Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university



Қолданбалы бағдарламалардағы қауіпсіздік механизмдері



Кіріспе: Қауіпсіздік маңыздылығы

Күнделікті өмір

Қолданбалы бағдарламалар біздің күнделікті өміріміздің ажырамас бөлігіне айналды. Банктік операциялардан бастап әлеуметтік желілерге дейін барлық салада қолданамыз.

Ақпараттық қауіпсіздік

Деректердің құпиялылығы, тұтастығы және қолжетімділігін сақтау – қазіргі заманғы технологиялық әлемнің негізгі талаптарының бірі болып табылады.

Қорғаныс құралдары

Қауіпсіздік механизмдері шабуылдардан қорғанудың негізгі құралдары ретінде қолданушылар мен ұйымдардың мүдделерін қорғайды.

Қолданбалы бағдарламалар түрлері

Жалпы қолданыстағы бағдарламалар

Microsoft Word, Excel, PowerPoint сияқты офистік пакеттер және Google Chrome, Mozilla Firefox сияқты веб-браузерлер күнделікті қолданыста кең тараған. Олар миллиондаған пайдаланушыларға қызмет етеді.

Арнайы қызметтегі бағдарламалар

Медициналық ақпараттық жүйелер, банктік қосымшалар және қаржылық талдау құралдары сезімтал деректермен жұмыс істейді. Олардың қауіпсіздігі өте маңызды.

Кәсіптік деңгейдегі бағдарламалар

ERP (кәсіпорынды басқару жүйелері), CRM (клиенттермен қарым-қатынасты басқару) және бухгалтерлік жүйелер ірі ұйымдардың негізгі процестерін автоматтандырады.



Қауіптер мен шабуылдар түрлері

Пассивті шабуылдар

Шабуылдаушы жүйедегі ақпаратты тек бақылайды және тыңдайды, деректерді өзгертпейді:

- Желілік трафикті ұстап қалу
- Электрондық поштаны мониторингілеу
- Байланыс каналдарын тыңдау
- Метадеректерді жинау

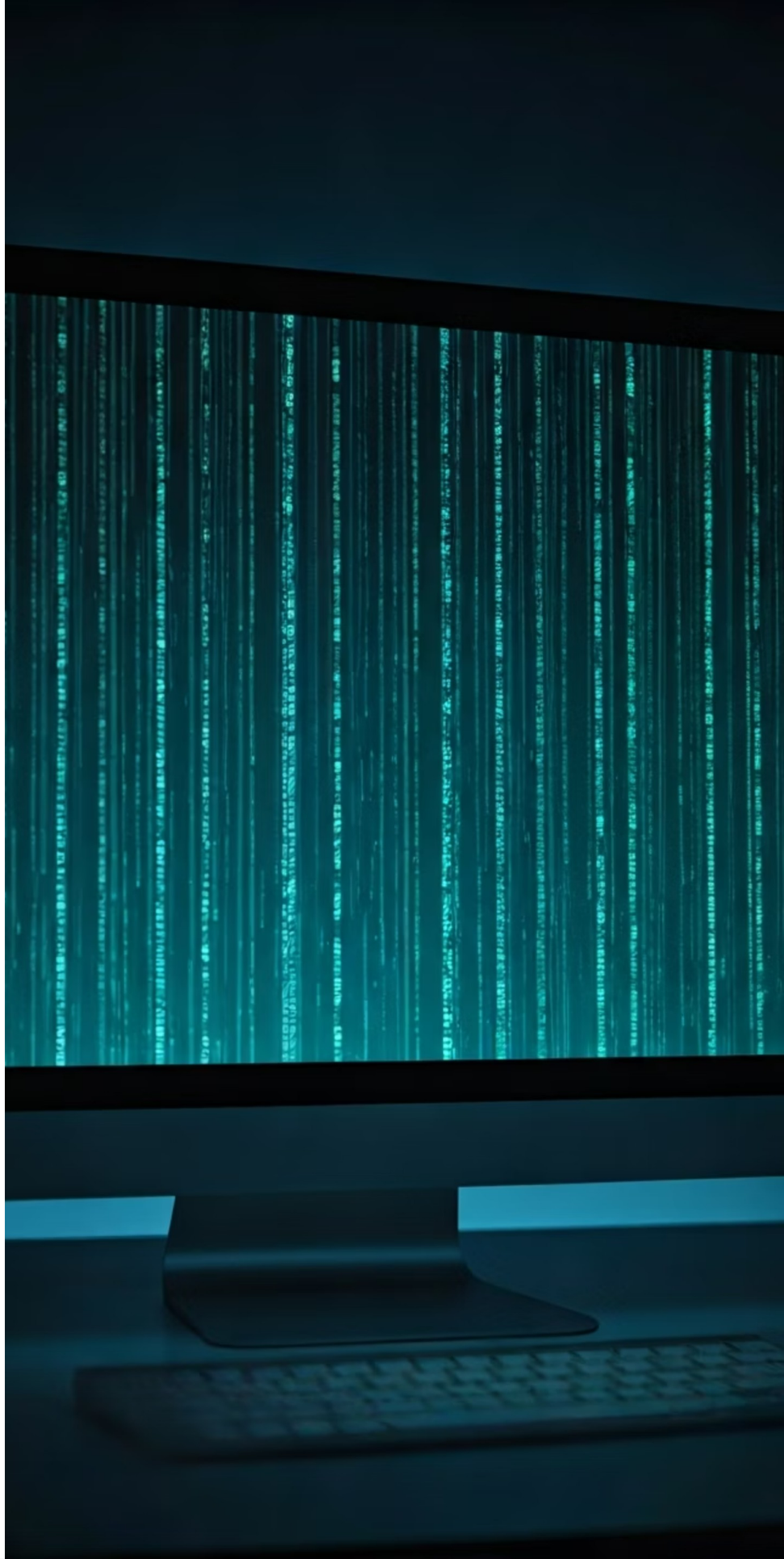
Активті шабуылдар

Шабуылдаушы белсенді түрде жүйеге араласып, деректерді өзгертеді немесе бұзады:

- Деректерді жалған мәліметтермен алмастыру
- DoS шабуылдары арқылы қызметтен бас тарту
- Man-in-the-middle шабуылдары
- Replay-шабуылдар және фальсификация

"Қауіптер күннен-күнге күрделенуде"

Киберқауіпсіздік саласындағы сарапшылар әр жыл сайын шабуылдардың күрделенуі мен санының артуын байқайды



Ақпараттық қауіпсіздіктің негізгі ұғымдары

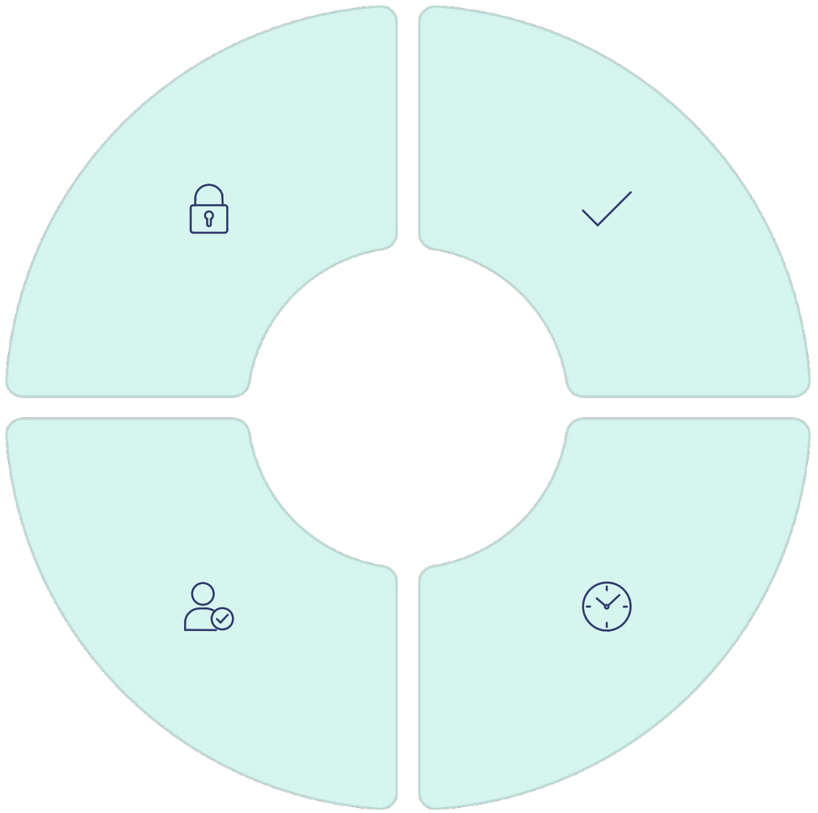
Ақпараттық қауіпсіздік үш негізгі тіректен тұрады – CIA триадасы деп аталатын модель:

Құпиялылық

Ақпаратқа тек рұқсат етілген пайдаланушылар қол жеткізе алады. Шифрлау және аутентификация арқылы қамтамасыз етіледі.

Жауапкершілік

Әрбір әрекетті орындаушыны анықтау мүмкіндігі. Аудит журналдары арқылы іске асырылады.



Тұтастық

Деректердің дұрыстығы мен толықтығы сақталады. Рұқсатсыз өзгертулер мен бұзулардан қорғалады.

Қолжетімділік

Жүйе мен деректер қажет кезінде пайдаланушыларға қолжетімді болуы тиіс. DoS шабуылдарынан қорғау маңызды.

Қауіпсіздік механизмдерінің түрлері

Аутентификация және авторизация

Пайдаланушының жеке басын растау және оның жүйедегі құқықтарын анықтау процестері. Қауіпсіздіктің бірінші қорғаныс желісі.

Шифрлау әдістері

Криптографиялық алгоритмдер арқылы деректерді қорғау. Симметриялық және асимметриялық шифрлау технологиялары қолданылады.

Қауіпсіздік саясаты

Рұқсаттар жүйесі мен қауіпсіздік ережелерін белгілеу. Әр пайдаланушыға минималды қажетті құқықтар беріледі.

Аудит және журнал

Барлық маңызды оқиғаларды тіркеу және талдау. Қауіпсіздік инциденттерін анықтау мен тергеуге көмектеседі.



Аутентификация әдістері

Құпия сөздер

Ең кең таралған әдіс. PIN-кодтар мен парольдер қарапайым, бірақ әлсіз болуы мүмкін.

Күшті құпия сөз:

- Кемінде 12 таңба
- Әріптер, сандар, символдар
- Тұрақты өзгертілу

Биометрия

Саусақ ізі, бет-әлпет тану, көз торшасы сканері арқылы анықтау.

Артықшылықтары:

- Жеке басты нақты растау
- Ұмыту мүмкіндігі жоқ
- Ыңғайлы қолдану

Екі факторлы аутентификация

Қосымша қорғаныс қабаты. SMS-код, аутентификатор қосымшасы немесе hardware токен.

2FA компоненттері:

- Білетін нәрсе (пароль)
- Иелік ететін нәрсе (телефон)
- Биологиялық белгі

Шифрлау технологиялары

Криптография ақпаратты қорғаудың математикалық негізі болып табылады. Заманауи шифрлау әдістері деректердің құпиялылығын және тұтастығын қамтамасыз етеді.

Симметриялық шифрлау

Шифрлау және дешифрлау үшін бір кілт қолданылады. AES, DES алгоритмдері жылдам жұмыс істейді, бірақ кілтті қауіпсіз тарату қиын.

- Жылдам өңдеу
- Үлкен деректер көлеміне қолайлы
- Кілт басқаруы қиын

Асимметриялық шифрлау

Ашық және жабық кілттер жұбын қолданады. RSA, ECC алгоритмдері қауіпсіз кілт алмасуды қамтамасыз етеді, бірақ баяу жұмыс істейді.

- Қауіпсіз кілт алмасу
- Цифрлық қолтаңба
- Өңдеу баяу

SSL/TLS протоколдары

Интернет байланысын шифрлау стандарты. HTTPS қауіпсіз веб-коммуникацияны қамтамасыз етеді. Барлық сезімтал деректер үшін міндетті.

- Веб-трафикті қорғау
- Сертификаттар арқылы растау
- End-to-end шифрлау

Қауіпсіздік саясатының рөлі

Қауіпсіздік саясаты – ұйымдағы ақпараттық қауіпсіздікті басқарудың негізі. Ол барлық процестер мен процедураларды регламенттейді.

Құқықтарды шектеу

Пайдаланушылардың жүйедегі рұқсаттарын минималды қажетті деңгейге дейін азайту принципі (Principle of Least Privilege).

Ережелерді бекіту

Қауіпсіздік стандарттарын, процедураларды және нұсқауларды әзірлеу, бекіту және бақылау процесі.

Оқиғаларды басқару

Қауіпсіздік инциденттеріне жауап беру, талдау және алдын алу шараларын қабылдау жүйесі.



Қауіпсіз кодтау принциптері

Қауіпсіз бағдарламалық қамтамасыз ету жасау үшін әзірлеушілер бірқатар негізгі принциптерді ұстануы қажет. Бұл принциптер осалдықтарды азайтады.

1

SQL Injection қорғанысы

Деректер базасына зиянды SQL командаларын енгізу шабуылдарынан қорғау үшін параметрленген сұраулар және енгізу деректерін валидациялау қолданылады.

2

XSS қорғанысы

Cross-Site Scripting шабуылдарынан қорғану үшін пайдаланушы енгізген барлық мәліметтерді escape және санитизация процестерінен өткізу керек.

3

Қате өңдеу

Жүйелік ақпаратты шабуылдаушыларға жария етпеу үшін қателерді дұрыс өңдеу және пайдаланушыға жалпы хабарламалар көрсету қажет.

4

Қауіпсіздік тестілеу

Penetration testing, code review және автоматтандырылған сканерлеу арқылы осалдықтарды ерте кезеңде анықтау және жою маңызды.

Қолданбалы бағдарламаларда қауіпсіздік кітапханалары мен фреймворктер

OWASP ұсыныстары

Open Web Application Security Project – әлемдік қауіпсіздік стандарттары:

- OWASP Top 10 – ең кең таралған осалдықтар тізімі
- Қауіпсіздік бойынша үздік тәжірибелер
- Тегін құралдар мен кітапханалар
- Қауғамдық білім базасы

Интеграция әдістері

Қауіпсіздік модульдерін жобаға қосу:

- Аутентификация кітапханалары
- Шифрлау API-лары
- Валидация фреймворктері



Автоматты сканерлер: OWASP ZAP, Burp Suite, SonarQube сияқты құралдар кодтағы қауіпсіздік осалдықтарын автоматты түрде анықтайды және есеп береді.

Қолданбалы бағдарламалардағы жаңартулар мен патчтар

01

Осалдықтарды анықтау

Қауіпсіздік сарапшылары немесе хакерлер жүйедегі әлсіз жерлерді табады. CVE (Common Vulnerabilities and Exposures) тізіміне енгізіледі.

02

Патч әзірлеу

Әзірлеушілер осалдықты жоятын код жазады және сынақтан өткізеді. Қауіпсіздік бюллетені жариялайды.

03

Таратуды ұйымдастыру

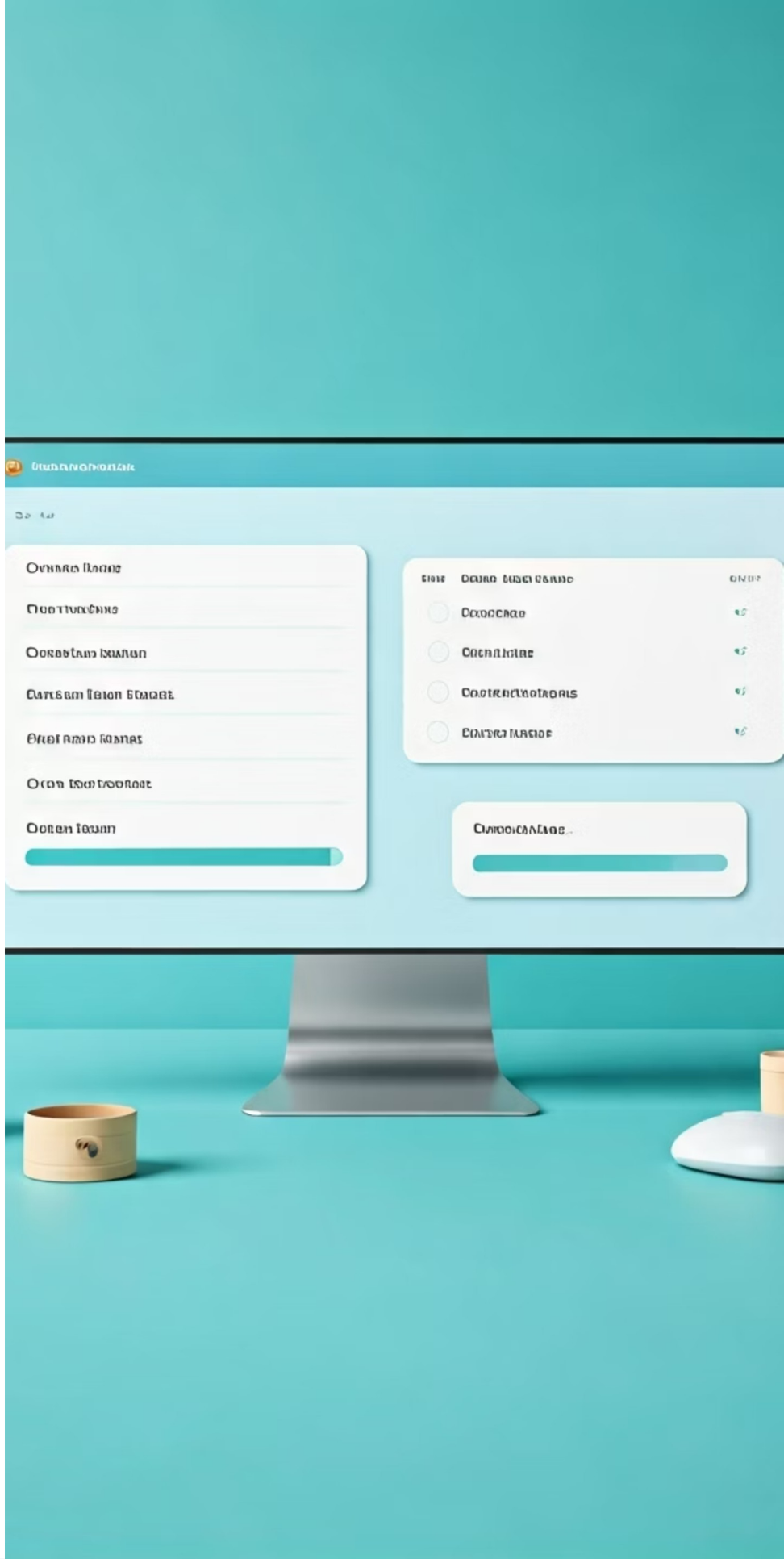
Патчты барлық пайдаланушыларға жеткізу механизмін қамтамасыз ету. Автоматты жаңарту жүйелері арқылы.

04

Хабарлама жіберу

Пайдаланушыларға осалдық туралы және жаңарту қажеттілігі туралы ақпарат беру. Критикалық патчтар үшін міндетті.

Тұрақты жаңартулар қауіпсіздіктің негізгі элементі болып табылады. Көптеген шабуылдар ескірген бағдарламалық қамтамасыз етудің белгілі осалдықтарын пайдаланады.



Желілік қауіпсіздік модельдері

Желілік қауіпсіздік қолданбалы бағдарламалардың сыртқы қауіптерден қорғалуын қамтамасыз етеді. Бірнеше деңгейлі қорғаныс қолданылады.

IPSec протоколы

IP деңгейінде деректерді шифрлау және аутентификациялау. VPN байланыстары үшін кең қолданылады. End-to-end қауіпсіздікті қамтамасыз етеді.

VPN технологиясы

Virtual Private Network қауіпсіз туннель құрады. Қашықтағы қолжетімділік пен филиалдарды қосу үшін қолданылады. Трафикті шифрлайды.

Firewall жүйелері

Қауіпсіздік қабырғалары трафикті сүзеді. Рұқсат етілмеген байланыстарды блоктайды. Ішкі желіні сыртқы қауіптерден қорғайды.

Желілік шабуылдар және қорғаныс

DoS және DDoS

Denial of Service шабуылдары жүйені шамадан тыс сұрауларға бөлейді:

- Қызмет көрсетуді тоқтату
- Ресурстарды толықтай пайдалану
- Легитимді пайдаланушыларды блоктау

Қорғаныс шаралары

- Rate limiting механизмдері
- CDN қызметтерін қолдану
- Трафикті талдау жүйелері
- Автоматты сүзу ережелері

IDS/IPS жүйелері

Intrusion Detection/Prevention Systems – шабуылдарды анықтау және алдын алу жүйелері.

IDS функциялары:

- Желілік трафикті мониторинг
- Қауіпті үлгілерді анықтау
- Хабарландыру жүйесі
- Инцидент логтарын жүргізу

IPS артықшылықтары:

- Нақты уақытта блоктау
- Автоматты жауап беру
- Шабуылды тоқтату



Қолданбалы бағдарламалар мен желілік қауіпсіздік интеграциясы

API қауіпсіздігі

REST API және GraphQL endpoint-терін қорғау. OAuth 2.0, API keys және rate limiting арқылы қолжетімділікті бақылау. CORS саясатын дұрыс конфигурациялау.

1

Сессия басқару

Қауіпсіз сессия токендерін генерациялау. Сессия timeout және автоматты logout. CSRF және session hijacking шабуылдарынан қорғау.

2

Сервер байланысы

Клиент пен сервер арасындағы коммуникацияны HTTPS, TLS 1.3 арқылы шифрлау. Сертификаттарды валидациялау және mutual authentication қолдану.

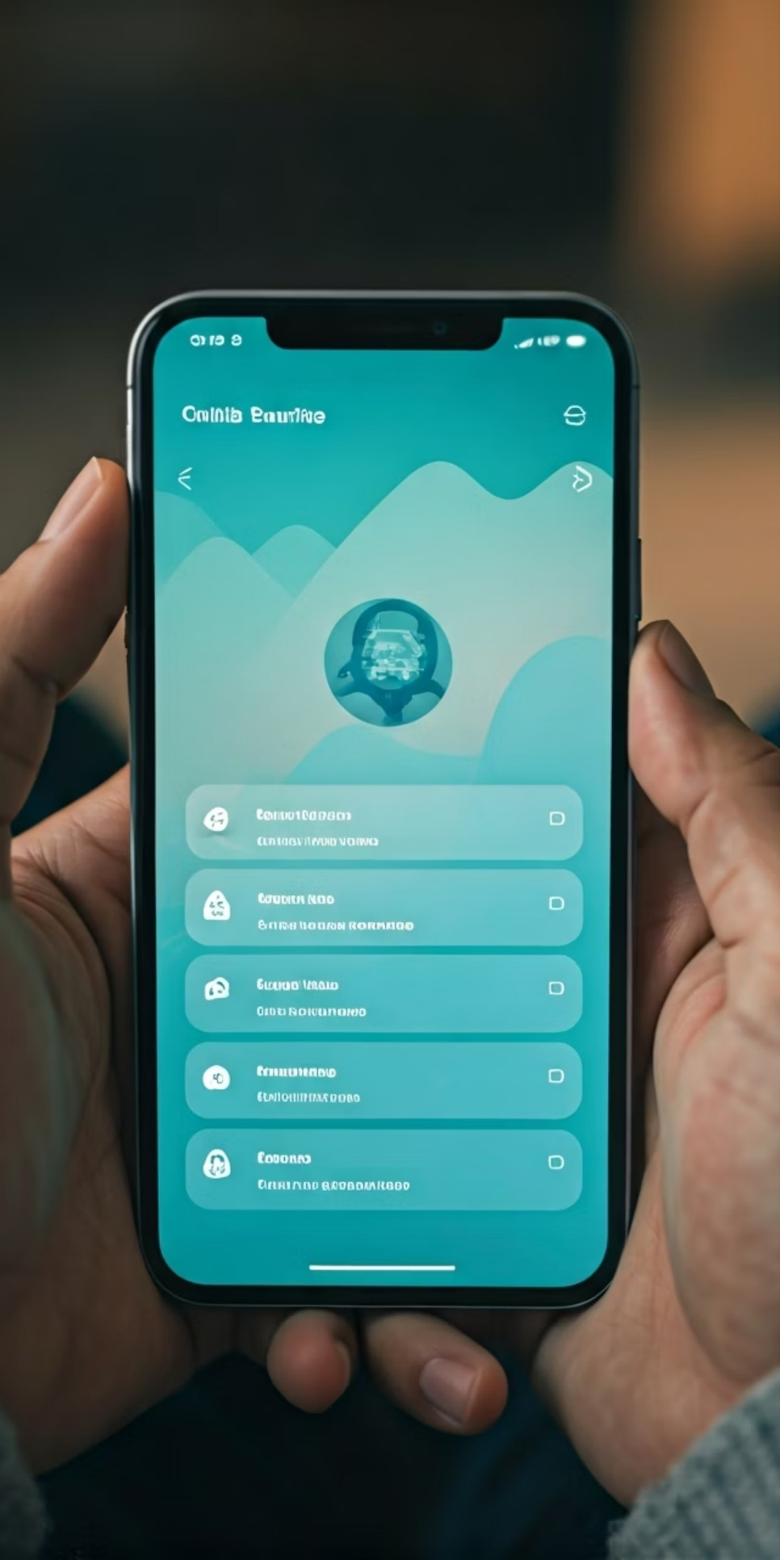
3

Қолданбалы бағдарламалар мен желілік қауіпсіздіктің тығыз интеграциясы жүйенің жалпы қауіпсіздік деңгейін арттырады. Әрбір компонент өзінің қорғаныс механизмдерімен қамтамасыз етілуі керек.

Желілік қауіптер

Заманауи желілік шабуылдардың схемасы және олармен күресу құралдары





Мобильді қолданбалардағы қауіпсіздік мәселелері

Смартфондардың кең таралуымен мобильді қосымшалар шабуылдаушылардың басты мақсатына айналды. Жеке деректер, банктік ақпарат және корпоративті деректер қауіп төндірумен бетпе-бет.

Деректер ұрлану

Құпия ақпараттың рұқсатсыз алынуы – ең үлкен қауіп. Жеке мәліметтер, парольдер, банктік деректер және геолокация мәліметтері қауіп астында.

- Шифрланбаған деректер сақтау
- Қауіпсіз емес желілік трафик
- Зиянды қосымшалар арқылы

Рұқсаттарды бақылау

Қосымшалар көбінесе қажетінен артық рұқсаттарды сұрайды. Камера, микрофон, контактілер және геолокацияға қолжетімділік.

- Артық рұқсаттар қауіпті
- Principle of Least Privilege принципі
- Runtime рұқсаттар жүйесі

Зиянды бағдарламалар

Malware және троян бағдарламалар мобильді құрылғыларды жұқтырады. Фишинг әдістері арқылы таралады.

- Тек ресми дүкендерден орнату
- Антивирус қолдану
- Күдікті сілтемелерді ашпау

Бұлттық қызметтердегі қауіпсіздік

Cloud computing технологиялары деректерді сақтау мен өңдеудің жаңа мүмкіндіктерін ашады, бірақ жаңа қауіпсіздік мәселелері де пайда болады.

Деректер қауіпсіздігі

Бұлттағы ақпараттың құпиялылығы мен тұтастығын қамтамасыз ету:

- End-to-end шифрлау
- Деректердің географиялық орналасуы
- Multi-tenancy изоляциясы
- Деректерді жою саясаты

Сертификаттар

Халықаралық стандарттарға сәйкестік:

- ISO 27001
- SOC 2 Type II
- GDPR сәйкестігі
- Индустрияға арнайы сертификаттар



Архитектура

Қауіпсіз бұлттық жүйелерді құру принциптері:

- Zero Trust архитектурасы
- Микросервистер изоляциясы
- API Gateway қауіпсіздігі
- Identity and Access Management
- Логтарды орталықтандыру

IoT және қолданбалы бағдарламалар қауіпсіздігі

Internet of Things құрылғыларының саны өсіп келеді, ал олардың қауіпсіздігі көбінесе елеусіз қалдырылады. IoT экосистемасы жаңа шабуыл векторларын ашады.

Құрылғылар осалдығы

Көптеген IoT құрылғылары әлсіз қауіпсіздік параметрлерімен шығарылады. Әдепкі парольдер, жаңартулардың болмауы.

Қорғаныс деңгейлері

Edge, fog және cloud деңгейлерінде қауіпсіздік шараларын қолдану. Көп қабатты қорғаныс.

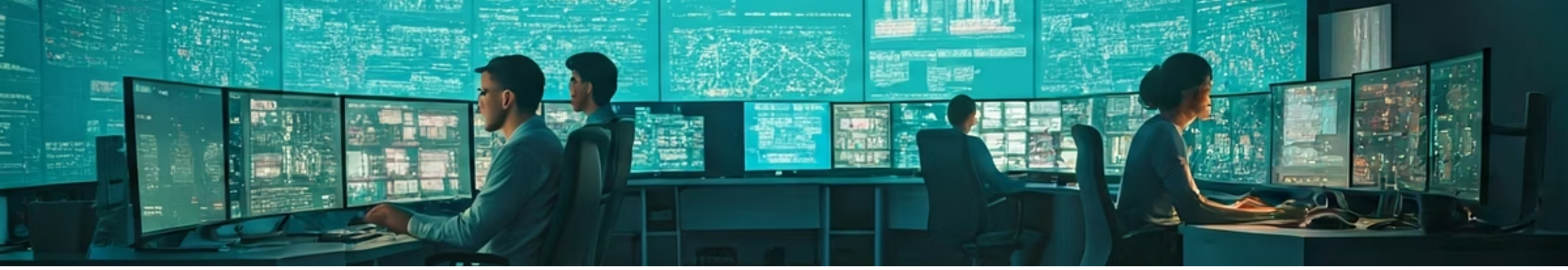


Аутентификация

Құрылғылардың жеке басын растау механизмдері. Сертификат негізіндегі аутентификация қолдану.

Қауіпсіздік хаттамалары

MQTT, CoAP сияқты IoT хаттамаларын қауіпсіз конфигурациялау. TLS шифрлауын қолдану.



Ұлттық үйлестіру орталығы (АҚҰҮО)

.Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы – Қазақстанның киберқауіпсіздік саласындағы негізгі мемлекеттік органы

Үйлестіру және бақылау

АҚҰҮО барлық мемлекеттік органдар мен критикалық инфрақұрылым объектілері арасында ақпараттық қауіпсіздік шараларын үйлестіреді. Киберинциденттерге жауап беруді .басқарады

Мемлекеттік саясат

Киберқауіпсіздік саласындағы ұлттық стратегияны әзірлейді және іске асырады. Қауіпсіздік стандарттары мен .нормативтерді белгілейді

Халықаралық ынтымақтастық

Басқа елдердің киберқауіпсіздік орталықтарымен ынтымақтастық жасайды. Ақпарат алмасу және .бірлескен жобалар жүргізу

Заңнамалық база және нормативтер

Негізгі заңдар

- «Ақпараттандыру туралы» Заң
- «Жеке деректер және оларды қорғау туралы» Заң
- «Байланыс туралы» Заң
- Қылмыстық кодекстің киберқауіпсіздік баптары

Қауіпсіздік талаптары

- Мемлекеттік ақпараттық жүйелер үшін талаптар
- Жеке деректерді өңдеу ережелері
- Критикалық инфрақұрылым қорғау
- Инцидент хабарлау міндеттері

Сертификаттау

- ҚР СТ ISO/IEC 27001 стандарты
- Ақпараттық жүйелерді сертификаттау
- Криптографиялық құралдарды лицензиялау
- Мамандарды аттестаттау

Қазақстанның ақпараттық қауіпсіздік заңнамасы үнемі жетілдіріліп отырады. Жаңа қауіптер мен технологияларға сәйкес нормативтер өзгертіледі.



Қауіпсіздік оқиғалары мен олардың салдары

Қазақстанда соңғы жылдары бірнеше ірі киберинциденттер тіркелді. Бұл оқиғалар қауіпсіздік шараларын күшейту қажеттілігін көрсетті.

1

Банктік сектор шабуылдары

Қазақстандық банктерге DDoS шабуылдары және фишинг науқандары жүргізілді. Миллиондаған теңге залал келтірілді. Екі факторлы аутентификация міндетті болды.

2

Мемлекеттік порталдар

Электрондық үкімет порталдарына деректерді ұрлау әрекеттері болды. Жүйелердің қауіпсіздігі күшейтілді. Жаңа сертификаттау талаптары енгізілді.

3

Ransomware шабуылдары

Түрлі ұйымдарға шифрлау вирустары арқылы шабуылдар жасалды. Резервтік көшірмелердің маңыздылығы расталды. Қорғаныс жүйелері жаңартылды.

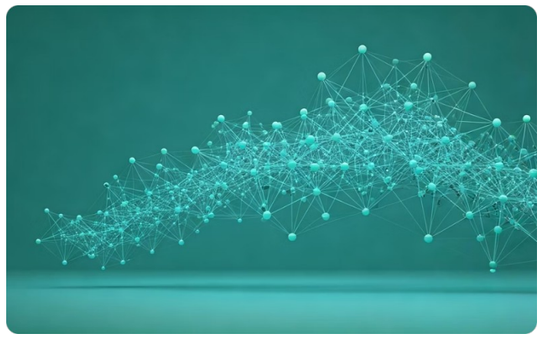
4

Алдын алу шаралары

Барлық инциденттер қауіпсіздік саясатын қайта қарауға әкелді. Мониторинг жүйелері жетілдірілді. Персоналды оқыту бағдарламалары кеңейтілді.

Жасанды интеллект және қауіпсіздік

Artificial Intelligence киберқауіпсіздік саласын түбегейлі өзгертуде. AI технологиялары қауіптерді анықтауды автоматтандырады және қорғанысты күшейтеді.



Алдын ала анықтау

Machine Learning алгоритмдері аномалияларды нақты уақытта анықтайды. Behavioral analysis арқылы әдеттен тыс әрекеттерді тауып, шабуылды бастамас бұрын тоқтатады.



Автоматты қорғаныс

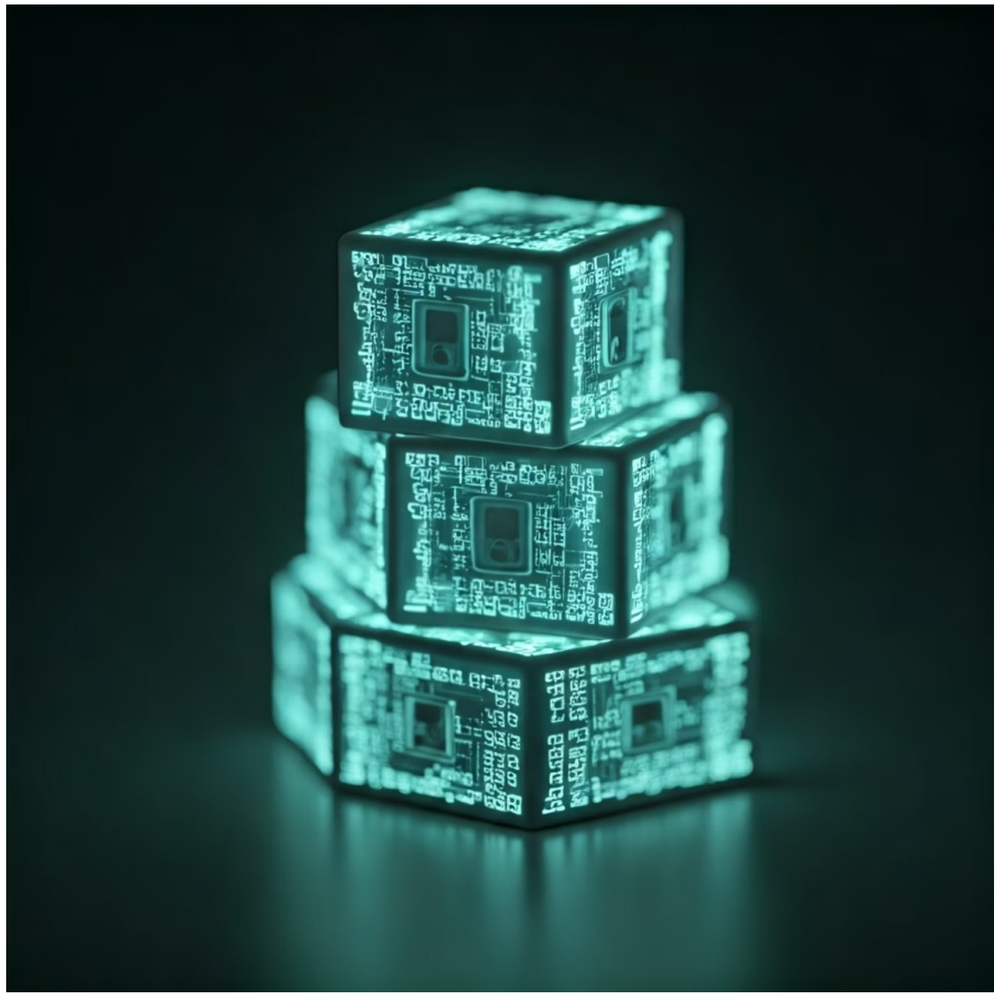
AI-негізделген жүйелер адам араласуынсыз қауіптерге жауап береді. Security Orchestration Automation and Response (SOAR) платформалары инциденттерді автоматты өңдейді.



Машиналық оқыту

Жүйе үнемі жаңа шабуыл үлгілерін үйреніп, бейімделеді. Threat intelligence деректерін талдап, болашақ қауіптерді болжайды. Қорғаныс тиімділігі артады.

Блокчейн технологиясы



Тұтастықты қамтамасыз ету

Блокчейн деректердің бұзылмауын криптографиялық тізбек арқылы қамтамасыз етеді. Әрбір блок алдыңғы блокпен байланысты, өзгерту мүмкін емес.

Қолдану салалары

- Цифрлық идентификация жүйелері
- Supply chain қауіпсіздігі
- Смарт-контракттар арқылы автоматтандыру
- Аудит журналдарын сақтау
- Децентрализацияланған PKI

Блокчейн қолданбалы бағдарламаларда деректердің шынайылығын растау және транзакциялардың қауіпсіздігін қамтамасыз ету үшін қолданылады.

Қауіпсіздік мәдениетін қалыптастыру

Технологиялық шешімдер жеткіліксіз – адам факторы ең әлсіз буын болып қала береді. Қауіпсіздік мәдениетін қалыптастыру өте маңызды.

Қолданушылар оқыту

Базалық ақпараттық сауаттылық және қауіпсіздік принциптерін үйрету.

Хабардарлық арттыру

Фишинг, әлеуметтік инженерия және басқа қауіптер туралы үнемі ақпарат беру.

Саясатты жетілдіру

Ұйымдық қауіпсіздік саясатын әзірлеу және орындауды бақылау жүйесін құру.

Мәдениет құру

Қауіпсіздікті компания мәдениетінің бөлігіне айналдыру. Әр қызметкердің жауапкершілігі.

Үздіксіз жетілдіру

Регулярлы тренингтер, тестілеу және қауіпсіздік практикасын жаңарту процесі.



Болашақ технологиялар

Қауіпсіздік механизмдері мен жаңа технологиялардың интеграциясы – киберқауіпсіздіктің келешегі

Қорытынды: Қауіпсіздік – үздіксіз процесс

Қолданбалы бағдарламалардағы қауіпсіздік механизмдерін зерттеу барысында біз бірқатар маңызды қорытындыларға келдік.

Үнемі жаңарту

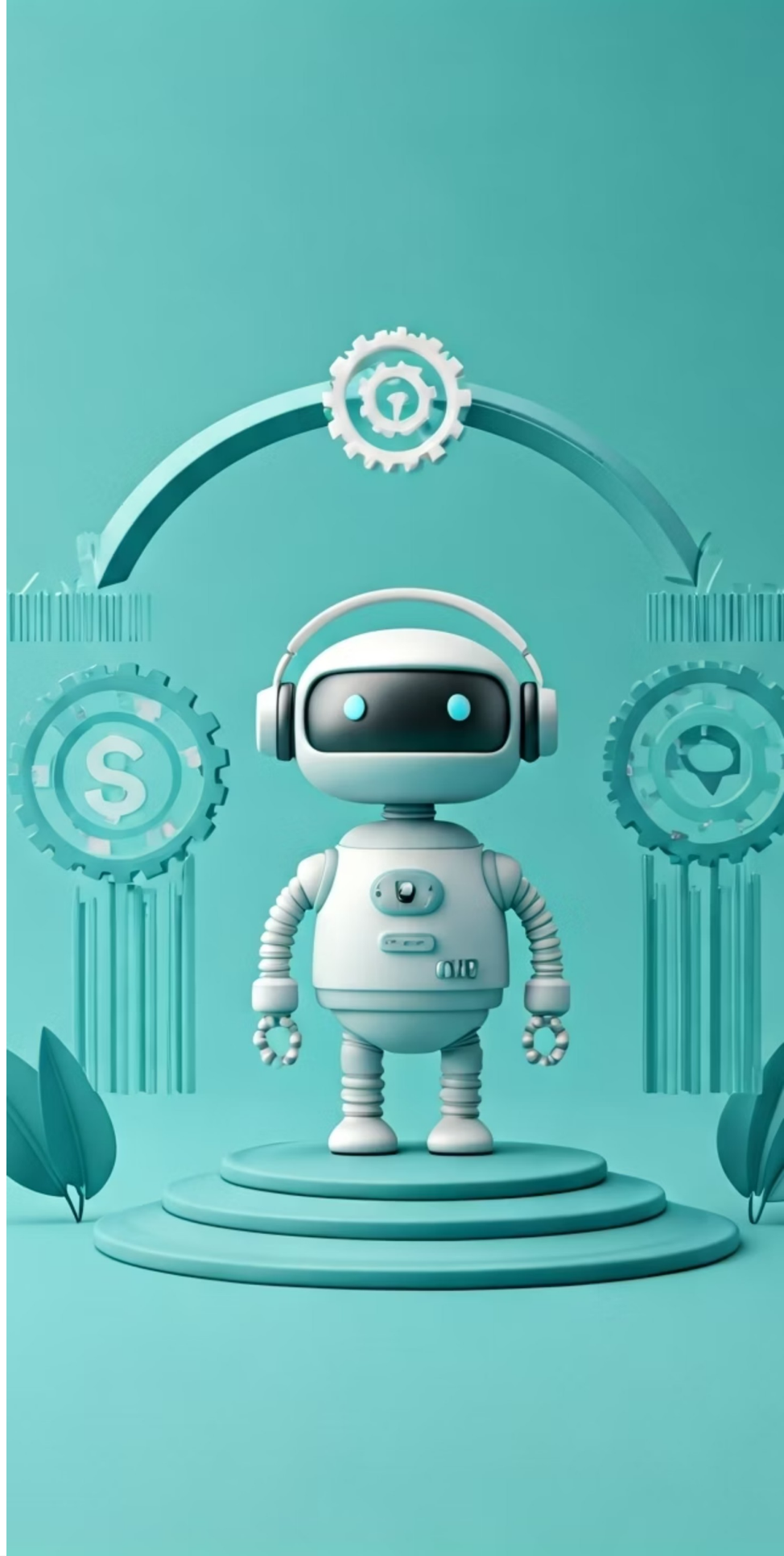
Қауіпсіздік механизмдері статикалық емес – олар үнемі дамып, жаңартылып отыруы тиіс. Жаңа қауіптер пайда болған сайын қорғаныс әдістері де жетілдірілуі керек.

Кешенді тәсіл

Қауіптерге қарсы күресте бір ғана шешім жоқ. Технологиялық, ұйымдастырушылық және адам факторларын қамтитын кешенді тәсіл қажет.

Қазақстанның дамуы

Біздің еліміздің ақпараттық қауіпсіздік саласы қарқынды дамуда. Заңнамалық база күшейтіліп, халықаралық стандарттарға сәйкестік қамтамасыз етілуде.



Ұсыныстар

Қазақстанның қолданбалы бағдарламалар қауіпсіздігін арттыру үшін келесі шараларды ұсынамыз:

1 Стандарттарды енгізу

Қолданбалы бағдарламаларды әзірлеу барысында халықаралық қауіпсіздік стандарттарын міндетті түрде қолдану. OWASP, ISO 27001 және басқа үздік тәжірибелерді интеграциялау. Secure Software Development Lifecycle (SSDLC) әдістемесін пайдалану.

2 Оқыту бағдарламалары

Қызметкерлер мен қолданушыларды ақпараттық қауіпсіздік бойынша жүйелі түрде оқыту. Awareness тренингтері, симуляциялық фишинг әрекеттері және практикалық жаттығулар өткізу. Қауіпсіздік мәдениетін қалыптастыру.

3 Ынтымақтастық

Мемлекеттік органдар мен жеке сектордағы компаниялар арасындағы ынтымақтастықты күшейту. Threat intelligence ақпаратын бөлісу, бірлескен жобалар жүргізу және тәжірибе алмасу. Киберқауіпсіздік кластерін құру.

Пайдаланылған әдебиеттер мен нормативтік құжаттар

Ғылыми әдебиеттер

- М.Ж.Көшкінбаева, «Ақпараттық қауіпсіздік негіздері», Алматы, 2015
- Б.С.Сагинов, «Киберқауіпсіздік және қорғаныс жүйелері», 2018
- Н.А.Калимолдаев, «Ақпараттық технологиялар қауіпсіздігі», 2020
- А.К.Жұмағалиева, «Қолданбалы бағдарламалар қауіпсіздігі», 2019

Халықаралық стандарттар

- ISO/IEC 27001:2013 – Ақпараттық қауіпсіздік менеджмент жүйелері
- ISO/IEC 27002:2022 – Ақпараттық қауіпсіздік бақылауы
- NIST Cybersecurity Framework
- PCI DSS – Төлем карталары қауіпсіздігі

ҚР заңнамасы

- «Ақпараттандыру туралы» ҚР Заңы, 2015
- «Жеке деректер және оларды қорғау туралы» ҚР Заңы, 2013
- «Электрондық құжат және электрондық цифрлық қолтаңба туралы» ҚР Заңы
- Қазақстан Республикасының Қылмыстық кодексі (киберқылмыс баптары)

OWASP ресурстары

- OWASP Top 10 – 2021
- OWASP Application Security Verification Standard (ASVS)
- OWASP Mobile Security Testing Guide
- OWASP API Security Top 10



Сұрақтар мен пікірлер

> Сіздің сұрақтарыңыз бен пікірлеріңіз маңызды. Қауіпсіздік – бұл диалог және үнемі даму процесі.

Қолданбалы бағдарламалардағы қауіпсіздік механизмдері туралы қосымша сұрақтарыңыз бар ма?

Практикалық іске асыру бойынша нақты кеңес қажет пе?

Өз ұйымыңызда қауіпсіздік деңгейін қалай бағалау керектігі туралы ақпарат алғыңыз келе ме?

