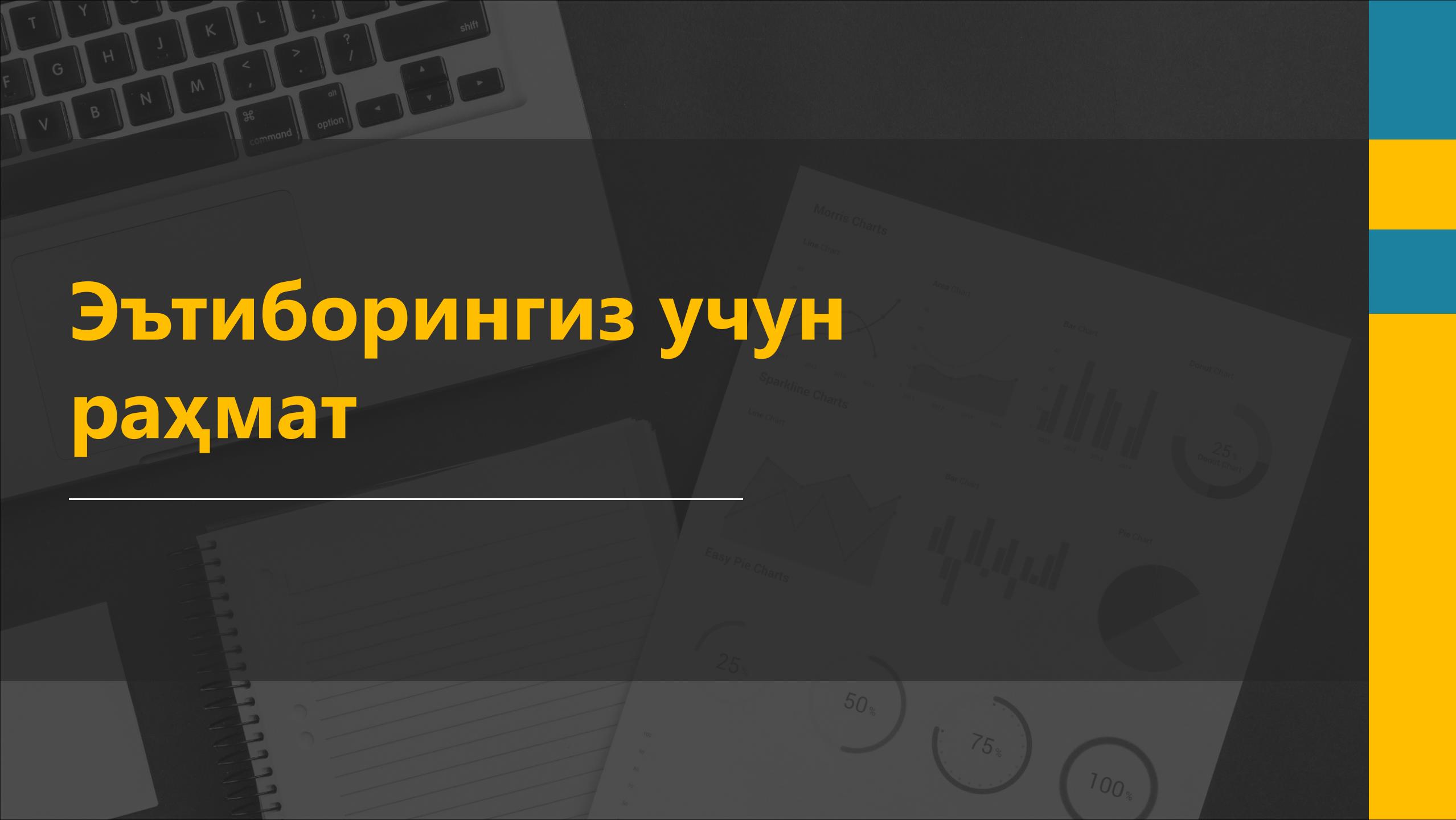
### **Harden Servers, Firewall**

Трансферга чеклов қўйиш, Сўровларга чеклов қўйиш, Тескари қидиувларни олиб ташлаш, Ички ва ташқи доменларни ажратиш, Ортиқча маълумотни олиб ташлаш, Дастурларни янгилаш

Ўхшаш доменларни мониторинг қилиш, Доменларни қулфлаш, Ҳақиқий контактлардан фойдаланиш, 24/7 қўлаб-қувватлаш, Self-Hosting

# Эътиборингиз учун раҳмат

---



# Тармоқ хавфсизлиги

---

9- маъруза · Физик сатҳда компьютер  
тармоғини ҳимоялаш.

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

# Физик сатҳ



OSI модели физик сатҳдан бошланади. Бунга физик тармоқ оммавий ахборот воситалари, тармоқ карталари (NIC) ва NICни бошқариш учун операцион тизим драйверлари киради. Ушбу қатламни бошқа барча

OSI қатламларидан ажратиб турадиган нарса - бу жисмоний мавжудлик; бошқа барча қатламлар виртуал. Жисмоний муҳит тури ва тармоқ тартиби (топология) тармоқнинг физик хавфсизлигини белгилайди.



OSI физик қатлами битта мақсадга эга: жисмоний канал орқали тўғридан-тўғри жисмоний оммавий ахборот воситалари билан алоқа қилиш. Ушбу алоқа физик алоқани ўрнатишни, маълумотни канал орқали узатишни ва маълумотни канал орқали олишни ўз ичига олади

- 7 - Application - A
- 6 - Presentation - Person
- 5 - Session - Sent
- 4 - Transport - Through
- 3 - Network - Network
- 2 - Data Link - Data
- 1 - Physical - Packets

- Physical - Please
- Data Link - Do
- Network - Not
- Transport - Throw
- Session - Sausage
- Presentation - Pizza
- Application - Away

# Физик сатҳда маълумотлар оқими

Физик сатҳи орқали умумий маълумотлар оқими маълумотларни узатиш ва қабул қилишнинг беш босқичли жараёни сифатида намоён бўлади.

Жисмоний қурилма драйвери жисмоний канал орқали маълумотларни узатиш учун тармоқ картасидан фойдаланади.

2



Қабул қилиш тизимидағи тармоқ картаси маълумотларни қабул қиласди.

3

Маълумотлар қабул қилувчининг физик қурилмаси драйверига узатилади

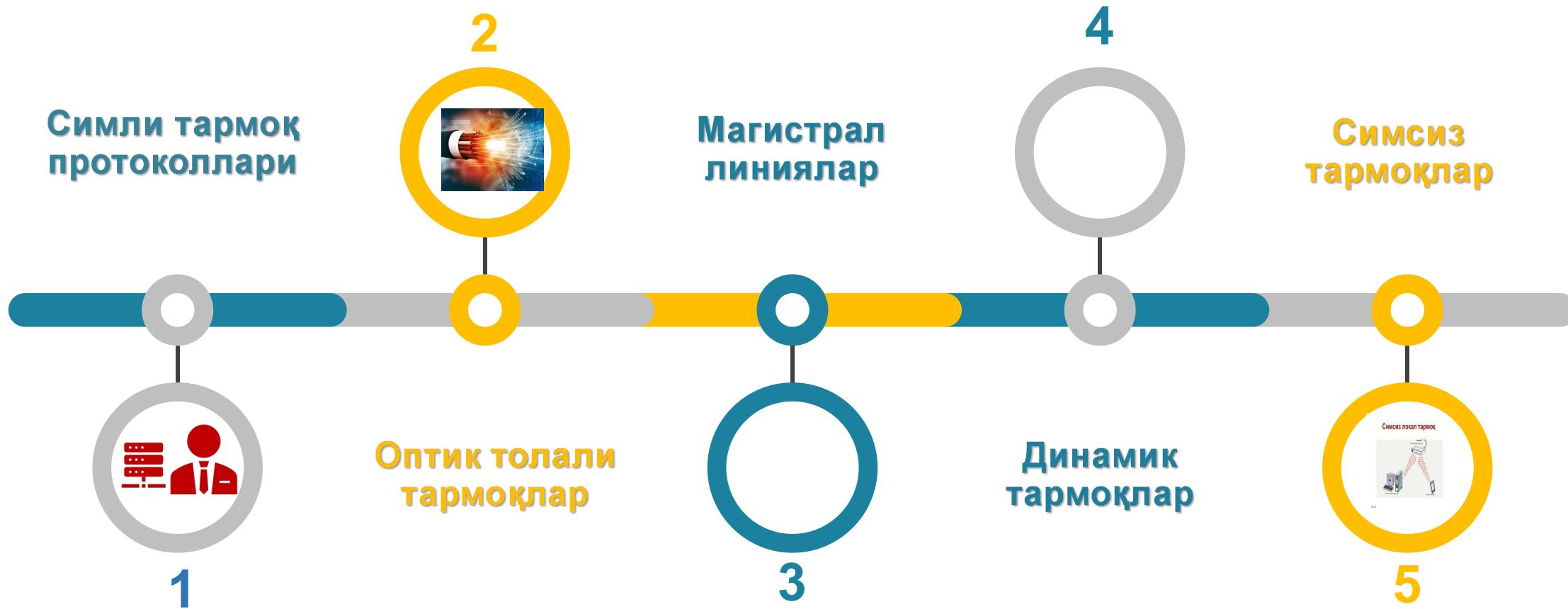
4

Жисмоний қурилма драйвери маълумотларни қайта ишлаш учун юқори даражадаги OSI катламларига узатади.

5

# Физик муҳитнинг турлари

Физик муҳит - бу маълумотларни юбориш ва қабул қилиш учун ҳамма нарсани, Маълумот сигнализацияси электр кучланиш, радиочастота (частота) ва ёруғликнинг модуляциясини ўз ичига олади.



# Физик тармоқ компонентлари

Физик қатlam маълумотлар узатувчи ва қабул қилувчи тармоқ таркибий қисмларидан иборат.

T  
A  
R  
M  
O  
K  
  
T  
U  
G  
U  
N  
I

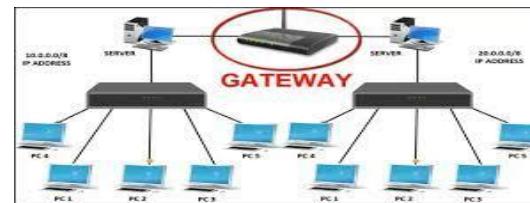
Компьютер



Кўприк



Шлюз



Маршрутизатор



Комутатор



Улагич

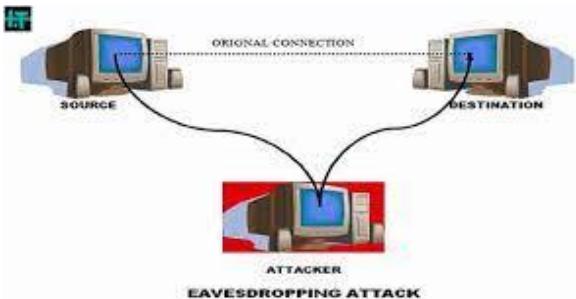


Репитер

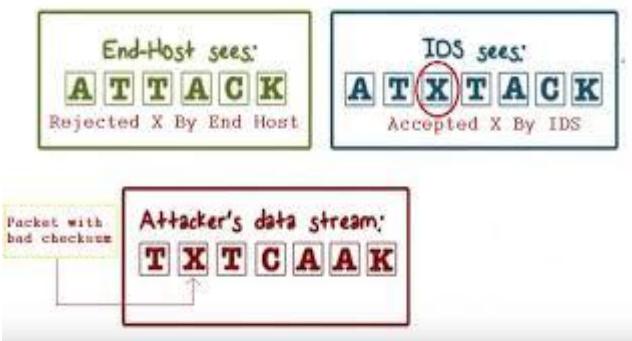


# Физик сатх хавф-хатарлари

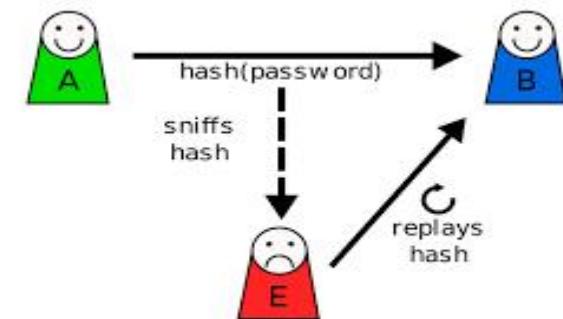
## Eavesdropping



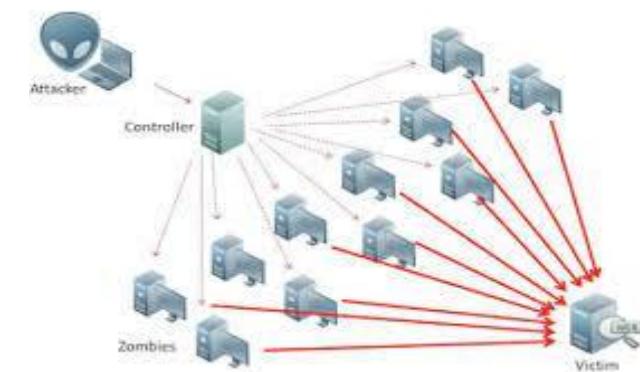
## Insertion



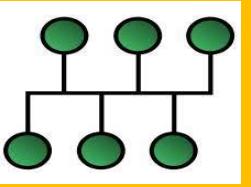
## Replay



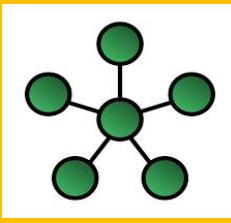
## Denial of Service (DoS)



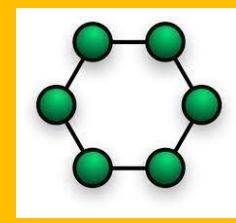
# Тармоқ топологиялари



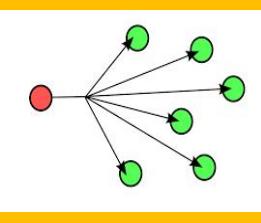
**Шина**  
топологияси  
барча түгунларни  
ўз ичига олган  
битта алоқа  
каналидан  
иборат



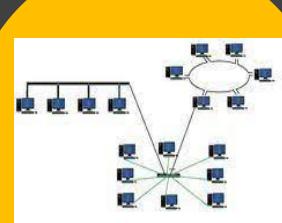
**Юлдуз**  
топологияси  
түгунлар билан  
алоқа қилиш учун  
марказий  
қурилмага  
эга



**Халқа**  
топологияси  
марказий  
қурилмани  
тармоқнинг  
марказидан ҳар  
бир түгунга  
кўчиради.



**Broadcast**  
топологияси  
маълумотлар бир  
нуқтадан бир  
нуқтага емас,  
балки  
радиочастоталар  
орқали  
узатилганда  
ишлатилади.

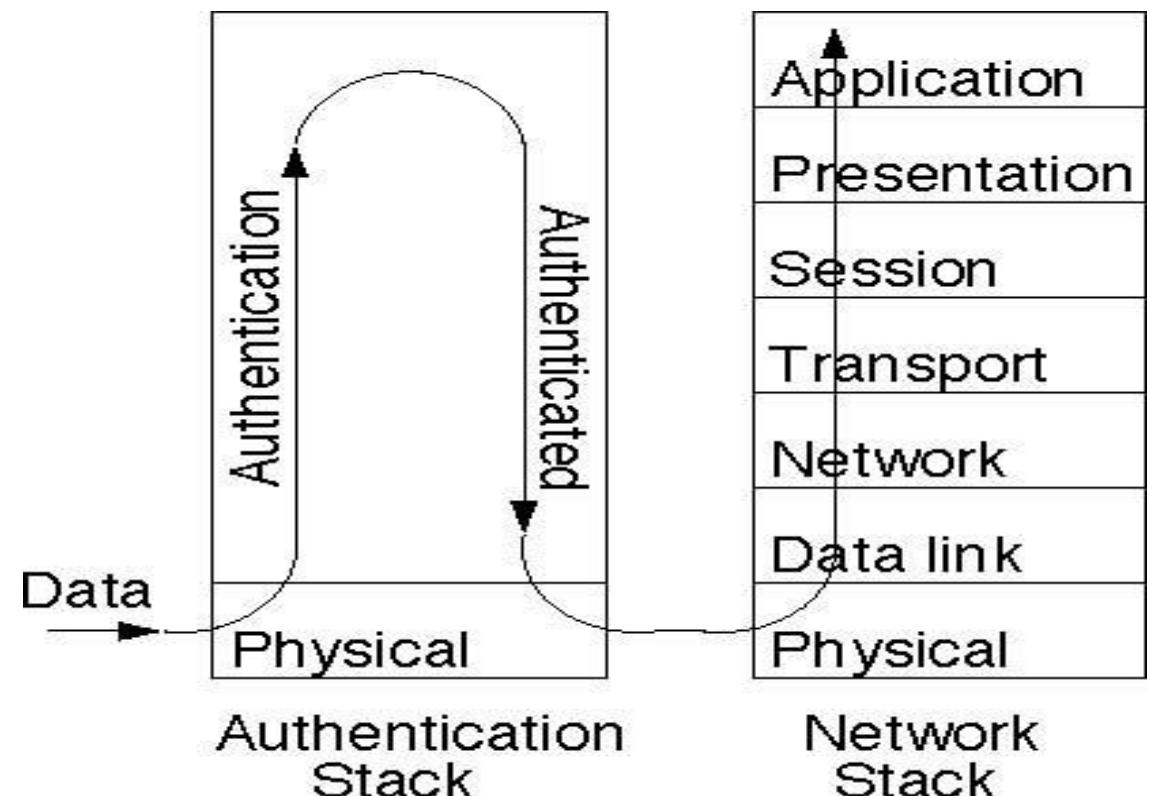


**Гибрид**  
топология бир  
нечта тармоқ  
архитектураларини  
афзалликларнинг  
комбинациясини  
таъминлаш учун  
бирлаштиради.

# ФИЗИК САТХ ХАВФИЗЛИГИ

Күпгина физик сатх протоколлари аутентификация қилиш учун юқори сатхлар билан чамбарчас боғлиқ. Бунга мисол қилиб диалуп линиялар ва симсиз тармоқларни көлтириш мүмкін. Диалуп тармоқ тез-тез фойдаланувчини тасдиқлаш учун PPP ёки SLIP (2-даражали протоколлар) га таянади. Худди шундай, симсиз тармоқ мижозларнинг ҳақиқийлигини текшириш учун Wired Equivalent Privacy (WEP) протоколи ва MAC манзилини филтрлашдан фойдаланади.

Тармоқни аутентификация қилиш түплами намунаси.



# Тармоқ муаммоларини аниқлаш



Физик сатх ҳужумининг манбасини аниқлаш қобилияти тармоқ муҳити ва конфигурациясига боғлиқ. Шина топологиясида ҳар бир тугун шинанинг бошқа барча тугунлари томонидан қабул қилинган сигнални ҳосил қиласди. Ушбу конфигурацияда тармоқ муаммоси манбасини аниқлаш жуда қийин бўлиши мумкин. Бундан фарқли ўлароқ, юлдуз топологияда бузилган тугунни қидиришни тезда марказнинг маълум бир портига қисқартириши мумкин; агар портдан фойдаланадиган битта тугун бўлса, у ҳолда портни осонгина аниқлаш мумкин.

Симсиз тармоқ узилишларини аниқлаш катта тармоқдаги номаълум тугунга қараганда анча қийинроқ бўлиши мумкин. Умуман олганда, физик сатҳдаги муаммоларни маҳсус воситаларсиз осонгина аниқлаш мумкин емас.



BUS



RING



Small networks



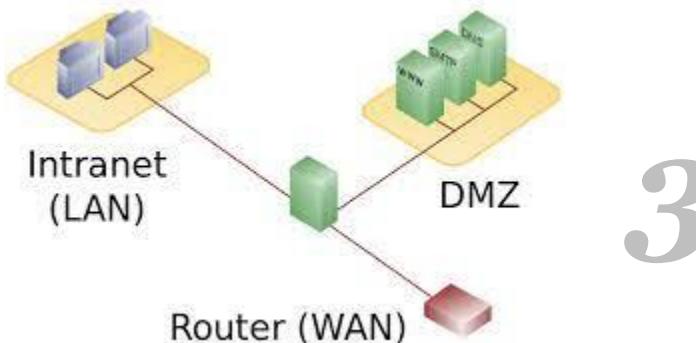
# Физик LAN

LAN



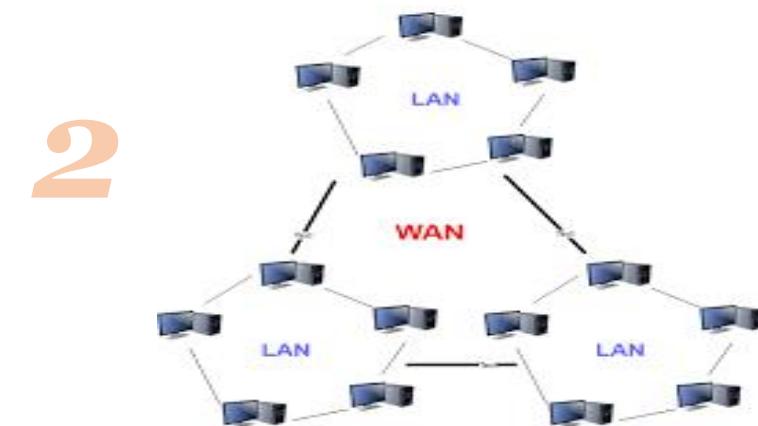
1

DMZ



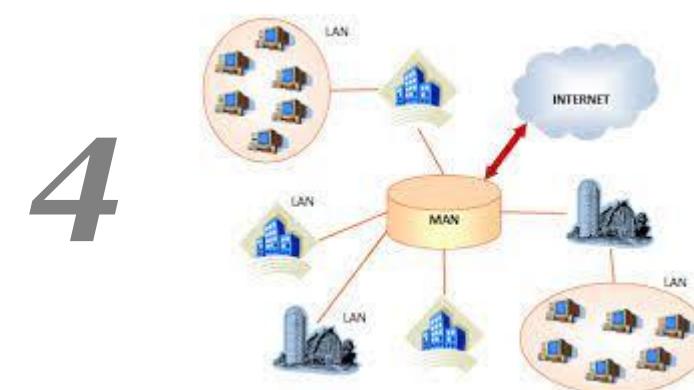
3

WAN



2

MAN



4

Физик тармоқ турлари



# Хұжум турлари

Симли тармоқлар учун асосий таҳдидлар бузилиш, шовқин, ҳидлаш, такрорлаш ва қўшилиш ҳұжумларидан иборат.

**Disruption**

Тармоқ сегментидаги тез-тез учрайдиган узилишларга електр узилиши ва узилган тармоқ кабеллари киради. Юмшатилиш усуллари одатда захира қувват манбаларини ва асосий тармоқ қурилмаларига чекланган киришни ўз ичига олади.

**Interference**

Тармоқ трафигини узатиш учун ишлатиладиган восита бошқа сигналларни ҳам узатиши мумкин. Агар воситага рухсациз сигнал (шовқин) кирса, у ҳолда тармоқ қурилмалари маълумотларни шовқиндан ажратадилар. Маълумотларни кодлаш техникаси таъсирни шовқинлардан юмшата олади.

**Intentional Attacks**

*Sniffing, replay* ва *insertion* ҳұжумларидан таҳдидлар қасдан қилинган ҳұжум турларига киради.

# Тармоқларааро экран (Firewall)

Тармоқларааро экран - бу тармоқ сегментлари ўртасида ўтиши билан тармоқ трафигини филтрлайдиган ва маълум тармоқ протоколлари асосида ҳимояни таъминлайдигам тизим тури. Тармоқларааро экран биринчи навбатда OSI нинг қуийи сатҳлари билан боғлиқ: физик, канал, тармоқ ва транспорт сатҳи. Тармоқ трафигини филтрлашга асосланган ҳар қандай ҳужумларни камайтириш усуллари тармоқларааро экранда амалга ошириш мумкин.

## Software Firewalls

**Дастурий тармоқларааро экран тармоқ филтрини тўғридан-тўғри тармоқ дастурлари ишлайдиган компьютерга жойлаштиради.**

## Hardware Firewalls

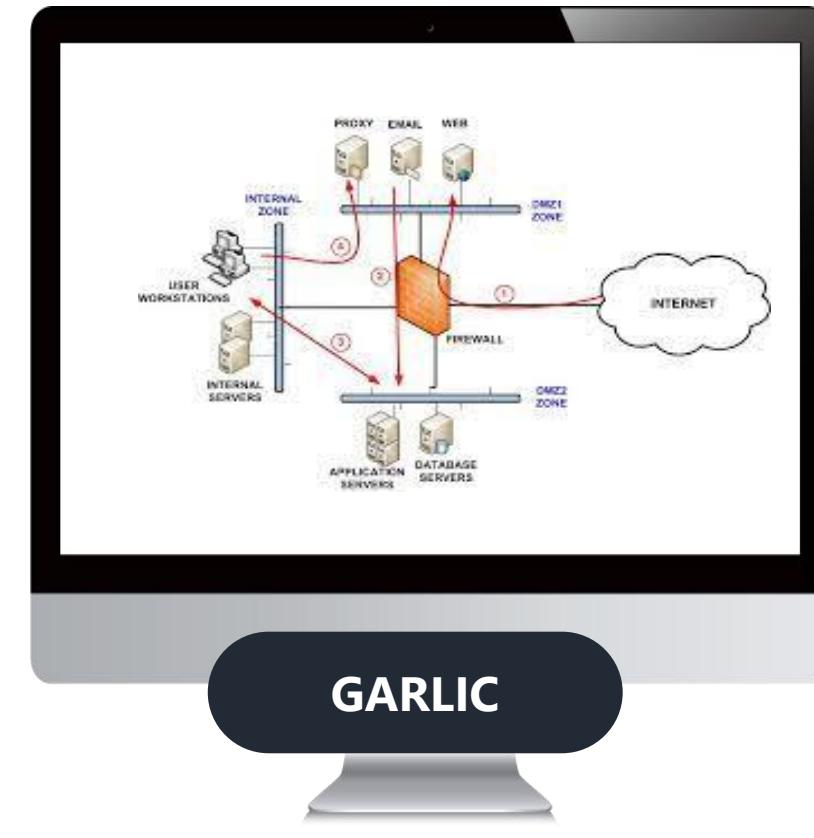
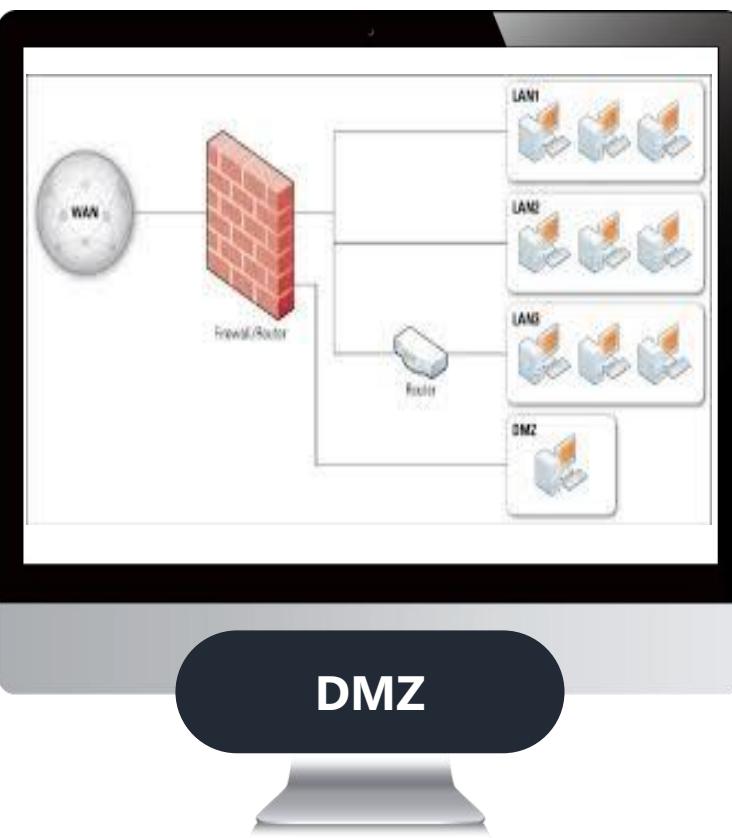
Ускуна тармоқларааро экранни дастурий тармоқларааро экранида мавжуд бўлмаган қўшимча ҳимоя воситаларини тақдим этади.

## Home Users and Firewalls

**Заарали тармоқ тажовузкорлари одатда уй фойдаланувчиларини нишонга олишади, чунки 65 фоиздан ортиқ уйлар ҳеч қандай тармоқларааро экрандан фойдаланмайди**

# Имтиёзли ҳудудлар

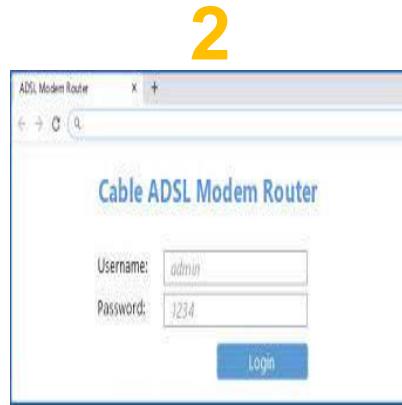
Тармоқлараро экран асосан унчалик ишончли бўлмаган WAN ва ишончли LAN ўртасида тўсиқ яратади. Битта тармоқлараро экран иккита имтиёзли зонани белгилайди. Ташкилот ичида кўпинча турли даражадаги ишонч мавжуд. Булар сегментланган топологиядан фойдаланган ҳолда физик сатҳда аниқ белгиланиши мумкин: ҳар бир ишонч даражасини сегментлаштирадиган қатор зоналар ҳосил қилиниши мумкин.



# Тармокларни улаш ва ундаги заифликлар

## Static Connections

### Modem Risks



### Modem Authentication Credentials



## Dynamic Connections

4



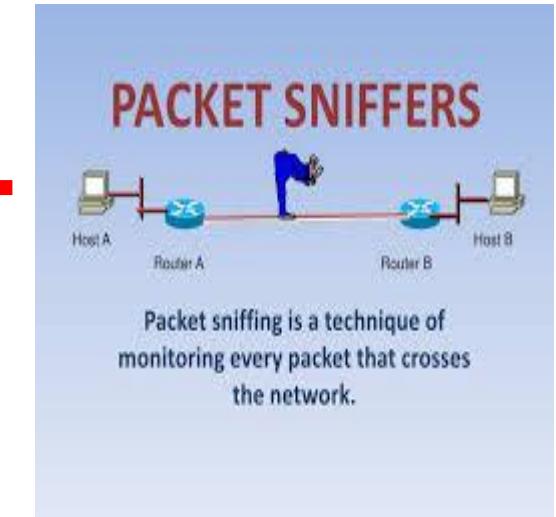
### Creating Secure Dynamic Connections



### Automated Callback

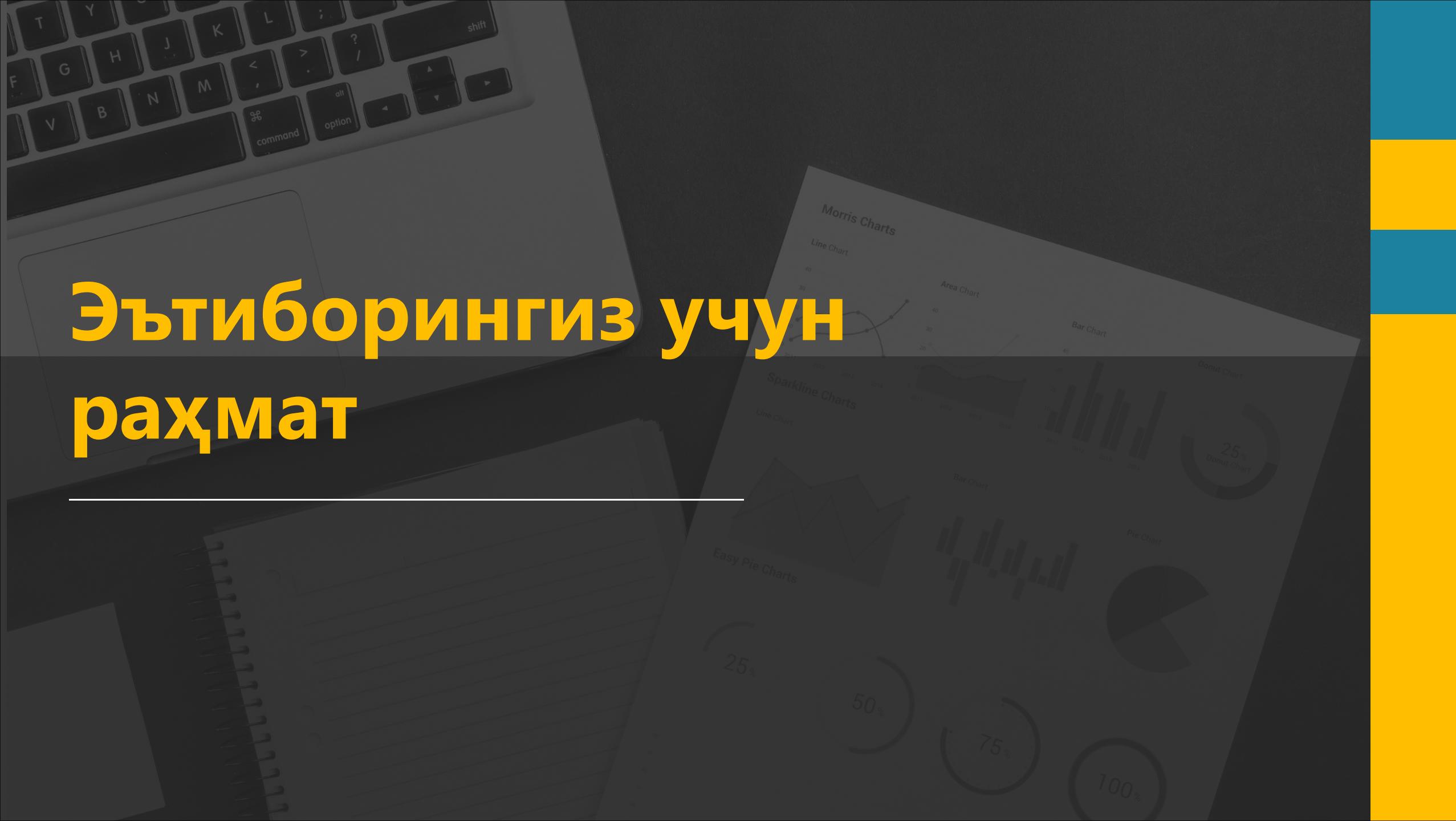


# Симсиз тармок протоколларининг хавфсизлик таҳлили



# Эътиборингиз учун раҳмат

---



# Тармоқ хавфсизлиги

---

Физик сатҳда компьютер тармоғини ҳимоялаш

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

# Физик сатҳ



OSI модели физик сатҳдан бошланади. Бунга физик тармоқ оммавий ахборот воситалари, тармоқ карталари (NIC) ва NICни бошқариш учун операцион тизим драйверлари киради. Ушбу қатламни бошқа барча

OSI қатламларидан ажратиб турадиган нарса - бу жисмоний мавжудлик; бошқа барча қатламлар виртуал. Жисмоний муҳит тури ва тармоқ тартиби (топология) тармоқнинг физик хавфсизлигини белгилайди.



OSI физик қатлами битта мақсадга эга: жисмоний канал орқали тўғридан-тўғри жисмоний оммавий ахборот воситалари билан алоқа қилиш. Ушбу алоқа физик алоқани ўрнатишни, маълумотни канал орқали узатишни ва маълумотни канал орқали олишни ўз ичига олади

- 7 - Application - A
- 6 - Presentation - Person
- 5 - Session - Sent
- 4 - Transport - Through
- 3 - Network - Network
- 2 - Data Link - Data
- 1 - Physical - Packets

- Physical - Please
- Data Link - Do
- Network - Not
- Transport - Throw
- Session - Sausage
- Presentation - Pizza
- Application - Away

# Физик сатҳда маълумотлар оқими

Физик сатҳи орқали умумий маълумотлар оқими маълумотларни узатиш ва қабул қилишнинг беш босқичли жараёни сифатида намоён бўлади.

Жисмоний қурилма драйвери жисмоний канал орқали маълумотларни узатиш учун тармоқ картасидан фойдаланади.

2



Маълумотлар қабул қилувчининг физик қурилмаси драйверига узатилади

Қабул қилиш тизимидағи тармоқ картаси маълумотларни қабул қиласди.

Жисмоний қурилма драйвери маълумотларни қайта ишлаш учун юқори даражадаги OSI катламларига узатади.

# Физик муҳитнинг турлари

Физик муҳит - бу маълумотларни юбориш ва қабул қилиш учун ҳамма нарсани, Маълумот сигнализацияси электр кучланиш, радиочастота (частота) ва ёруғликнинг модуляциясини ўз ичига олади.



# Физик тармоқ компонентлари

Физик қатlam маълумотлар узатувчи ва қабул қилувчи тармоқ таркибий қисмларидан иборат.

T A R M O Q T U G U N I

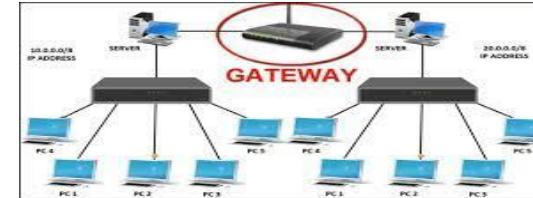
Компьютер



Кўприк



Шлюз



Маршрутизатор



Комутатор



Улагич

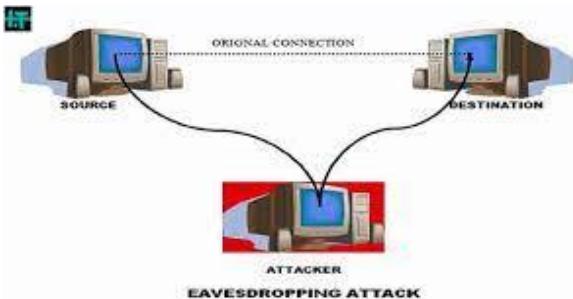


Репитер

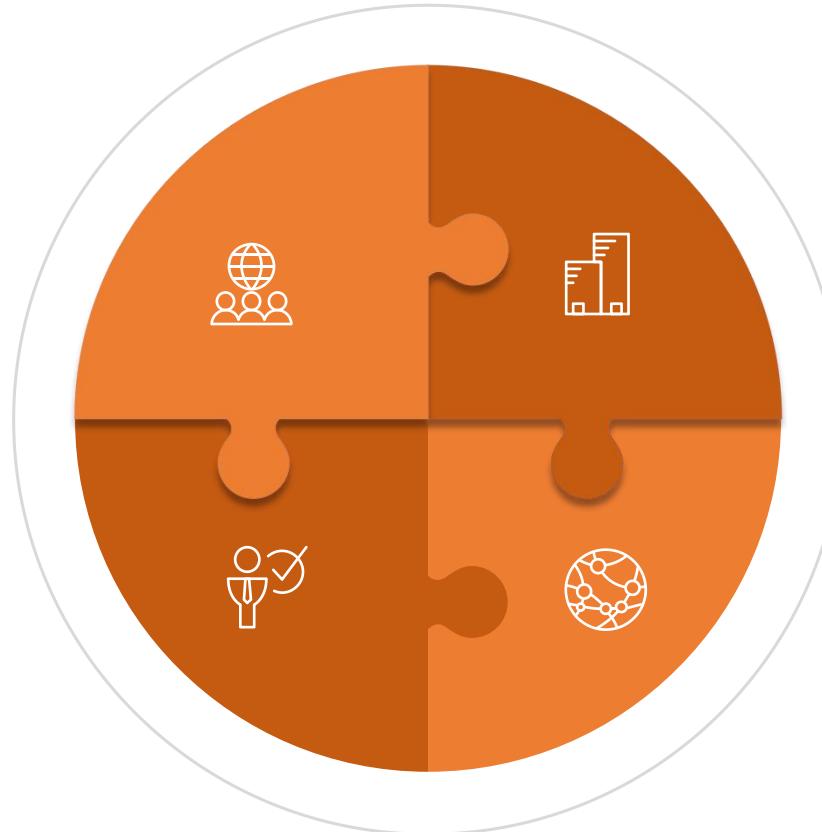
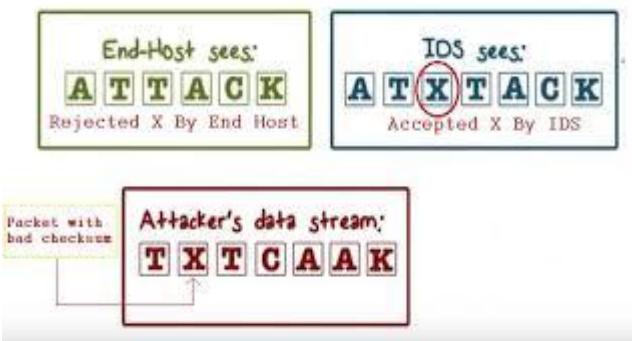


# Физик сатх хавф-хатарлари

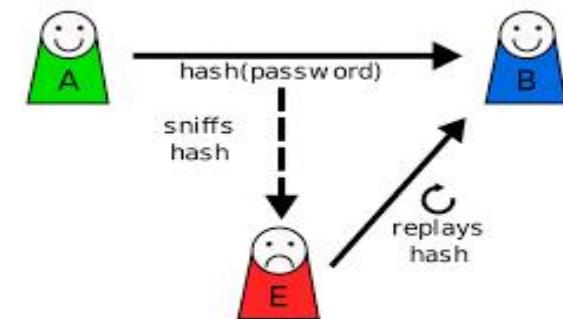
## Eavesdropping



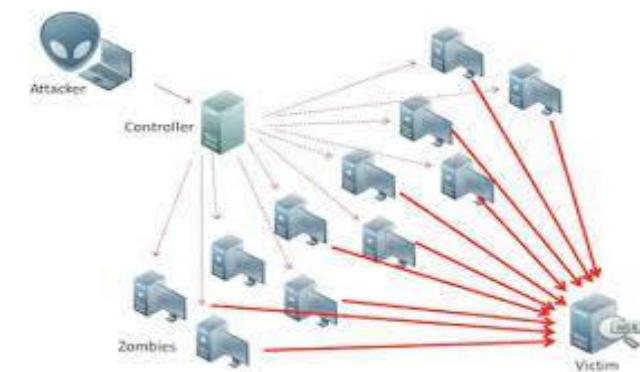
## Insertion



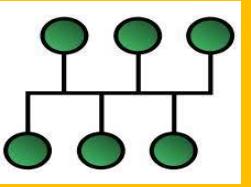
## Replay



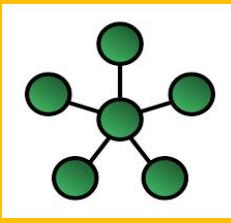
## Denial of Service (DoS)



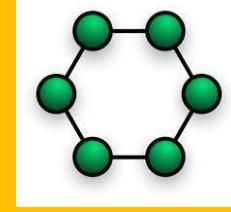
# Тармоқ топологиялари



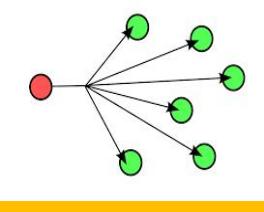
**Шина**  
топологияси  
барча түгунларни  
ўз ичига олган  
битта алоқа  
каналидан  
иборат



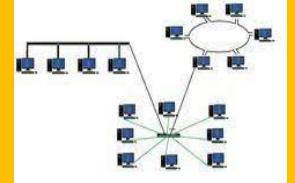
**Юлдуз**  
топологияси  
түгунлар билан  
алоқа қилиш учун  
марказий  
қурилмага  
эга



**Халқа**  
топологияси  
марказий  
қурилмани  
тармоқнинг  
марказидан ҳар  
бир түгунга  
кўчиради.



**Broadcast**  
топологияси  
маълумотлар бир  
нуқтадан бир  
нуқтага емас,  
балки  
радиочастоталар  
орқали  
узатилганда  
ишлатилади.

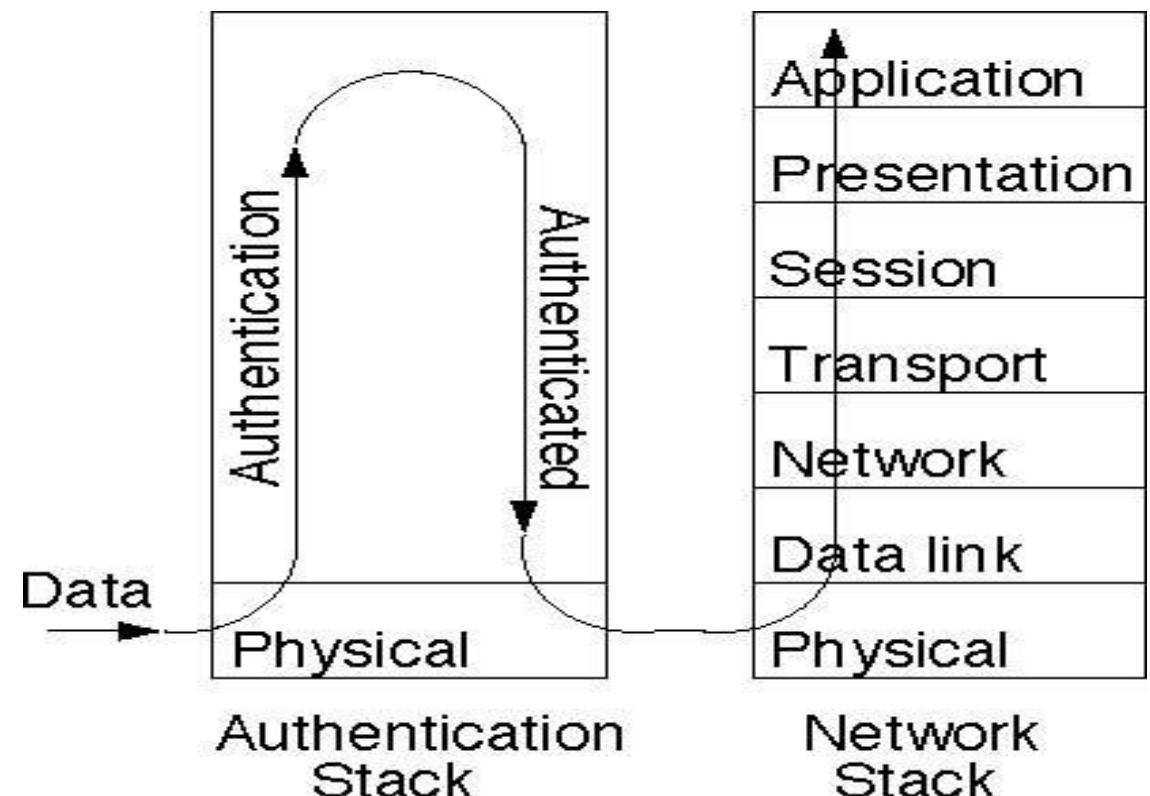


**Гибрид**  
топология бир  
нечта тармоқ  
архитектураларини  
афзалликларнинг  
комбинациясини  
таъминлаш учун  
бирлаштиради.

# ФИЗИК САТХ ХАВФИЗЛИГИ

Күпгина физик сатх протоколлари аутентификация қилиш учун юқори сатхлар билан чамбарчас боғлиқ. Бунга мисол қилиб диалуп линиялар ва симсиз тармоқларни көлтириш мүмкін. Диалуп тармоқ тез-тез фойдаланувчини тасдиқлаш учун PPP ёки SLIP (2-даражали протоколлар) га таянади. Худди шундай, симсиз тармоқ мижозларнинг ҳақиқийлигини текшириш учун Wired Equivalent Privacy (WEP) протоколи ва MAC манзилини филтрлашдан фойдаланади.

Тармоқни аутентификация қилиш түплами намунаси.



# Тармоқ муаммоларини аниқлаш



Физик сатх ҳужумининг манбасини аниқлаш қобилияти тармоқ муҳити ва конфигурациясига боғлиқ. Шина топологиясида ҳар бир тугун шинанинг бошқа барча тугунлари томонидан қабул қилинган сигнални ҳосил қиласди. Ушбу конфигурацияда тармоқ муаммоси манбасини аниқлаш жуда қийин бўлиши мумкин. Бундан фарқли ўлароқ, юлдуз топологияда бузилган тугунни қидиришни тезда марказнинг маълум бир портига қисқартириши мумкин; агар портдан фойдаланадиган битта тугун бўлса, у ҳолда портни осонгина аниқлаш мумкин.

Симсиз тармоқ узилишларини аниқлаш катта тармоқдаги номаълум тугунга қараганда анча қийинроқ бўлиши мумкин. Умуман олганда, физик сатҳдаги муаммоларни маҳсус воситаларсиз осонгина аниқлаш мумкин емас.



**BUS**



**RING**

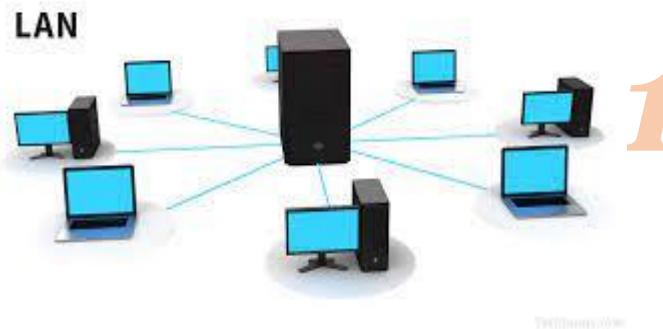


**Small networks**



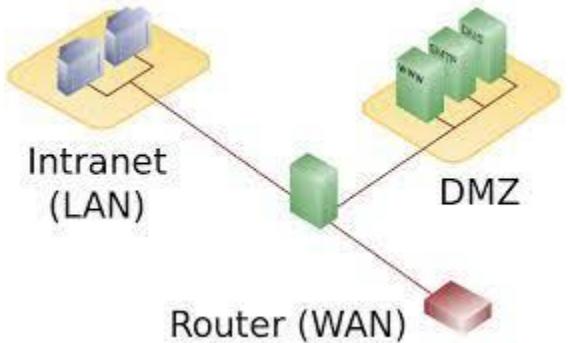
# Физик LAN

LAN



1

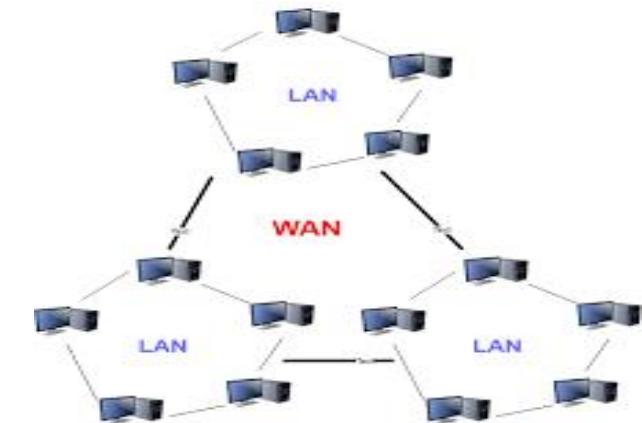
DMZ



3

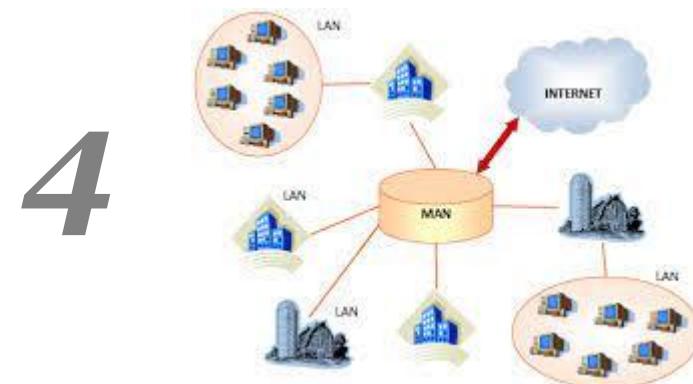


WAN



2

MAN



4

# Хұжум турлари

Симли тармоқлар учун асосий таҳдидлар бузилиш, шовқин, ҳидлаш, такрорлаш ва қўшилиш ҳұжумларидан иборат.

**Disruption**

Тармоқ сегментидаги тез-тез учрайдиган узилишларга електр узилиши ва узилган тармоқ кабеллари киради. Юмшатилиш усуллари одатда захира қувват манбаларини ва асосий тармоқ қурилмаларига чекланган киришни ўз ичига олади.

**Interference**

Тармоқ трафигини узатиш учун ишлатиладиган восита бошқа сигналларни ҳам узатиши мүмкін. Агар воситага рухсациз сигнал (шовқин) кирса, у ҳолда тармоқ қурилмалари маълумотларни шовқиндан ажратадилар. Маълумотларни кодлаш техникаси таъсирни шовқинлардан юмшата олади.

**Intentional Attacks**

*Sniffing, replay* ва *insertion* ҳұжумларидан таҳдидлар қасдан қилинган ҳұжум турларига киради.

# Тармоқларааро экран (Firewall)

Тармоқларааро экран - бу тармоқ сегментлари ўртасида ўтиши билан тармоқ трафигини филтрлайдиган ва маълум тармоқ протоколлари асосида ҳимояни таъминлайдигам тизим тури. Тармоқларааро экран биринчи навбатда OSI нинг қуийи сатҳлари билан боғлиқ: физик, канал, тармоқ ва транспорт сатҳи. Тармоқ трафигини филтрлашга асосланган ҳар қандай ҳужумларни камайтириш усуллари тармоқларааро экранда амалга ошириш мумкин.

## Software Firewalls

**Дастурий тармоқларааро экран тармоқ филтрини тўғридан-тўғри тармоқ дастурлари ишлайдиган компьютерга жойлаштиради.**

## Hardware Firewalls

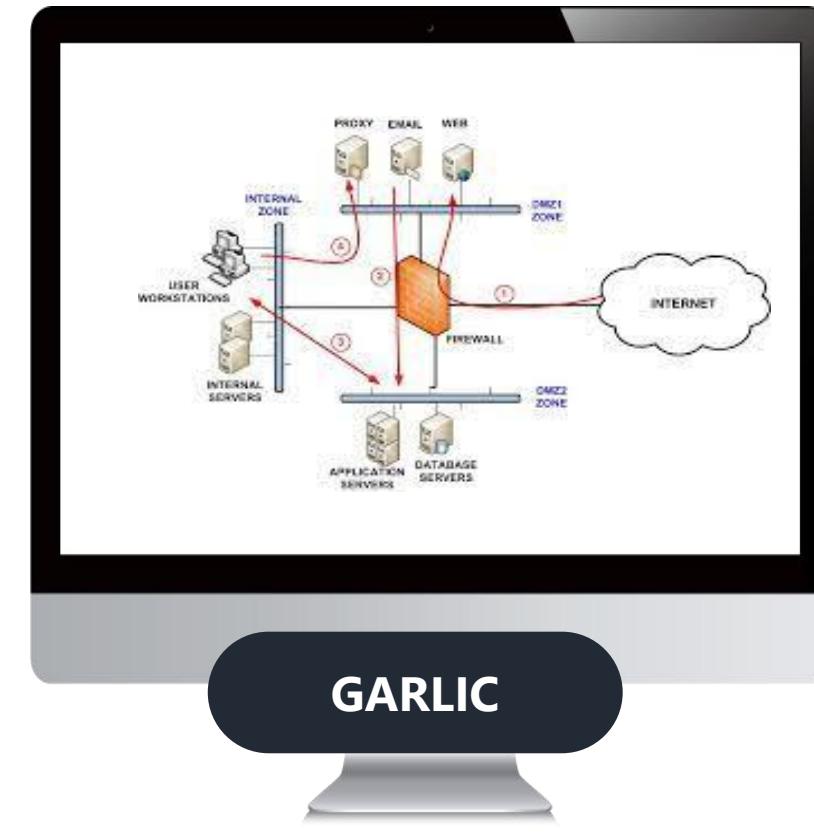
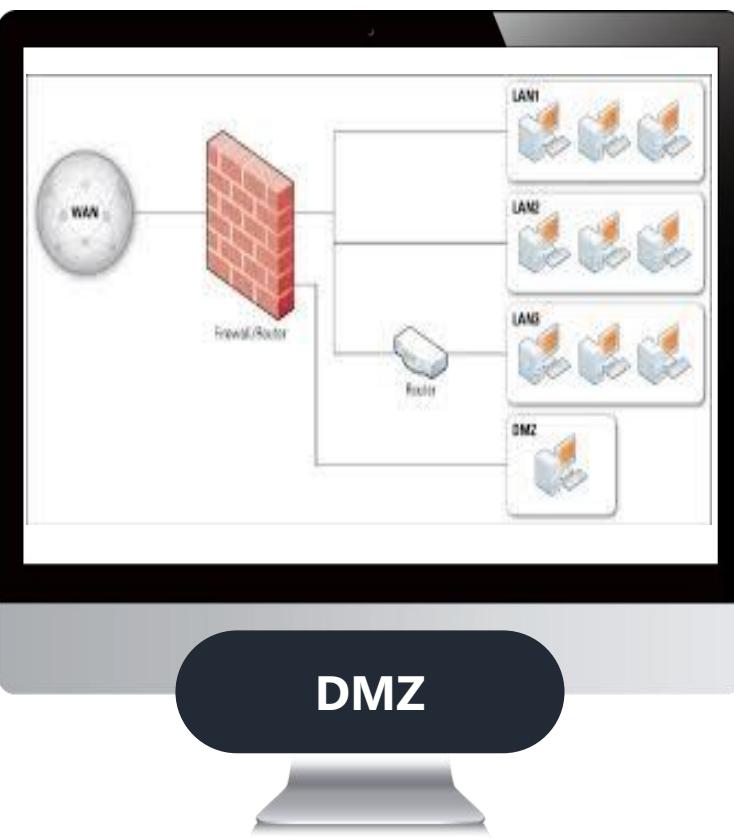
Ускуна тармоқларааро экранни дастурий тармоқларааро экранида мавжуд бўлмаган қўшимча ҳимоя воситаларини тақдим этади.

## Home Users and Firewalls

**Заарали тармоқ тажовузкорлари одатда уй фойдаланувчиларини нишонга олишади, чунки 65 фоиздан ортиқ уйлар ҳеч қандай тармоқларааро экрандан фойдаланмайди**

# Имтиёзли ҳудудлар

Тармоқлараро экран асосан унчалик ишончли бўлмаган WAN ва ишончли LAN ўртасида тўсиқ яратади. Битта тармоқлараро экран иккита имтиёзли зонани белгилайди. Ташкилот ичида кўпинча турли даражадаги ишонч мавжуд. Булар сегментланган топологиядан фойдаланган ҳолда физик сатҳда аниқ белгиланиши мумкин: ҳар бир ишонч даражасини сегментлаштирадиган қатор зоналар ҳосил қилиниши мумкин.



DMZ

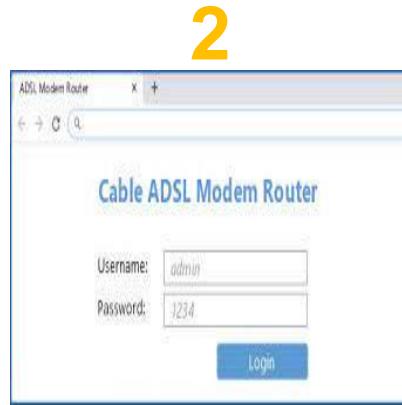
ONION

GARLIC

# Тармокларни улаш ва ундаги заифликлар

## Static Connections

### Modem Risks



### Modem Authentication Credentials



## Dynamic Connections

4



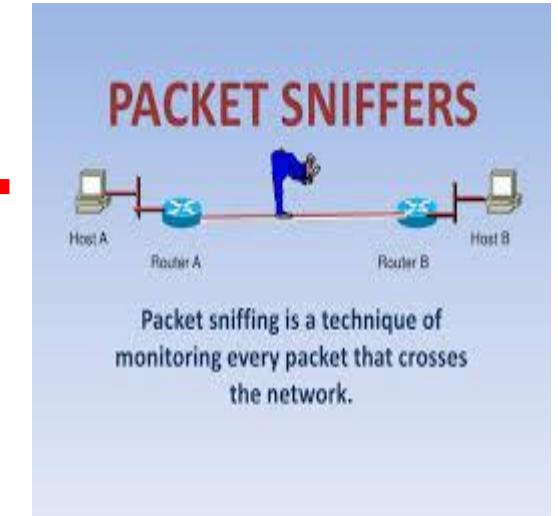
### Creating Secure Dynamic Connections



### Automated Callback

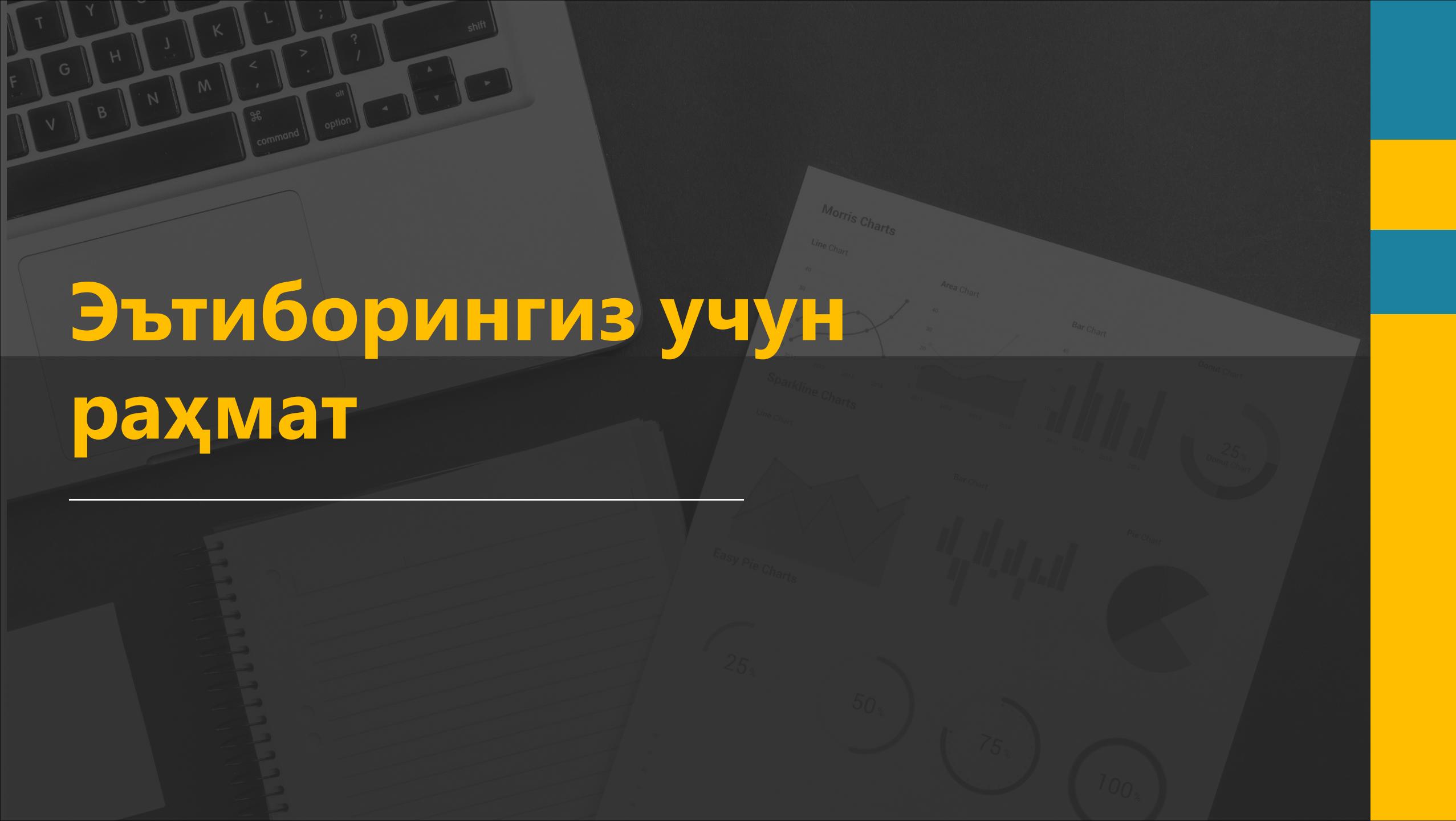


# Симсиз тармок протоколларининг хавфсизлик таҳлили



# Эътиборингиз учун раҳмат

---



# Тармоқ хавфсизлиги

Kompyuter tarmoqlariga masofaviy hujumlar



+998 71 238 6525



@tarmoq\_xavfsizligi



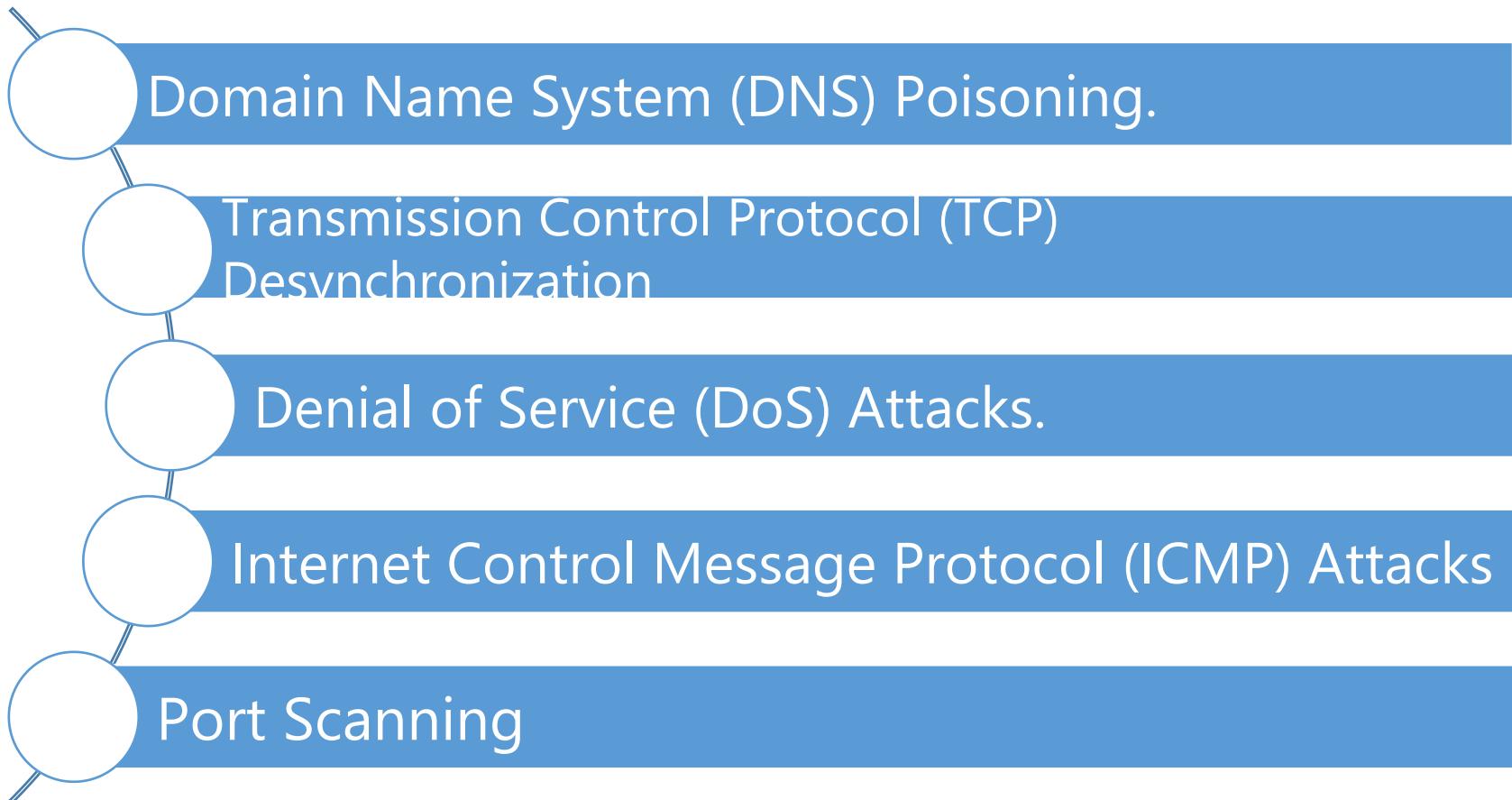
[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

# Reja



# Hujumchilarning motivlari

Mafkura

Hactivism  
Kiberterrorizm

Suruval  
oazonish

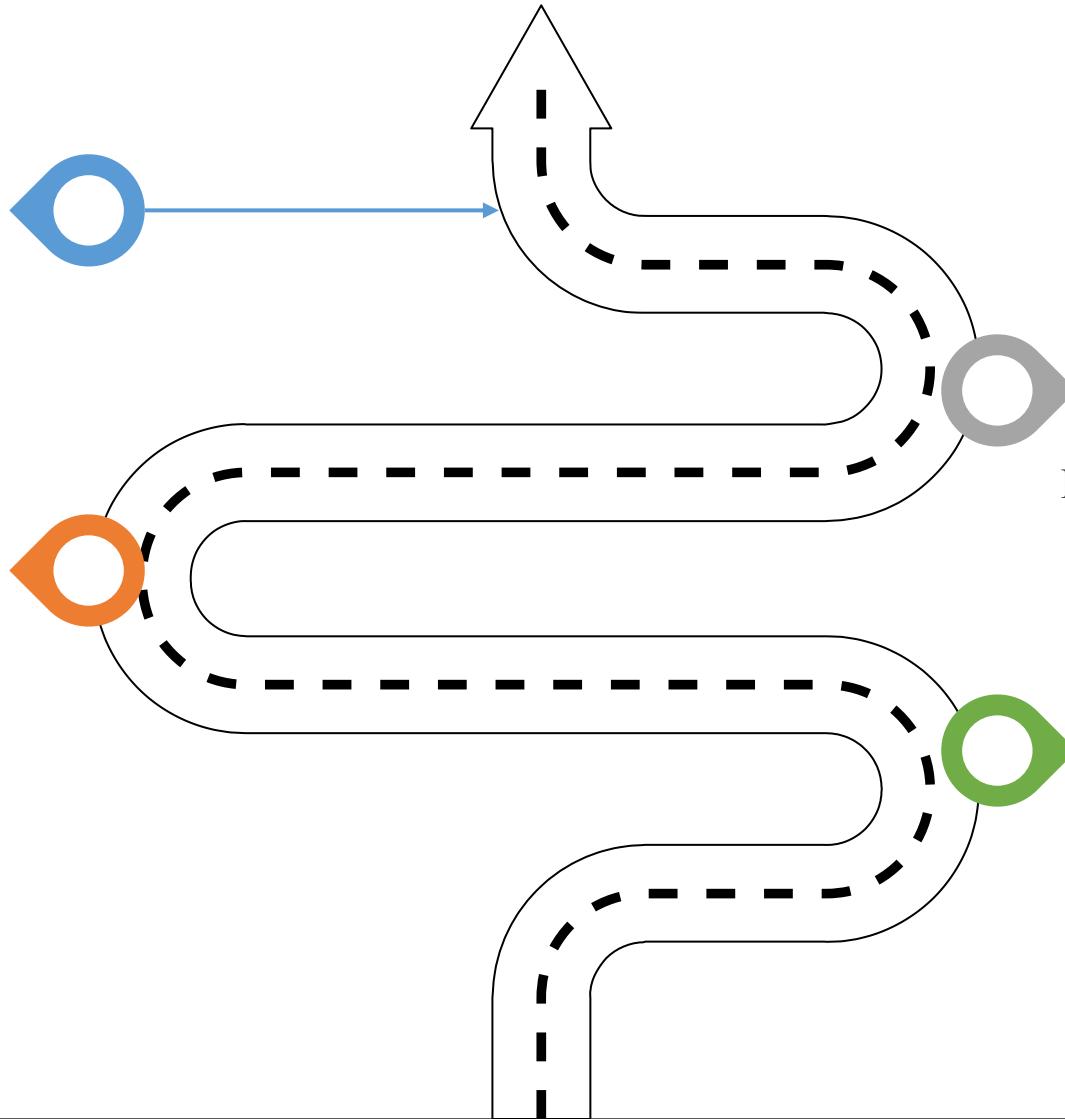
Ular tan olinishni  
xohlashadi

FAT /  
Josuslik

Moliyaviy daromad olish, Boshqa  
davlatga josuslik qilish

Kuch-  
Qudrat

Muvaffaqiyatli hujumlar  
ularga kuch hissini beradi



# Hujumchilarning motivlari

## 1) Kuch-Qudrat uchun hujum

- Ba'zilar go'yoki yengib bo'lmaydigan narsalarni mag'lub etish uchun intellektual qiyinchiliklardan zavqlanishadi
- Muvaffaqiyatli hujumlar ularga kuch hissini beradi

## 2) Shon-sharaf uchun hujum

- Ba'zilar faqat sinovdan qoniqmaydilar
- Ular tan olinishni xohlashadi - hatto taxallus bilan bo'lsa ham (OAVda taxallusini ko'rishdan zavqlanishadi)

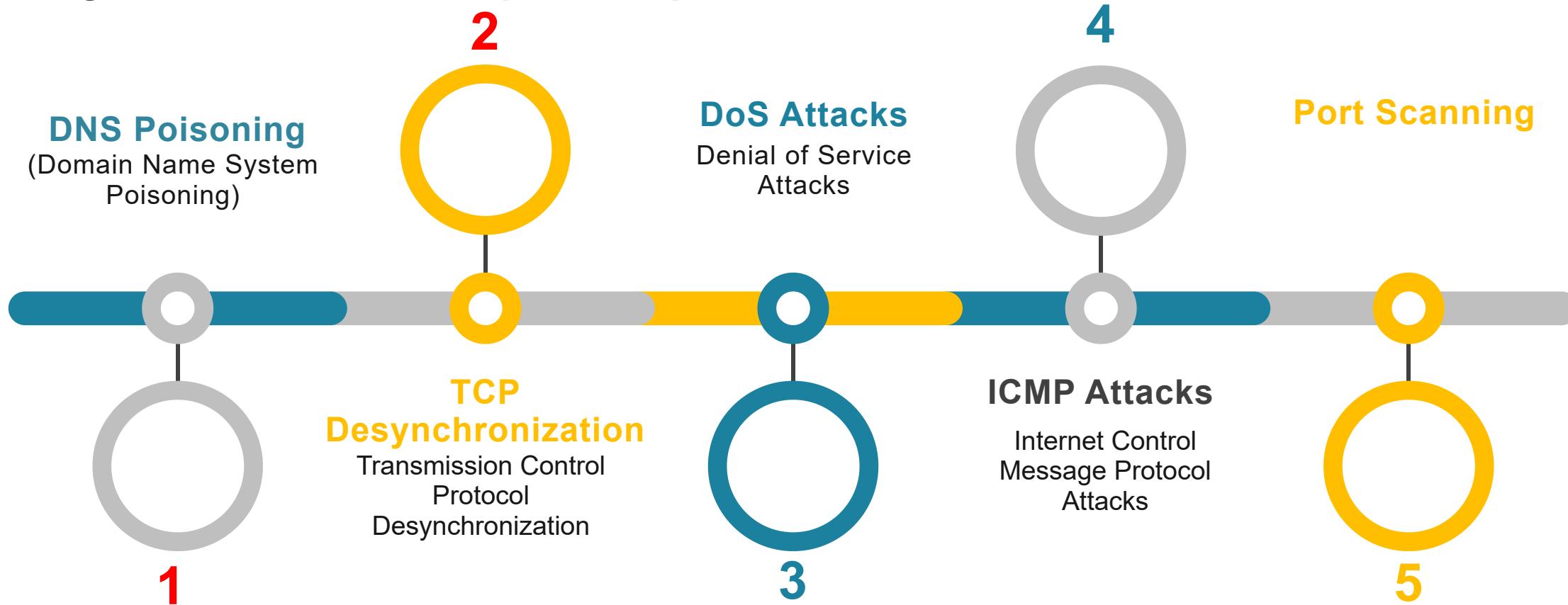
## 3) Pul / josuslik uchun hujum

- To'g'ridan-to'g'ri moliyaviy daromad olish uchun hujum qilish
- O'z mamlakatining raqobatbardoshligini oshirishga harakat qilish
- Ba'zi mamlakatlar o'z sanoatlariga yordam berish uchun sanoat josligrini qo'llab-quvvatlaydi
- Boshqa davlatga josuslik qilish/zarar keltirish uchun hujum qilish (sirlarni o'g'irlash, mudofaa infratuzilmasiga zarar yetkazish va h.k.)

## 4) Mafkurani targ'ib qilish uchun hujum

- Mafkuraviy hujumlarning ikki turi:
  - Hactivism (siyosiy yoki ijtimoiy o'zgarishlarni ilgari surish uchun hakerlik amaliyoti)
  - Kiberterrorizm (insonlarni o'limi, jiddiy iqtisodiy zarar)

**Masofaviy hujum** - bu bitta yoki kompyuter tarmog'iga qaratilgan zararli harakat. Masofaviy hujum tajovuzkor foydalanayotgan kompyuterga ta'sir qilmaydi. Buning o'rniغا, tajovuzkor kompyuter yoki tarmoqning xavfsizlik dasturlarida kompyuter yoki tizimga kirish uchun zaif nuqtalarni topadi.



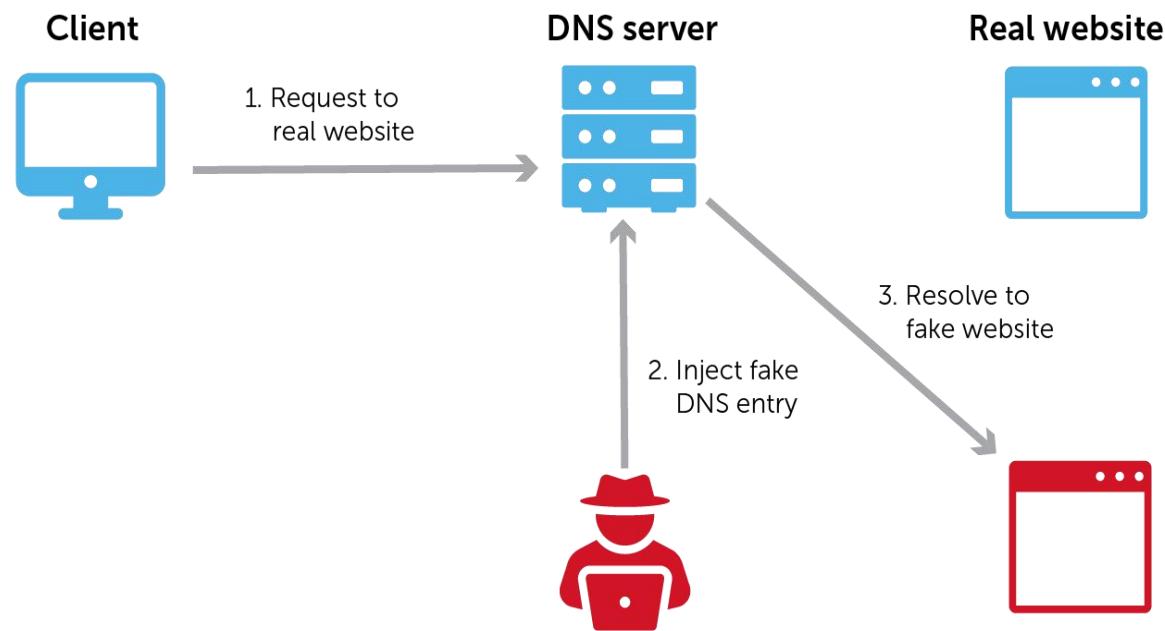


## DNS Poisoning

Bunda DNS-serverni soxta ma'lumotlarni haqiqiy va domen egasidan olingan deb qabul qilish uchun aldaydi. Noto'g'ri ma'lumotlar ma'lum vaqt davomida saqlanadi, bu esa tajovuzkorga domenlar manzillarini so'ragan kompyuterlarga DNS javoblarini o'zgartirish imkonini beradi.

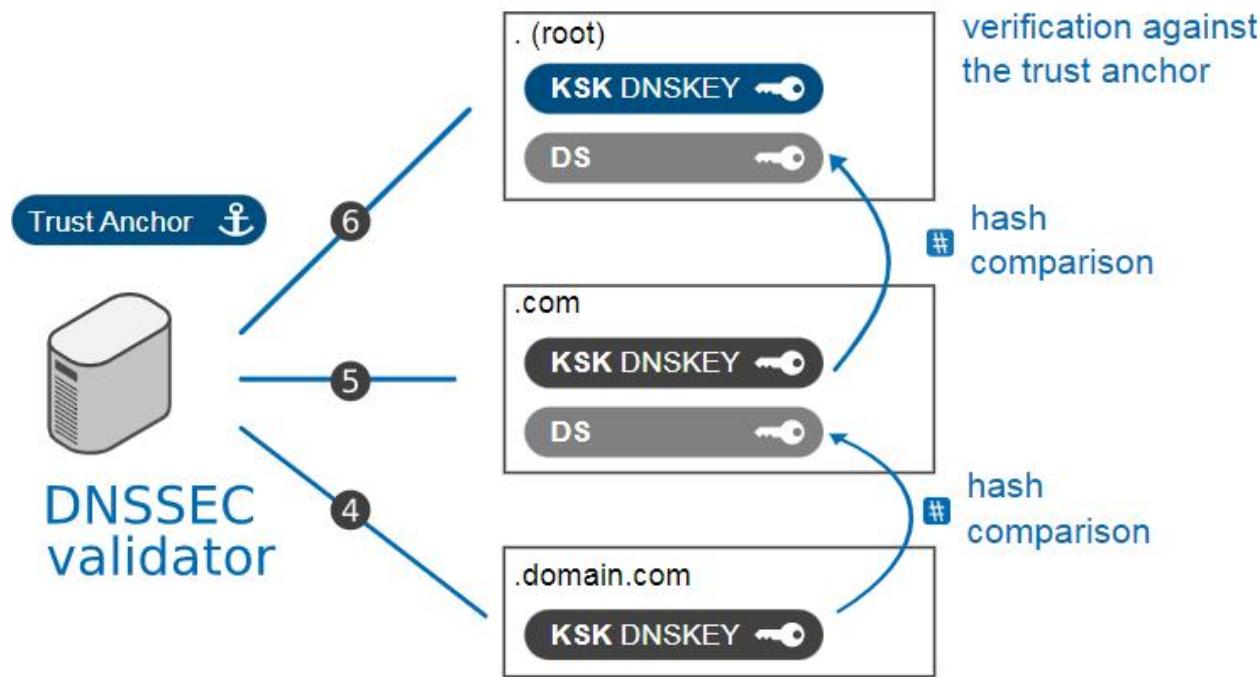
Zaharlangan DNS serverlariga kirgan foydalanuvchilar veb-saytlarga yo'naltiriladi, ular o'zlari mo'ljallangan asl kontentdan ko'ra bilmasdan viruslar va boshqa zararli kontentni yuklab oladilar..

## DNS poisoning



# DNS Poisoning ga qarshi kurashish

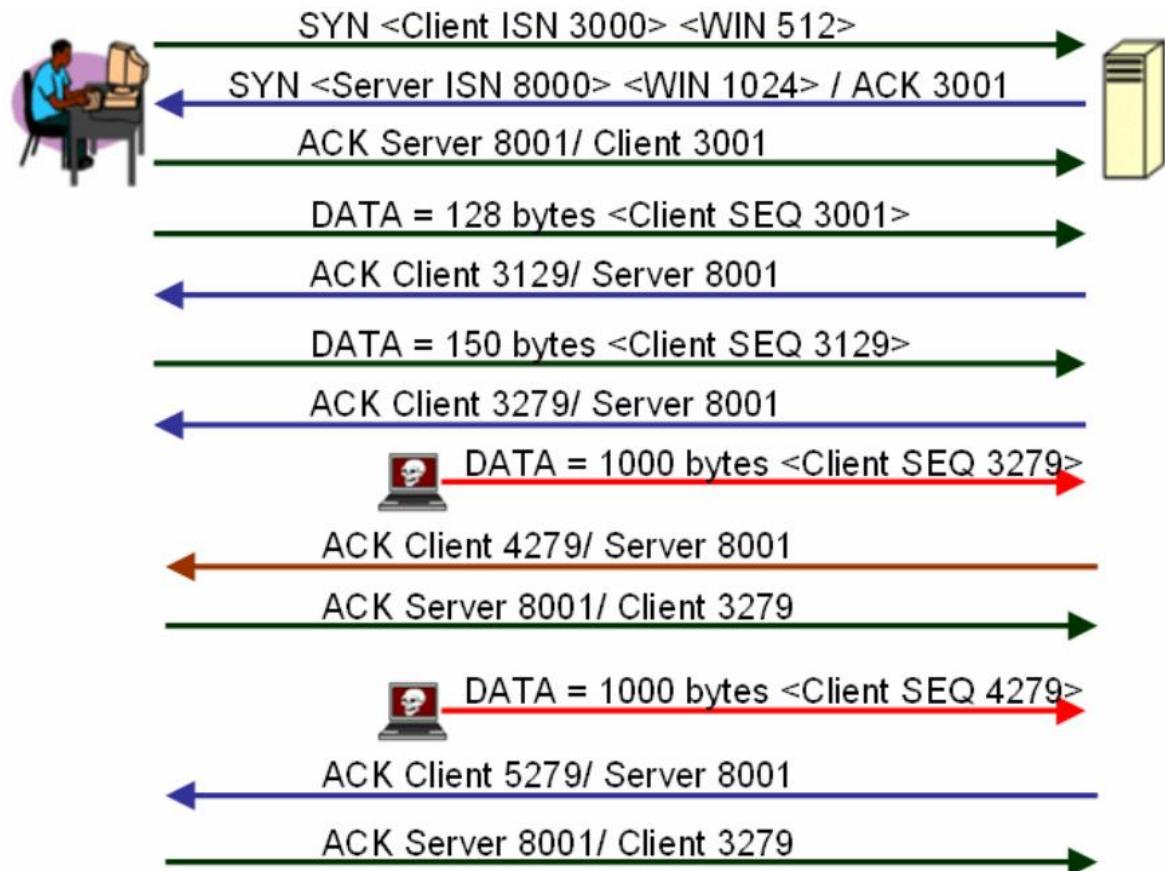
Internet Protocol (IP) tarmoqlarida domen nomlari tizimida (DNS) almashinadigan ma'lumotlarni xavfsizligini ta'minlash uchun Internet Engineering Task Force (IETF) tomonidan kengaytirilgan spetsifikatsiyalar to'plamidir. Protokol ma'lumotlarning kriptografik autentifikatsiyasini, mavjudligini rad etishning haqiqiyligini va ma'lumotlar yaxlitligini ta'minlaydi, ammo mavjudligi yoki maxfiyligini ta'minlamaydi..





## TCP Desynchronization

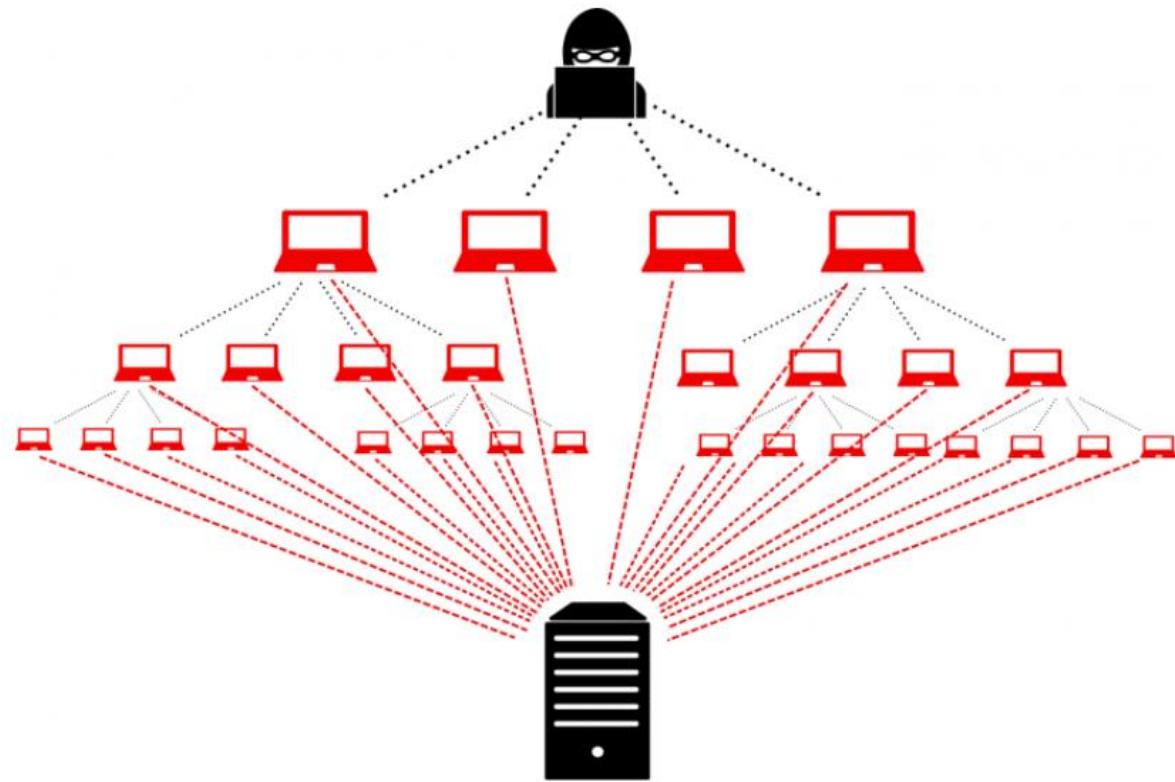
Bu ma'lumotlar paketlarining kutilayotgan soni haqiqiy sondan farq qilganda ishga tushadi. Kutilmagan paketlar tugatiladi. Xaker kerakli paketlarni aniq ketma-ket raqam bilan ta'minlaydi. Maqsadli tizim paketlarni qabul qiladi va xaker peer-to-peer yoki server-mijoz aloqlariga xalaqit bera oladi.





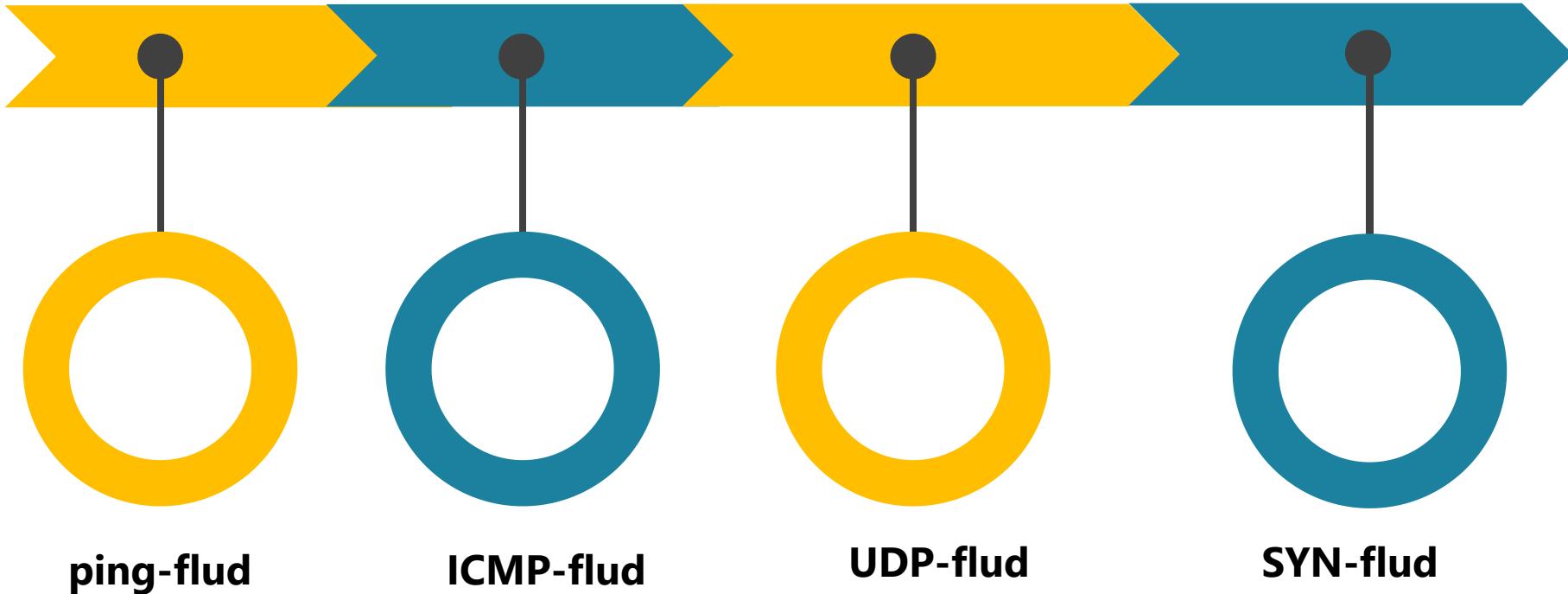
## DOS

. Server, kompyuter yoki tarmoqni foydalanuvchilari va mijozlari uchun soxta mijoz so'rovlar bilan to'ldirib, foydalanishning katta sur'atini taqlid qiladigan usul. Bu foydalanuvchilar o'rtaqidagi aloqaga to'sqinlik qiladi, chunki server ko'p miqdorda kutilayotgan so'rovlar bilan band bo'lib qoladi.



DDoS attack creation

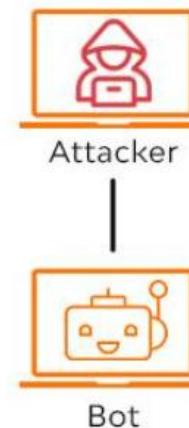
# DoS-hujumlar klassifikatsiyasi



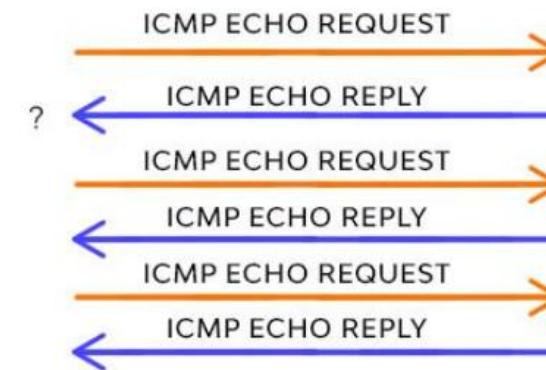


## ICMP-hujum

Tarmoqqa ulagan kompyuterlar tomonidan xatolarni tekshirish xabarlarini yuborish uchun foydalaniladigan Internet protokoli. ICMP autentifikatsiyani talab qilmaydi, ya'ni tajovuzkor ushbu zaiflikdan foydalanishi va DoS hujumlarini boshlashi mumkin.



## ICMP (Ping) Flood attack



## Port skaneri - IP manzil bilan ko'rsatilgan portni skanerlash dasturi



01

Standard ports/services running and responding

-ports: 80-HTTP,  
25-

02

Nishondagi tizimda  
o'rnatilgan OT

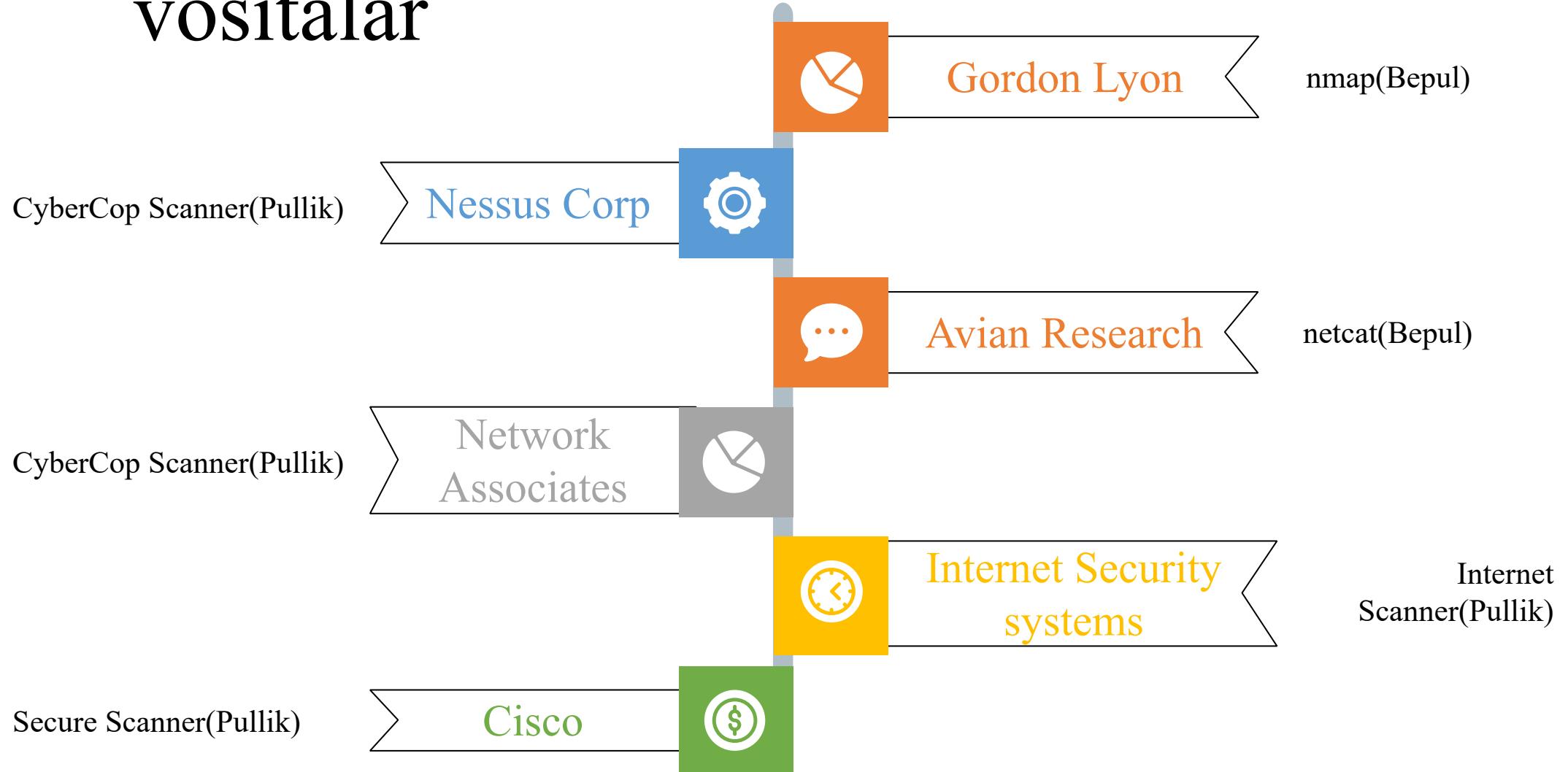
03

Nishondagi tizimda o'rnatilgan  
llovalar va llova versiyalari  
ma'lumotlari

Misol: **nmap**

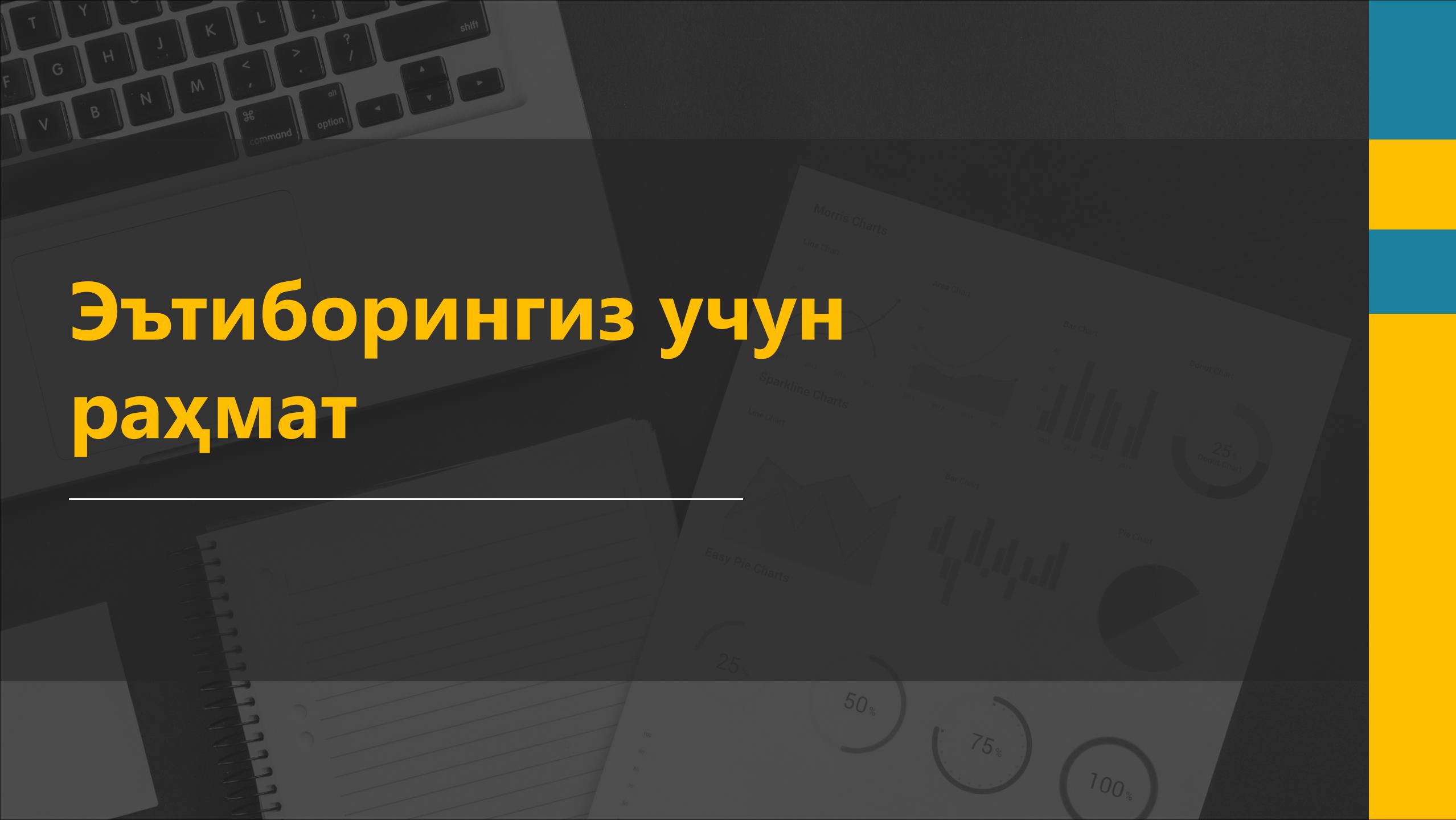
- **nmap -sP 192.168.100.\***
  - Tezkor amalga oshiriladi (20-30 s) ping scan („P”)
  - “wild card” haqida ma'lumot beradi
- **nmap -sT 192.168.100.102**
  - Sekin amalga oshiriladi (~10 min.) TCP port scan („T”)

# Port skannerlovchi vositalar



# Эътиборингиз учун раҳмат

---



# Virtual xususiy tarmoq (VPN)



# REJA



01

➤VPN tarmog`ining paydo bo`lishi,  
tushunchasi va uning turlari

02

➤VPN tarmoqlari va uning  
klassifikatsiyasi

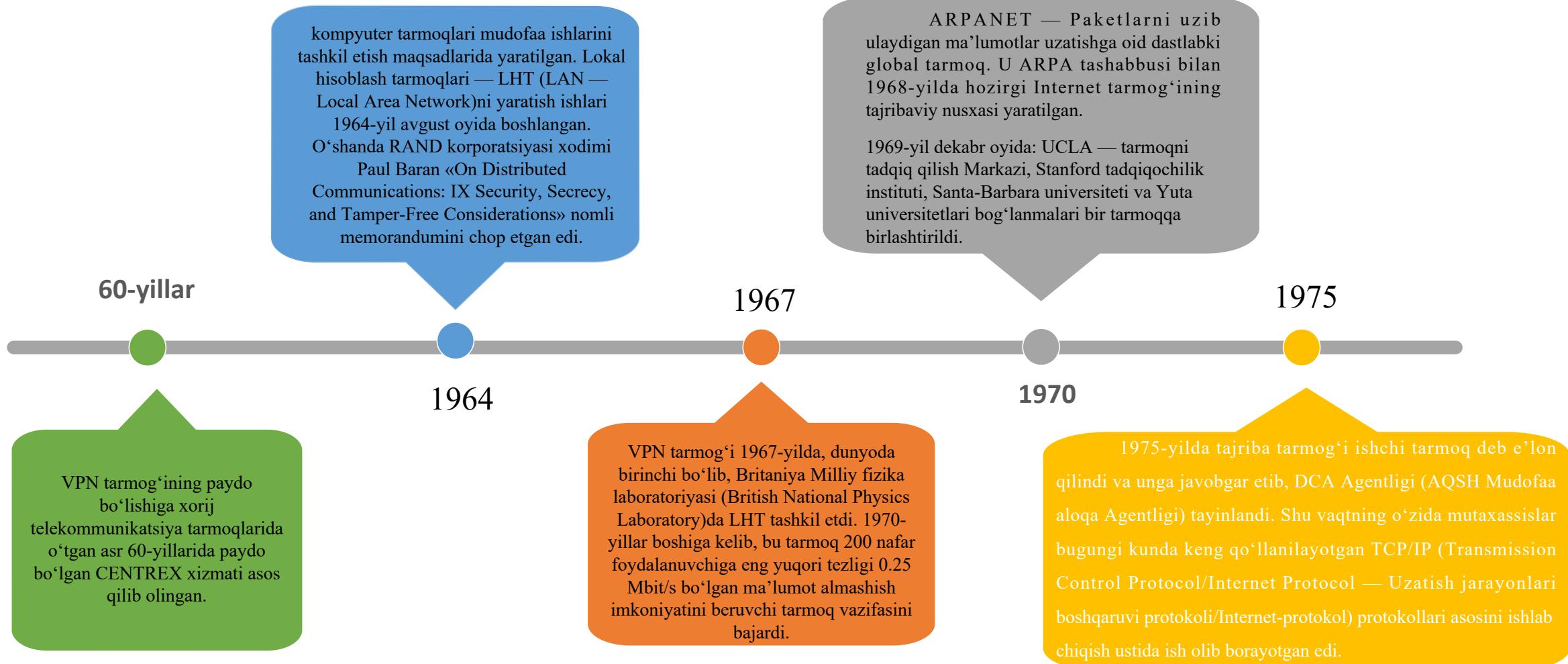
03

➤VPN tarmoq qurishning asosiy  
turlari



VPN  
tarmog`ining  
paydo bo`lishi,  
tushunchasi va  
turlari

# VPN tarmog‘ining paydo bo‘lishi



# VPN tushunchasi mazmuni.



1/

VPN (Virtual Private Network — virtual xususiy tarmoq) — mantiqiy tarmoq bo‘lib, o‘zidan yuqoridagi boshqa tarmoq, masalan, Internet asosida quriladi.



2/

Bu tarmoqda kommunikatsiyalarda umumiyl xavfsiz bo‘lmasan tarmoq protokollaridan foydalanimishiga qaramay, shifrlashdan foydalangan holda, axborot almashinishda begonalarga berk bo‘lgan kanallar tashkil qilinadi.



3/

VPN tashkilotning bir necha ofislarini ular o‘rtasida nazorat qilinmaydigan kanallardan foydalangan holda, yagona tarmoqqa birlashtirish imkonini beradi.

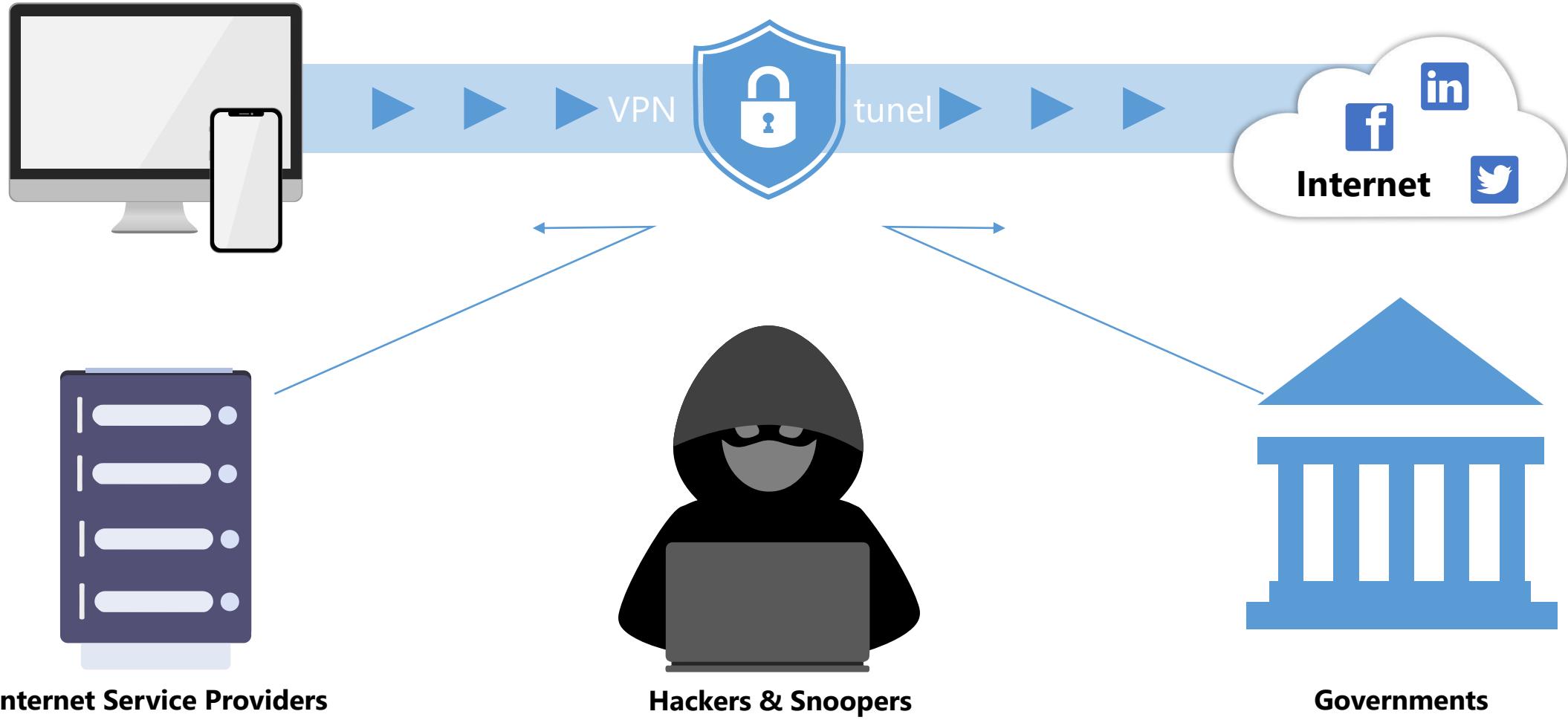


4/

O‘z navbatida, VPN alohida tarmoq xususiyatlarini qamrab olgan, lekin bu tarmoq umumiyl foydalanimish tarmog‘i, masalan, Internet orqali amalga oshiriladi.

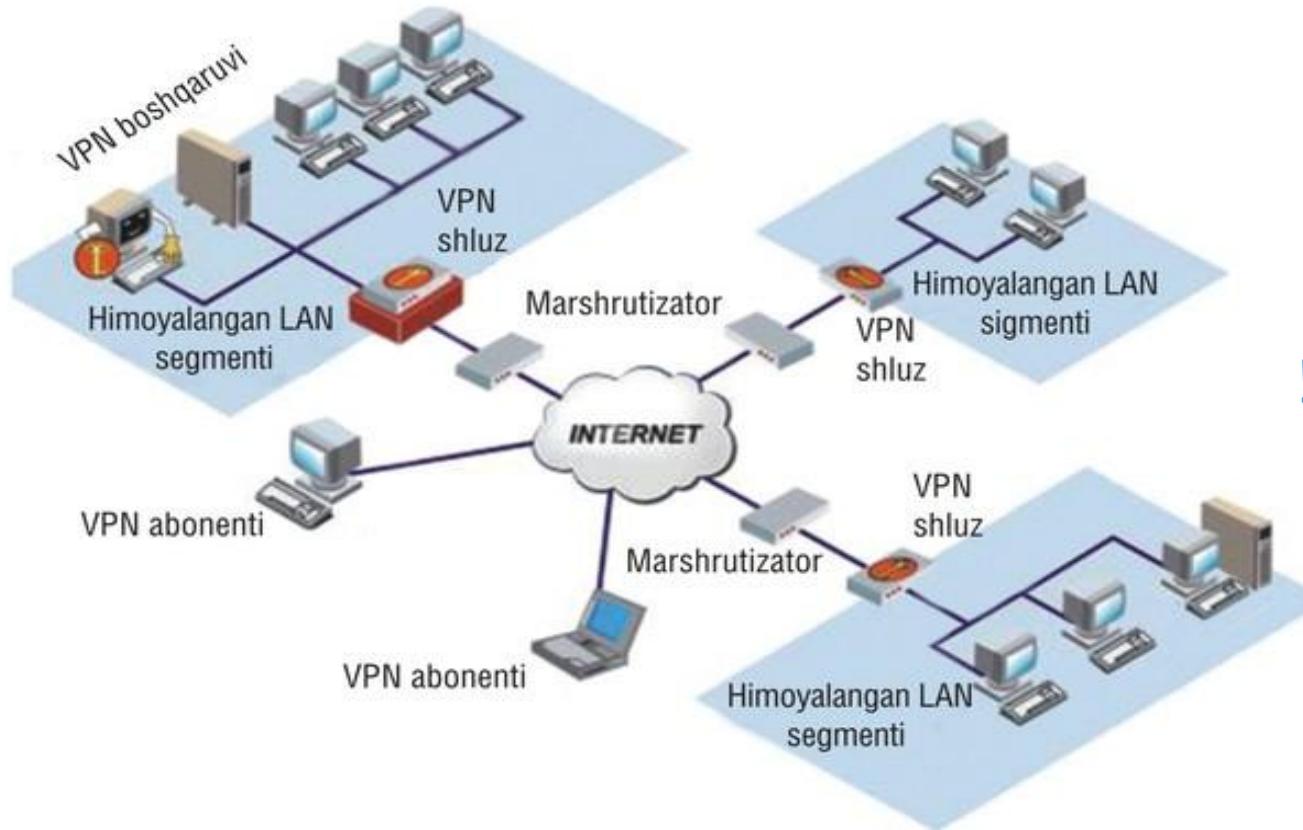


# VPN



# SHUNDAY QILIB, VPN — BU:

- ! kriptografiyaga asoslangan trafik himoyasi;
- ! dunyoning istalgan nuqtasidan ichki resurslardan foydalanish imkonini beruvchi kafolatlangan himoyalovchi kommunikatsiya vositasi;



! korporatsiyaning kommunikatsiya tizimini alohida ajratilgan liniya qurishga sarf etiladigan vositalarni ishlatmasdan rivojlanishidir.



1-rasm.VPN tarmog'i asosida yaratilgan lokal tarmoq.

# VPN metodi

Tunnellashtirish metodi yordamida ma'lumotlar paketi umumiyl foydalanish tarmog'i orqali xuddi oddiy ikki nuqtali bog'lanishdagi kabi translyatsiya qilinadi. Har qaysi «ma'lumot jo'natuvchi-qabul qiluvchi» juftligi o'rtasida ma'lumotlarni bir protokoldan ikkinchi protokolga inkapsulyatsiya qilish imkonini beruvchi o'ziga xos tunnel — xavfsiz mantiqiy bog'lanish o'rnatiladi.

“ Quyidagilar tunnelning asosiy komponentlari hisoblanadi:

- tashabbuskor;
- marshrutlanuvchi tarmoq;
- tunnel kommutatori;
- bir yoki bir necha tunnel terminatorlari.

”



# VPN tarmog`ining klassifikatsiyasi

# VPN tarmog`i klassifikatsiyasi

Axborotni VPN tuneli bo`yicha uzatilishi jarayonidagi himoyalash quydagi vazifalarni bajarishga asoslangan:



O`zaro aloqadagi taraflarni autentifikatsiyalash

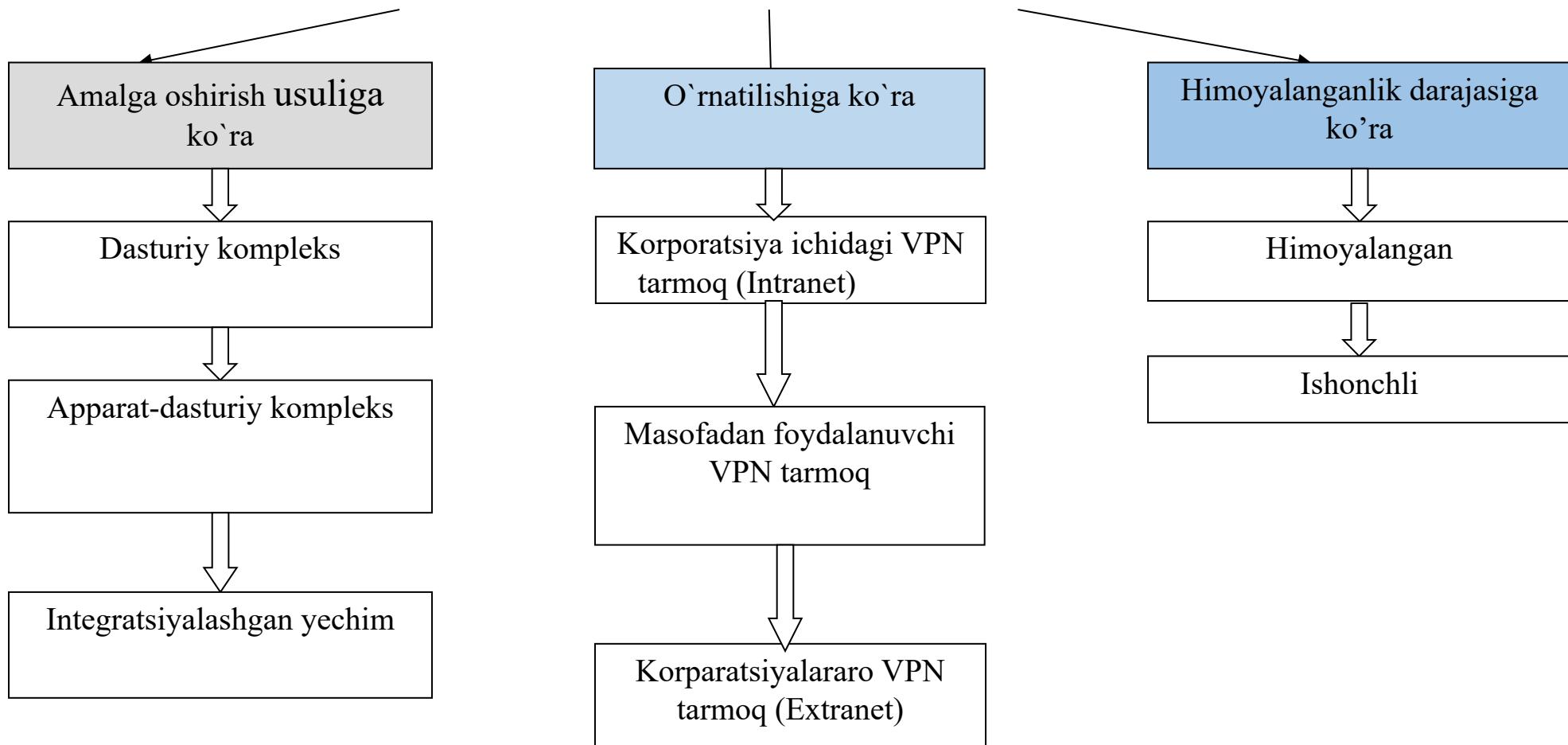


Uzatiluvchi ma`lumotlarni kriptografik berkitish (shifrlash)

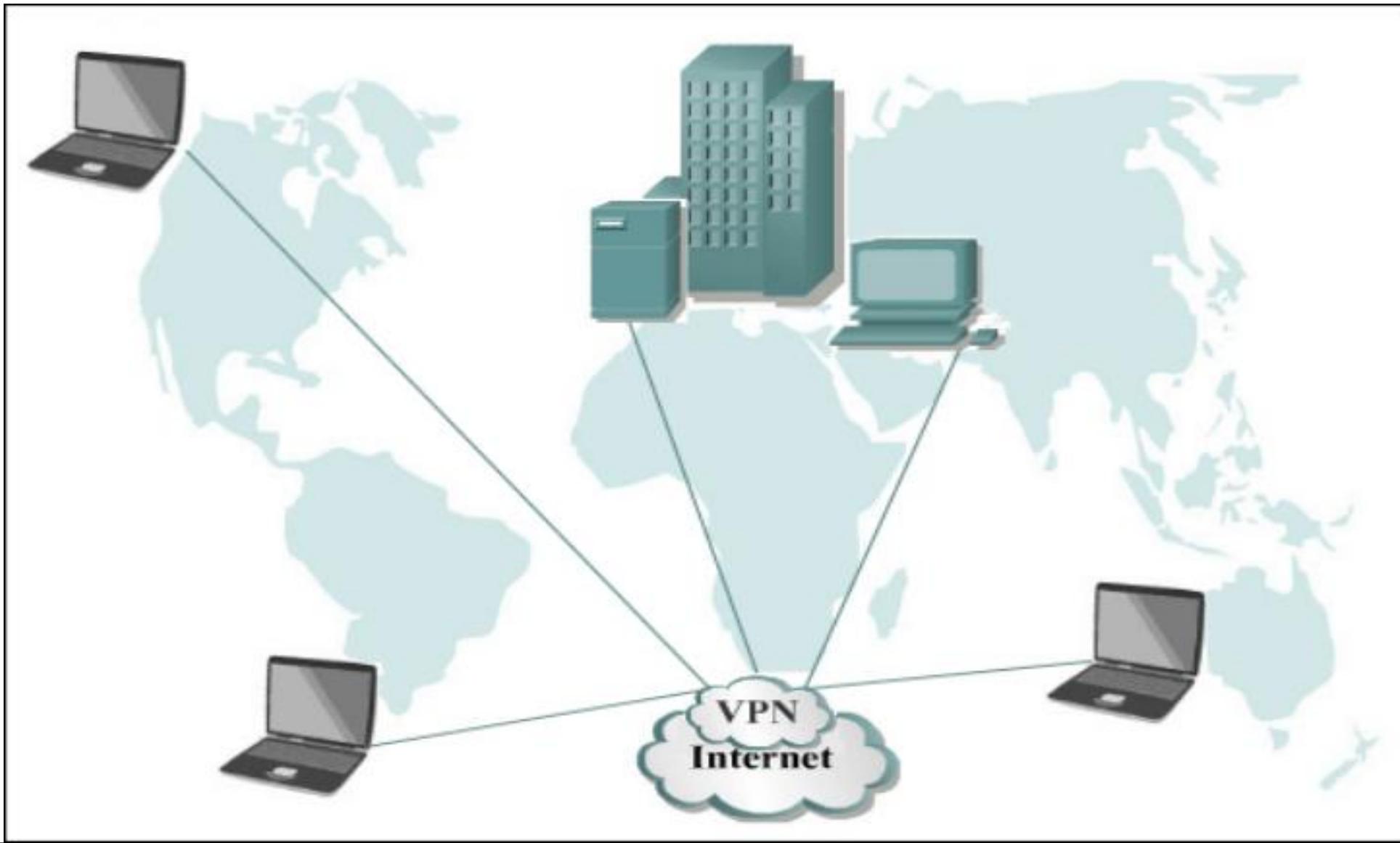


Yetkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish

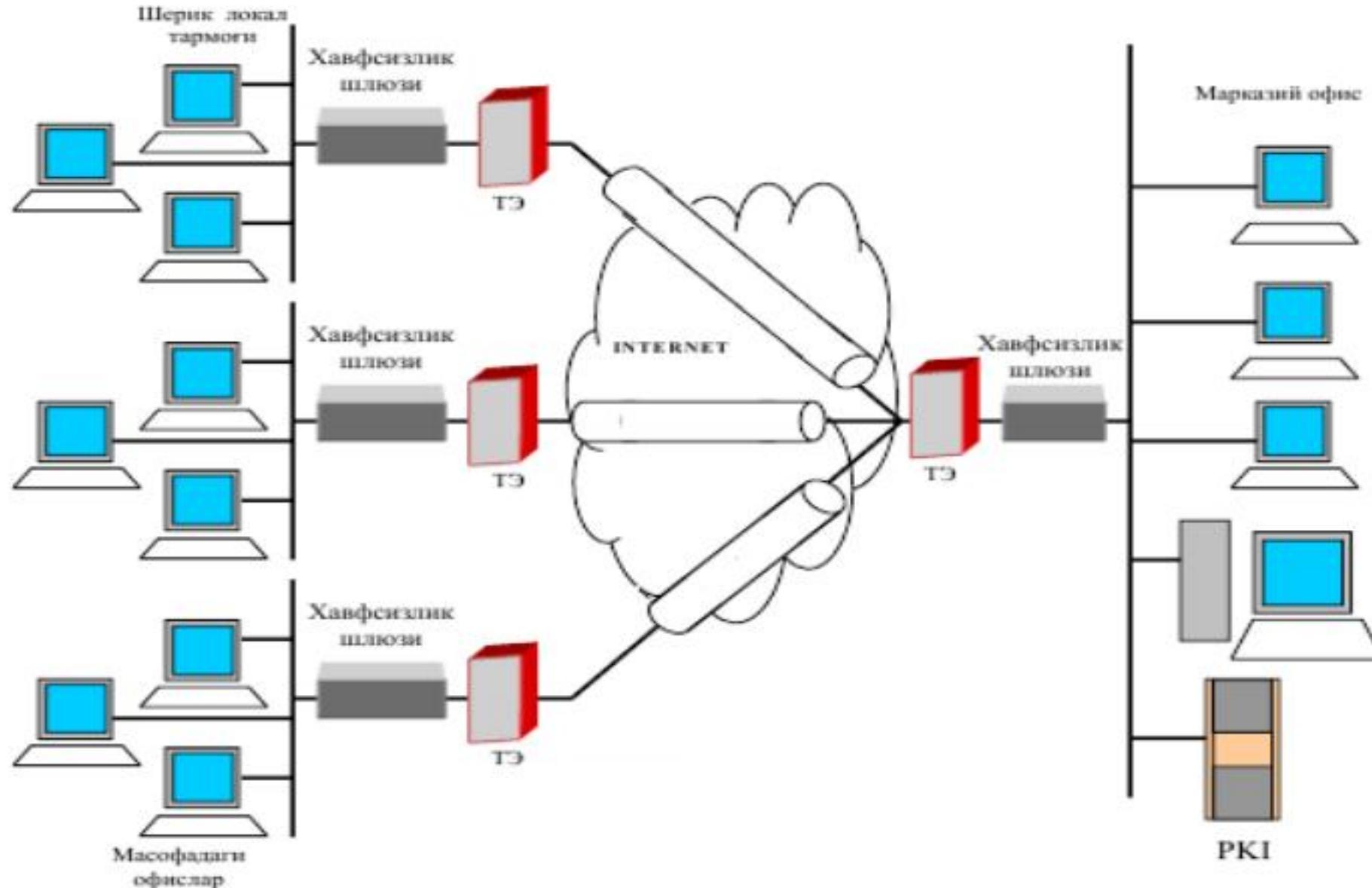
# VPN tavsiflanishi



# Masofadan ruhsat berish orqali tashkil qilingan VPN (Remote access)



# Korparatsiyalararo VPN тармогъи

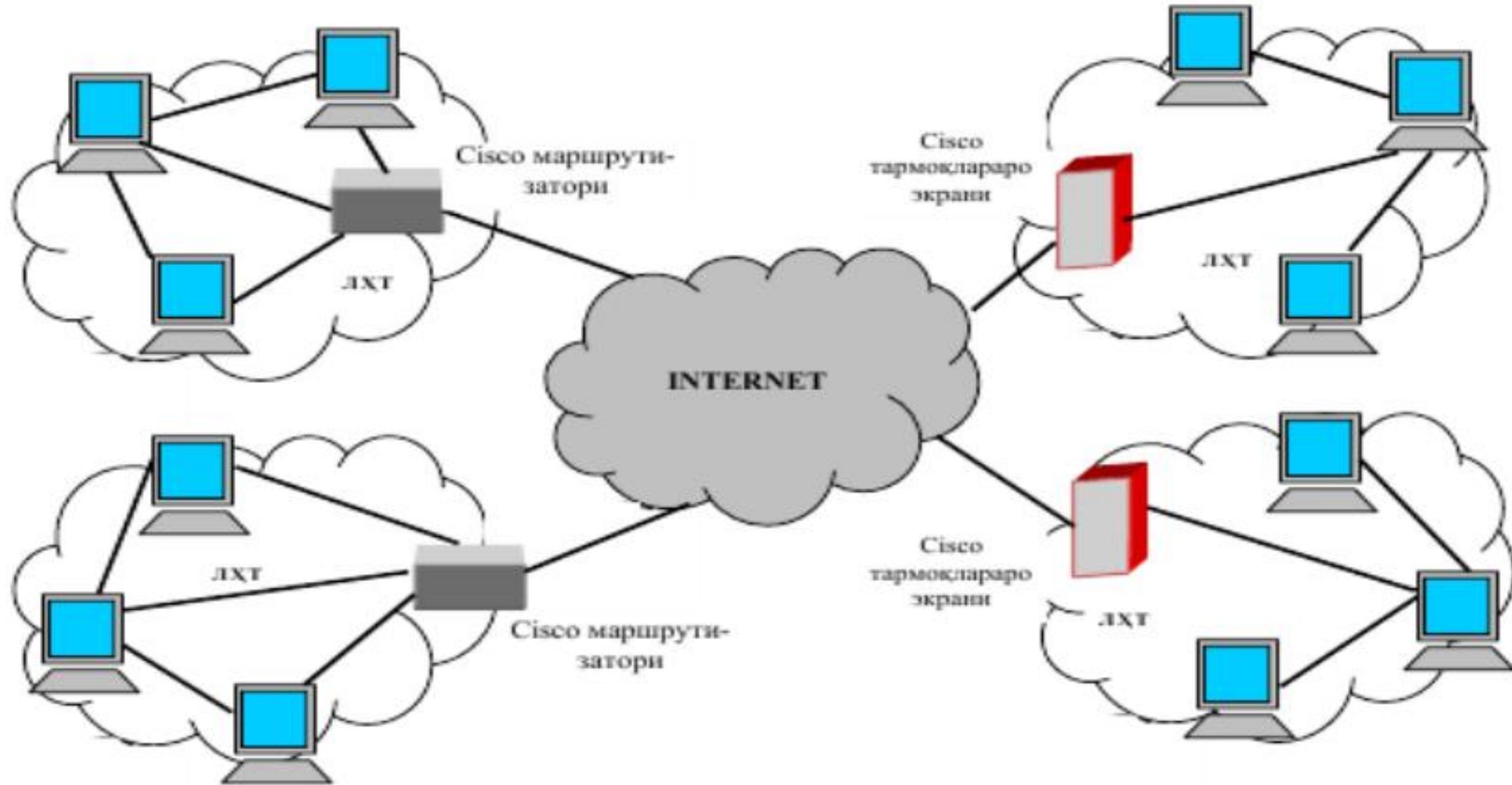


# Mashrutizatorlar asosidagi VPN

VPN qurishning ushbu usuliga binoan himoyalangan kanallarni yaratishda marshrutizatorlardan foydalaniladi. Lokal tarmoqdan chiquvchi barcha axborot marshrutizator orqali o`tganligi sababli unga shifrlash vazifasini yuklash tabiiy. Marshrutizator asosidagi VPN asbob uskunalariga misol tariqasida Cisco systems kompaniyasining qurilmalarini ko`rsatish mumkin.



# Cisco мар shrutizatorlari asosida korparativ VPN tarmog`ini qurishning namunaviy sxemasi

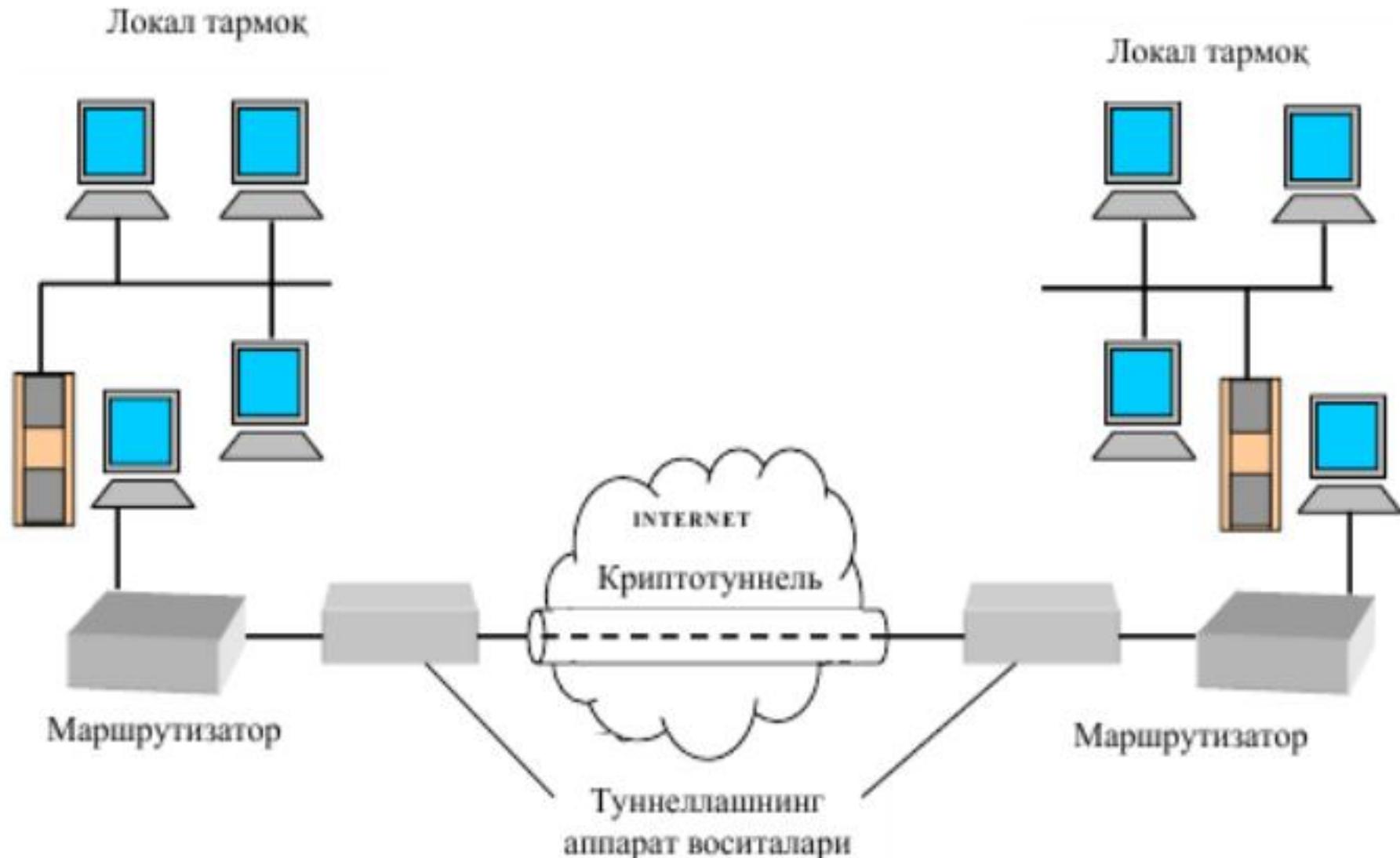


# Dasturiy ta'minot asosidagi VPN

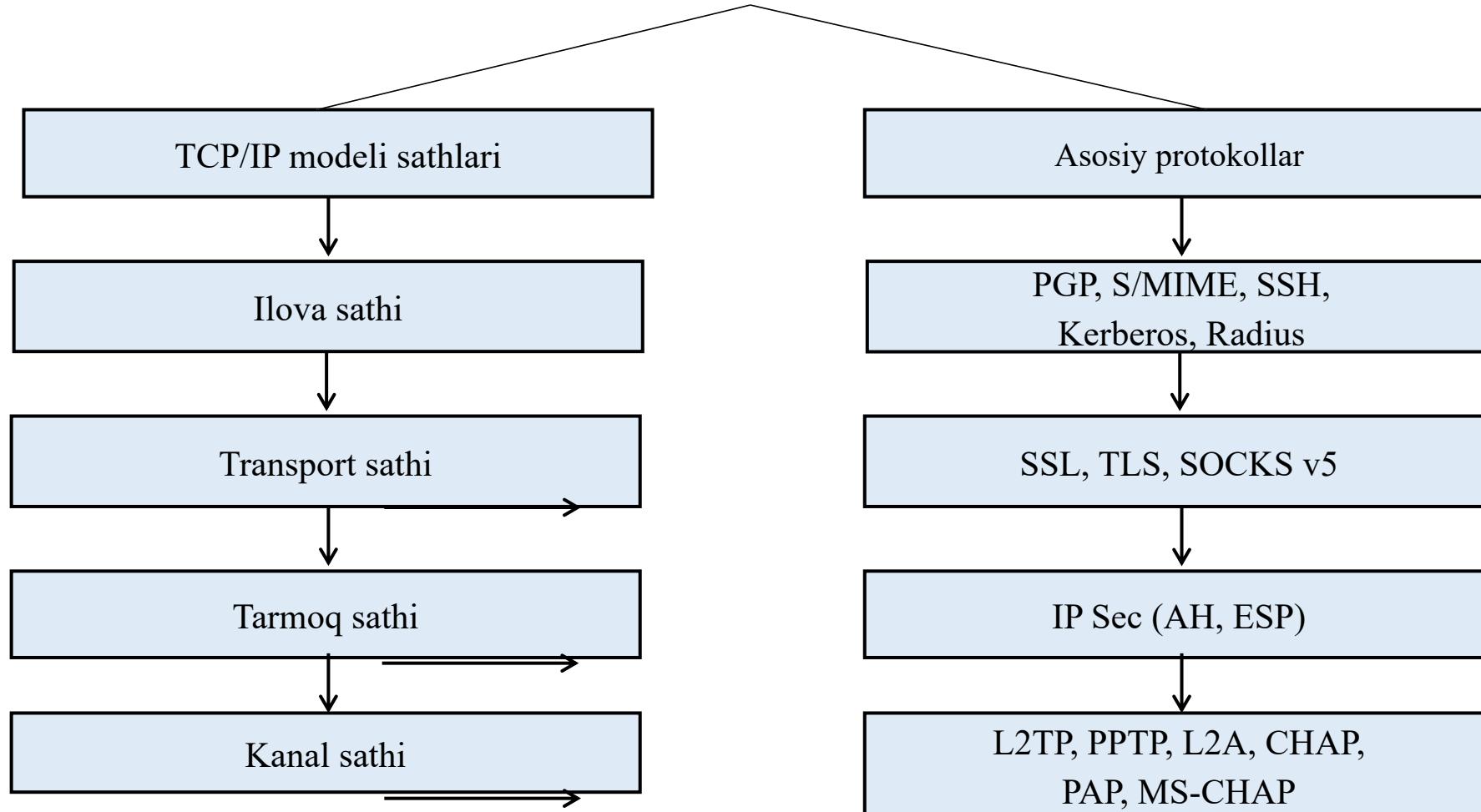
Dasturiy usul bo'yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan qurilmadan qolishsada, VPN-tarmoqlarni amalga oshirilishida yetarli quvvatga ega. Ta'kidlash lozimki, masofadan foydalanishda zaruriy o'tkazish poloskasiga zarurat kuchli emas. Shu sababli dasturiy maxsulotlarning o'zi masofadan foydalanish uchun yetarli unumdorlikni ta'minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi qo'llanishining moslashuvchanligi va qulayligi, hamda narxining nisbatan yuqori emasligi.



# Ixtisoslashtirilgan apparat vositalar asosida tunellash sxemasi



# VPN protokollarining TCP/IP modeli sathlarida joylashishi sxemasi





**E'tiboringiz  
uchun rahmat!**

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

# Hujumlarni aniqlash tizimi. IDS/IPS texnologiyalari. IPS signaturasi. IPS ni qo'llash



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



108 Amir Temur Street,  
Tashkent, Uzbekistan

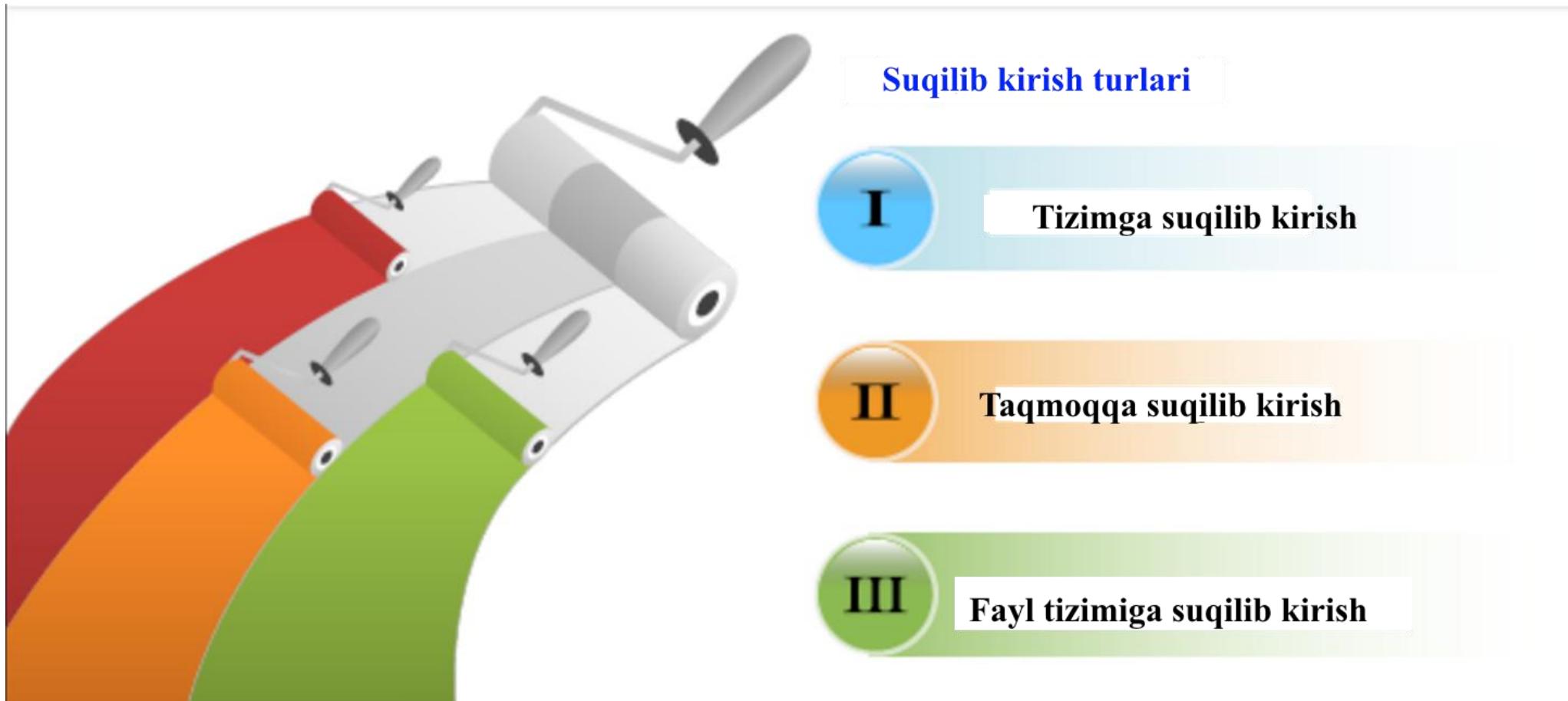
100200

# Modullari

- Har xil suqulib kirishlar va ularning turlarini tushunish
- IDPSni tushuntirish
- IDPS ni qo'llashda muhim tushunchalar
- Tarmoqni himoya qilishda IDPS roli
- IDS ishlash prinsplari, funksiyalari va tarkibiy qismlarini tavsiflab berish
- Turli xil IDS tizimlarini amalga oshirilish haqida tushuntirish
- NIDS and HIDS-larning bosqichma-bosqich joylashtirilishini tavsiflash
- IDS qo'shimcha funksiyalarini muhokama qilish
- IDSni amalga oshirish xususiyatlarini muhokama qilish.
- IDSni amalga oshirish xatolari va ularni yo'q qilish usullarini tavsiflash
- IPSni amalga oshirish turlarini tushuntirish
- Tegishli IDSP mahsulotini tanlash uchun talablarni aniqlash

# Suqilib kirish

Suqilib kirish - bu konfidentsiallikni, yaxlitlik va foydalanish imkoniyatlarini xavf ostiga qo'yishi yoki kompyuter tizimining xavfsizlik mexanizmlarini xavf ostiga qo'yadi.



# Suqulib kirishning umumiyl belgilari



- Yangi, notanish fayllar yoki dasturlarning mavjudligi
- Fayllarga kirishdagi o'zgarishlar
- Yo'qotib bo'lmaydigan fayl hajmi o'zgarishi
- Qalbaki fayllar tasdiqlangan asosiy fayllar bilan mos kelmasligi
- Yo'qolgan fayllar



- Qurilmada takroriy tekshirish xizmati mavjudligi
- Noma'lum manzillardan xabarlar
- Masofadan qurilmalarga kirishga urinishi
- Fayllardagi tasodifiy ma'lumotlarni rad etish yoki xizmat ko'rsatishni to'xtatish urinishlarini ko'rsatilishi

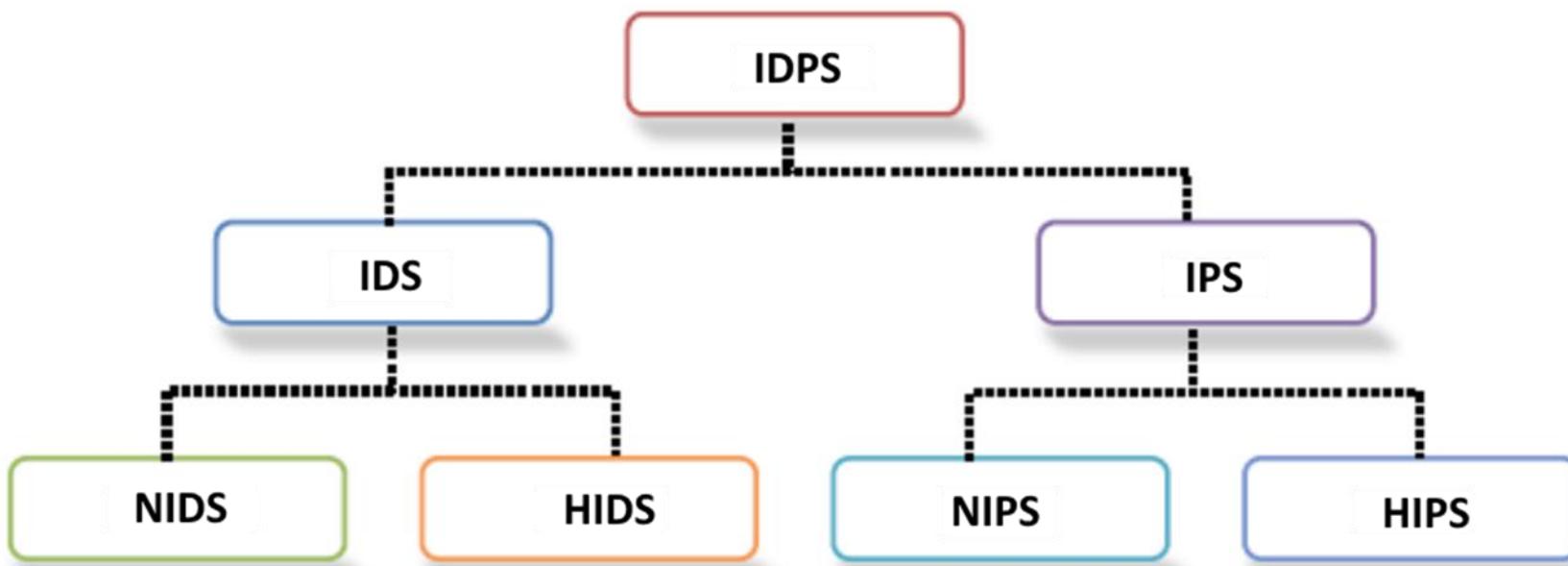


- Qisqa yoki to'liq bo'lмаган ма'lumotlar
- Tizimni noodatiy ishlashi
- Egalari noma'lum jo'natmalar, yo'qotilan ma'lumotlar va noto'g'ri ma'lumotlar
- Tizim dasturiy ta'minotini va konfiguratsiya fayllarini o'zgartirish
- Noodatiy shakldagi rasmlar va matnli xabarlar
- Tizimdagи bo'shliqlar
- Tizimini o'chishi yoki qayta yuklanishi
- Tizimga taalluqli bo'lмаган jarayonlar

# Suqulib kirishlarni aniqlash va oldini olish tizimlari (IDPS)

- IDPS suqulib kirishlarga qarshi ishlatiladi
- Bunday tizimlar IDS va IPS ga bo'linadi
- IDS ruxsatsiz kirishlarni aniqlaydi, IPS esa ruxsatsiz kirishlarni aniqlash bilan birgalikda ularga qarshi hujum choralarini o'rganadi

## IDPS klassifikatsiyasi

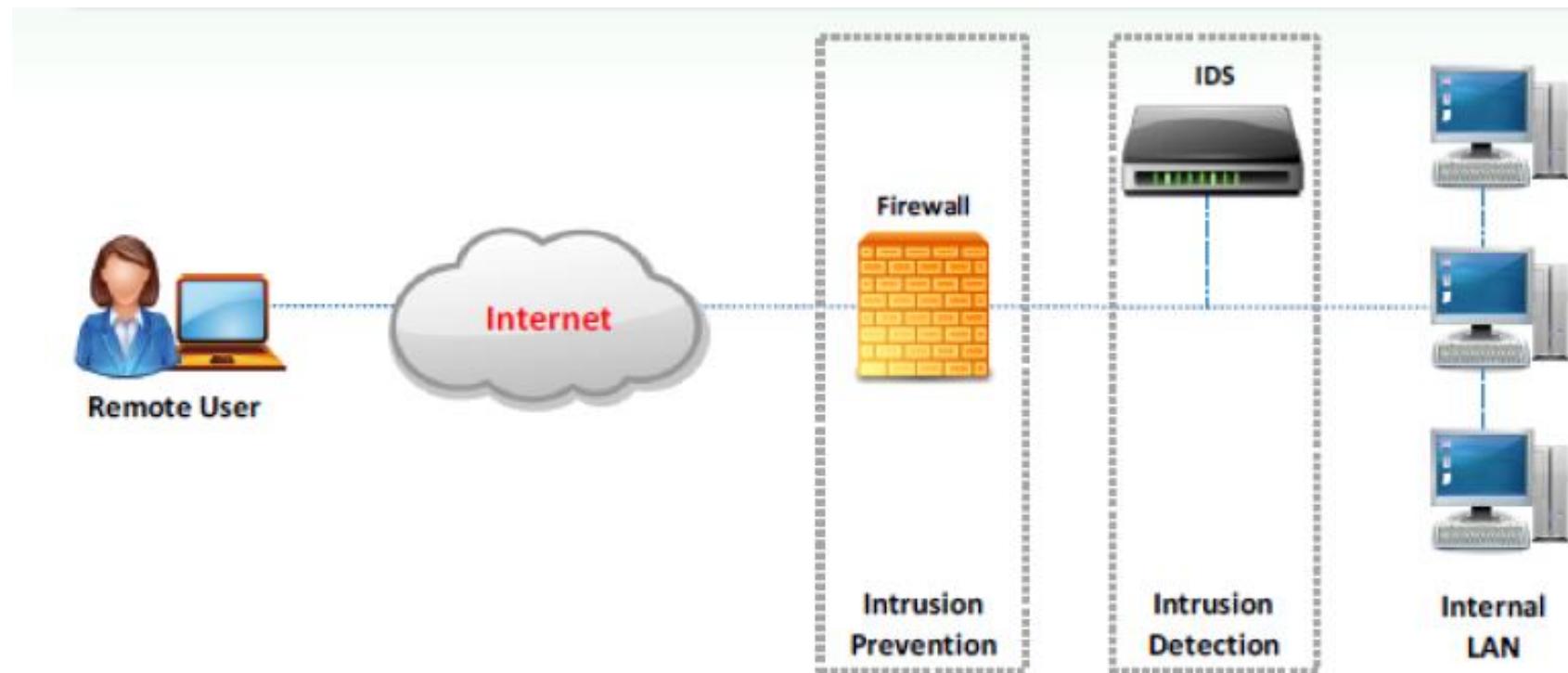


# IDPS nima uchun kerak?

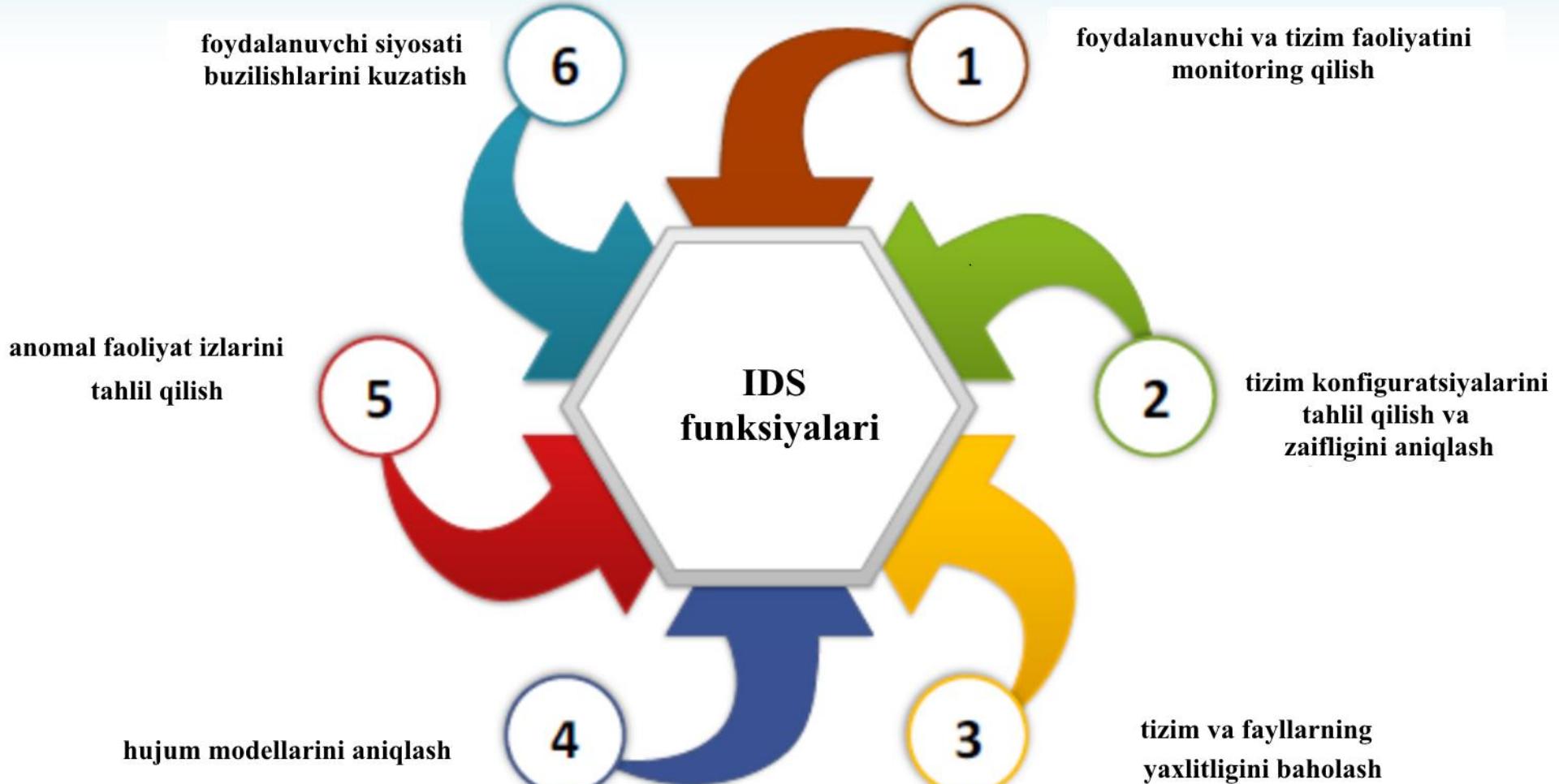
- 
- 1 • IDPS “chuqurlik” himoya tamoyili bo'yicha qo'shimcha tarmoq xavfsizligini ta'minlaydi
  - 2 • IDPS tarmoqlararo ekran bajarolmaydigan ba'zi parametrlarni ham bajara oladi
  - 3 • IDPS xavfsizlik tahdidlarini yo'qotish ehtimolini kamaytirishga yordam beradi
  - 4 • IDPS noto'g'ri boshqaruvi IDPS muvaffaqiyatsizligini ta'minlaydi
  - 5 • IDPS ehtiyyotkorlik bilan rejalashtirish, tayyorlash, rototiplash , test va maxsus ta'lif bilan amalga oshiriladi

# Tarmoq himoyasida IDSni roli

- IDS tarmoqda ishlaydi, taqmoqlararo ekrandan farqli ravishda suqulib kirishlar bilan bog'liq bo'ladi



# IDS funksiyalari



# IDS tekshirish hodisasi qanday bajariladi?

IDS kompyuter tarmog'inining faoliyatini kuzatib boradi, siyosatni buzmasligiga ishonch hosil qilish uchun maxsus siyosat va harakat modellari kuzatib boriladi

konfiguratsiya fayllaridagi zaifliklarni aniqlaydi

tarmoqda ruxsatsiz xizmatlarning yo'qligiga ishonch hosil qilish uchun xizmat konfiguratsiya fayllarini tekshiradi



Viruslarga, keylogger shaklidagi yashirin zararli dasturlarni kuzatib boradi

tarmoqdagi avtorizatsiya fayllari foydalanuvchilar va guruhlarning avtorizatsiyasini o'z ichiga oladi. IDS muntazam ravishda bu avtorizatsiya holatini tekshiradi ular soxta emasligini ta'minlaydi

# Quyidagilardan qaysilari IDS hisoblanmaydi?



Tarmoq hodisalarini qayd  
qilish tizimi



Zaifliklarni baholash  
vositasi

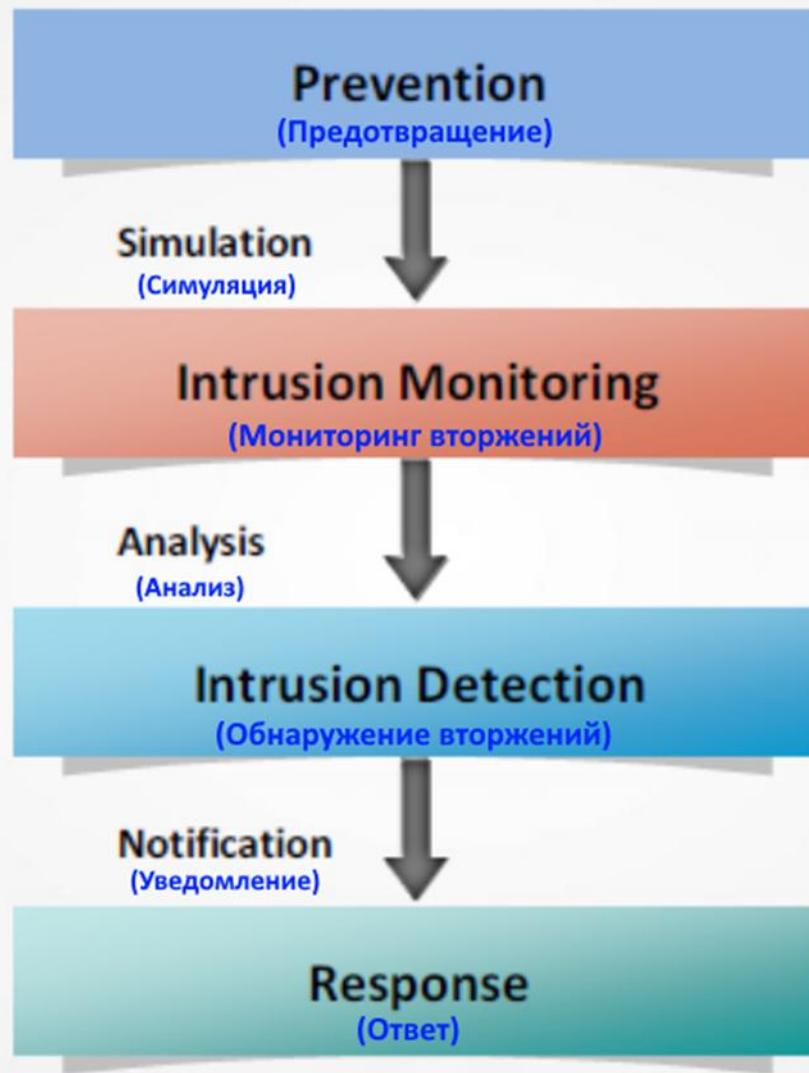


Antivirus mahsuloti

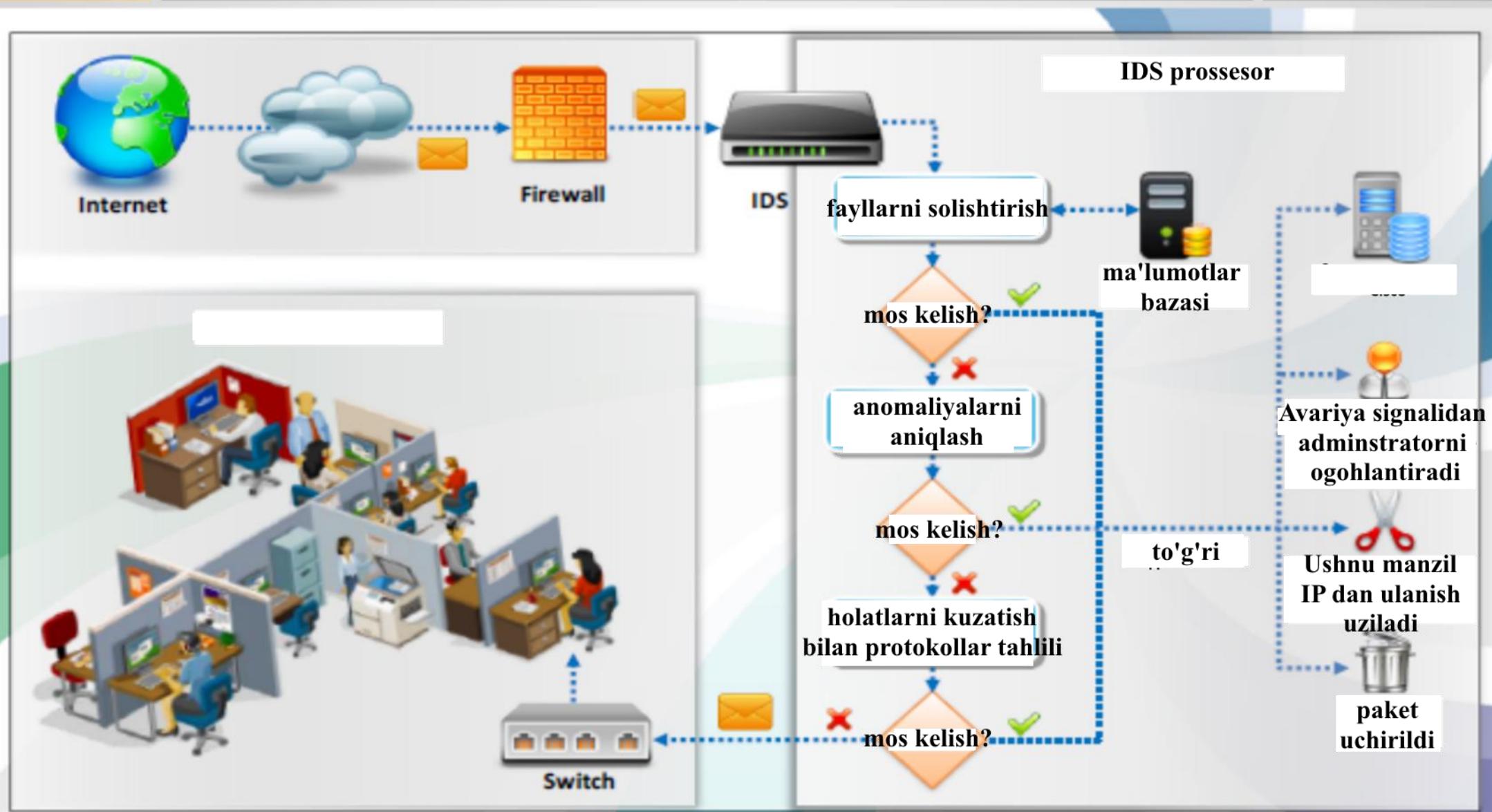


Xavfsizlik tizimlari/  
kriptografiya

# IDS faoliyati

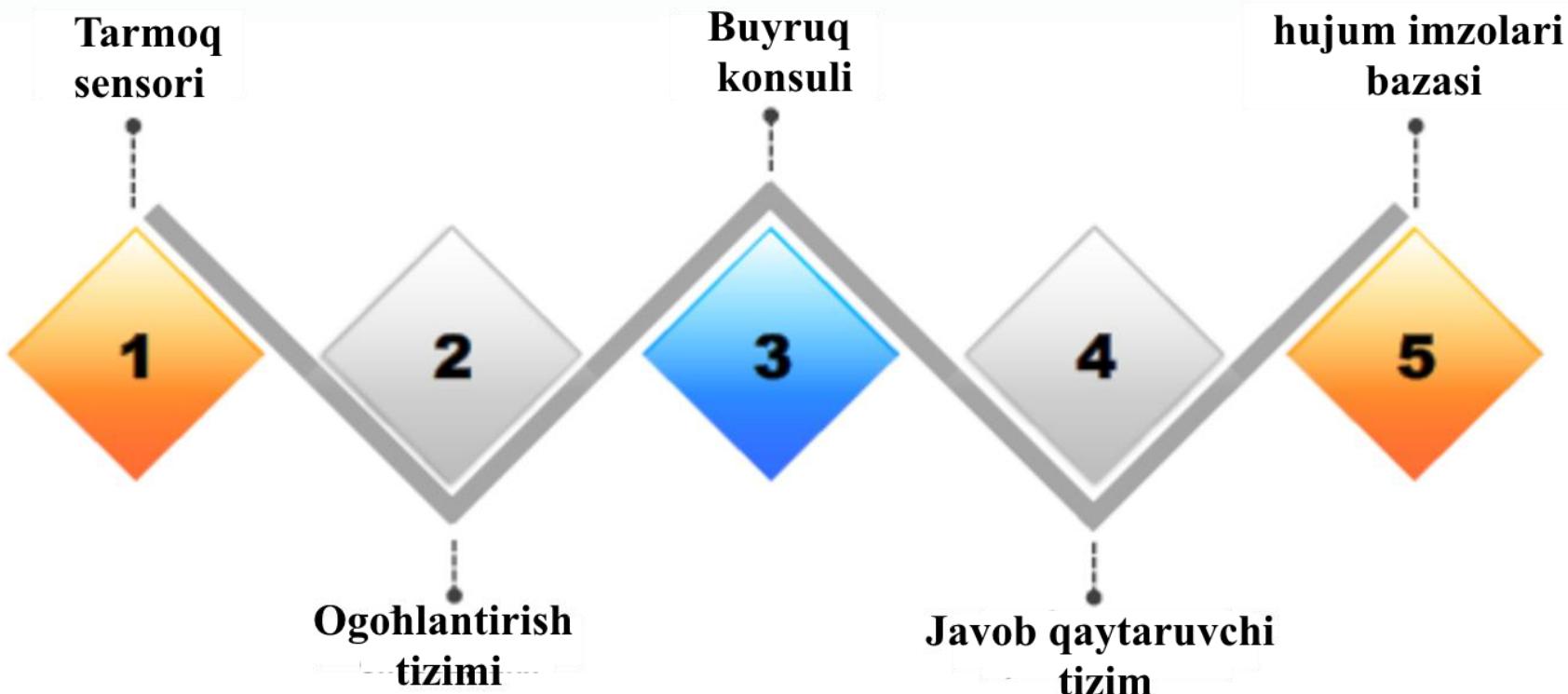


# IDS qanday ishlaydi?



# IDS komponentlari

- 1) IDS tizimi turli xil komponentlardan quriladi
- 2) Adminstrator komponentalarni funksional ishlashlarini va tarmoqda IDSning har bir komponentalarini joylashtirilishini bilishi zarur
- 3) IDS tizimi an'anaviy kopmonentalarga ega



E'tiboringiz uchun  
rahmat...

---

# Tarmoq xavfsizligi

---

*“Bulutli” hisoblash tizimlarida axborot xavfsizligi*

---



+998 71 238 6525



@tarmoq\_xavfsizligi



[www.tuit.uz](http://www.tuit.uz)



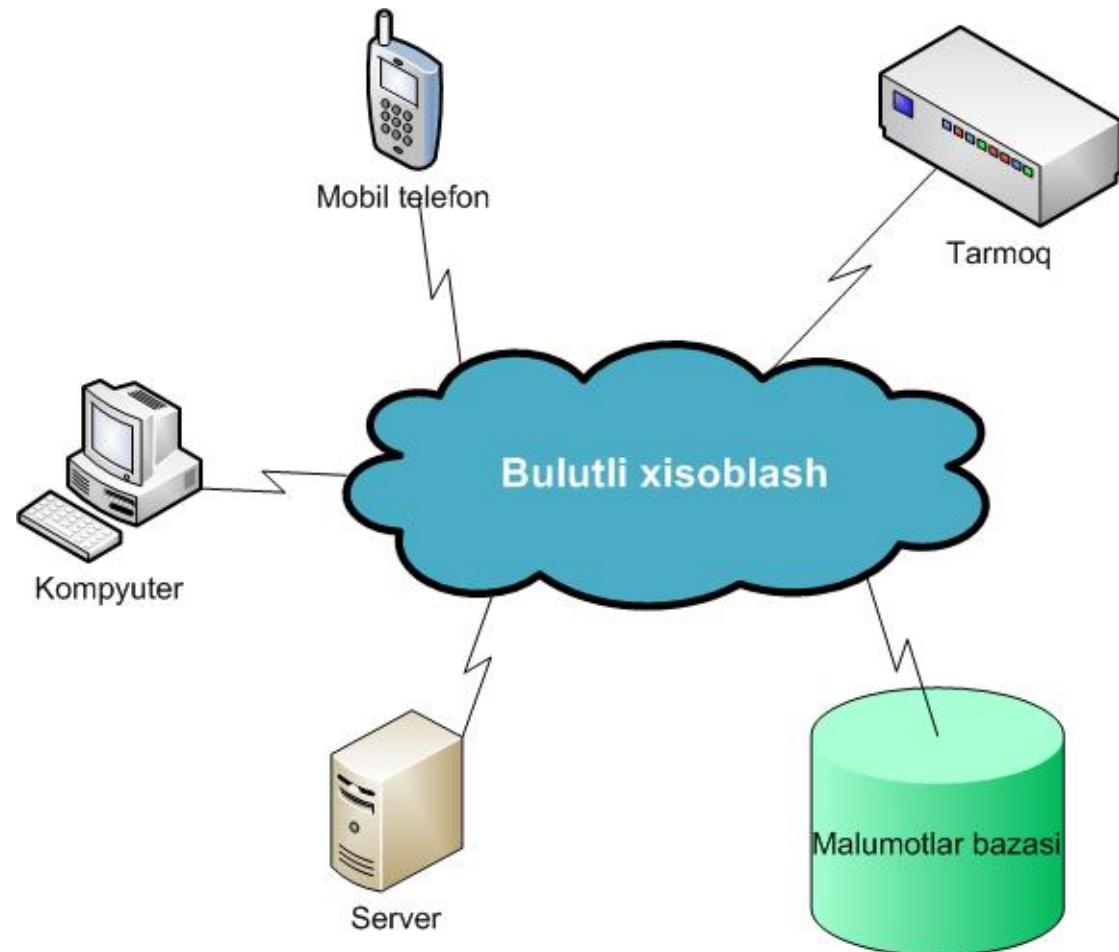
108 Amir Temur Street,  
Tashkent, Uzbekistan

100200

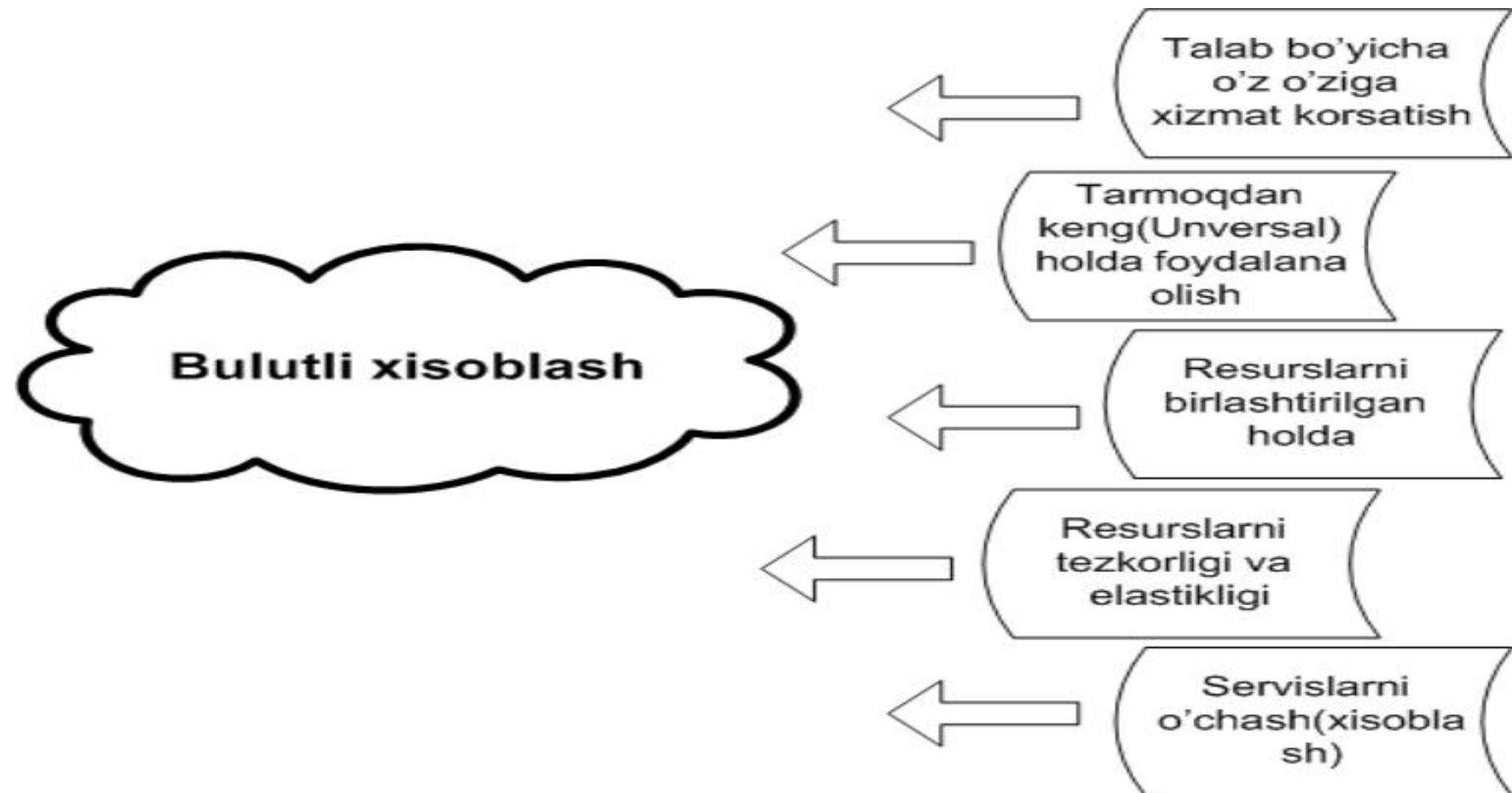
# Bulutli hisoblash tizimlari

**Bulutli hisoblash** (inglizcha cloud computing) - ma'lumotlarni taqsimlangan holda hisoblash texnologiyasi bo'lib, bunda kompyuter resurslari foydalanuvchiga internet xizmati tarzida taqdim etiladi.

**Bulut** – AT- infratuzilma tashkilotlarining innovatsion modeli (konsepsiya) xisoblanib, u aloxida ajratilgan va taqsimlangan konfiguratsiyalangan apparat va tarmoq resurslaridan, dasturiy taminotdan tashkil topgan va ular masofadagi provayderlarni malumotlar markazida yotadi.



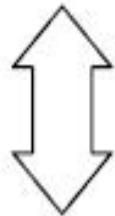
# Bulutli hisoblash tizimlarining xususiyatlari



# Bulutli hisoblash tizimi modellari

SaaS

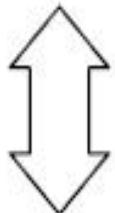
Xizmat  
sifatida  
dasturiy  
taminot



CRM, Email,  
Office, ERP(1C),  
HRP

PaaS

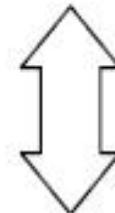
Ximat sifatida platforma



Execution runtime,  
database, web  
server, development  
tools

IaaS

Xizmat sifatida infratuzilma



Virtual machines,  
servers, storage,  
load balancers,  
network

Активаци  
чтобы актив

активации

# Bulutli hisoblash ma'lumotlari arxitekturasi

	Ta'rif
<b>Bulutli iste'molchi</b> Cloud Consumer	Biznes aloqalarini qo'llab-quvvatlaydigan va bulutli provayderlar xizmatlaridan foydalanadigan shaxs yoki tashkilot.
<b>Bulutli provayder</b> Cloud Provider	Bulutli xizmatni bulutli iste'molchilarga taqdim etish uchun mas'ul shaxs, tashkilot yoki yuridik shaxs.
<b>Bulutli auditor</b> Cloud Auditor	Bulutli xizmatlarni mustaqil baholash (baholash), axborot tizimlariga texnik xizmat ko'rsatish, bulutni amalga oshirish samaradorligi va xavfsizligini amalga oshiradigan ishtirokchi.
<b>Bulutli broker</b> Cloud Broker	Bulutli xizmatlardan foydalanish, unumдорлик va yetkazib berishni boshqaradigan hamda bulutli provayderlar va bulutli iste'molchilar o'rtaida aloqalarni o'rnatuvchi tashkilot.
<b>Bulutli tashuvchi</b> Cloud Carrier	Bulutli provayderlardan bulutli iste'molchilarga bulut xizmatlarini ulash va transport (aloqa xizmatlari) bilan ta'minlovchi vositachi.

# Bulutli hisoblash tizimlari afzalliklari

Foydalanuvchi uchun  
iqtisodiy foyda

Mahsulorlikni  
oshirish

IT infratuzilmasi  
samaradorligini  
oshirish

Ta'mirlash bilan bog'liq  
muammolarni  
kamaytirish

Sotib olingen dasturiy  
ta'minot narxini  
pasaytirish

Doimiy dasturiy  
yangilanishlar

Mavjud hisoblash  
quvvatini oshirish

Cheksiz ma'lumotlarni  
saqlash

OT mustaqilligi

Hujjat formatining  
mosligi

Bir guruhi  
foydalanuvchilar bilan  
samarali ishslash

Hujjatlarga istalgan  
joyda kirish

Har doim eng so'nggi  
va eng yangi versiya

Turli qurilmalardan  
foydalanish imkoniyati

Tabiatga do'stona  
munosabat

Uskunaning  
o'g'irlanishiga yoki  
ma'lumotlarning  
yo'qolishi qarshi  
chidamliligi

# Bulutli hisoblash tizimlari kamchiliklari



Doimiy internet tarmog'i



Ishlash tezligining pastligi

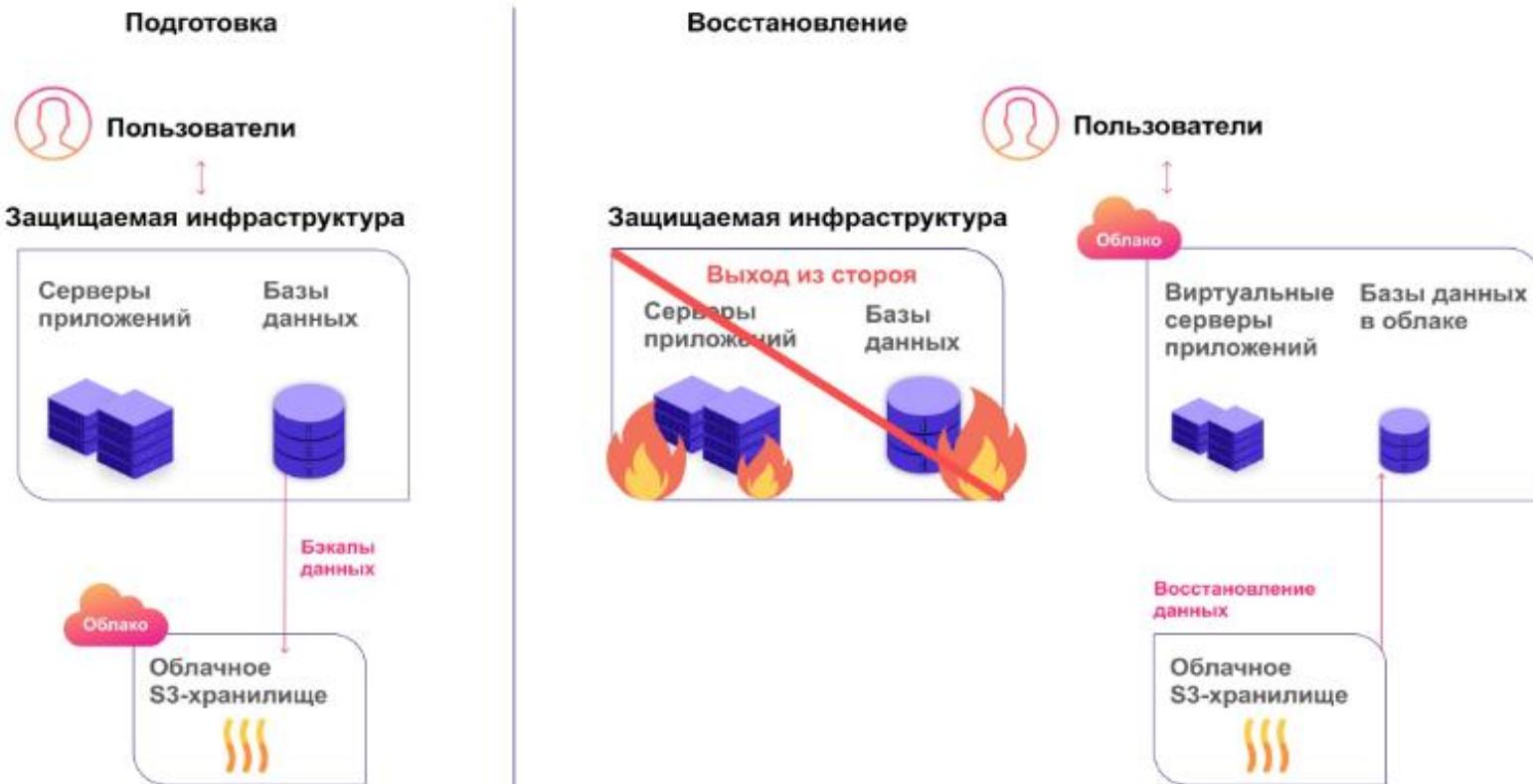


Funksional imkoniyatlarga  
ega bo'lmaslik



Malumotlar xavfsizligiga  
xavf borligi

# Bulutli hisoblash tizimi ma'lumotlarni zaxiralash (Zaxiralash va tiklash yechimi)

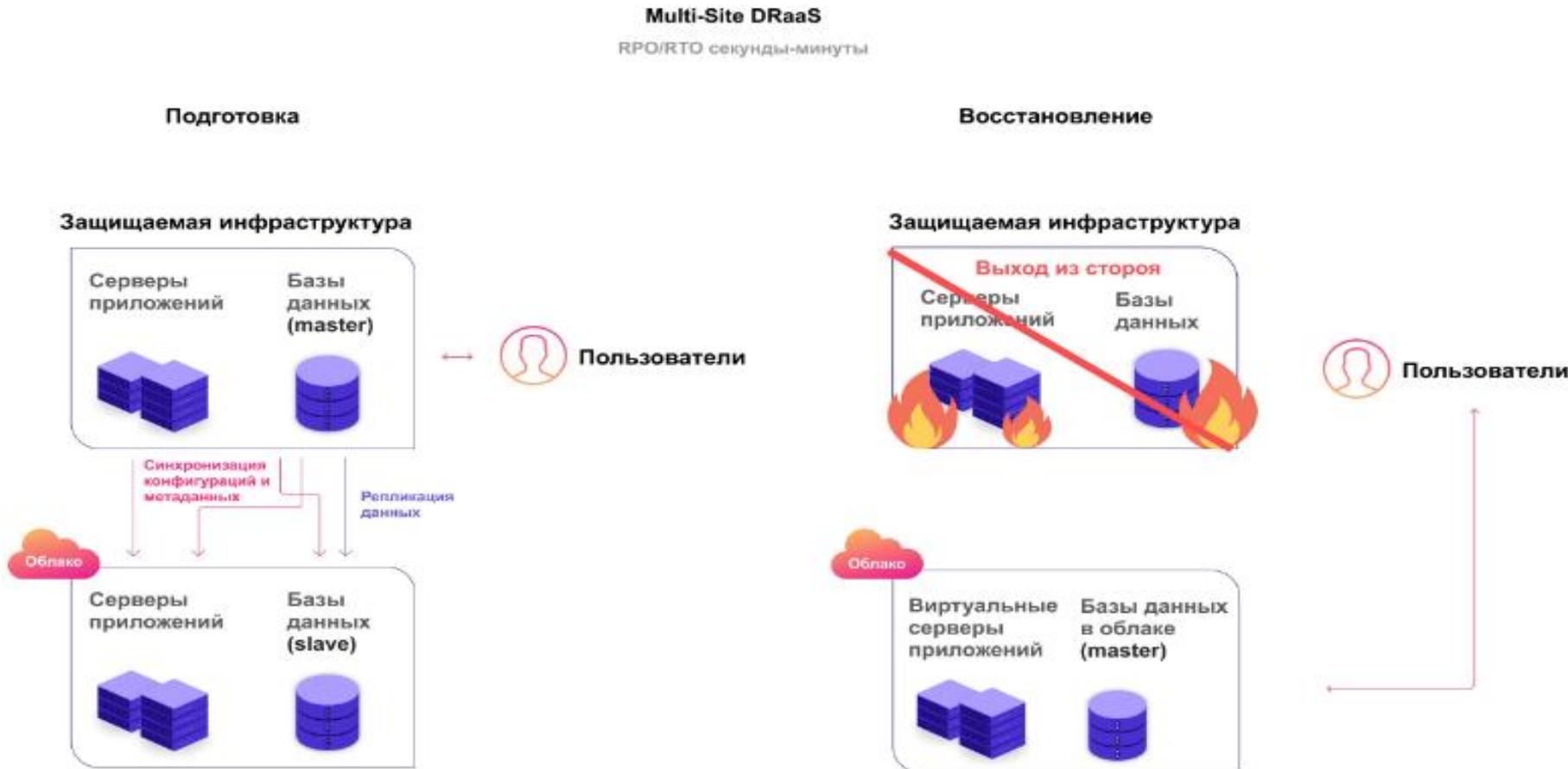


# Bulutli hisoblash tizimi ma'lumotlarni zaxiralash (Tez tiklash yechimi)

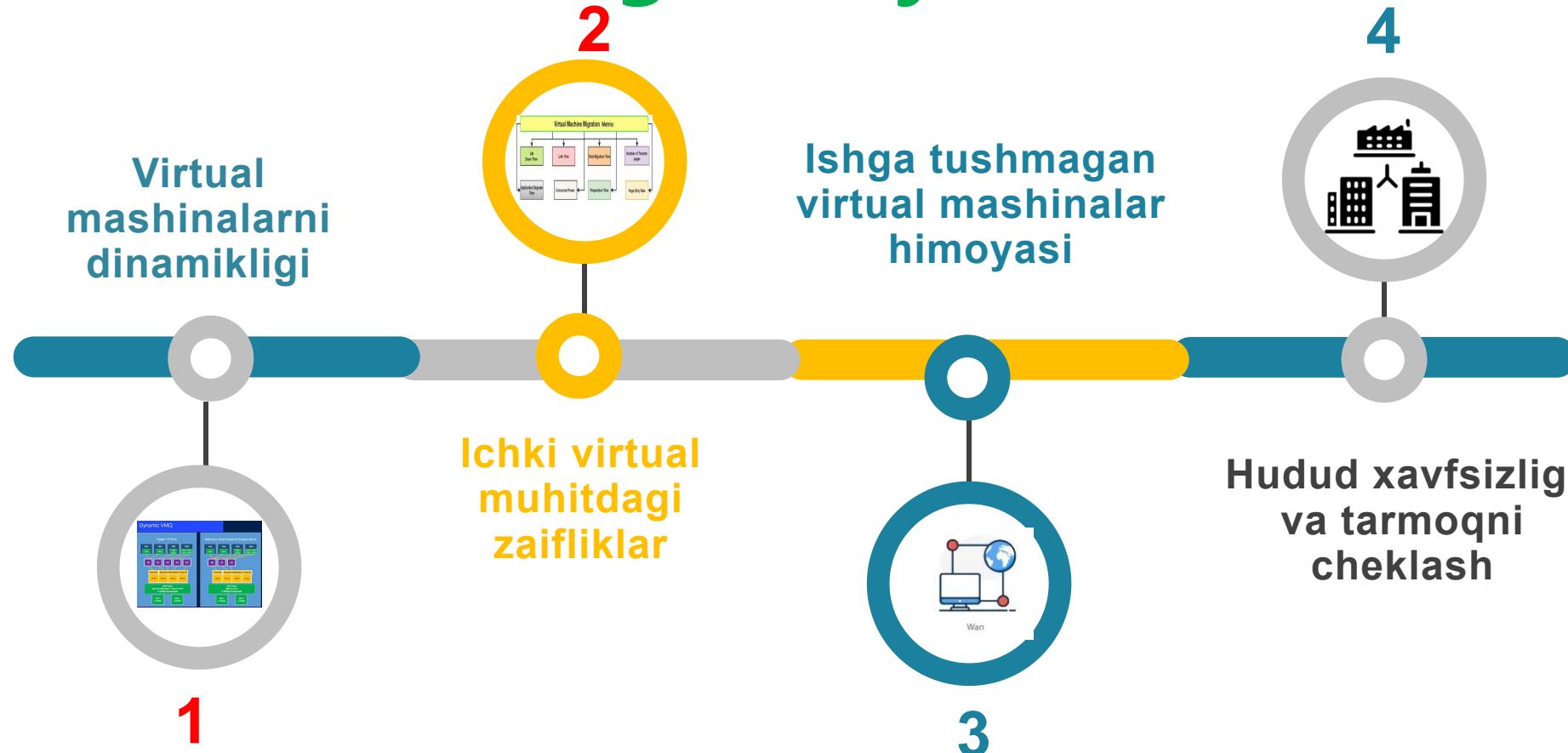
Quick Recovery DRaaS  
RPO/RTO минуты-десятки минут



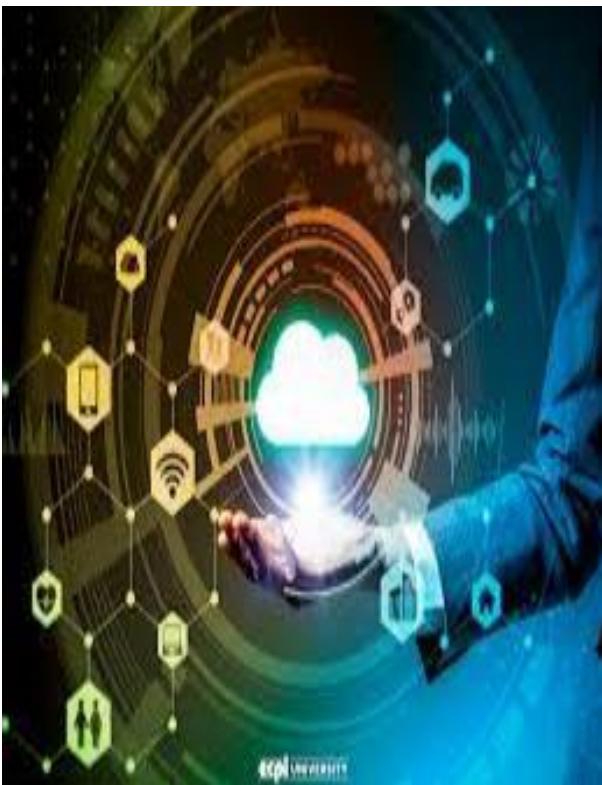
# Bulutli hisoblash tizimi ma'lumotlarni zaxiralash (Parallel infratuzilma)



# Bulutli hisoblash tizimlari xavfsizligini taminlashdagi mavjud muammolar



# Bulutli texnologiyalarda mavjud hujumlar



*DTda ananaviy hujumlar*

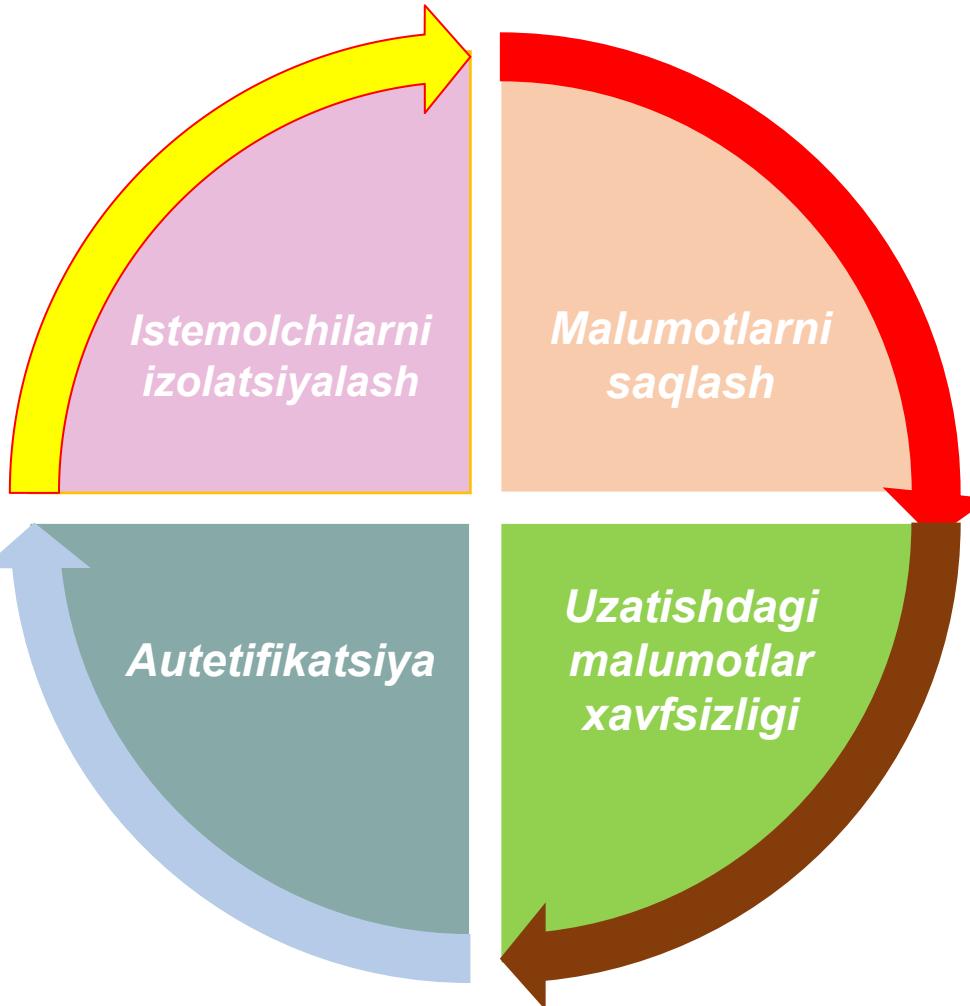
*Bulut elementlarida funksional hujumlar*

*Mijozlarga hujumlar*

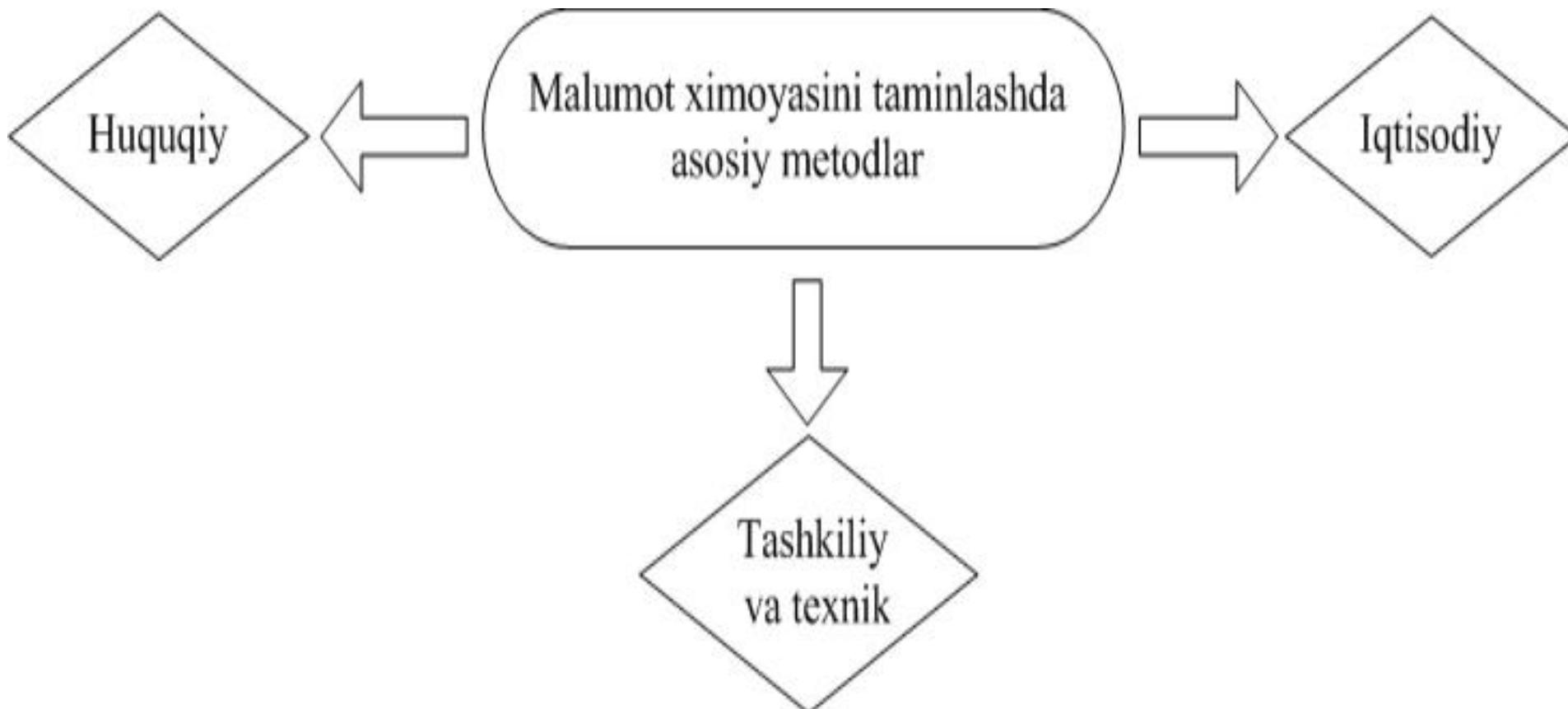
*Gipervizorga hujumlar*

*Boshqarish tizimidagi hujumlar*

# Bulutli texnologiyalarda xavfsizlikni ta'minlash yo'llari



# Bulutli texnologiyalarda malumot himoyasini ta'minlashda asosiy metodlar



# Bulutli texnologiyalarda xavfsizlikni ta'minlash choralarini



*Xizmat ko'rsatish darajasidagi moslashtirish.*

*Tizimgacha bo'lgan bulut xavfsizlik kanalini o'rnatish*

*Malumotdan foydalanishda rollarni taqsimlash*

*Virtual mashinalarni segmentlash*

*Bulutda saqlanilayotgan malumotlarni shifrlangan holda olib borish*

*Malumotlarni shifrlashda proksi serverdan foydalanish*

*Bulutdagi tuzatish imkoniyati yoq malumotlarga ishlov berish*

**E'tiboringiz uchun rahmat**

---