Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Ақпараттық қауіп-қатерлер мен қауіпсіздік саясаты





Ақпараттық қауіпсіздік негіздері

Ақпараттық қауіпсіздік – бұл заманауи қоғамның іргетасы. Мемлекеттік және жеке секторлардағы ақпараттық ресурстарды қорғау, киберкеңістіктің тұрақтылығын қамтамасыз ету және цифрлық экономиканың дамуына негіз жасау үшін ақпараттық қауіпсіздік негіздерін түсіну өте маңызды.

Ақпараттық қауіпсіздік дегеніміз не?



Негізгі анықтама

Ақпараттық қауіпсіздік – мемлекеттік және жеке ақпараттық ресурстарды заңсыз қол жеткізуден, өзгертуден, жоюдан және басқа да қауіпті әрекеттерден қорғаудың кешенді жүйесі.

Үш негізгі қағида:

- **Құпиялылық** – ақпаратқа тек рұқсаты бар адамдар ғана қол жеткізе алады
- **Тұтастық** – ақпарат өзгеріссіз және дәл сақталады
- **Қолжетімділік** – рұқсаты бар пайдаланушылар қажет кезде ақпаратқа қол жеткізе алады

Ақпараттық қауіпсіздіктің үш негізгі қағидасы

Жасырындылық

Ақпаратты рұқсаты жоқ тұлғалардан қорғау және оның құпиялығын сақтау. Шифрлау, парольдік қорғау және қол жеткізу құқықтарын басқару арқылы қамтамасыз етіледі.

Тұтастық

Ақпараттың дәлдігі мен толықтығын сақтау, оның заңсыз өзгертілуінен немесе бүлінуінен қорғау. Хеш-функциялар мен цифрлық қолтаңбалар арқылы тексеріледі.

Қолжетімділік

Рұқсаты бар пайдаланушылардың қажет кезінде ақпаратқа және жүйелерге кедергісіз қол жеткізе алуын қамтамасыз ету. Резервтік көшірмелер және қосарлау арқылы қорғалады.

Бұл үш қағиданы CIA триадасы деп те атайды (Confidentiality, Integrity, Availability). Олар кез келген ақпараттық қауіпсіздік жүйесінің негізі болып табылады және бір-бірімен өзара байланысты.



Ақпарат ағыны мен қорғау қабаттары

Заманауи ақпараттық жүйелерде деректер көптеген қабаттар арқылы өтеді: физикалық инфрақұрылымнан бастап, желілік деңгейге, қолданбаларға және пайдаланушы интерфейсіне дейін. Әрбір қабатта өзіндік қауіпсіздік шаралары қолданылуы керек.

01

Физикалық қабат

Серверлер мен құрылғыларды қорғау

02

Желілік қабат

Трафикті бақылау және фильтрация

03

Қолданба қабаты

Бағдарламалық қауіпсіздік

04

Пайдаланушы қабаты

Аутентификация және авторизация

Ақпараттық қауіпсіздік саясатының мәні

Кешенді тәсіл

Ақпараттық қауіпсіздік саясаты – бұл құқықтық, ұйымдастырушылық және техникалық шаралардың үйлестірілген жиынтығы. Ол ұйымның барлық деңгейінде қауіпсіздікті қамтамасыз етуге бағытталған.

Негізгі компоненттер:

- Қауіптерді анықтау және талдау
- Қорғау механизмдерін енгізу
- Мониторинг және аудит жүргізу
- Оқиғаларға жедел жауап беру
- Үздіксіз жетілдіру процесі



Тиімді қауіпсіздік саясаты ұйымның бизнес-мақсаттарына сәйкес келуі және барлық қызметкерлер тарапынан қолдау табуы керек. Ол тек техникалық құралдармен шектелмейді, сонымен қатар адам факторын да ескереді.

Қазақстан Республикасының ақпараттық қауіпсіздік заңнамасы

1

2004 жылғы №965 қаулысы

Қазақстан Республикасының Үкіметі "Мемлекеттік органдардың ақпараттандыру объектілерінде ақпараттық қауіпсіздікті қамтамасыз ету" туралы қаулы қабылдады. Бұл құжат ақпараттық қауіпсіздік саласындағы негізгі нормативтік базаны қалады.

2

Мемлекеттік құпиялар заңы

Мемлекеттік құпияларды қорғау, жіктеу, сақтау және пайдалану тәртібі белгіленді. Құпия ақпаратпен жұмыс істеуге қойылатын қатаң талаптар енгізілді.

3

Жаңартулар мен толықтырулар

Заңнама киберқауіптердің дамуына байланысты үнемі жаңартылып отырады. Жаңа технологиялар мен қауіп-қатерлерге сәйкес қосымша талаптар енгізіледі.



Ұлттық үйлестіру орталығы (АҚҰҮО)

Қазақстанның киберқауіпсіздік орталығы

2018 жылы Қазақстанда Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы (АҚҰҮО) құрылды. Бұл орталық киберкеңістіктегі қауіпсіздікті қамтамасыз етудегі басты мемлекеттік орган болып табылады.

Негізгі функциялары:

1. Киберқауіптерді мониторингілеу және талдау
2. Инциденттерге жедел жауап беру
3. Мемлекеттік органдарды үйлестіру
4. Халықаралық ынтымақтастық
5. Қауіпсіздік стандарттарын әзірлеу
6. Мамандарды даярлау және кеңес беру



Маңызды: АҚҰҮО Қазақстанның ұлттық киберқауіпсіздік архитектурасының орталық буыны болып табылады және халықаралық CERT желісінің мүшесі.

Ақпараттық қауіп-қатерлердің түрлері

Заманауи киберкеңістікте қауіп-қатерлер үнемі дамып, күрделеніп отырады. Шабуылдаушылар жаңа технологияларды пайдаланып, ұйымдар мен жеке тұлғаларға зиян келтіру үшін әртүрлі әдістерді қолданады. Қауіп-қатерлердің түрлерін білу және олардан қорғану тәсілдерін меңгеру өте маңызды.



Қауіп-қатерлердің негізгі түрлері



Зиянкестер және хакерлер

Сыртқы шабуылдаушылар (хакерлік топтар, мемлекеттік акторлар) және ішкі қауіптер (қанағаттанбаған қызметкерлер, абайсыздық). Әлеуметтік инженерия және фишинг әдістерін қолданады.



Зиянды бағдарламалар

Вирустар, трояндар, ransomware, шпиондық бағдарламалар және ботнеттер. Жүйелерді жұқтырып, деректерді ұрлайды немесе жояды, құрылғыларды бақылауға алады.



Фишинг шабуылдары

Жалған электрондық хаттар, SMS-хабарламалар немесе веб-сайттар арқылы құпия ақпаратты алу әрекеттері. Банк деректері, парольдер мен жеке мәліметтерді ұрлауға бағытталған.



Деректердің жоғалуы

Ақпараттың заңсыз өзгертілуі, жойылуы немесе сыртқа ағып кетуі. Техникалық ақаулардан, адам қатесінен немесе қасақана әрекеттерден туындауы мүмкін.

Осы қауіптердің әрқайсысы ұйымдарға айтарлықтай залал келтіре алады: қаржылық шығындар, беделдің нашарлауы, заңдық жауапкершілік және бизнес-процестердің тоқтауы.

Ішкі қауіптер: қызметкерлердің рөлі

Ішкі қауіптердің сипаттамасы

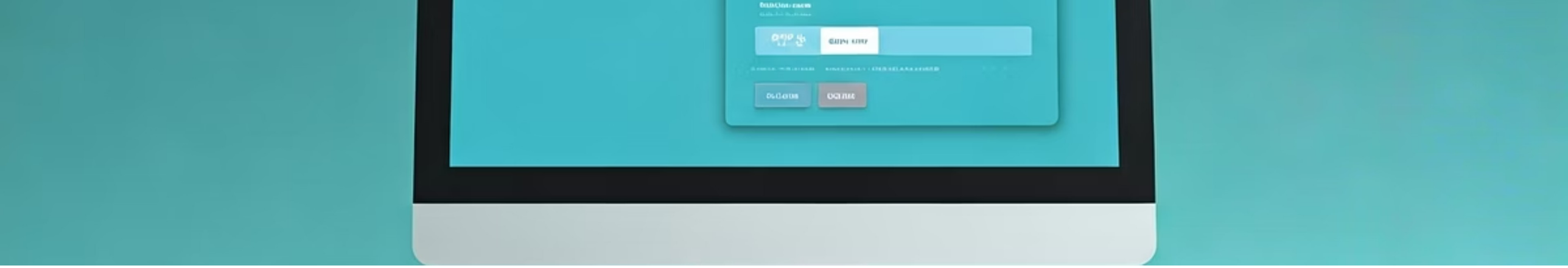
Статистика көрсеткендей, ақпараттық қауіпсіздік инциденттерінің 30-40%-ы ұйым ішінен келеді. Бұл қасақана әрекеттер немесе қызметкерлердің абайсыздығы болуы мүмкін.

Ішкі қауіптердің түрлері:

- **Қасақана әрекеттер:** Құпия ақпаратты ұрлау, бәсекелестерге сату, жүйелерді саботаждау
- **Абайсыздық:** Қауіпсіздік ережелерін білмеу немесе елемеу, әлсіз парольдер қолдану
- **Әлеуметтік инженерия:** Қызметкерлерді алдап, құпия ақпарат алу
- **Құрылғыларды жоғалту:** Ноутбук, USB-жад құрылғыларын сақтамау



Қауіпсіздік саясатын бұзудың нақты мысалдары: Жеке құрылғыларда жұмыс деректерін сақтау, қорғалмаған Wi-Fi желілерін пайдалану, парольдарды басқалармен бөлісу, фишингтік хаттардағы сілтемелерді басу.



Фишинг шабуылдарының әдістері

Фишингтік электрондық хат

Танымал ұйымдар (банктер, мемлекеттік қызметтер) атынан жалған хаттар жіберіледі

Смишинг

SMS арқылы алаяқтық хабарламаларын жіберу және жалған сілтемелер беру

Жалған веб-сайттар

Түпнұсқа сайттарға өте ұқсас көшірме сайттар жасалып, логин мен парольдерді ұрлайды

Фишинг шабуылдарының сәттілік коэффициенті өте жоғары, себебі олар психологиялық әдістерді қолданады: шұғыл әрекет ету қажеттігін жасайды, сенім тудырады және адамның эмоцияларын пайдаланады.

Ақпараттық қауіпсіздік саясатының элементтері

Тиімді ақпараттық қауіпсіздік саясаты бірнеше өзара байланысты элементтерден тұрады. Әрбір элемент маңызды рөл атқарады және бірге олар кешенді қорғау жүйесін құрайды. Осы элементтерді дұрыс біріктіру ұйымның қауіпсіздік деңгейін айтарлықтай арттырады.



Қатынас құруды ерікті және мәжбүрлі басқару

Ерікті басқару (Discretionary Access Control - DAC)

Ресурстың иесі өз қалауы бойынша басқа пайдаланушыларға рұқсаттар береді. Икемділік пен басқарудың қарапайымдығын қамтамасыз етеді, бірақ ресурс иесінің шешіміне тәуелді.

Мәжбүрлі басқару (Mandatory Access Control - MAC)

Рұқсаттар орталықтандырылған саясатқа сәйкес қатаң белгіленеді. Жоғары қауіпсіздік деңгейін қамтамасыз етеді, өйткені пайдаланушылар өз рұқсаттарын өзгерте алмайды.

Қауіпсіздік тамғалары (Security Labels)

Деректер мен пайдаланушыларға арнайы тамғалар беріледі (мысалы: "Құпия", "Жариялы"). Қол жеткізу тек тамғалар сәйкес келген жағдайда ғана рұқсат етіледі.

Аудит және бақылау

Барлық қол жеткізу әрекеттері тіркеледі және тұрақты талданады. Бұл қауіпсіздік саясатының бұзылуын анықтауға және тергеуге мүмкіндік береді.



Кепілдік және есеп берушілік

Операциялық кепілдіктер

Барлық маңызды әрекеттер тіркеледі: кім, қашан, қандай операция орындады. Бұл түпнұсқалықты растау және даулы жағдайларда дәлелдеме ретінде қолданылады.

- Пайдаланушылардың әрекеттерін логтау
- Жүйе өзгерістерін бекіту
- Транзакцияларды хаттамалау

Технологиялық кепілдіктер

Техникалық құралдар арқылы деректердің түпнұсқалығы мен тұтастығы қамтамасыз етіледі. Цифрлық қолтаңбалар, хеш-функциялар және блокчейн технологиялары қолданылады.

- Цифрлық қолтаңба және сертификаттар
- Хеш-функциялар арқылы тексеру
- Уақыт белгілері (timestamps)

Хаттамалау және оқиғаларды тіркеу

Барлық қауіпсіздік оқиғалары, қатынас әрекеттері және жүйе өзгерістері арнайы log-файлдарда сақталады. Бұл мәліметтер инциденттерді тергеу және аудит жүргізу үшін қолданылады.

- Орталықтандырылған логтау жүйесі
- Логтарды қауіпсіз сақтау
- Автоматты талдау және ескерту

Техникалық және ұйымдастырушылық шаралар

Техникалық шаралар

- **Криптография**

  Деректерді шифрлау және электрондық қолтаңбалар қолдану

- **Антивирустық қорғау**

  Зиянды бағдарламаларды анықтау және жою жүйелері

- **Брандмауэрлер**

  Желілік трафикті бақылау және фильтрациялау

- **DLP жүйелері**

  Деректердің ағып кетуін болдырмау технологиялары

- **SIEM шешімдері**

  Қауіпсіздік оқиғаларын орталықтандырылған басқару

Ұйымдастырушылық шаралар

- **Қызметкерлерді оқыту**

  Тұрақты тренингтер және қауіпсіздік хабардарлығын арттыру

- **Саясаттар мен процедуралар**

  Нақты қауіпсіздік ережелері мен нұсқаулықтарды әзірлеу

- **Қол жеткізуді басқару**

  Рұқсаттарды беру және қадағалау процедуралары

- **Аудит және тексерулер**

  Қауіпсіздік деңгейін тұрақты бағалау

- **Инцидентке жауап беру**

  Қауіпсіздік оқиғаларын басқару жоспарлары

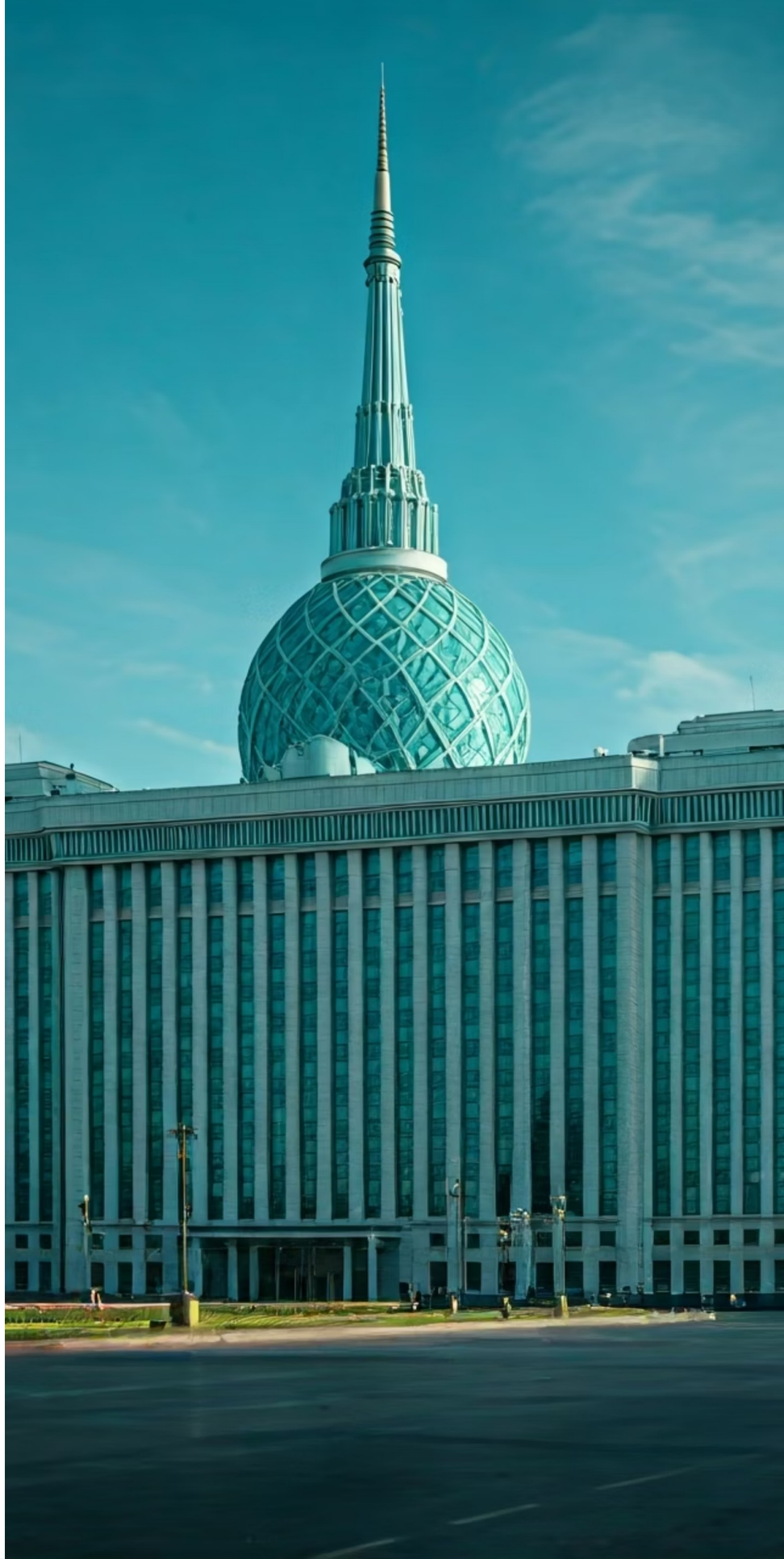
Ақпараттық қауіпсіздік саясатының құрылымы



Ақпараттық қауіпсіздік саясатының құрылымы пирамида түрінде ұйымдастырылады. Жоғарғы деңгейде жалпы стратегия мен саясаттар орналасады, ал төменгі деңгейлерде нақты стандарттар, процедуралар және күнделікті нұсқаулықтар қамтылады. Әрбір деңгей өзінен жоғары тұрған деңгейдің талаптарын нақтылай түседі.

Қазақстандағы ақпараттық қауіпсіздік тәжірибесі

Қазақстан ақпараттық қауіпсіздік саласында айтарлықтай жетістіктерге қол жеткізді. Мемлекеттік деңгейде қауіпсіздік инфрақұрылымы дамытылып, халықаралық стандарттар енгізілуде. Отандық тәжірибе мен озық әлемдік практиканы біріктіру Қазақстанның киберқауіпсіздік жүйесін нығайтуға мүмкіндік береді.



Мемлекеттік құпияларды қорғау шаралары



Құпия ақпаратты қорғау жүйесі

Мемлекеттік құпиялар – елдің ұлттық қауіпсіздігіне, қорғанысына және мемлекеттік мүдделеріне қатысты ақпарат. Оны қорғау ерекше мән мен жауапкершілікті талап етеді.

1

Құпиялылық деңгейлері

"Ерекше маңызды", "Өте құпия", "Құпия" және "Қызмет бабында пайдалануға" деңгейлері белгіленген

2

Өңдеу талаптары

Арнайы сертификатталған жабдықтар мен бағдарламалық қамтамасыз етулерді қолдану міндетті

3

Сақтау шарттары

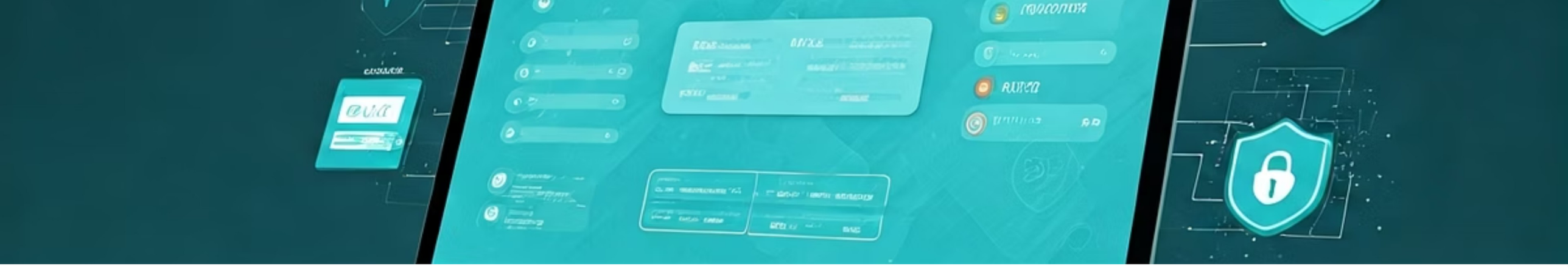
Физикалық қорғалған, қол жеткізуі бақыланатын арнайы үй-жайларда сақталады

4

Рұқсат беру

Тек арнайы тексеруден өткен және рұқсат алған қызметкерлер ғана жұмыс істейді

"Үкіметтің мобильдік офисі" жүйесі де қатаң қауіпсіздік стандарттарына сәйкес жұмыс істейді: деректер шифрланады, қол жеткізу көп факторлы аутентификациямен қорғалады, барлық әрекеттер логталады.



Электрондық үкіметтің ақпараттық қауіпсіздігі

01

Интеграция қағидалары

Ақпараттандыру объектілерін біріктіру кезінде қауіпсіздік талаптары міндетті түрде сақталады

02

Деректерді қорғау

Азаматтардың жеке деректері мен мемлекеттік ақпарат қатаң қорғалады және шифрланады

03

Аутентификация

Электрондық цифрлық қолтаңба (ЭЦҚ) арқылы пайдаланушылардың сәйкестігі расталады

04

Мониторинг

Жүйелердің жұмысы мен қауіпсіздік оқиғалары тәулік бойы бақыланады

2018 жылғы №123 бұйрық

Мемлекеттік органдардың ақпараттандыру объектілерін интеграциялау қағидалары бекітілді. Бұл құжат электрондық үкіметтің барлық жүйелері үшін біртұтас қауіпсіздік стандарттарын белгіледі.

Жаңартулар мен дамыту

Технологиялардың дамуына қарай қауіпсіздік стандарттары үнемі жаңартылады. Жаңа қауіптерге жауап ретінде қосымша қорғау шаралары енгізіледі.

Ақпараттық жүйелерді қорғау тәжірибесі

Ғылыми зерттеулер мен практикалық енгізулер

Қазақстандық университеттер мен ғылыми орталықтар ақпараттық қауіпсіздік саласында белсенді зерттеулер жүргізуде. Олардың жұмыстары теория мен практиканы біріктіреді.

Тараз мемлекеттік университетінің үлесі:

- Ақпараттық жүйелердің қауіпсіздігін бағалау әдістемелері әзірленді
- Қорғау механизмдерін тестілеу зертханасы жұмыс істейді
- Қауіпсіздік саясатын енгізу бойынша кейс-стадилер жарияланды
- Мамандарды даярлау бағдарламалары жетілдірілуде



"Біздің зерттеулер көрсеткендей, қауіпсіздік саясатын сәтті енгізу үшін техникалық шаралармен қатар қызметкерлердің білімі мен санасы өте маңызды"

"Практикалық тәжірибе университеттердің теориялық базасымен үйлескенде ең жақсы нәтижелер алынады"

Қазақстанның киберқауіпсіздік инфрақұрылымы

АҚҰҰО

Орталық үйлестіру және мониторинг

Халықаралық серіктестер

Ақпарат алмасу және ынтымақтастық

Білім орталықтары

Зерттеулер және мамандар даярлау



Мемлекеттік органдар

Секторлық қауіпсіздік жауапкершілігі

CERT командалары

Инциденттерге жедел жауап беру

Интернет-провайдерлер

Желілік қауіпсіздік және бақылау

Қазақстанның киберқауіпсіздік инфрақұрылымы барлық маңызды акторларды біріктіреді. Бұл циклдік өзара әрекет модель қауіптерге тиімді жауап беруге және қауіпсіздік деңгейін үнемі жақсартуға мүмкіндік береді.

Қауіптерге қарсы әрекет және басқару

Ақпараттық қауіптерді тиімді басқару – бұл проактивті тәсіл, оперативті жауап беру және үздіксіз жетілдіру үдерісі. Қауіптерді алдын ала анықтап, оларға дер кезінде әрекет ету ұйымның қауіпсіздігін айтарлықтай арттырады және потенциалды зардаптарды азайтады.



Қауіптерді анықтау және бағалау

Активтерді инвентаризациялау

Барлық ақпараттық активтерді (деректер, жүйелер, жабдықтар) анықтау және жіктеу. Әрбір актив үшін құндылық деңгейін белгілеу.

Әлсіз жерлерді талдау

Техникалық әлсіздіктерді (бағдарламалық қателер, конфигурация қателері) және ұйымдастырушылық кемшіліктерді (әлсіз процедуралар, оқытылмаған қызметкерлер) анықтау.

Қауіптерді сәйкестендіру

Ықтимал қауіп көздерін (хакерлер, вирустар, табиғи апаттар, ішкі қауіптер) және олардың әлсіз жерлерді пайдалану әдістерін анықтау.

Тәуекелдерді бағалау

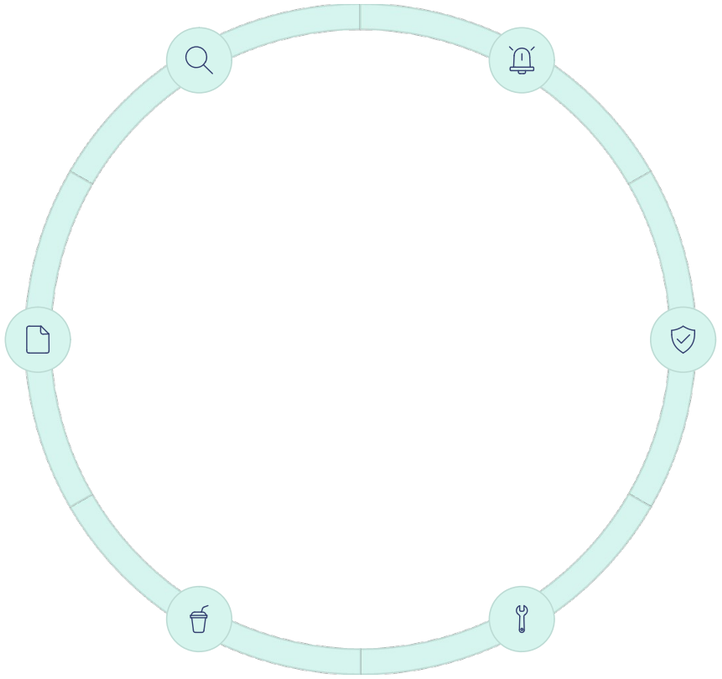
Әрбір қауіптің ықтималдығы мен потенциалды зардабын бағалау. Тәуекел матрицасын құру: жоғары/орташа/төмен деңгейлер.

Қорғау шараларын жоспарлау

Жоғары тәуекелді қауіптерді жою немесе азайту үшін нақты шараларды әзірлеу. Бюджет пен ресурстарды бөлу.

Жедел әрекет ету және оқиғаларды басқару

Инцидентке жауап беру циклі



Анықтау

Қауіпсіздік оқиғасын тіркеу

Бағалау

Ауырлық деңгейін анықтау

Локализация

Зардаптарды шектеу

Жою

Қауіпті толығымен жою

Қалпына келтіру

Қалыпты жұмысты қайта бастау

Талдау

Инциденттен сабақ алу

CERT командасының рөлі

Computer Emergency Response Team (CERT) – бұл қауіпсіздік инциденттеріне жедел жауап беретін арнайы топ.

Негізгі міндеттері:

- Тәулік бойы мониторинг және дабыл жүйелері
- Инциденттерге жедел жауап беру
- Қауіп туралы хабарламалар тарату
- Басқа CERT-тармен ынтымақтастық
- Post-mortem талдау жүргізу
- Қауіпсіздікті жақсарту ұсыныстары



Қауіпсіздік саясатын жаңарту және жетілдіру

Үздіксіз мониторинг

Ақпараттық жүйелердің жай-күйін, қауіпсіздік оқиғаларын және жаңа қауіптерді тұрақты бақылау. SIEM жүйелері және автоматты сканерлеу құралдарын қолдану.

Саясатты қайта қарау

Қауіпсіздік саясаты мен процедураларын кемінде жылына бір рет немесе ірі өзгерістер болған кезде қайта қарау және жаңарту.

Қызметкерлерді дамыту

Қауіпсіздік мәдениетін қалыптастыру үшін тұрақты оқытулар, тренингтер, фишинг симуляциялары және хабардарлық науқандары өткізу.

Инновацияларды енгізу

Жаңа технологиялар мен озық тәжірибелерді үнемі зерттеп, ұйымның қауіпсіздік жүйесіне интеграциялау.

Тәуекелдерді қайта бағалау

Қауіп ландшафты үнемі өзгереді: жаңа шабуыл әдістері пайда болады, ескі әлсіздіктер жойылады, технологиялар дамиды. Сондықтан тәуекелдерді тұрақты қайта бағалау қажет.

Метрикалар мен KPI

Қауіпсіздік деңгейін өлшеу үшін нақты көрсеткіштерді белгілеу керек: инциденттер саны, жауап беру уақыты, оқыту қамтуы, сәттілік коэффициенті.

Жедел әрекет командасының жұмысы

1

Дайындық

Инцидентке жауап беру жоспары, құралдар, оқытылған команда

2

Анықтау

Қауіпсіздік оқиғасын тіркеу және растау

3

Әрекет

Қауіпті локализациялау және жою

4

Қалпына келтіру

Жүйелерді қайта іске қосу және бақылау

5

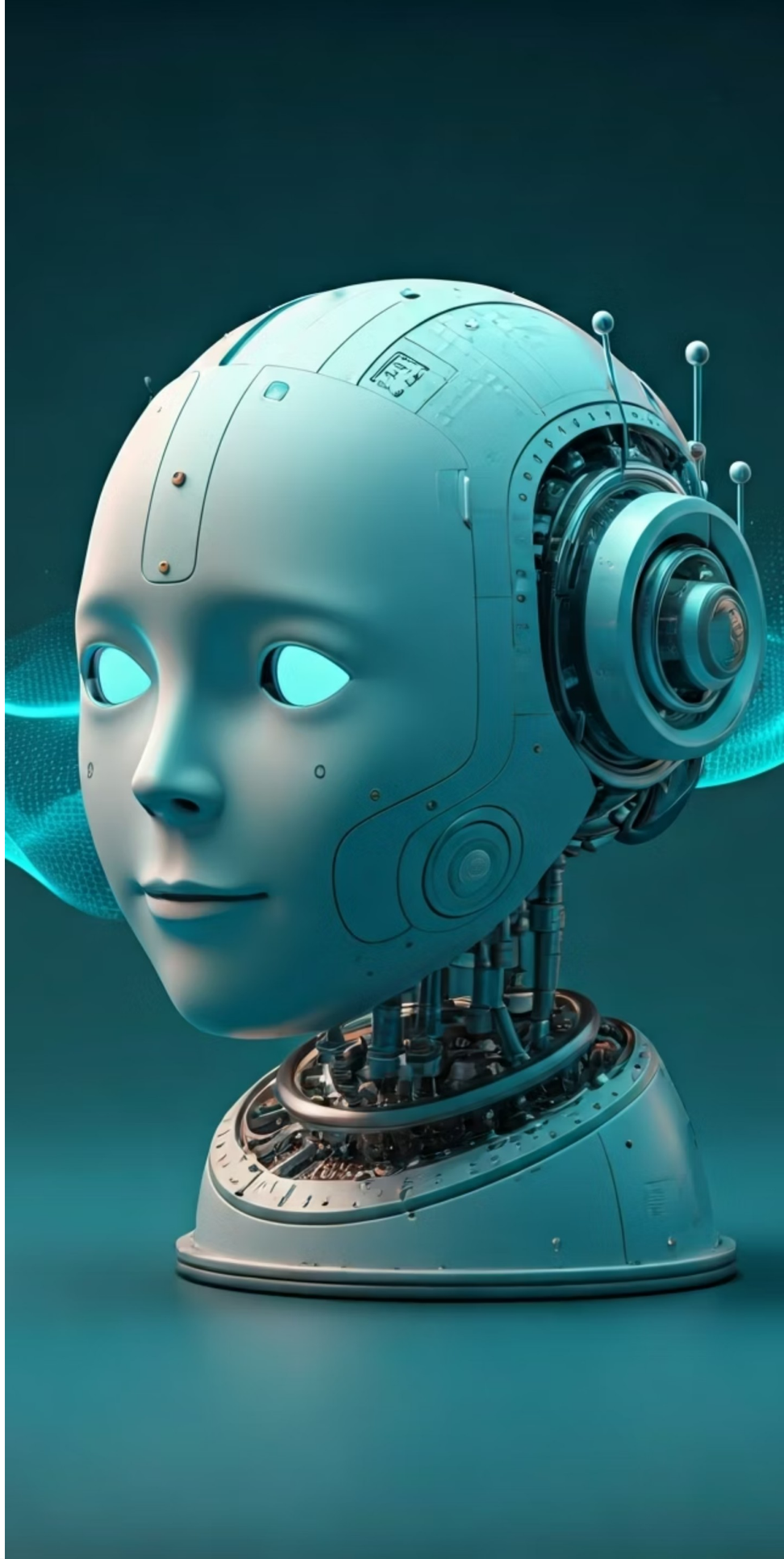
Сабақ

Инциденттен сабақ алу және жетілдіру

Тиімді инцидентке жауап беру командасы нақты процедураларға сәйкес жұмыс істейді, арнайы құралдар мен автоматтандыруды қолданады, басқа командалармен үйлесімді әрекет етеді және әрбір инциденттен тәжірибе жинақтайды.

Қазіргі заманғы қауіптер мен трендтер

Технологиялардың қарқынды дамуы жаңа мүмкіндіктермен қатар жаңа қауіптерді де тудырады. Жасанды интеллект, бұлттық технологиялар және Заттар интернеті (IoT) киберқауіпсіздік ландшафтын түбегейлі өзгертуде. Осы трендтерді түсіну және оларға дайын болу өте маңызды.



Жасанды интеллект және ақпараттық қауіпсіздік

ЖИ қорғаныста

Қауіптерді автоматты анықтау

Машиналық оқыту алгоритмдері аномалияларды мен жаңа шабуыл үлгілерін адамнан жылдам анықтай алады

Болжамды аналитика

ЖИ үлкен деректерді талдап, әлеуетті қауіптерді алдын ала анықтауға көмектеседі

Автоматты жауап беру

SOAR жүйелері ЖИ көмегімен қарапайым инциденттерге автоматты түрде жауап береді

ЖИ шабуылдарда

Дербес фишинг

ЖИ жеке тұлғаға арналған, өте сенімді фишинг хаттарын жасай алады

Автоматтандырылған шабуылдар

Боттар мен ЖИ әлсіз жерлерді іздеуді және шабуылдарды автоматтандырады

Deepfake технологиялары

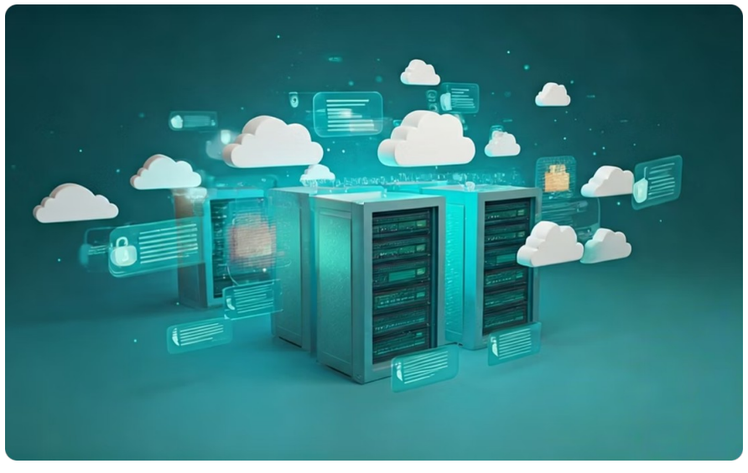
Жалған видео мен аудио үлгілерін жасап, әлеуметтік инженерия шабуылдарында қолданады

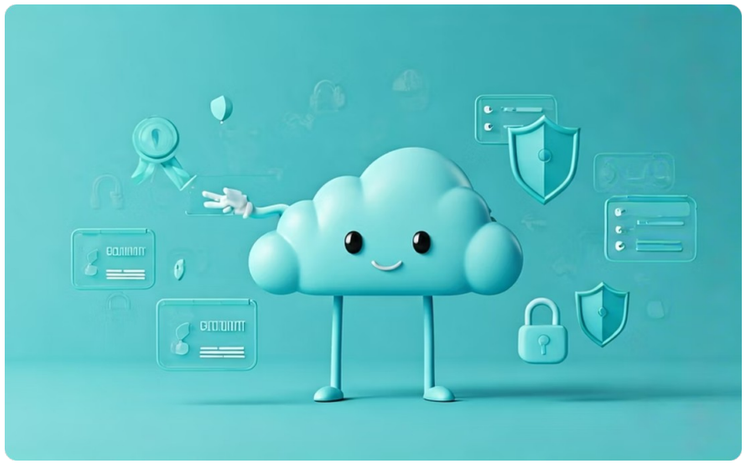
Жасанды интеллект киберқауіпсіздікте "қос жүзді қылыш" болып табылады – ол қорғанушыларға да, шабуылдаушыларға да артықшылықтар береді. Сондықтан ұйымдар ЖИ-ны өз қорғаныс стратегиясына енгізуі керек.



Бұлттық технологиялар және қауіпсіздік







Деректерді қорғау мәселелері

Бұлттық қызметтерде деректер үшінші тарап провайдерлерінде сақталады. Бұл қосымша тәуекелдер тудырады: деректердің орналасқан жері, шифрлау, рұқсаттарды басқару және провайдердің қауіпсіздік деңгейі.

Гибридті және көп бұлтты ортада

Көптеген ұйымдар бірнеше бұлттық провайдерлерді қолданады. Бұл күрделілікті арттырады: әртүрлі қауіпсіздік модельдері, интеграция мәселелері, біртұтас бақылауды қамтамасыз ету қиындығы.

Қазақстандағы талаптар

Қазақстанда бұлттық қызметтерге арнайы талаптар қойылған: кейбір деректердің елде сақталуы, лицензиялау, мемлекеттік органдардың бұлтты пайдалану шарттары. Халықаралық провайдерлер осы талаптарға бейімделуде.

Бұлттық қауіпсіздік принциптері: Жауапкершілікті бөлісу моделі (Shared Responsibility Model), шифрлау (тыныштықта және транзитте), жеткілікті рұқсат беру (Least Privilege), тұрақты аудит және мониторинг.

IoT құрылғыларының қауіптері



Заттар интернетінің қауіпсіздік проблемалары

IoT құрылғылары – ақылды үй жүйелері, өндірістік сенсорлар, медициналық құрылғылар – қарқынды дамуда. Бірақ олардың көбі қауіпсіздікті ескермей жобаланған.

Әлсіз құрылғылар

Әдепкі парольдер, жаңартылмайтын firmware, шифрлаудың жоқтығы

Ботнет тәуекелі

IoT құрылғылары Mirai сияқты ботнеттерге қосылып, DDoS шабуылдары үшін қолданылады

Жеке өмір қаупі

Камералар, микрофондар арқылы тыңдау және бақылау

Физикалық қауіп

Өндірістік немесе медициналық IoT құрылғыларын бұзу өмірге қауіпті

Қорғану шаралары:

- IoT құрылғыларын бөлек желіге (VLAN) бөлу
- Әдепкі парольдерді міндетті түрде өзгерту
- Firmware-ді тұрақты жаңарту
- Қажет емес құрылғыларды өшіру
- Желілік трафикті мониторингілеу

Киберқауіптер мен технологиялық трендтер

Жасанды интеллект

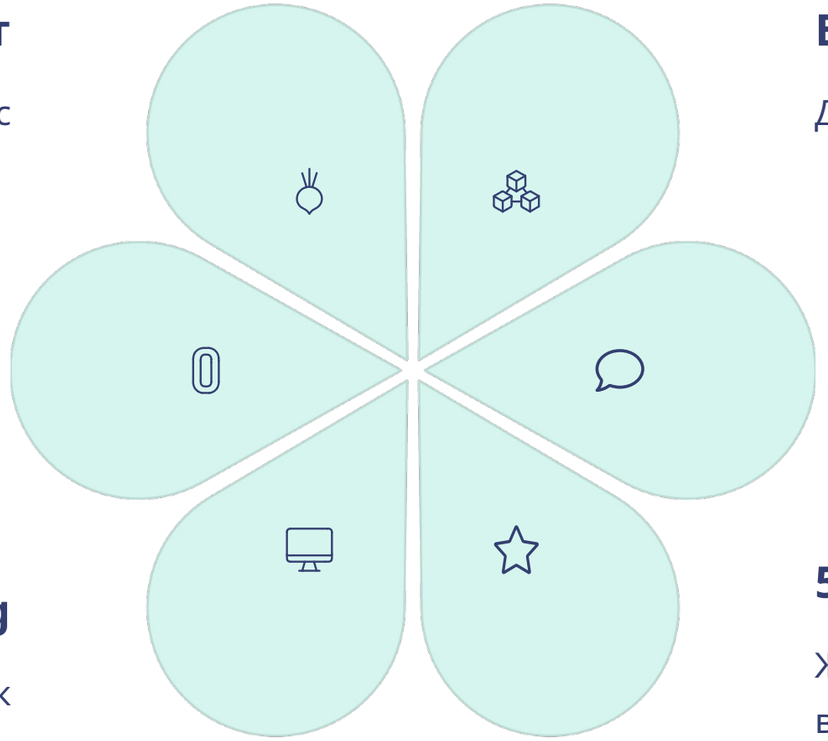
ЖИ негізіндегі шабуылдар мен қорғаныс

Блокчейн

Децентрализацияланған қауіпсіздік

Zero Trust

"Ешкімге сенбеу" қауіпсіздік моделі



Квантты есептеу

Криптографияға қауіп және жаңа әдістер

Edge computing

Шеткі есептеу және таратылған қауіпсіздік

5G желілері

Жылдам байланыс және жаңа шабуыл векторлары

Бұл технологиялық трендтер бір-бірімен тығыз байланысты және киберқауіпсіздік стратегиясын әзірлеу кезінде барлығын ескеру керек. Олар жаңа мүмкіндіктер мен қауіптерді бірдей тудырады.



Қорытынды және ұсыныстар

Ақпараттық қауіпсіздік – бұл бір реттік жоба емес, үздіксіз процесс. Тиімді қауіпсіздік саясаты заңнамалық талаптарды, техникалық шараларды, ұйымдастырушылық процестерді және адам факторын біріктіреді. Қазақстан бұл бағытта айтарлықтай жетістіктерге қол жеткізді, бірақ қауіптер үнемі дамып отырады және біз де дамуымыз керек.

Ақпараттық қауіпсіздік саясатын тиімді жүргізу үшін

Заңнамалық база

Қазақстан Республикасының барлық заңнамалық талаптарын қатаң сақтау: ақпараттық қауіпсіздік туралы заңдар, мемлекеттік құпияларды қорғау ережелері, деректерді қорғау стандарттары.

Ұйымдастырушылық құрылым

Қауіпсіздік функциялары мен жауапкершіліктерді нақты бөлу. Ақпараттық қауіпсіздік бөлімін құру немесе CISO (Chief Information Security Officer) тағайындау.

Техникалық шаралар

Заманауи қауіпсіздік технологияларын енгізу: брандмауэрлер, антивирустар, SIEM жүйелері, DLP шешімдері, шифрлау құралдары. Жабдықтарды үнемі жаңарту.

Үйлестіру

Барлық қауіпсіздік шараларын бір-бірімен үйлестіру. Техникалық, ұйымдастырушылық және заңдық аспектілердің сәйкестігін қамтамасыз ету.

Үздіксіз жақсарту

Қауіпсіздік саясатын тұрақты қайта қарау және жаңарту. Жаңа қауіптерге бейімделу және озық тәжірибелерді қолдану.

Бюджеттеу

Қауіпсіздікке жеткілікті қаржы бөлу. Бұл шығын емес, инвестиция екенін түсіну – инциденттердің құны қорғаныстан әлдеқайда қымбатырақ.

Қызметкерлерді оқыту және ақпараттық мәдениетті дамыту

Бастапқы оқыту

Жаңа қызметкерлерге базалық қауіпсіздік ережелері

Тұрақты тренингтер

Жылына кемінде 2-3 рет қауіпсіздік бойынша оқу

Кері байланыс

Қызметкерлерден ұсыныстар алу және өңдеу

Фишинг симуляциялары

Қызметкерлердің дайындығын тексеру

Сертификаттау

Маңызды позициялардағы қызметкерлерді сертификаттау

Хабардарлық науқандары

Плакаттар, хабарламалар, кеңестер

Маңызды: Қауіпсіздік ережелерін тек түсіндіру жеткіліксіз – оларды қызметкерлердің күнделікті мінез-құлқына айналдыру керек. Қауіпсіздік мәдениеті ұйымның корпоративтік мәдениетінің ажырамас бөлігі болуы тиіс.



Қауіптерге қарсы инновациялық технологияларды енгізу

Криптографияның жаңа әдістері

01

Постквanттық криптография

Кванттық компьютерлерге төзімді шифрлау алгоритмдері

02

Гомоморфтық шифрлау

Деректерді дешифрлемей өңдеуге мүмкіндік беретін технология

03

Blockchain қолданулары

Деректердің тұтастығын қамтамасыз ету және өзгертпеу

04

Квант кілт бөлу (QKD)

Абсолютті қауіпсіз кілттер алмасу технологиясы

Автоматтандырылған жүйелер

01

ЖИ негізіндегі SIEM

Қауіптерді автоматты анықтау және жіктеу

02

SOAR платформалары

Security Orchestration, Automation and Response

03

Мінез-құлық аналитикасы (UBA)

Пайдаланушылардың аномальды әрекеттерін анықтау

04

Автоматты vulnerability scanning

Әлсіздіктерді үздіксіз іздеу және жою

Ақпараттық қауіпсіздік саласындағы болашақ технологиялар



Кванттық технологиялар

Кванттық криптография абсолютті қауіпсіз байланысты қамтамасыз етеді. Кванттық компьютерлер қазіргі шифрлау әдістерін бұза алады, сондықтан постквантты криптографияны дамыту маңызды.



Биометриялық қауіпсіздік

Саусақ ізі, бет тану, көз торының сканерлеуі, дауыс тану сияқты биометриялық әдістер парольдарды алмастыруда. Көп факторлы биометриялық аутентификация дамиды.



Zero Trust архитектурасы

"Ешкімге сенбеу, бәрін тексеру" принципіне негізделген жаңа қауіпсіздік моделі. Әрбір қол жеткізу әрекеті расталады, ішкі және сыртқы қауіптер бірдей қарастырылады.

Болашақ технологиялары қауіпсіздік деңгейін айтарлықтай арттырады, бірақ олардың енгізілуі жаңа қауіптерді де тудыруы мүмкін. Сондықтан инновацияларды мұқият бағалап, дұрыс енгізу маңызды.

Қазақстанның ақпараттық қауіпсіздік саласындағы жетістіктері

АҚҰҰО құрылуы

2018 жылы Ақпараттық қауіпсіздік ұлттық үйлестіру орталығы құрылып, киберкеңістіктегі қауіпсіздікті орталықтандырылған басқаруды қамтамасыз етті. Орталық халықаралық CERT желісіне қосылды.

Заңнамалық база

Ақпараттық қауіпсіздік саласында кешенді заңнамалық база қалыптасты: мемлекеттік құпияларды қорғау, жеке деректерді қорғау, киберқылмыстарға қарсы күрес туралы заңдар қабылданды.

Техникалық инфрақұрылым

Ұлттық деңгейде киберқауіпсіздік инфрақұрылымы дамытылды: мониторинг жүйелері, инциденттерге жауап беру орталықтары, қауіпсіз байланыс желілері орнатылды.

Халықаралық ынтымақтастық

Қазақстан ТМД елдерімен, ШЫҰ-мен, Интерполмен және басқа халықаралық ұйымдармен киберқауіпсіздік бойынша белсенді ынтымақтасуда. Ақпарат алмасу және бірлескен жаттығулар өткізіледі.

Білім беру бағдарламалары

Университеттер мен колледждерде киберқауіпсіздік мамандықтары бойынша оқу бағдарламалары ашылды. Халықаралық сертификаттау орталықтары жұмыс істейді.

Инцидент статистикасы

АҚҰҰО жылына мыңдаған инциденттерді өңдейді, ірі шабуылдарды тоқтатады және ұйымдарға кеңес береді. Инцидентке жауап беру уақыты қысқарды.



Ақпараттық қауіпсіздік

Біздің ортақ жауапкершілігіміз!

> Қауіпсіздік саясатын бірге жетілдірейік – әрбір қызметкердің үлесі маңызды

> Қорғаныс – ақпараттық қоғамның негізі және болашағымыздың кепілі

Мемлекеттің рөлі

- Заңнамалық база
- Ұлттық инфрақұрылым
- Халықаралық ынтымақтастық

Ұйымдардың рөлі

- Қауіпсіздік саясатын енгізу
- Қызметкерлерді оқыту
- Технологияларға инвестиция

Азаматтардың рөлі

- Қауіпсіздік ережелерін білу
- Сақ болу және хабарлау
- Үздіксіз оқу

Ақпараттық қауіпсіздік – бұл технология ғана емес, мәдениет. Біз барлығымыз – мемлекет, ұйымдар, әрбір азамат – осы қауіпсіздікті қамтамасыз етуге жауаптымыз. Тек бірлескен күш-жігерімізбен ғана біз цифрлық кеңістікті қауіпсіз етіп, елімізді киберқауіптерден қорғай аламыз. Рахмет сіздерге назар аударғаныңыз үшін!