Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university



Ақпараттық қауіпсіздік модельдері және стандарттары

Ақпараттық қауіпсіздік дегеніміз не?

Мемлекеттік деңгей

Ақпараттық қауіпсіздік – бұл мемлекеттік және жеке ақпараттық ресурстарды заңсыз қол жеткізуден, жоюдан, өзгертуден және басқа да қауіпті әрекеттерден қорғау жүйесі. Ол ұлттық қауіпсіздіктің маңызды құрамдас бөлігі болып табылады.

Жеке деңгей

Азаматтардың, ұйымдардың және мемлекеттің ақпараттық кеңістіктегі құқықтары мен заңды мүдделерін қамтамасыз ету. Бұл жеке деректердің құпиялылығы, интеллектуалдық меншік және бизнес-процестердің үздіксіздігін қамтиды.





Ақпараттық қауіпсіздік – мемлекеттің қорғанысы

Заманауи кибершабуылдар күннен-күнге күрделене түсуде. Мемлекеттік инфрақұрылым, қаржы жүйелері, энергетика және денсаулық сақтау саласы – барлығы қорғауды талап етеді.



Ақпараттық қауіпсіздік модельдері – жалпы түсінік

Ақпараттық қауіпсіздік модельдері – бұл ақпараттық жүйелерді қорғаудың теориялық негіздері мен практикалық шешімдерінің жиынтығы. Олар қауіпсіздік саясатын қалыптастыру, талаптарды анықтау және тиімді қорғаныс стратегиясын әзірлеу үшін қажет.

Әрбір модель өзінің ерекше мақсаттары мен қолдану аясына ие, бірақ барлығы бірге кешенді қорғаныс жүйесін құрайды.



Ақпараттық жүйенің қауіпсіздік моделі дегеніміз не?

Анықтама

Ақпараттық жүйенің қауіпсіздік моделі – бұл жүйенің қорғаныс құрылымын формальды түрде сипаттайтын ережелер мен қағидалар жиынтығы. Ол қауіпсіздік саясатын техникалық және ұйымдастырушылық тілге аударады.

Негізгі міндеттері

- Қауіпсіздік талаптарын нақты анықтау
- Қорғаныс механизмдерін жобалау
- Қауіпсіздік саясатының сақталуын тексеру
- Қауіптерді бағалау және басқару

Белгілі ақпараттық қауіпсіздік модельдері

Bell-LaPadula

Құпиялылыққа басымдық беретін, әскери және үкіметтік жүйелерде қолданылатын классикалық модель

Biba

Мәліметтердің тұтастығын сақтауға бағытталған, қаржы және банк жүйелерінде танымал

Clark-Wilson

Транзакциялардың сенімділігін қамтамасыз ететін, коммерциялық қолданбаларға арналған

Brewer-Nash

Қызығушылық қақтығысын болдырмайтын, консалтинг және аудит компанияларына арналған

Bell-LaPadula моделі: Құпиялылыққа басымдық

Негізгі мақсат

Құпия ақпараттың ағып кетуін (information leakage) болдырмау. Модель әскери және үкіметтік ұйымдарда қолданылады, мұнда мәліметтердің құпиялылық деңгейлері бар.

"No read up, no write down" қағидасы

Пайдаланушы өзінің құпиялылық деңгейінен жоғары ақпаратты оқи алмайды (no read up), ал төменгі деңгейге жаза алмайды (no write down). Бұл құпияның төменгі деңгейлерге таралуын болдырмайды.

> Bell-LaPadula моделі 1973 жылы әзірленген және әлі де көптеген қауіпсіздік жүйелерінің негізі болып табылады.



Biba моделі: Мәлімет тұтастығын сақтау

Модельдің принциптері

Biba моделі Bell-LaPadula-ның қарама-қарсы тәсілін қолданады. Мұнда басты мақсат – мәліметтердің тұтастығын (integrity) сақтау, яғни мәліметтердің заңсыз өзгертілуін болдырмау.

"No write up, no read down" қағидасы

- Төменгі тұтастық деңгейіндегі субъект жоғарыға жаза алмайды
- Жоғарғы тұтастық деңгейіндегі субъект төменнен оқи алмайды
- Құжаттардың өзгертілуін қатаң бақылау
- Тексерілмеген деректердің таралуын шектеу



Biba моделі қаржы жүйелері, бухгалтерлік есеп және медициналық деректер қорларында кеңінен қолданылады.



Clark-Wilson моделі: Транзакциялардың сенімділігі

01

Қатаң бақылау механизмдері

Барлық операциялар тексерілген процедуралар (Transformation Procedures) арқылы орындалады, бұл мәліметтердің үнемі дұрыс күйде болуын қамтамасыз етеді.

02

Аудит және журналдау

Әрбір транзакция толық журналданады, бұл кейіннен тексеруге және қате анықтауға мүмкіндік береді. Аудит жазбалары өзгертілуден қорғалған.

03

Бөлінген міндеттер

Қолданушының рұқсаттарын басқару арқылы міндеттерді бөлу (separation of duties) принципі іске асырылады. Бір адам барлық критикалық операцияларды орындай алмайды.



Brewer-Nash моделі: Қызығушылық қақтығысын болдырмау

Динамикалық қауіпсіздік

Brewer-Nash моделі "Қытай қабырғасы" (Chinese Wall) деп те аталады. Бұл модель пайдаланушының алдыңғы әрекеттеріне негізделген динамикалық рұқсаттар жүйесін пайдаланады.

Егер пайдаланушы бір компанияның деректеріне қол жеткізсе, онда бәсекелес компанияның деректеріне қол жеткізу автоматты түрде бұғатталады.

Қолдану аясы

- Консалтинг компаниялары
- Аудиторлық фирмалар
- Заң кеңестері
- Инвестициялық банктер

Модель құпиялылық пен тәуелсіздікті сақтай отырып, бірнеше клиенттерге қызмет көрсетуге мүмкіндік береді.

Модельдердің салыстырмалы сипаттамасы

Модель	Негізгі мақсат	Қолдану саласы	Ерекшелігі
Bell-LaPadula	Құпиялылық	Әскери, үкіметтік	Статикалық деңгейлер
Biba	Тұтастық	Қаржы, медицина	Тексерілген деректер
Clark-Wilson	Транзакциялар	Коммерциялық	Процедуралық бақылау
Brewer-Nash	Қақтығыс болдырмау	Консалтинг	Динамикалық рұқсаттар

Ақпараттық қауіпсіздік стандарттары

Ақпараттық қауіпсіздік стандарттары – бұл ұйымдарға қауіпсіздік жүйелерін құруға және басқаруға көмектесетін халықаралық және ұлттық деңгейдегі талаптар мен нұсқаулықтар. Олар үздік тәжірибелерді біріктіреді және қауіпсіздік деңгейін арттыруға ықпал етеді.



ISO/IEC 27000 сериясы: Халықаралық стандарттар

ISO/IEC 27001

Ақпараттық қауіпсіздік басқару жүйесін (АҚБЖ) құру және сертификаттау үшін негізгі стандарт. Ол қауіпсіздік саясатын, қауіптерді басқаруды, ішкі аудитті және үздіксіз жетілдіруді қамтиды. 114 бақылау шарасын ұсынады.

ISO/IEC 27002

Ақпараттық қауіпсіздік бойынша тәжірибелік нұсқаулық, қауіпсіздік шараларының толық каталогын ұсынады. 14 бөлімде 93 бақылау шарасы мен олардың іске асыру нұсқаулықтары берілген. 27001-ді толықтырады.

ISO/IEC 27005

Ақпараттық қауіпсіздік қауіптерін басқару бойынша нұсқаулық. Қауіптерді анықтау, талдау, бағалау және өңдеу процестерін сипаттайды. Қауіпті басқару әдістемелері мен құралдарын ұсынады.

NIST стандарттары (АҚШ)



NIST SP 800-53

Федералдық ақпараттық жүйелер мен ұйымдар үшін қауіпсіздік және құпиялылық бақылауларының толық каталогы. 20 отбасында 1000-нан астам бақылау шарасын қамтиды.

NIST Cybersecurity Framework

Киберқауіпсіздік қауіптерін басқарудың бес негізгі функциясы:

1. Анықтау (Identify)
2. Қорғау (Protect)
3. Анықтау (Detect)
4. Жауап беру (Respond)
5. Қалпына келтіру (Recover)



Қазақстандағы ақпараттық қауіпсіздік стандарттары

Нормативтік-құқықтық база

ҚР Үкіметінің қаулылары, Премьер-Министрдің бұйрықтары, ведомстволық нормативтік актілер және техникалық регламенттер ақпараттық қауіпсіздіктің барлық аспектілерін реттейді.

Саясат талаптары

Мемлекеттік органдар мен квазимемлекеттік сектор үшін ақпараттық қауіпсіздік саясатын әзірлеу және енгізу міндетті. Бұл жеке деректерді, мемлекеттік құпияларды және бизнес-ақпаратты қорғауды қамтиды.

Сәйкестік аудиті

Ақпараттық жүйелер мен технологиялар үздіксіз аудиттен өтуі тиіс. Сертификатталған аудиторлар мен тексеру органдары нормативтік талаптарға сәйкестікті растайды.

ҚР 965 қаулысы: Мемлекеттік ақпараттық қауіпсіздік шаралары

Мемлекеттік құпияларды қорғау

ҚР Үкіметінің №965 қаулысы мемлекеттік құпия болып табылатын ақпаратты қорғау жөніндегі шараларды белгілейді. Ол құпия деректерді өңдейтін ақпараттық жүйелерге қойылатын талаптарды анықтайды.

Криптографиялық қорғау

Қаулы мемлекеттік құпиялы ақпаратты криптографиялық құралдармен қорғауды міндеттейді. Пайдаланылатын алгоритмдер мен құрылғылар ҚР уәкілетті органының сертификатын алуы тиіс.

Мобильдік құрылғылар

Мобильдік құрылғыларды пайдалану тәртібі қатаң реттеледі: шифрлау, қашықтағы өшіру мүмкіндігі, қауіпсіз аутентификация және корпоративтік деректерді жеке деректерден бөлу талап етіледі.

Ақпараттық жүйелердің сәйкестік талаптары

Сертификаттау процесі

Техникалық және бағдарламалық құралдардың сертификатталуы ақпараттық қауіпсіздік талаптарына сәйкестігін растайды. Сертификатсыз құралдарды мемлекеттік ақпараттық жүйелерде пайдалануға болмайды.



Премьер-Министрдің бұйрықтары

- Ақпараттық жүйелерді пайдалануға қабылдау тәртібі
- Деректерді сақтау және резервтік көшірмелеу талаптары
- Инциденттерді тіркеу және есепке алу процедуралары
- Персоналды оқыту және сертификаттау талаптары
- Аудит пен мониторинг жүргізу ережелері



Қазақстан Республикасының ақпараттық қауіпсіздік инфрақұрылымы

Мемлекеттік деңгейде ақпараттық қауіпсіздік инфрақұрылымы Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы (АҚҰҮО) негізінде құрылған. Орталық киберқауіптерді мониторингілеуді, инциденттерге жауап беруді және мемлекеттік органдар мен критикалық инфрақұрылым объектілері арасында үйлестіруді жүзеге асырады.

Ақпараттық қауіпсіздік саясаты және басқару

Ақпараттық қауіпсіздік саясаты – бұл ұйымның ақпараттық активтерін қорғау бойынша стратегиялық құжаты. Ол қауіпсіздік мақсаттарын, принциптерін, міндеттерін және жауапкершілікті анықтайды. Тиімді саясат технологиялармен қатар адамдар мен процестерді де қамтиды.



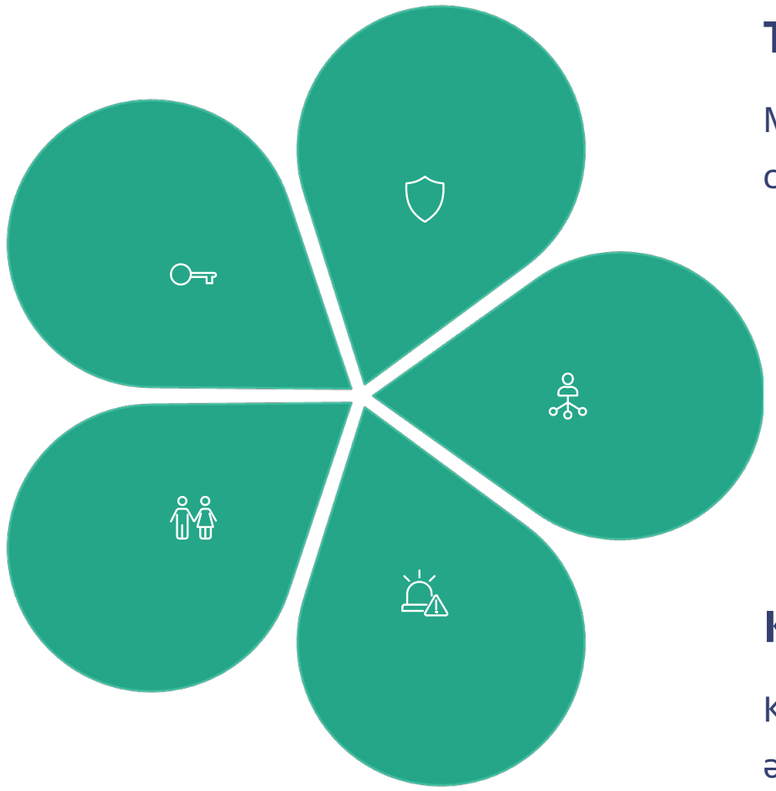
Ақпараттық қауіпсіздік саясатының негізгі элементтері

Құпиялылық

Ақпаратты рұқсатсыз қол жеткізуден қорғау және тек уәкілетті адамдарға қолжетімділікті қамтамасыз ету

Жауапкершілік

Әрбір қызметкердің ақпараттық қауіпсіздіктегі рөлі мен міндеттерін анық анықтау



Тұтастық

Мәліметтердің дұрыстығы мен толықтығын сақтау, заңсыз өзгертуден қорғау

Қолжетімділік

Уәкілетті пайдаланушыларға қажетті уақытта ақпаратқа қол жеткізуді қамтамасыз ету

Қауіпті басқару

Қауіптерді анықтау, бағалау және олардың әсерін азайту үшін шаралар қабылдау

Ақпараттық қауіпсіздік саясатын әзірлеу кезеңдері

1. Қауіптерді анықтау

Ұйымға қатысты қауіптерді жүйелі түрде анықтау: техногендік, антропогендік, табиғи және комбинацияланған қауіптер. Активтердің маңыздылығын бағалау және әлсіз жақтарды табу.

2. Қауіптерді бағалау

Анықталған қауіптердің ықтималдығы мен әсерін талдау. Қауіп деңгейін есептеу және басым қауіптерді анықтау. Матрицалар мен сандық әдістерді қолдану.

3. Қауіпсіздік шараларын таңдау

Қауіптерді азайту үшін тиісті бақылау шараларын таңдау: техникалық, әкімшілік және физикалық. Шығындар мен пайданы салыстыру, оңтайлы шешім табу.

4. Мониторинг және аудит

Енгізілген шаралардың тиімділігін үздіксіз бақылау. Ішкі және сыртқы аудит жүргізу. Метрикаларды өлшеу және нәтижелерді талдау.

5. Жетілдіру

Аудит нәтижелері мен инциденттерден алынған сабақтар негізінде саясатты жаңарту. Үздіксіз жетілдіру циклын қамтамасыз ету.



Ұйымдағы ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ)

ISO/IEC 27001 талаптары

АҚБЖ ISO/IEC 27001 стандартына сәйкес құрылады. Ол келесі негізгі элементтерді қамтиды:

- Контекст пен қолдану аясын анықтау
- Басшылықтың рөлі мен міндеттемесі
- Қауіптерді басқару процесі
- Қауіпсіздік мақсаттары мен жоспарлау
- Операциялық басқару және бақылау
- Өнімділікті бағалау
- Үздіксіз жетілдіру

Қауіпсіздік мәдениеті

АҚБЖ тек технологиялар емес, ең алдымен адамдар туралы. Қауіпсіздік мәдениетін қалыптастыру үшін қажет:

- Үнемі оқыту және хабардарлықты арттыру
- Басшылықтың үлгілік мінез-құлқы
- Саясаттың қарапайым және түсінікті болуы
- Қауіпсіз әрекеттерді ынталандыру
- Ашық қарым-қатынас және кері байланыс

Ақпараттық қауіпсіздік оқиғаларын басқару

Анықтау

Қауіпсіздік оқиғаларын уақтылы анықтау үшін мониторинг құралдары (SIEM, IDS/IPS) және процестерді қолдану. Оқиғаларды классификациялау.

Жіберу

Инциденттер туралы тиісті адамдарға хабарлау. Эскалация тізбегін белгілеу. Инцидент жауап беру тобын (IRT) белсендіру.

Жауап беру

Зиянды әсерді азайту үшін шұғыл шаралар қабылдау: зақымдалған жүйелерді оқшаулау, қауіпті жою, деректерді қалпына келтіру.

Талдау

Инциденттің түбірлік себептерін анықтау және сабақ алу. Есеп дайындау және ұсыныстар әзірлеу. Процестерді жетілдіру.





Ақпараттық қауіпсіздік саясатының құрылымы

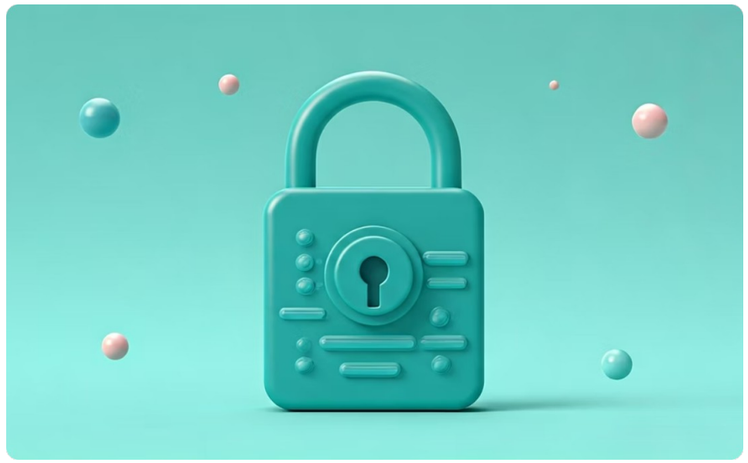
Тиімді ақпараттық қауіпсіздік саясаты иерархиялық құрылымға ие. Жоғарғы деңгейде жалпы саясат құжаты орналасады, ол стратегиялық бағыттарды белгілейді. Орта деңгейде нақты саладағы стандарттар мен процедуралар (мысалы, қол жеткізуді басқару, инциденттерге жауап беру) орналасқан. Төменгі деңгейде жұмыс нұсқаулықтары мен техникалық конфигурациялар бар.

Ақпараттық қауіпсіздік технологиялары мен құралдары

Заманауи ақпараттық қауіпсіздік технологиялары қауіпсіздік саясатын техникалық тұрғыдан іске асыруды қамтамасыз етеді. Олар профилактикалық, детективтік және реактивті шаралардың кешенін біріктіреді. Дұрыс таңдалған технологиялар қорғанысты күшейтіп қана қоймай, бизнес-процестерге кедергі келтірмейді.



Қауіпсіздік технологияларының түрлері



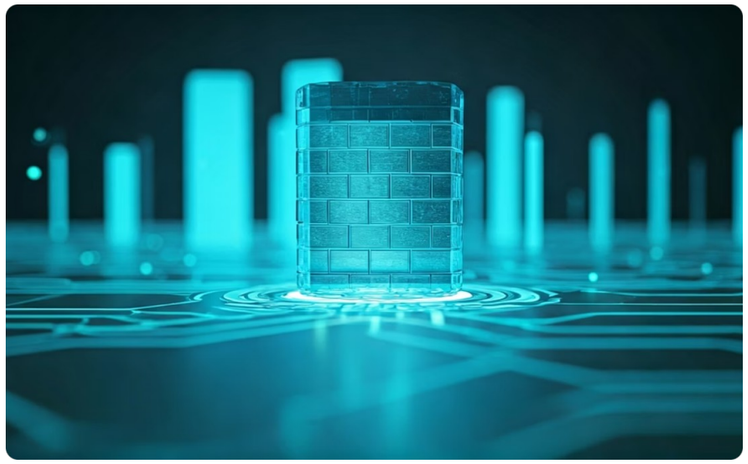
Шифрлау және криптография

Ақпаратты рұқсатсыз қол жеткізуден қорғайтын математикалық алгоритмдер. Симметриялық (AES) және асимметриялық (RSA, ECC) шифрлау. Деректерді сақтау және тасымалдау кезінде қолданылады.



Аутентификация және авторизация

Пайдаланушының жеке басын растау және рұқсаттарды басқару. Көпфакторлы аутентификация (MFA), биометрия, токендер. SSO және федеративті басқару жүйелері.



Желілік қауіпсіздік құралдары

Желілік трафикті бақылау және қорғау жүйелері. Firewall, IDS/IPS, WAF. Желіні сегменттеу және VLAN. DDoS-қа қарсы қорғаныс шешімдері.

Қауіпсіздік құралдарының мысалдары

Firewall және IDS/IPS

Желілік қабырға (Firewall) рұқсатсыз байланыстарды бұғаттайды. Шабуылдарды анықтау жүйелері (IDS) мен алдын алу жүйелері (IPS) күдікті әрекеттерді табады және бұғаттайды. Next-Generation Firewall (NGFW) қосымшаларды бақылайды.

VPN және SSL/TLS

Виртуалды жеке желілер (VPN) қауіпсіз қашықтан қосылуды қамтамасыз етеді. SSL/TLS протоколдары веб-трафикті шифрлайды (HTTPS). IPSec – желілік деңгейдегі шифрлау. Қауіпсіз туннельдер құру.

Антивирус және антишпиондық

Зиянды бағдарламаларды анықтайтын және жоятын құралдар. Дербес компьютерлер, серверлер, мобильді құрылғылар үшін. Қолтаңба негізінде және мінез-құлық анализі арқылы анықтау. EDR (Endpoint Detection and Response) шешімдері.

SIEM жүйелері

Қауіпсіздік ақпаратын және оқиғаларын басқару (Security Information and Event Management). Журналдарды жинақтау, корреляциялық талдау, нақты уақыт режимінде ескерту. SOC операторларына аналитикалық құрал.

Қазақстандағы ақпараттық қауіпсіздік инфрақұрылымы



Ұлттық үйлестіру орталығы (АҚҰҮО)

Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы (АҚҰҮО) – Қазақстандағы киберқауіпсіздік саласындағы негізгі мемлекеттік орган. Орталықтың негізгі функциялары:

- Киберқауіптерді 24/7 мониторингілеу
- Ақпараттық қауіпсіздік инциденттеріне жауап беру
- Критикалық инфрақұрылым объектілерін қорғауды үйлестіру
- Киберқауіптер туралы хабарламалар тарату
- Халықаралық ынтымақтастық

Мемлекеттік бағдарламалар

«Цифрлық Қазақстан» бағдарламасы киберқауіпсіздікті басым бағыт ретінде белгілейді. Бұл критикалық инфрақұрылымды қорғау, персоналды дайындау және инновациялық шешімдерді енгізу жобаларын қамтиды.



Ақпараттық қауіпсіздік технологияларының интеграцияланған архитектурасы

Заманауи қауіпсіздік архитектурасы көп қабатты қорғанысты (Defense in Depth) іске асырады. Бұл тәсілде әртүрлі қауіпсizdik құралдары бірігіп жұмыс істейді: желілік қабырғалар периметрді қорғайды, IDS/IPS трафикті талдайды, антивирус қондырғыларды қорғайды, SIEM барлық оқиғаларды біріктіріп талдайды. Әрбір қабат қосымша қорғаныс деңгейін қамтамасыз етеді.



Ақпараттық қауіпсіздік стандарттарын енгізу тәжірибесі

Стандарттарды енгізу – бұл күрделі ұйымдастырушылық және техникалық процесс. Сәтті енгізу басшылықтың қолдауын, адекватты ресурстарды, анық жоспарлауды және үздіксіз жетілдіруге деген ұмтылысты талап етеді. Үздік тәжірибелерден үйрену қателіктерден аулақ болуға және жақсы нәтижеге жетуге көмектеседі.

Қазақстандағы ірі компаниялар мен мемлекеттік ұйымдар тәжірибесі

Банк секторы

Қазақстанның ірі банктері (Kaspi Bank, Halyk Bank, ForteBank) ISO/IEC 27001 сертификатын алған. Олар қаржылық операциялардың қауіпсіздігін қамтамасыз ету үшін криптографиялық құралдарды, көпфакторлы аутентификацияны және үздіксіз мониторингті пайдаланады.

Телекоммуникация

Kcell, Beeline және Tele2 операторлары жүздеген терабайт абоненттік деректерді сақтайды. Олар ISO/IEC 27001 және PCI DSS стандарттарын енгізген. Желілік қауіпсіздік, деректерді шифрлау және бөлу басты назарда.

Мемлекеттік органдар

Электрондық үкімет порталы (egov.kz) мен басқа да мемлекеттік ақпараттық жүйелер ҚР нормативтік талаптарына және ISO/IEC 27001-ге сәйкес. Жеке деректерді қорғау және киберқауіпсіздік басым бағыттар.

Энергетика

КазАтомӨнеркәсіп және KEGOC критикалық инфрақұрылым объектілері ретінде ерекше талаптарға сәйкес келуі тиіс. IEC 62443 (өнеркәсіптік жүйелер) және ISO/IEC 27001 стандарттары енгізіледі.

Қиындықтар мен шешімдер

Негізгі қиындықтар

- **Қызметкерлердің сауаттылығы**

  Персоналдың ақпараттық қауіпсіздік бойынша білімінің жеткіліксіздігі ең үлкен қауіп. Адам факторы инциденттердің 80%-ының себебі.

- **Ресурстардың тапшылығы**

  Киберқауіпсіздік мамандарының жетіспеушілігі және қауіпсіздік шараларына қаржыландырудың шектеулілігі.

- **Ескірген жүйелер**

  Көптеген ұйымдарда ескі, қолдауы тоқтатылған бағдарламалық қамтамасыз ету пайдаланылады, оларды жаңартуға қаражат қажет.

Ұсынылатын шешімдер



- **Оқыту бағдарламалары:** Үнемі оқыту, хабардарлық науқандары, симуляцияланған фишинг тесттері
- **Автоматтандыру:** Рутинді тапсырмаларды автоматтандыру арқылы адам қатесін азайту
- **Outsourcing:** Қауіпсіздік операцияларын (SOC) сыртқы мамандарға тапсыру
- **Кезеңдік енгізу:** Басым активтерден бастап сатылай енгізу

Болашақ бағыттар мен инновациялар

2024-2025

Қауіпсіздік автоматтандыруыSOAR (Security Orchestration, Automation and Response) платформалары инциденттерге жауапты автоматтандырады, адам араласуын азайтады және жауап беру уақытын қысқартады.

2026-2027

Zero Trust архитектурасы"Ешкімге сенбе, әрқашан тексер" принципі. Барлық қол жеткізу талаптары расталады, желі бөлінеді, микросегментация қолданылады.

1

2

3

4

2025-2026

Жасанды интеллектAI және машиналық оқыту аномалияларды анықтауда, қауіптерді болжауда және киберқауіптерді талдауда қолданылады. Шабуылдарды болдырмау проактивті сипат алады.

2027+

Кванттық қауіпсіздікКванттық есептеудің дамуы қазіргі криптографияны бұзуы мүмкін. Пост-кванттық криптография стандарттары әзірленуде және енгізілуде.



Ақпараттық қауіпсіздік саласындағы инновациялар

Киберқауіпсіздік технологиялары үздіксіз дамуда. Жасанды интеллект қазірдің өзінде қауіптерді анықтауды жақсартып, нақты уақыт режимінде шабуылдарды бұғаттауға мүмкіндік береді. Blockchain технологиясы деректердің тұтастығын қамтамасыз етеді. Биометриялық аутентификация дәстүрлі парольдерді ауыстырады. Бұл инновациялар болашақта қауіпсіздікті жаңа деңгейге көтереді.

Ақпараттық қауіпсіздік – тұрақты даму кепілі

Ақпараттық қауіпсіздік – бұл бір реттік жоба емес, үздіксіз процесс. Қауіптер эволюцияланууда, технологиялар дамуда, ал стандарттар жаңартылуда. Тұрақты даму үшін ұйымдар қауіпсіздікті өздерінің стратегиясының орталық бөлігіне айналдыруы керек. Бұл тек технологияларға инвестициялауды ғана емес, қауіпсіздік мәдениетін қалыптастыруды, персоналды дамытуды және үздік тәжірибелерді үнемі үйренуді талап етеді.



Негізгі қорытындылар

1 Модельдер мен стандарттардың маңызы

Ақпараттық қауіпсіздік модельдері (Bell-LaPadula, Biba, Clark-Wilson, Brewer-Nash) теориялық негіз береді, ал халықаралық стандарттар (ISO/IEC 27001, NIST) практикалық шешімдерді ұсынады. Олардың үйлесімі тиімді қорғанысты қамтамасыз етеді.

2 Нормативтік-құқықтық база

Қазақстанда ақпараттық қауіпсіздік саласы қатаң реттеледі. ҚР Үкіметінің қаулылары, Премьер-Министрдің бұйрықтары және техникалық регламенттер мемлекеттік және жеке секторға нақты талаптар қояды. Оларға сәйкестік міндетті.

3 Басқару мен технологиялар

Тиімді басқару (АҚБЖ, саясат, процестер) және дұрыс таңдалған технологиялар (шифрлау, аутентификация, SIEM, firewall) бірігіп қауіпсіздіктің барлық аспектілерін қамтиды. Адам факторы – қауіпсіздіктің маңызды буыны.

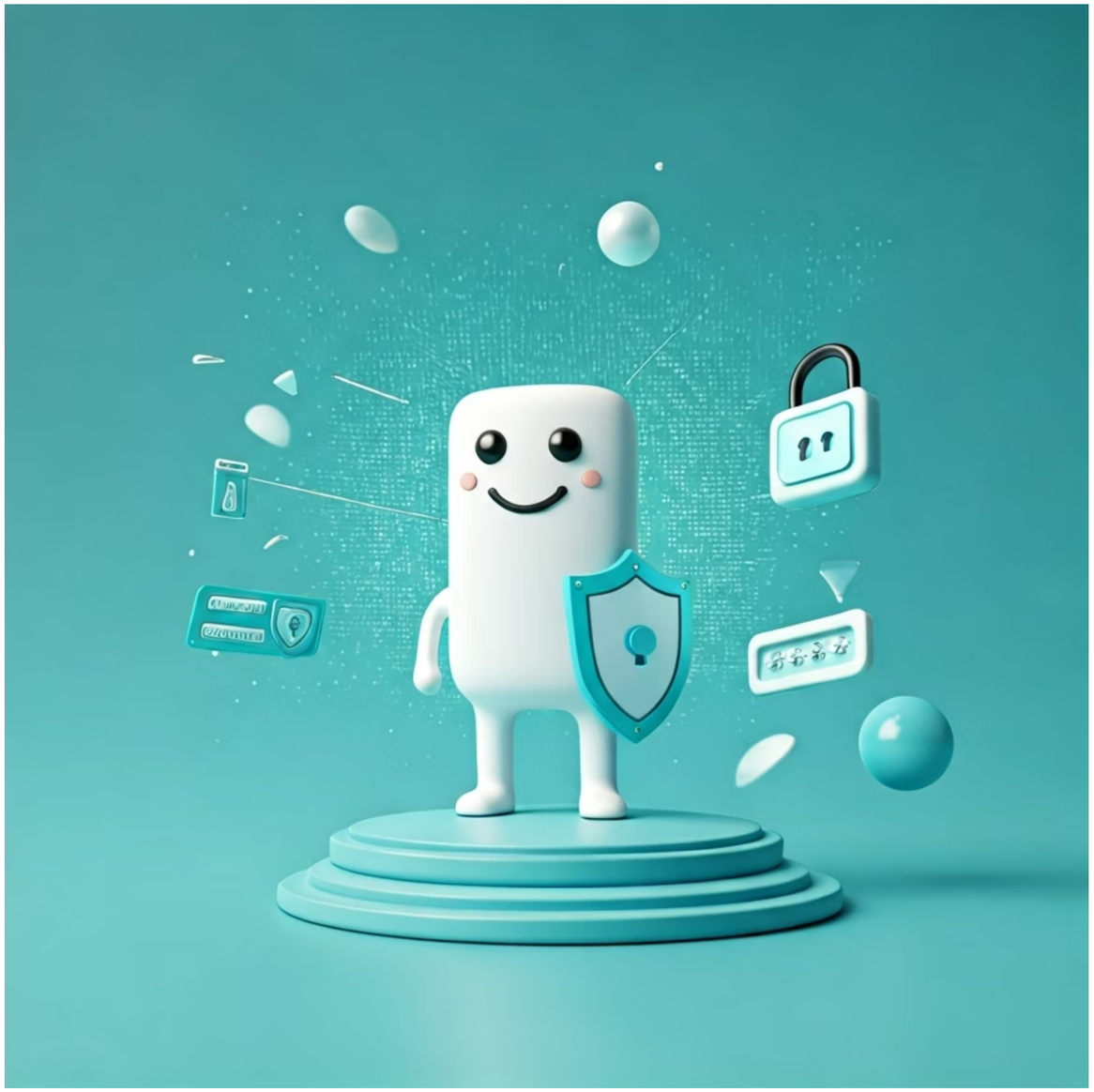
Қауіпсіздік мәдениетін қалыптастыру – әркімнің міндеті

Ұйымдық деңгей

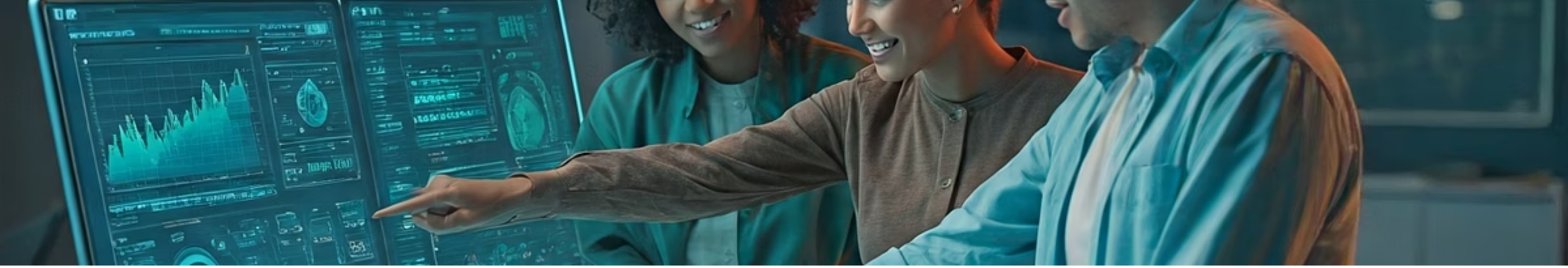


- Басшылықтың қауіпсіздікті басым міндет деп жариялауы
- Нақты саясат пен процедураларды әзірлеу
- Үнемі оқыту және хабардарлық бағдарламалары
- Қауіпсіз мінез-құлықты ынталандыру
- Ашық қарым-қатынас мәдениеті – қателер үшін жазаламау, оқыту
- Қауіпсіздік метрикаларын өлшеу және есепке алу

Жеке тұлға деңгейінде



- Күрделі және бірегей парольдерді пайдалану
- Көпфакторлы аутентификацияны қосу
- Фишингтік хаттарды тану және хабарлау
- Бағдарламаларды үнемі жаңарту
- Жеке және жұмыс құрылғыларын бөлу
- Күдікті әрекеттер туралы хабарлау
- Қауіпсіздік саясатын білу және сақтау



Қорытынды шақыру

> **Ақпараттық қауіпсіздік – бұл бір адамның немесе бөлімнің міндеті емес, бүкіл ұйымның жауапкершілігі**

Хабардарлық

Қауіптерді білу және сақ болу

Оқыту

Үздіксіз білім алу және дағдыларды дамыту

Енгізу

Үздік тәжірибелерді жүзеге асыру

Жетілдіру

Үнемі талдау және оңтайландыру

Ақпараттық қауіпсіздікке жауапкершілікпен қарау – бұл біздің цифрлық болашағымыздың негізі. Әрбір ұйым өзінің активтерін, клиенттерін және әріптестерін қорғау үшін қауіпсіздік стандарттары мен үздік тәжірибелерді енгізуге міндетті. Бұл тек қаржылық шығындарды емес, сондай-ақ беделдік тәуекелдерді де азайтады.