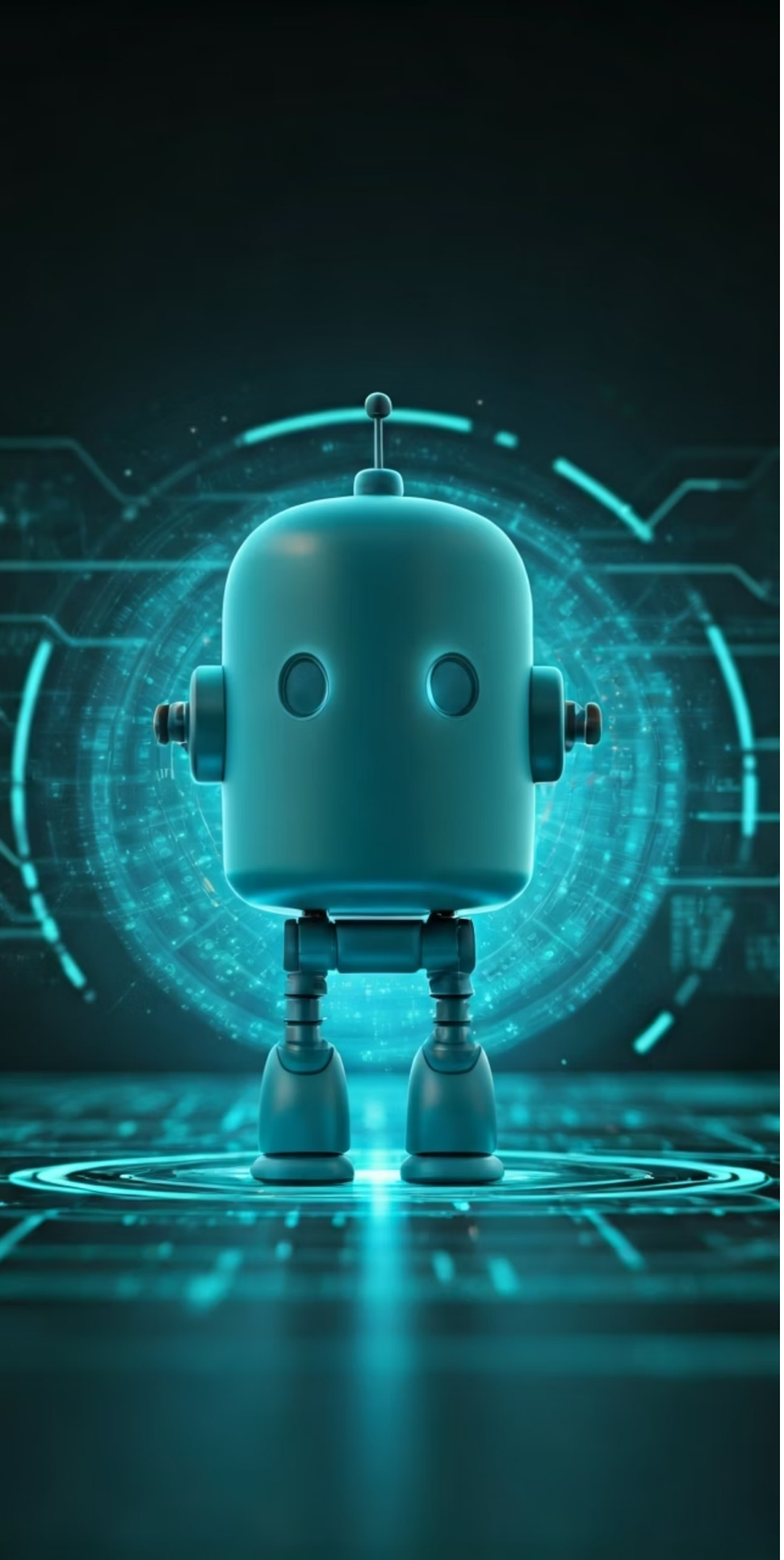
Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Желілік қауіпсіздік құралдары және протоколдар





Желілік қауіпсіздікке кіріспе

Желілік қауіпсіздік – бұл ақпараттық жүйелер мен желілерді түрлі қатерлерден қорғаудың кешенді жүйесі. Бұл бөлімде біз желілік қауіпсіздіктің негізгі ұғымдары мен маңызын қарастырамыз.

Желілік қауіпсіздік дегеніміз не?

Желілік қауіпсіздік – ақпараттық жүйелер мен желілерді зиянды шабуылдардан, рұқсатсыз қолжетімділіктен және мәліметтердің жоғалуынан қорғаудың жан-жақты жүйесі. Бұл тек технологиялық шараларды ғана емес, сонымен қатар ұйымдастырушылық және құқықтық шараларды да қамтиды.

Қазақстанда желілік қауіпсіздік саласының өзектілігі күннен-күнге артуда. Мемлекеттік және жеке ұйымдар өздерінің ақпараттық активтерін қорғауға үлкен көңіл бөлуде. 6B06303 «Желілік қауіпсіздік» мамандығы осы саладағы мамандарды даярлауда негізгі рөл атқарады.



Желілік қауіпсіздіктің негізгі мақсаттары

Құпиялылықты сақтау

Ақпаратқа рұқсат етілген адамдар ғана қол жеткізе алады. Мәліметтерді шифрлау, аутентификация және қатаң рұқсат жүйелері арқылы құпиялылық қамтамасыз етіледі.

Мәліметтердің тұтастығын қамтамасыз ету

Ақпарат рұқсатсыз өзгертілмеуі керек. Хэш-функциялар, цифрлық қолтаңбалар және бақылау механизмдері арқылы мәліметтердің бүлінбеуі қамтамасыз етіледі.

Қол жетімділікті бақылау

Рұқсат етілген пайдаланушылар қажетті уақытта жүйеге қол жеткізе алуы тиіс. DDoS шабуылдарынан қорғау және жүйелердің үздіксіз жұмыс істеуі қамтамасыз етіледі.

Бұл үш мақсат – CIA триадасы (Confidentiality, Integrity, Availability) деп аталады және желілік қауіпсіздіктің негізін құрайды. Әрбір ұйым өз қауіпсіздік стратегиясын осы принциптерге сүйене отырып құруы керек.

Желілік қауіпсіздіктің заманауи қатерлері

DDoS шабуылдары

2025 жылы әлем бойынша DDoS шабуылдарынан болатын экономикалық шығын 15 миллиард долларға жетеді деп болжануда. Бұл шабуылдар серверлерді өте көп сұранымдармен қамтып, қызметтің тоқтап қалуына әкеледі.

Фишинг және әлеуметтік инженерия

Қолданушыларды алдау арқылы құпия ақпаратты алу әдістері. Фишингтік электрондық хаттар, жалған веб-сайттар және телефон арқылы алаяқтық – әлеуметтік инженерияның негізгі құралдары.

Зиянды бағдарламалар мен вирустар

Троялар, ransomware, шпиондық бағдарламалар және басқа да зиянды кодтар желілерге үлкен қауіп төндіреді. Олар мәліметтерді ұрлауға, бұзуға немесе баспана ретінде пайдалануға бағытталған.



Желілік шабуылдардың схемасы

Желілік шабуылдар көп қабатты процесс болып табылады. Хакерлер әртүрлі әдістер мен құралдарды пайдаланып, қорғаныс қабаттарын бұзуға тырысады. Заманауи қорғаныс жүйелері де көп деңгейлі болып келеді: брандмауэрлер, IDS/IPS жүйелері, антивирустар және басқа құралдар бірлесіп жұмыс істейді.





Желілік қауіпсіздік құралдары

Желілік қауіпсіздікті қамтамасыз ету үшін көптеген арнайы құралдар мен технологиялар қолданылады. Бұл бөлімде ең маңызды және кеңінен таралған қауіпсіздік құралдарын қарастырамыз.

Қауіпсіздік құралдарының түрлері

Брандмауэрлер (Firewall)

Желі трафигін бақылайтын және сүзетін құрылғылар немесе бағдарламалар. Олар белгілі бір ережелер бойынша трафикті өткізу немесе блоктау туралы шешім қабылдайды.

Антивирус және антишпиондық бағдарламалар

Зиянды бағдарламаларды анықтау, оқшаулау және жою үшін арналған бағдарламалық қамтамасыз ету. Олар үнемі жаңартылатын вирус қолтаңбалары базасын пайдаланады.

VPN және шифрлау құралдары

Виртуалды жеке желілер мен шифрлау технологиялары мәліметтерді қорғалған түрде беруді қамтамасыз етеді. Олар ашық желілерде қауіпсіз байланыс орнатуға мүмкіндік береді.

Бұл құралдардың әрқайсысы өз міндеттерін атқарады, бірақ олардың барлығын бірлесіп пайдаланған кезде ең жоғары қауіпсіздік деңгейіне қол жеткізуге болады.

Брандмауэрлердің рөлі

Негізгі функциялар

- Желіні сыртқы шабуылдардан қорғау – рұқсат етілмеген қосылыстарды блоктау
- Трафикті сүзу және бақылау – кіріс және шығыс трафикті талдау
- Желі ережелерін қолдану – қауіпсіздік саясатын енгізу
- Журналдау және есеп беру – желілік әрекеттерді тіркеу

Танымал шешімдер: Cisco ASA, Palo Alto Networks, Fortinet FortiGate, Check Point. Бұл өнімдер корпоративті деңгейде кеңінен қолданылады және жоғары сенімділік пен өнімділікті қамтамасыз етеді.





VPN технологиясы

01

Қашықтан қауіпсіз қосылу

VPN қызметкерлерге кез келген жерден корпоративті желіге қауіпсіз қосылуға мүмкіндік береді. Бұл қашықтан жұмыс істеу кезінде өте маңызды.

02

Мәліметтерді шифрлау арқылы қорғау

Барлық трафик шифрланады, бұл үшінші тараптардың оны ұстап оқуын болдырмайды. IPsec, SSL/TLS сияқты протоколдар қолданылады.

03

IP-мекенжайды жасыру

VPN пайдаланушының IP-мекенжайын жасырып, анонимдылықты қамтамасыз етеді. Бұл геолокация шектеулерін айналып өтуге көмектеседі.

Қазақстанда VPN технологиясы банктер, үкімет мекемелері және ірі корпорацияларда белсенді түрде қолданылады. Қашықтан жұмыс істеу мәдениетінің дамуымен VPN-нің маңызы арта түсуде.

Антивирус бағдарламаларының маңызы

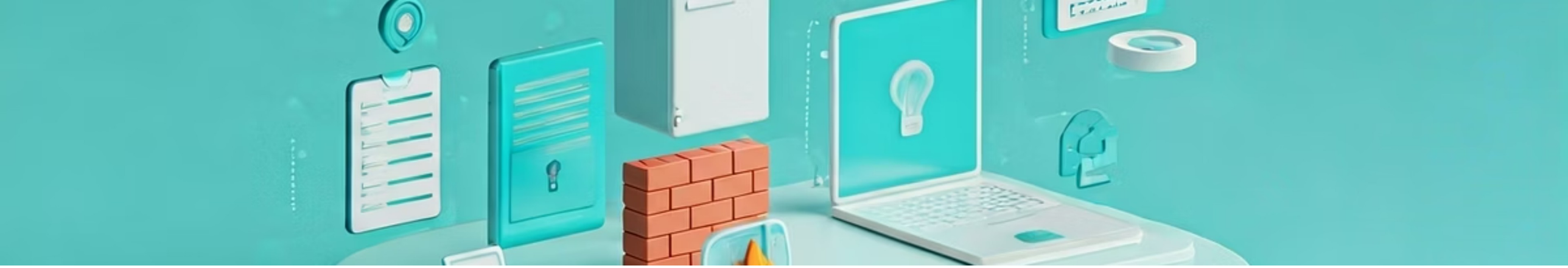


Негізгі міндеттер

Антивирустық бағдарламалар зиянды кодтарды анықтау және жою үшін арнайы әзірленген. Олар сигнатуралық талдау, эвристикалық әдістер және мінез-құлық талдауын пайдаланады.

- **Касперский** – ресейлік өнім, Қазақстанда кеңінен танымал
- **ESET NOD32** – жеңіл және тиімді антивирус
- **Norton** – американдық кешенді қауіпсіздік шешімі
- **Avast** – тегін және ақылы нұсқалары бар танымал өнім

Антивирус бағдарламаларын үнемі жаңарту және толық сканерлеу жүргізу қажет. Олар желілік қауіпсіздіктің бірінші қорғаныс желісі болып табылады.



Желілік қауіпсіздік құралдарының архитектурасы

Заманауи желілік қауіпсіздік архитектурасы көп қабатты қорғанысты қамтиды. Периметрлік қорғаныс (брандмауэрлер), ішкі сегментация, endpoint қорғанысы, мониторинг жүйелері және инцидентке жауап беру жүйелері бірлесіп жұмыс істейді. Бұл құрылым желіні әртүрлі деңгейдегі қатерлерден қорғауға мүмкіндік береді.

Желілік протоколдар және олардың қауіпсіздігі

Желілік протоколдар – бұл желідегі құрылғылардың қалай байланыс жасайтынын анықтайтын ережелер жиынтығы. Қауіпсіздік протоколдары мәліметтерді қорғалған түрде беруді қамтамасыз етеді.



Желілік протоколдар дегеніміз не?

Желілік протоколдар – желідегі құрылғылардың өзара әрекеттесу ережелері. Олар мәліметтердің форматын, беру тәртібін, қателерді өңдеуді және басқа да параметрлерді анықтайды.

Протоколдар әртүрлі деңгейлерде жұмыс істейді – физикалық, канал, желілік, тасымалдау, сеанс, презентация және қолданбалы деңгейлерде (OSI моделі бойынша).

Қауіпсіздік протоколдарының маңызы: Олар аутентификация, шифрлау, тұтастықты тексеру және рұқсатсыз қол жетімділіктен қорғауды қамтамасыз етеді. Протоколсыз қауіпсіз байланыс мүмкін емес.



Ең көп қолданылатын қауіпсіздік протоколдары

SSL/TLS

Веб-қосымшаларды қорғау үшін қолданылады. HTTPS протоколы SSL/TLS негізінде жұмыс істейді. Браузер мен сервер арасындағы мәліметтерді шифрлайды.

IPsec

Желілік деңгейдегі шифрлау протоколы. VPN-да кеңінен қолданылады. IP пакеттерін шифрлау және аутентификациялау арқылы қорғауды қамтамасыз етеді.

SSH

Қауіпсіз қашықтан басқару протоколы. Серверлерге қауіпсіз қосылу үшін пайдаланылады. Құпия сөздер мен кілттер арқылы аутентификация жүргізеді.

Бұл протоколдар интернет қауіпсіздігінің негізін құрайды және күнделікті миллиардтаған қосылымдарды қорғайды. Олардың әрқайсысы белгілі бір міндеттерді шешуге бағытталған.

SSL/TLS протоколының жұмыс істеу принципі

1

Қол алысу (Handshake)

Клиент пен сервер арасында байланыс орнатылады. Протокол нұсқасы, шифрлау алгоритмдері келіседі, сертификаттар тексеріледі.

2

Кілттерді алмасу

Ашық кілт криптографиясы арқылы сеанс кілттері қауіпсіз түрде алмасылады. Бұл кілттер мәліметтерді шифрлау үшін пайдаланылады.

3

Мәліметтерді шифрлау және беру

Барлық деректер симметриялық шифрлау арқылы қорғалады. Әр пакет шифрланып, тұтастығы тексеріліп жіберіледі.

SSL/TLS – интернет-банкинг, электрондық сауда және басқа да сенімді байланысты қажет ететін қызметтердің негізі.



IPsec протоколы

Негізгі ерекшеліктері

IPsec – IP деңгейінде қауіпсіздікті қамтамасыз ететін протоколдар жиынтығы. Ол екі режимде жұмыс істей алады: тасымалдау (Transport) және туннельдеу (Tunnel).

- **AH (Authentication Header)** – аутентификация және тұтастықты қамтамасыз етеді
- **ESP (Encapsulating Security Payload)** – шифрлау, аутентификация және тұтастық
- **IKE (Internet Key Exchange)** – кілттерді басқару

IPsec VPN-да кеңінен қолданылады және site-to-site немесе remote access байланыстарын қорғайды.



Қазақстандағы қолданылуы: Мемлекеттік ұйымдар мен банктер филиалдар арасында қауіпсіз байланыс үшін IPsec VPN-ді белсенді пайдаланады.

SSH протоколы

1

Қашықтан серверге қауіпсіз қосылу

SSH (Secure Shell) серверлерді қашықтан басқару үшін қолданылады. Ол telnet сияқты қауіпсіз емес протоколдардың орнын алды. Барлық командалар мен мәліметтер шифрланады.

2

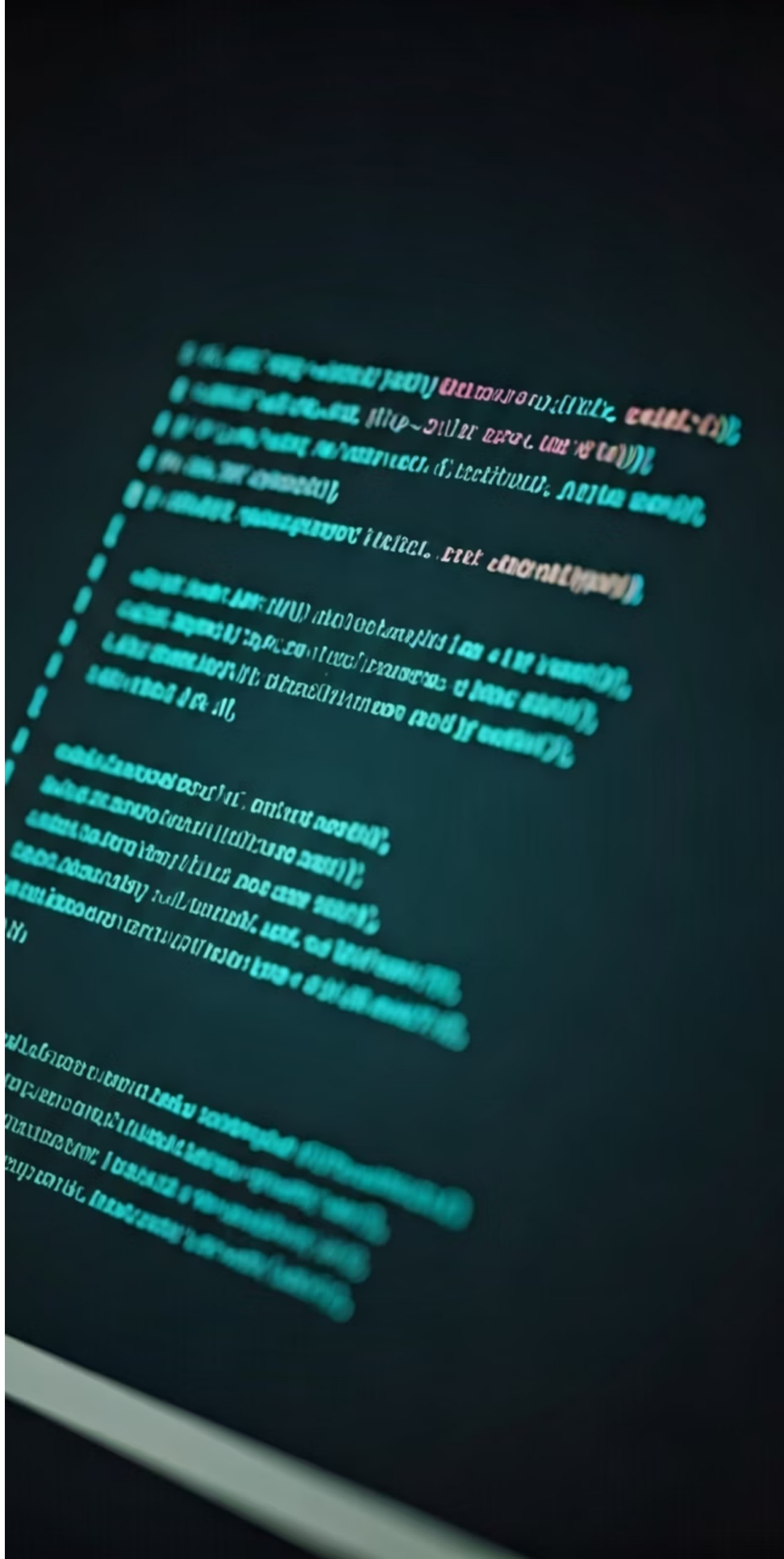
Құпия сөздер мен кілттер арқылы аутентификация

SSH құпия сөз немесе ашық кілт криптографиясын пайдаланады. Кілттік аутентификация құпия сөзден қауіпсізірек және ыңғайлырақ болып саналады.

3

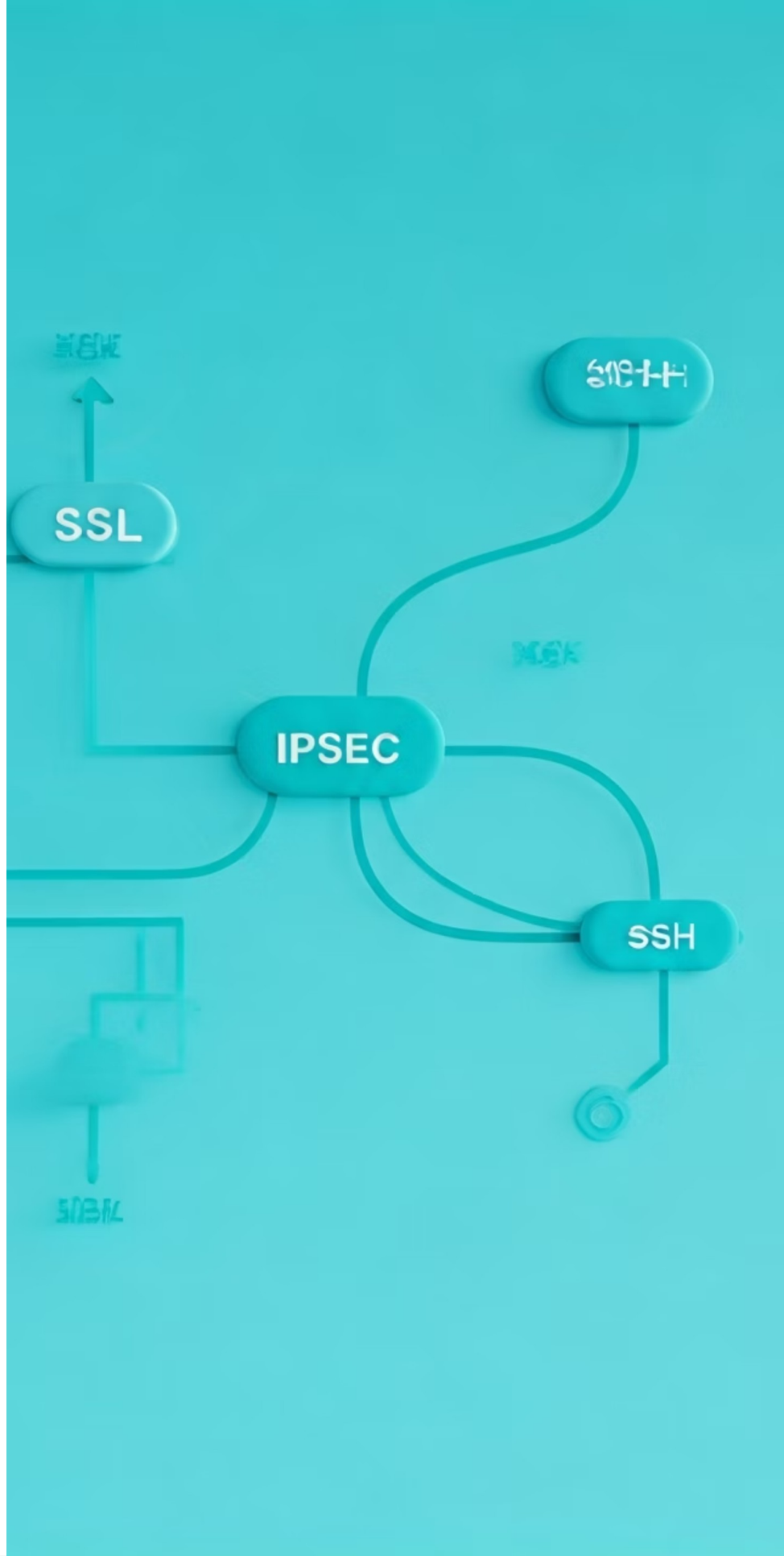
Файлдарды қауіпсіз беру

SCP және SFTP протоколдары SSH негізінде жұмыс істейді және файлдарды қауіпсіз түрде көшіруге мүмкіндік береді. FTP сияқты қауіпсіз емес протоколдар орнына қолданылады.



Протоколдардың жұмыс схемасы

SSL/TLS, IPsec және SSH протоколдары әртүрлі деңгейлерде және сценарийлерде қолданылады. SSL/TLS – веб-трафик үшін, IPsec – желілік деңгейдегі VPN үшін, SSH – серверлерді басқару үшін. Олардың әрқайсысы өз салаларында үздік қауіпсіздікті қамтамасыз етеді және бірлесіп кешенді қорғаныстыны құрайды.

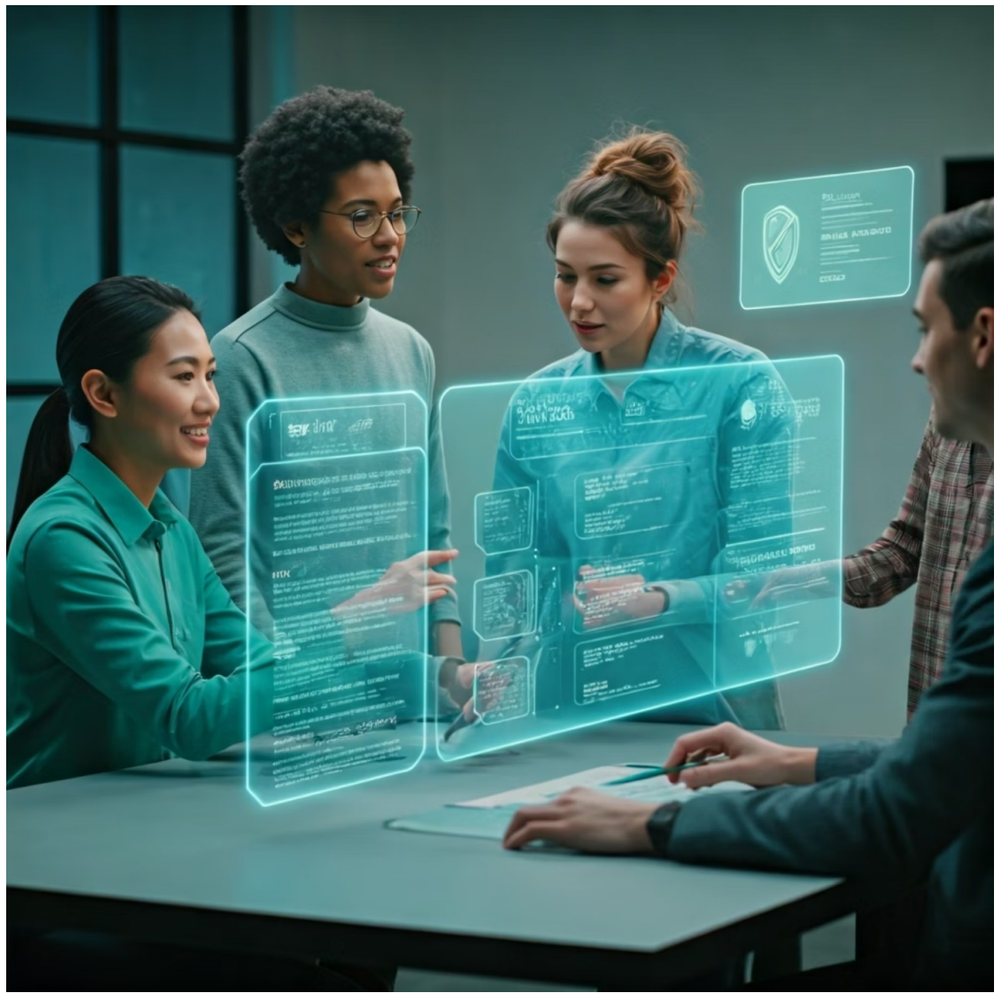




Қауіпсіздік саясаты және желіні қорғау стратегиялары

Тиімді желілік қауіпсіздік технологиялардан ғана емес, сонымен қатар дұрыс ұйымдастырылған саясат пен стратегиядан тұрады. Бұл бөлімде қауіпсіздік саясатын әзірлеу және енгізу мәселелерін қарастырамыз.

Ұйымдағы қауіпсіздік саясатының маңызы



Негізгі компоненттер

Қауіпсіздік саясаты – ұйымдағы ақпараттық қауіпсіздікті қамтамасыз етудің негізі. Ол бекітілген ережелер, рәсімдер және нұсқаулықтар жиынтығынан тұрады.

1. **Қауіпсіздік ережелерін бекіту** – құпия сөздер саясаты, қол жеткізу құқықтары, мәліметтерді жіктеу
2. **Қызметкерлерді оқыту және бақылау** – тұрақты тренингтер, қауіпсіздік хабардарлығын арттыру
3. **Инциденттерге жауап беру жоспары** – шабуыл жағдайында қандай әрекеттер жасау керектігін анықтау

Қауіпсіздік саясатын тек қабылдау жеткіліксіз – оны үнемі қолдану, бақылау және жаңарту қажет.

Қауіпсіздік деңгейін бағалау

01

Желілік аудит жүргізу

Желілік инфрақұрылымды жан-жақты тексеру, әлсіз жақтарды анықтау, конфигурацияларды талдау. Бұл процесс автоматтандырылған құралдар мен қолмен тексеруді қамтиды.

02

Ену тестілеуі (Penetration Testing)

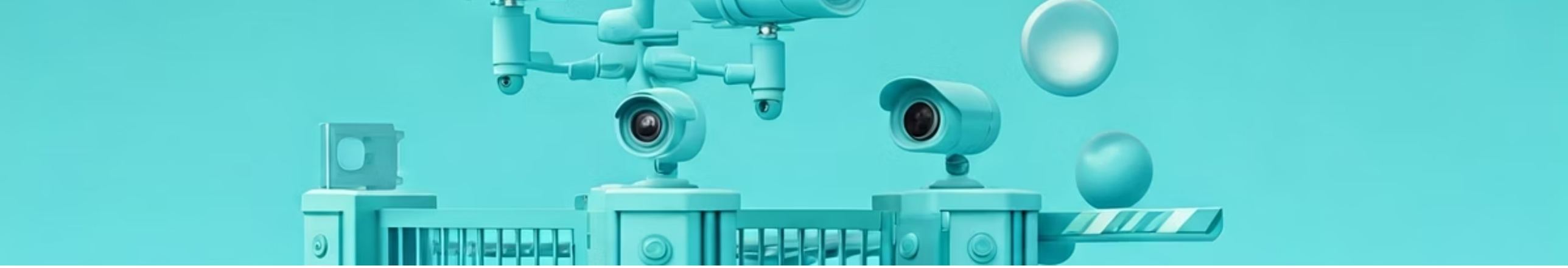
Этикалық хакерлер жүйені нақты шабуыл сценарийлері бойынша тексереді. Бұл әлсіз жерлерді олар пайдаланылғанға дейін табуға көмектеседі.

03

Қазақстандағы стандарттарға сәйкестікті тексеру

Ұлттық стандарттар мен халықаралық ISO 27001, PCI DSS сияқты стандарттарға сәйкестікті қамтамасыз ету. Бұл заңды талаптар мен үздік тәжірибелерге сай келуді білдіреді.

Қауіпсіздік деңгейін жылына кемінде бір рет бағалау және үнемі мониторинг жүргізу ұсынылады.



Қауіпсіздік шараларының кешені

Технологиялық шаралар Брандмауэрлер, антивирус, IDS/IPS, VPN, шифрлау құралдары – технологиялық қорғаныс негізі	**Ұйымдастырушылық шаралар** Саясаттар, рәсімдер, нұсқаулықтар, рөлдер мен жауапкершіліктерді анықтау
Физикалық шаралар Сервер бөлмелерін қорғау, қол жетімді бақылау жүйелері, бейнебақылау	**Адами фактор** Қызметкерлерді оқыту, қауіпсіздік мәдениетін қалыптастыру, әлеуметтік инженерияға қарсы күрес

Құралдар мен протоколдарды үйлестіру, мониторинг және инциденттерге жедел жауап беру – бұл кешенді қауіпсіздіктің міндетті элементтері.

Желілік шабуылдарға қарсы күрес әдістері

IDS/IPS жүйелері

IDS (Intrusion Detection System) – бұзушылықты анықтау жүйесі. Желілік трафикті талдап, күдікті әрекеттерді табады және оның туралы хабарлайды.

IPS (Intrusion Prevention System) – бұзушылықтың алдын алу жүйесі. IDS функцияларынан басқа, анықталған қауіптерді автоматты түрде блоктайды.

- Сигнатуралық анықтау – белгілі шабуылдар үлгілерін іздеу
- Аномалия анықтау – қалыпты мінез-құлықтан ауытқуларды табу
- Мінез-құлық талдауы – күдікті әрекеттерді анықтау



Қауіпсіздік қабаттарын арттыру

Defense in Depth стратегиясы – көп қабатты қорғаныс. Егер бір қабат бұзылса, басқалары қорғай береді.

Әрбір қабат өз функциясын атқарады: периметрлік қорғаныс, сегментация, endpoint қорғанысы, қосымшалар қауіпсіздігі.

Желілік қауіпсіздік архитектурасының үлгісі

Заманауи қауіпсіздік архитектурасы көп деңгейлі қорғанысты ұсынады. Сыртқы периметрден бастап, ішкі сегменттерге дейін әрбір деңгейде әртүрлі қорғаныс механизмдері орналасқан. Мониторинг орталығы барлық қабаттарды бақылап, инциденттерді анықтау және жауап беру функцияларын атқарады. Бұл модель кәсіпорындарға икемді және сенімді қауіпсіздік инфрақұрылымын құруға көмектеседі.





Қазіргі заманғы желілік қауіпсіздік технологиялары

Желілік қауіпсіздік технологиялары үнемі дамып, жаңаруда. Бұлттық шешімдер, жасанды интеллект және жаңа архитектуралық тәсілдер қауіпсіздік саласын трансформациялауда.

Құрылғылар мен бағдарламалық шешімдер

Next-Generation Firewall (NGFW)

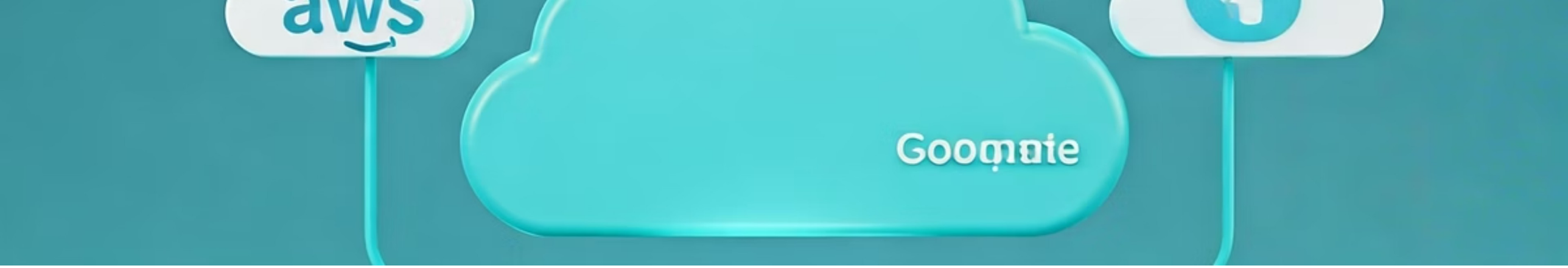
Келесі буын брандмауэрлері дәстүрлі функциялардан тыс мүмкіндіктерді ұсынады. Олар қосымшаларды анықтау, ену алдын алу (IPS), веб-сүзгілеу, SSL инспекциясы және басқа да қосымша функцияларды орындайды.

NGFW трафикті порт және протокол деңгейінде ғана емес, қосымша деңгейінде де талдайды. Бұл нақтырақ бақылау жасауға мүмкіндік береді.

SIEM (Security Information and Event Management)

Қауіпсіздік ақпаратын және оқиғаларын басқару жүйесі барлық қауіпсіздік құралдарынан деректерді жинап, талдайды. SIEM нақты уақытта қауіптерді анықтауға, инциденттерді тергеуге және есептер құруға көмектеседі.

Танымал SIEM шешімдері: Splunk, IBM QRadar, ArcSight, LogRhythm. Олар корпоративті деңгейде кеңінен қолданылады.



Бұлттық қауіпсіздік

AWS қауіпсіздік құралдары

Amazon Web Services кеңінен қауіпсіздік қызметтерін ұсынады: AWS WAF (веб-қосымшалар брандмауэрі), AWS Shield (DDoS қорғанысы), Amazon GuardDuty (қауіп анықтау), AWS Security Hub (орталықтандырылған басқару).

Azure қауіпсіздік шешімдері

Microsoft Azure қауіпсіздік қызметтері: Azure Security Center, Azure Sentinel (SIEM), Azure DDoS Protection, Azure Firewall. Microsoft-тың корпоративті сегменттегі тәжірибесі қауіпсіздік шешімдеріне де көрініс тапқан.

Google Cloud Security

Google Cloud Platform қауіпсіздік құралдары: Cloud Armor (DDoS қорғанысы), Cloud IAM (рұқсат басқару), Security Command Center, Chronicle (қауіп анықтау). Google-дың зерттеулері негізінде әзірленген.

Бұлттық инфрақұрылымды қорғау дәстүрлі желілерден өзгеше. Бұл жерде ортақ жауапкершілік моделі (Shared Responsibility Model) қолданылады – провайдер инфрақұрылымды, тұтынушы өз деректері мен қосымшаларын қорғайды.

Машина оқыту және жасанды интеллект

ЖИ-дің рөлі қауіпсіздікте

Жасанды интеллект пен машина оқыту желілік қауіпсіздікті революциялық түрде өзгертуде. Олар үлкен көлемдегі деректерді талдап, аномалияларды анықтауда адамдарға қарағанда жылдамырақ әрі дәлірек.

- **Қауіптерді алдын ала анықтау** – Machine Learning модельдері белгісіз шабуылдарды да табады
- **Автоматтандырылған жауап беру** – AI жүйелері өздігінен қауіпті блоктайды
- **Жалған дабыларды азайту** – интеллектуалды сүзгілер шынайы қауіптерді ажыратады



Алайда, хакерлер де ЖИ-ді қолданады – шабуылдарды автоматтандыру, фишинг хаттарын жасау, қорғанысты айналып өту үшін. Бұл AI гонкасын туғызады.



Zero Trust архитектурасы

«Ешкімге сенбе, бәрін тексер» қағидасы

Zero Trust моделі дәстүрлі «периметрлік қорғаныс» тұжырымдамасын жояды. Бұл модельде ешқандай пайдаланушы немесе құрылғы автоматты түрде сенімді деп саналмайды – тіпті ішкі желіде тұрса да.

Қолданушылар мен құрылғыларды үздіксіз аутентификациялау

Әрбір қосылым, әрбір сұраныс тексеріледі. Көп факторлы аутентификация, контекстік талдау (құрылғы, орналасу, уақыт) және микросегментация қолданылады.

Ең аз артықшылықтар принципі

Пайдаланушылар мен қосымшалар тек қажетті минимум ресурстарға ғана қол жеткізе алады. Бұл потенциалды залалдың ауқымын шектейді.

Zero Trust – бұл тек технология емес, бұл қауіпсіздікке жаңа көзқарас. Ол гибридті және бұлттық орталарда әсіресе тиімді.



Zero Trust желілік қауіпсіздік моделі

Zero Trust архитектурасы сенім шекарасын желі периметрінен әрбір пайдаланушы мен құрылғыға көшіреді. Бұл модельде микросегментация, динамикалық саясаттар, үздіксіз бақылау және автоматтандырылған жауап беру бірлесіп жұмыс істейді. Идентификация басқару платформасы (IAM) орталық рөл атқарып, барлық қол жетімді бақылайды. Нәтижесінде инсайдерлік қауіптер мен латералды қозғалыстар шектеледі.

Қазақстандағы желілік қауіпсіздік жағдайы және нормативтік база

Қазақстан желілік қауіпсіздікті мемлекеттік деңгейде басым бағыт ретінде қарастырады. Заңнамалық база мен мамандар даярлау жүйесі белсенді дамуда.



Қазақстандағы желілік қауіпсіздік саласындағы заңдар мен стандарттар

«Ақпараттандыру туралы» Заңы

Ақпараттық жүйелердің қауіпсіздігі, жеке деректерді қорғау және ақпараттық қауіпсіздік талаптарын реттейтін негізгі заң. Ұйымдар мен мемлекеттік органдар үшін міндетті нормалар белгілейді.

6B06303 «Желілік қауіпсіздік» мамандығы

Қазақстандық жоғары оқу орындарында желілік қауіпсіздік бойынша мамандар даярлау бағдарламасы. Бұл мамандық технологиялық дағдыларды, криптографияны, желілік протоколдарды және киберқорғанысты қамтиды.

Ақпараттық қауіпсіздік бойынша мемлекеттік бағдарламалар

«Цифрлық Қазақстан» бағдарламасы шеңберінде киберқауіпсіздікті дамыту шаралары жүзеге асырылуда. Ұлттық қауіпсіздік жүйесін нығайту, инфрақұрылымды қорғау және халықаралық ынтымақтастықты дамыту назарда.

Қазақстан халықаралық киберқауіпсіздік ұйымдарымен белсенді ынтымақтасады және озық тәжірибелерді енгізуде.

Ұлттық қауіпсіздік агенттігінің рөлі



Негізгі функциялар

Ұлттық қауіпсіздік агенттігі (ҰҚА) Қазақстанның киберқауіпсіздігін қамтамасыз етуде жетекші рөл атқарады.

- **Желілік қауіпсіздік мониторингі** – сыни маңызды инфрақұрылымды үздіксіз бақылау
- **Қауіптерге қарсы іс-қимыл** – кибершабуылдарды анықтау және жою
- **Халықаралық ынтымақтастық** – басқа елдермен киберқауіптер туралы ақпарат алмасу
- **Стандарттар әзірлеу** – ұлттық қауіпсіздік талаптарын белгілеу

ҰҚА мемлекеттік органдар мен критикалық инфрақұрылым объектілеріне киберқорғаныс бойынша кеңес береді.



Қазақстандағы желілік шабуылдар мен олардың салдары

1

2023 жыл

Бірнеше мемлекеттік порталдарға DDoS шабуылдары жасалды. Қызметтер уақытша тоқтатылды, бірақ деректер жоғалған жоқ. Қорғаныс жүйелері күшейтілді.

2

2024 жыл

Банк секторына фишинг науқаны бағытталды. Бірнеше клиенттер құрбан болды, бірақ банктердің жедел әрекеті залалды азайтты. Қауіпсіздік хабардарлығын арттыру науқандары өткізілді.

3

2025 жыл

Ransomware шабуылдары жеке компанияларға бағытталды. Киберқылмыскерлер құпия деректерді шифрлап, төлем талап етті. Бұл инциденттер бекап жасаудың маңыздылығын көрсетті.

Қорғаныс шараларының тиімділігі артуда – инциденттерге жауап беру уақыты қысқарды, автоматтандыру деңгейі өсті, мамандардың біліктілігі жоғарылады.



Қазақстандағы киберқауіпсіздік инфрақұрылымы

Қазақстанның киберқауіпсіздік инфрақұрылымы мемлекеттік мониторинг орталықтары, сыни инфрақұрылым объектілерінің қорғаныс жүйелері, зерттеу орталықтары және мамандар даярлау мекемелерінен тұрады. Ұлттық CERT (Computer Emergency Response Team) киберинциденттерге жедел жауап береді. Халықаралық ынтымақтастық аясында озық технологиялар мен тәжірибелер енгізілуде.

Практикалық кеңестер мен ұсыныстар

Теориялық білімді практикаға қолдану – желілік қауіпсіздіктің ең маңызды аспектісі. Бұл бөлімде нақты кеңестер мен ұсыныстар берілген.



Желілік қауіпсіздікті қамтамасыз етудің негізгі ережелері

1 Құпия сөздерді үнемі жаңарту

Күрделі құпия сөздерді қолданыңыз: кемінде 12 символ, әріптер, сандар, арнайы белгілер. Әр қызметке әр түрлі құпия сөз пайдаланыңыз. Құпия сөздер менеджерін (Password Manager) қолданған тиімді. Құпия сөзді 3-6 айда бір рет ауыстырыңыз.

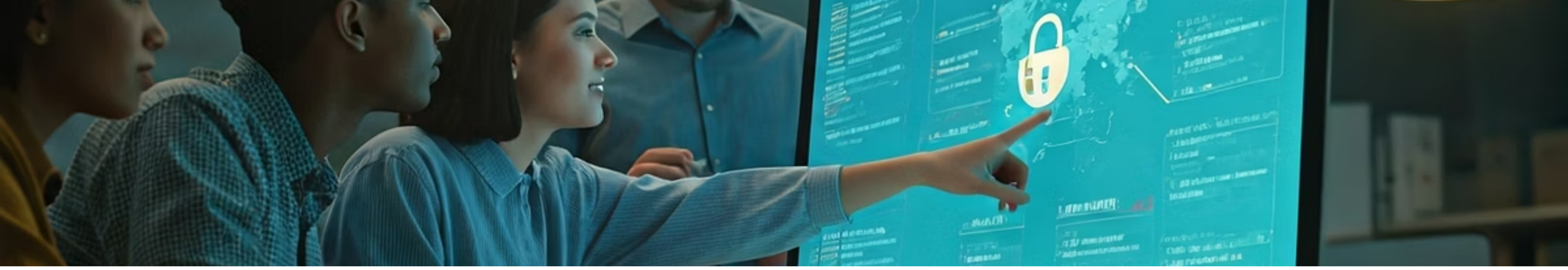
2 Құрылғылар мен бағдарламаларды жаңарту

Операциялық жүйелерді, қосымшаларды және антивирус базаларын үнемі жаңартып отырыңыз. Жаңартулар қауіпсіздік олқылықтарын жояды. Автоматты жаңарту функциясын қосыңыз. Қолдау тоқтатылған бағдарламаларды пайдаланбаңыз.

3 Қызметкерлерді оқыту

Барлық қызметкерлерге киберқауіпсіздік бойынша тұрақты тренингтер өткізіңіз. Фишингті танып білуге үйретіңіз. Қауіпсіздік инциденттері туралы хабарлау рәсімін түсіндіріңіз. Қауіпсіздік мәдениетін қалыптастырыңыз.

Маңызды ескерту: Қауіпсіздік – бір реттік шара емес, үздіксіз процесс. Үнемі сақ болу және жаңа қауіптерді қадағалау қажет.



Қауіпсіздік инциденттеріне дайындық

Жедел әрекет ету жоспары дайындау

Инцидент жағдайында не істеу керектігін алдын ала жоспарлаңыз. Жауапты адамдарды тағайындаңыз, байланыс тізімін жасаңыз, эскалация процедурасын белгілеңіз. Жоспарды жазбаша түрде ресімдеңіз.

Инциденттерді анықтау және оқшаулау

Мониторинг жүйелері арқылы күдікті әрекеттерді анықтаңыз. Зардап шеккен жүйелерді желіден оқшаулаңыз. Қосымша залалдың алдын алыңыз. Барлық әрекеттерді құжаттаңыз.

Қалпына келтіру және талдау

Зақымдалған жүйелерді тазалаңыз немесе қайта орнатыңыз. Бекаптардан деректерді қалпына келтіріңіз. Инцидент себептерін талдап, олқылықтарды жойыңыз. Есепті әзірлеп, қорытынды жасаңыз.

Үйрену және жетілдіру

Инциденттен сабақ алыңыз. Қорғаныс жүйесін күшейтіңіз. Рәсімдерді жетілдіріңіз. Қызметкерлерге қосымша оқыту өткізіңіз. Кезекті тестілеу жүргізіңіз.

Қорытынды: Желілік қауіпсіздік – тұрақты даму кепілі

Кешенді тәсіл

Қауіпсіздік құралдары мен протоколдарды үйлестіріп қолдану – технологиялық, ұйымдастырушылық және адами факторларды біріктіру арқылы максималды қорғанысқа жету.

Үздіксіз даму

Киберқауіптер үнемі эволюцияланууда, сондықтан қорғаныс жүйелері де дамып отыруы керек. Жаңа технологияларды енгізу, мамандарды оқыту, тәжірибе алмасу маңызды.

Ұлттық қауіпсіздік

Қазақстанның цифрлық қауіпсіздігін нығайтуға әрбір маман, әрбір ұйым үлес қоса алады. Бірлескен күш-жігер арқылы қауіпсіз цифрлық кеңістік құрамыз.

Желілік қауіпсіздік – бұл бір жолы емес, үздіксіз саяхат. Технологиялар дамып, қауіптер өзгеріп, қорғаныс әдістері жетіліп отырады. Маңыздысы – сақ болу, білім жинау және қауіпсіздік мәдениетін қалыптастыру. Осы принциптерді ұстана отырып, біз сенімді және қауіпсіз цифрлық болашақ құра аламыз.

Назар аударыңыз: Бұл презентация желілік қауіпсіздіктің негізгі аспектілерін қамтыды. Тереңірек зерттеу үшін арнайы әдебиеттермен танысыңыз, практикалық тәжірибе жинаңыз және кәсіби сертификаттар алуды қарастырыңыз (CEH, CISSP, CompTIA Security+).