Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Ақпаратты қорғаудағы техникалық және бағдарламалық кешендер



Ақпараттық қауіпсіздік маңызы

Ақпарат – құнды ресурс

Заманауи цифрлық экономикада ақпарат ең құнды стратегиялық активке айналды. Жеке деректерден бизнес-процестерге дейін барлық деректер тиісті қорғауды қажет етеді.

Кешенді қорғаныс

Қорғаудың техникалық және бағдарламалық кешендері – ақпараттық қауіпсіздіктің негізі. Олар көп деңгейлі қорғанысты қамтамасыз етіп, киберқауіптерден сенімді қалқан болады.



Ақпараттық қауіпсіздік: Қазақстандағы ұлттық деңгей

АҚҰҰО – негізгі координатор

2018 жылы құрылған Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (АҚҰҰО) елдегі киберқауіпсіздік саласындағы орталық координациялық орган болып табылады.

Орталық келесі негізгі функцияларды атқарады:

- ҚР киберкеңістігін қорғауды үйлестіру
- Халықаралық ынтымақтастықты дамыту
- Киберқауіптерді мониторингілеу
- Инциденттерге жедел жауап беру

2018 жылдан бастап АҚҰҰО Қазақстанның киберқауіпсіздігін қамтамасыз етудің ұлттық жүйесін құруда жетекші рөл атқарады.

Қазақстанның киберқауіпсіздік инфрақұрылымы

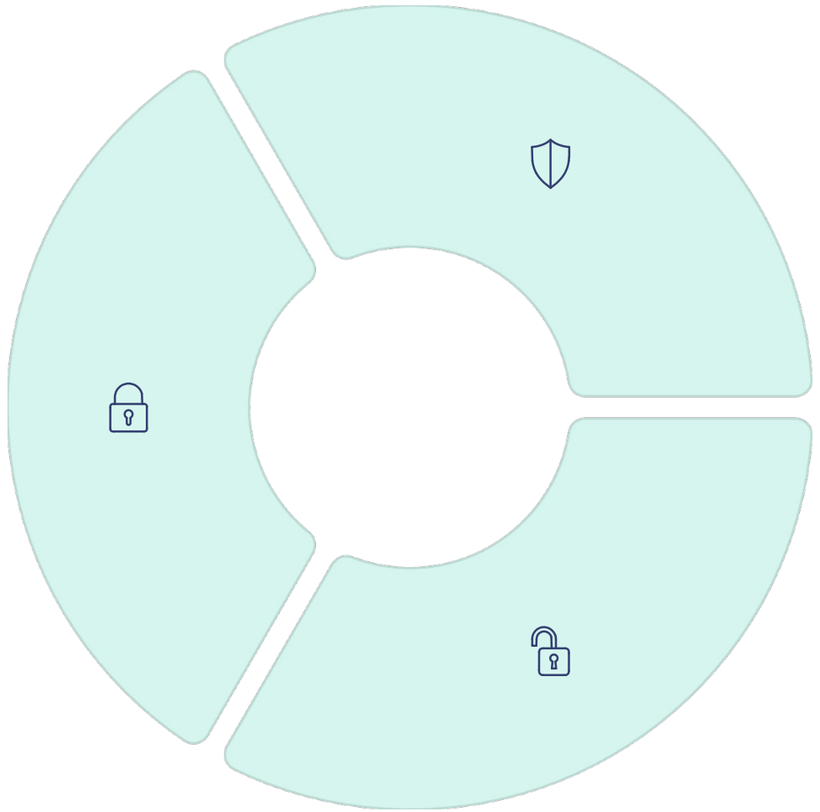
Ұлттық киберқауіпсіздік инфрақұрылымы мемлекеттік органдар, жеке сектор және халықаралық ұйымдардың тығыз өзара іс-қимылын қамтиды. Орталық координациялық орталықтар, аймақтық бөлімшелер және арнайы жауап беру топтары бірыңғай қорғаныс желісін құрайды.



Ақпараттық қауіпсіздіктің негізгі қағидаттары

Құпиялылық

Ақпаратты рұқсат етілмеген қол жеткізуден қорғау. Деректерге тек авторизацияланған пайдаланушылар ғана қол жеткізе алады.



Бүтіндік

Ақпараттың дұрыстығы мен толықтығын қамтамасыз ету. Деректердің рұқсатсыз өзгеруін болдырмау.

Қолжетімділік

Рұқсат етілген пайдаланушыларға қажетті уақытта ақпаратқа қол жеткізуді қамтамасыз ету.

Сонымен қатар, заңнамалық талаптарды сақтау және үздік халықаралық тәжірибелерді қолдану ақпараттық қауіпсіздік жүйесінің тиімділігін арттырады.



Ақпараттық қорғау кешендерінің құрылымы

Аппараттық құралдар

Желілік құрылғылар, қауіпсіздік шлюздері, шифрлау модульдері және басқа техникалық компоненттер.

Бағдарламалық қамтамасыз ету

Антивирустық жүйелер, файрволлдар, шифрлау бағдарламалары және мониторинг құралдары.

Ұйымдастырушылық шаралар

Саясаттар, процедуралар, қызметкерлерді оқыту және қауіпсіздік мәдениетін қалыптастыру.

Аппараттық құралдар

Қауіпсіздік шлюздері (Firewall)

Желілік трафикті бақылайды және сүзеді. Ішкі желі мен сыртқы әлем арасындағы шекара күзетшісі ретінде әрекет етеді, қауіпті байланыстарды блоктайды.

Антивирус және антишпиондық жүйелер

Зиянды бағдарламаларды анықтау, оқшаулау және жою. Нақты уақыт режимінде жүйені қорғау және үнемі жаңартылатын қауіптер базасын пайдалану.

Инциденттерді анықтау жүйелері (IDS/IPS)

Желілік мониторинг және күдікті белсенділікті анықтау. IPS жүйелері шабуылдарды автоматты түрде блоктау мүмкіндігін қамтамасыз етеді.

Негізгі түрлері

Шифрлау

Құпиялылықты қамтамасыз ететін шифрлау бағдарламалары деректерді рұқсатсыз қол жеткізуден қорғайды.

Симметриялық және асимметриялық алгоритмдер қолданылады.

Аутентификация

Қол жеткізуді бақылау және пайдаланушыларды тексеру жүйелері сәйкестікті растайды.

Көп факторлы аутентификация қауіпсіздікті арттырады.

Аудит құралдары

Қауіпсіздік аудиті және логтарды талдау құралдары инциденттерді анықтауға көмектеседі.

Автоматтандырылған талдау тиімділікті арттырады.

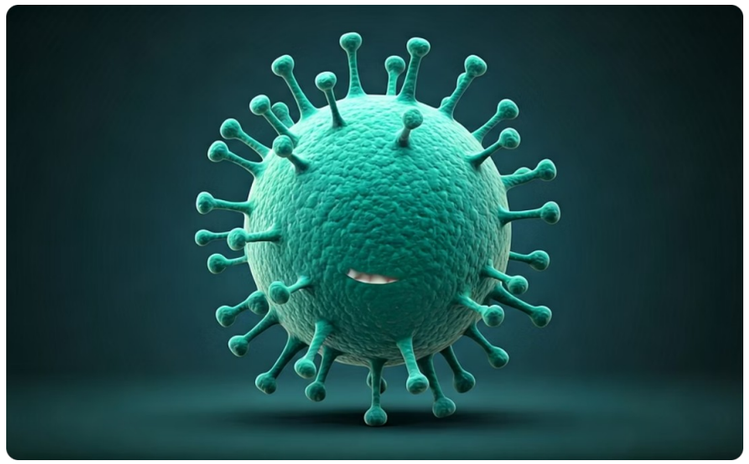




Желілік қауіпсіздік құрылғылары

Заманауи желілік қауіпсіздік құрылғылары аппараттық және бағдарламалық компоненттерді біріктіріп, көп деңгейлі қорғанысты қамтамасыз етеді. Интуитивті интерфейстер әкімшілерге жүйені оңай басқаруға және конфигурациялауға мүмкіндік береді.

Ақпараттық шабуылдардың түрлері және оларға қарсы кешендер



Вирустар мен трояндар

Зиянды бағдарламалар жүйені зақымдап, деректерді ұрлайды. Антивирустық жүйелер мен қауіпсіздік патчтары қорғанысты қамтамасыз етеді.



Фишинг

Әлеуметтік инженерия арқылы құпия деректерді ұрлау. Қызметкерлерді оқыту және электрондық пошта сүзгілері тиімді қорғаныс құралдары.



DDoS шабуылдары

Қызметті бұзу мақсатында жүйені шамадан тыс жүктеу. Арнайы қорғаныс жүйелері мен CDN желілері қолданылады.

Honeypot тұзақтары мен Machine Learning негізіндегі қорғаныс жүйелері жаңа қауіптерді ертерек анықтауға және оларға тиімді жауап беруге мүмкіндік береді.

Қазақстандағы ақпараттық қауіпсіздік саясаты

«Қазақтелеком» АҚ тәжірибесі

«Қазақтелеком» АҚ ақпараттық қауіпсіздік саясаты халықаралық стандарттарға сәйкес әзірленген және жүзеге асырылады.

Компания ISO 27001 сертификатын алып, үздік тәжірибелерді енгізуде көшбасшы болып табылады.

- Кешенді қауіпсіздік бағдарламалары
- Үздіксіз мониторинг және бағалау
- Қызметкерлерді оқыту бағдарламалары

Заңнамалық негіздер

Дербес деректерді қорғау және ақпараттық қауіпсіздікті қамтамасыз ету ҚР заңнамасында айқын регламенттелген.

> Ақпараттық қауіпсіздік талаптарын бұзғаны үшін әкімшілік және қылмыстық жауапкершілік көзделген.

Ақпараттық қауіпсіздікті қамтамасыз етудің жүйелі тәсілі

01

Қауіпсіз қашықтан қол жеткізу

Ақпараттық ресурстарға қауіпсіз қашықтан қол жеткізуді ұйымдастыру VPN технологиялары мен көп факторлы аутентификация арқылы жүзеге асырылады.

02

Интернетті қауіпсіз пайдалану

Веб-трафикті фильтрлеу, қауіпті сайттарды блоктау және SSL/TLS шифрлауды қолдану интернетті қауіпсіз пайдалануды қамтамасыз етеді.

03

Артықшылықты пайдаланушыларды бақылау

Әкімші құқықтары бар пайдаланушылардың әрекеттерін үздіксіз мониторингілеу және логтау ішкі қауіптерді азайтады.

Zero Trust тұжырымдамасы: жаңа қауіпсіздік парадигмасы

Ешкімге сенбеу қағидаты

Zero Trust моделі барлық қатынастарды әдепкі бойынша сенімсіз деп санайды – ол желінің ішінде немесе сыртында болса да.

Бұл жаңа көзқарас дәстүрлі периметрлік қорғанысты біржола өзгертеді.

Үздіксіз тексеру

Қол жеткізуді үздіксіз тексеру және бақылау әрбір транзакцияның қауіпсіздігін қамтамасыз етеді.

Пайдаланушылар, құрылғылар және қосымшалар үнемі аутентификациядан өтеді.

Минималды артықшылықтар

Әрбір пайдаланушыға тек қажетті минималды қол жеткізу құқықтары беріледі.

Бұл потенциалды зиян аумағын айтарлықтай азайтады.



Zero Trust архитектурасы

Zero Trust архитектурасы деректерді, қосымшаларды, активтерді және қызметтерді қорғайтын бірнеше қауіпсіздік деңгейлерін қамтиды. Бұл модель қазіргі заманғы гибридті және бұлтты орталарда ерекше тиімді болып табылады.

Ақпараттық қауіпсіздікке арналған аппараттық кешендердің мысалдары

Қауіпсіздік шлюздері

- **Cisco ASA** – кәсіби деңгейдегі файрволл
- **Fortinet FortiGate** – UTM шешімі
- **Palo Alto Networks** – жаңа буын файрволл
- **Check Point** – кешенді қауіпсіздік платформасы

Бұл шешімдер жоғары өнімділік пен кең функционалдылықты ұсынады.

Желілік құрылғылар

- **Маршрутизаторлар** – трафикті басқару
- **Коммутаторлар** – желіні сегменттеу
- **IDS/IPS жүйелері** – қауіптерді анықтау
- **VPN концентраторлары** – қауіпсіз қосылым

Желілік инфрақұрылым қауіпсіздіктің негізі болып табылады.



Бағдарламалық кешендердің мысалдары

Антивирус шешімдері

Kaspersky – кең таралған ресейлік антивирус

ESET – жылдам және тиімді қорғаныс

Symantec – кәсіпорындар үшін шешімдер

Шифрлау жүйелері

PGP – электрондық пошта шифрлауы

VeraCrypt – дискілерді шифрлау

BitLocker – Windows үшін шифрлау

Аутентификация жүйелері

LDAP – каталог қызметтері

Kerberos – желілік аутентификация

OAuth/SAML – заманауи протоколдар



Ұйымдастырушылық шаралар мен кадрлық қамтамасыз ету

Қызметкерлерді оқыту

Ақпараттық қауіпсіздік бойынша тұрақты оқыту бағдарламалары персоналдың хабардарлығын арттырады және адами факторға байланысты қауіптерді азайтады.

Қауіпсіздік мәдениеті

Ұйымдастырушылық мәдениетте ақпараттық қауіпсіздікті қалыптастыру ұзақ мерзімді табысқа жеткізеді. Әрбір қызметкер қауіпсіздіктің маңыздылығын түсінуі керек.

Жедел орталық

Ақпараттық қауіпсіздік жедел орталығы (SOC) инциденттерді үздіксіз мониторингілейді, талдайды және оларға жедел жауап береді.

Ақпараттық қауіпсіздік инциденттерін басқару

1

Анықтау

Инциденттерді ерте анықтау үшін автоматтандырылған мониторинг жүйелері мен аналитикалық құралдарды қолдану.

2

Тіркеу

Барлық инциденттерді жүйелі түрде тіркеу және құжаттау, кейінгі талдау үшін деректерді жинау.

3

Жою

Қауіптерді тез арада оқшаулау және жою, зардаптарды минимизациялау шараларын қабылдау.

4

Қалпына келтіру

Жүйелерді қалыпты жұмыс режиміне қайтару, зақымданған деректерді қалпына келтіру.

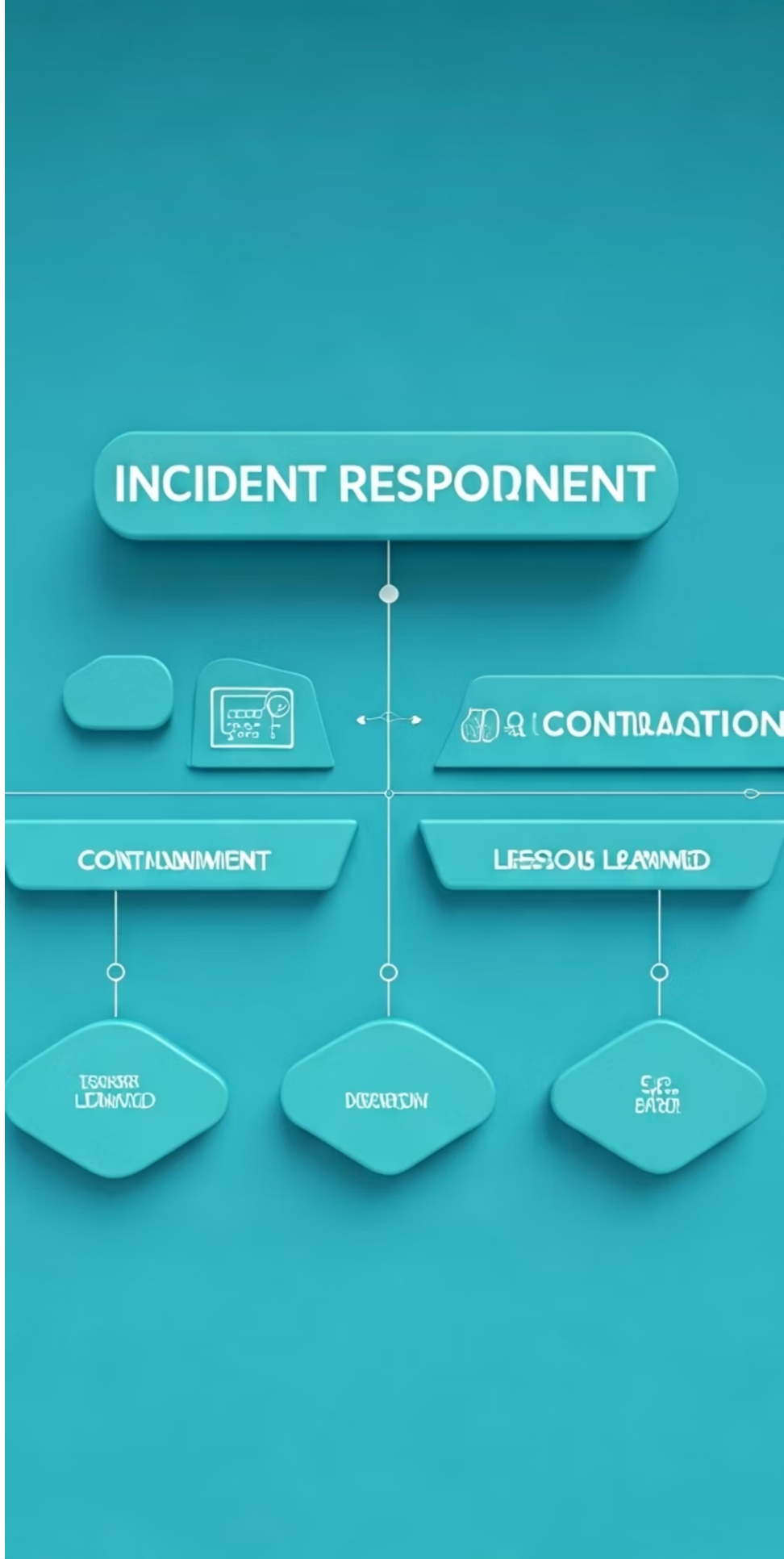
5

Сабақ алу

Инциденттерді талдау, себептерін анықтау және қауіпсіздік шараларын жетілдіру.

Инциденттерді басқару процесі

Инциденттерді басқарудың стандартталған процесі ұйымға қауіптерге тез және тиімді жауап беруге мүмкіндік береді. Әрбір кезең нақты рөлдер мен жауапкершіліктерді талап етеді.



Мемлекеттік нормативтік-құқықтық база

ҚР «Ақпараттандыру туралы» Заңы

2015 жылы қабылданған «Ақпараттандыру туралы» Заң Қазақстанның ақпараттық қауіпсіздік саласындағы негізгі заңнамалық актісі болып табылады.

Заңның негізгі бағыттары:

- Ақпараттық жүйелерді қорғау талаптары
- Дербес деректердің қауіпсіздігі
- Криптографиялық қорғаудың қолданылуы
- Ақпараттық қауіпсіздік саласындағы мемлекеттік реттеу

Заң ақпараттық қауіпсіздік талаптарын бекіту және олардың орындалуын бақылау механизмдерін белгілейді.

Маңызды: Заңды бұзғаны үшін қатаң жауапкершілік көзделген, соның ішінде ірі айыппұлдар мен қылмыстық жазалар.

Ақпараттық жүйелердің сәйкестік сертификаттары

Техникалық сәйкестік

Техникалық және бағдарламалық кешендер белгіленген қауіпсіздік талаптарына сәйкестігін растау үшін сертификаттауды өтуі керек. Бұл процесс өнім сапасын кепілдейді.

Халықаралық стандарттар

ISO/IEC 27001, Common Criteria және басқа халықаралық стандарттар ақпараттық қауіпсіздік жүйелерін бағалаудың бірыңғай критерийлерін қамтамасыз етеді.

Мемлекеттік стандарттар

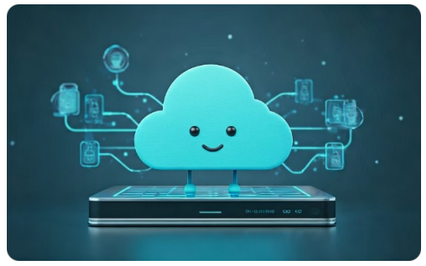
Қазақстанда ақпараттық қауіпсіздік саласында ұлттық стандарттар жүйесі жұмыс істейді. Олар халықаралық нормалармен үйлесімді және елдің ерекшеліктерін ескереді.

Ақпараттық қауіпсіздік саласындағы инновациялар



Жасанды интеллект

Machine Learning алгоритмдері қауіптерді үлгілерді талдау арқылы болжауға және жаңа шабуылдарды автоматты түрде анықтауға мүмкіндік береді. AI жүйелері үлкен деректер көлемін өңдеп, аномалияларды тез табады.



Бұлтты қауіпсіздік

Бұлттық технологиялардың дамуымен бірге олардағы қауіпсіздікті қамтамасыз ету жаңа тәсілдерді талап етеді. CASB, CWPP және басқа бұлтты қорғаныс шешімдері қолданылады.



Жасанды интеллект көмегімен қауіптерді анықтау

Заманауи AI жүйелері нейрондық желілер мен терең машиналық оқыту технологияларын пайдаланып, қауіптерді дәстүрлі әдістерге қарағанда әлдеқайда тез және дәл анықтайды. Олар әрекеттердің үлгілерін үйреніп, күдікті белсенділікті нақты уақыт режимінде анықтай алады.

Honeypot тұзақтары: шабуылдарды алдау және талдау

Honeypot технологиясының мәні

Honeypot – бұл шабуылдарды тартуға арналған әдейі осал етіп жасалған жалған мақсат. Ол нақты жүйелерден шабуылдарды алшақтатады және киберқылмыскерлердің тактикасын зерттеуге мүмкіндік береді.

Қолданылуы:

- Шабуылдардың әдістерін зерттеу
- Жаңа қауіптерді анықтау
- Қауіпсіздік шараларын жетілдіру
- Шабуылдарды нақты жүйелерден алшақтату

Қазақстандағы тәжірибе

Қазақстанның ақпараттық қауіпсіздік орталықтары honeypot технологияларын белсенді қолданады.

> Honeypot жүйелері киберқауіптердің эволюциясын бақылауға және проактивті қорғаныс стратегияларын әзірлеуге көмектеседі.

Қашықтан жұмыс және ақпараттық қауіпсіздік

VPN технологиялары

Virtual Private Network (VPN) қашықтан жұмыс істейтін қызметкерлер үшін қауіпсіз байланыс арнасын қамтамасыз етеді. Барлық трафик шифрланып, корпоративті желіге қауіпсіз қол жеткізу мүмкін болады.

Шифрланған байланыс

SSL/TLS протоколдары, end-to-end шифрлау және қауіпсіз мессенджерлер қашықтан жұмыс кезіндегі коммуникацияның құпиялылығын қорғайды.

Қол жеткізуді басқару

Қашықтан қол жеткізуді басқару көп факторлы аутентификация, қауіпсіздік саясаттарын автоматты түрде қолдану және қол жеткізу құқықтарын динамикалық түрде басқаруды қамтиды.



Аппараттық кешендердің даму үрдістері

IoT құрылғыларын қорғау

Заттар интернетінің (IoT) дамуымен бірге миллиардтаған қосылған құрылғылар жаңа қауіпсіздік қауіптері тудырады. Арнайы IoT қауіпсіздік шлюздері мен шифрлау модульдері әзірленуде.

Қауіпсіздік модульдері (TPM)

Trusted Platform Module (TPM) – бұл криптографиялық кілттерді сақтау және құрылғының бүтіндігін тексеру үшін арнайы аппараттық чип. Заманауи компьютерлерде стандартты болып табылады.

Аппараттық шифрлау

Жылдамдық пен қауіпсіздікті арттыру үшін шифрлау процестері аппараттық деңгейде орындалады. Бұл бағдарламалық шифрлауға қарағанда әлдеқайда тиімді.

Бағдарламалық кешендердің даму бағыттары

Автоматтандырылған жүйелер

Ақпараттық қауіпсіздіктегі автоматтандыру SOAR (Security Orchestration, Automation and Response) платформалары арқылы жүзеге асырылады.

Бұл жүйелер:

- Рутинді тапсырмаларды автоматтандырады
- Инциденттерге жауап беру уақытын қысқартады
- Адами қателіктерді азайтады

DevSecOps тәсілі

Қауіпсіздікті әзірлеу процесіне енгізу DevSecOps философиясының негізі болып табылады.

Негізгі принциптер:

- Қауіпсіздікті бастапқыдан енгізу
- Автоматтандырылған қауіпсіздік тестілері
- Үздіксіз мониторинг және жақсарту



Қазақстандағы жетекші компаниялар

«Ұлттық ақпараттық технологиялар» АҚ

ҰАТ мемлекеттік ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуде жетекші рөл атқарады. Компания отандық ақпараттық қауіпсіздік шешімдерін әзірлейді және енгізеді.

«Қазақтелеком» АҚ

Қазақстанның ең ірі телекоммуникациялық операторы ретінде «Қазақтелеком» желілік қауіпсіздіктің озық стандарттарын қолданады және киберқауіпсіздік саласында инновацияларды дамытады.

Басқа маңызды ойыншылар

CERT-Қазақстан, «Казинформзащита» және тағы басқа мамандандырылған компаниялар ақпараттық қауіпсіздік нарығында белсенді жұмыс істейді.



Ақпараттық қауіпсіздік саласындағы халықаралық ынтымақтастық

CERT желілері

CERT-Қазақстан (Computer Emergency Response Team) халықаралық CERT желілерімен белсенді ынтымақтастықта.

Негізгі бағыттар:

- Киберинциденттер туралы ақпарат алмасу
- Бірлескен зерттеулер жүргізу
- Үздік тәжірибелерді бөлісу
- Халықаралық жаттығуларға қатысу

Халықаралық стандарттар

Қазақстан халықаралық ақпараттық қауіпсіздік стандарттарын белсенді енгізуде:

- ISO/IEC 27001 – ақпараттық қауіпсіздікті басқару
- NIST Cybersecurity Framework
- COBIT – IT басқару
- PCI DSS – төлем карталарының қауіпсіздігі

Нақты оқиғалар мен сабақтар

2019 жылғы банктік секторға шабуыл

Қазақстанның бірнеше банкіне бағытталған DDoS шабуылы қызметтерді уақытша тоқтатты. Бұл оқиға банктік сектордағы қауіпсіздік шараларын күшейтуге әкелді.

Сабақ: резервтік жүйелер мен DDoS қорғанысының маңыздылығы.

Мемлекеттік порталдарға фишинг науқандары

Азаматтарды алдап, құпия деректерді ұрлауға бағытталған фишинг сайттары анықталды. Хабардарлық науқандары мен техникалық шаралар арқылы жойылды.

Сабақ: қызметкерлерді оқытудың және көпшілікті хабардар етудің маңыздылығы.

Ақпараттық қауіпсіздік саласындағы кадр тапшылығы және шешімдер

Мамандарды даярлау

Қазақстанда киберқауіпсіздік мамандарына сұраныс жылдан жылға артып келеді, бірақ кадр тапшылығы мәселесі өзекті болып қала береді.

Шешімдер:

- Университеттерде мамандандырылған бағдарламалар
- Ақпараттық қауіпсіздік академиялары
- Халықаралық сертификация бағдарламалары
- Практикалық хакатондар мен жарыстар

Үздіксіз даму

Ақпараттық қауіпсіздік саласында тек бастапқы білім жеткіліксіз – үздіксіз кәсіби даму қажет.

Мамандар үшін қолжетімді:

- Онлайн курстар және вебинарлар
- Халықаралық конференциялар
- Практикалық зертханалар

Ақпараттық қауіпсіздік мәдениетін қалыптастыру

Хабардарлық

Қызметкерлердің ақпараттық қауіптер туралы хабардарлығын арттыру арқылы олардың сауатты әрекеттерін қамтамасыз ету. Тұрақты оқыту және симуляциялар маңызды.

Жауапкершілік

Әрбір қызметкер ақпараттық қауіпсіздік үшін жауапты екенін түсінуі керек. Дербес жауапкершілік мәдениетін қалыптастыру қажет.

Саясаттар мен ережелер

Нақты және түсінікті ұйымдық саясаттар мен ережелерді әзірлеу және қолдану. Олар практикалық және орындалатын болуы тиіс.

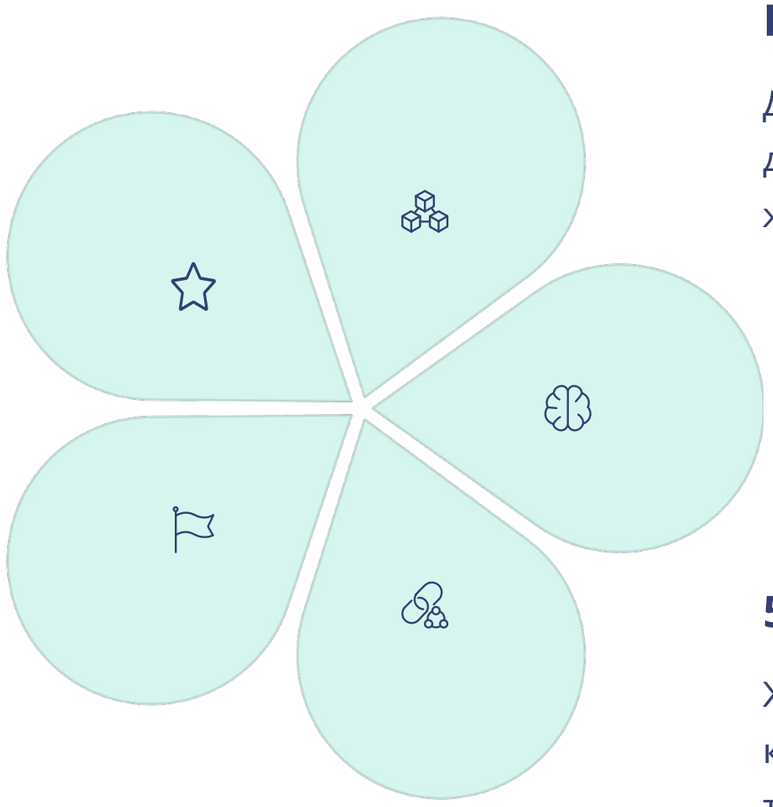
Болашаққа көзқарас: ақпараттық қауіпсіздіктің дамуы

Кванттық криптография

Кванттық есептеу технологияларының дамуы жаңа шифрлау әдістерін талап етеді. Кванттық криптография абсолютті қауіпсіздікті қамтамасыз етеді.

Қазақстанның стратегиясы

Ұлттық цифрлық қауіпсіздік стратегиясы елді технологиялық тәуелсіз және киберқауіпті етуге бағытталған.



Блокчейн

Децентрализацияланған технологиялар деректердің бүтіндігін қамтамасыз етуде жаңа мүмкіндіктер ашады.

AI эволюциясы

Жасанды интеллект қауіпсіздік саласында одан әрі дамып, проактивті қорғанысты қамтамасыз етеді.

5G қауіпсіздігі

Жаңа буын байланыс желілері жаңа қауіпсіздік қауіптері мен мүмкіндіктерді тудырады.



Кванттық криптография

Кванттық криптография кванттық механика заңдарын пайдаланып, теориялық тұрғыдан бұзуға болмайтын шифрлау әдістерін ұсынады. Бұл технология болашақтың цифрлық қауіпсіздігінің негізі болып табылады.

Ақпараттық қорғау кешендерін енгізу кезеңдері

1-кезең: Қажеттілікті анықтау

1

Ұйымның ақпараттық активтерін инвентаризациялау, қауіптерді бағалау және қауіпсіздік талаптарын анықтау. Бизнес-талаптарды техникалық шешімдерге аудару.

2-кезең: Жүйені жобалау

2

Қауіпсіздік архитектурасын әзірлеу, технологияларды таңдау және жобалық құжаттаманы дайындау. Барлық компоненттердің үйлесімділігін қамтамасыз ету.

3-кезең: Енгізу және конфигурация

3

Таңдалған шешімдерді орнату, конфигурациялау және интеграциялау. Толық тестілеуден өткізу және персоналды оқыту.

4-кезең: Мониторинг және жетілдіру

4

Жүйенің тиімділігін үздіксіз бақылау, жаңа қауіптерді анықтау және қауіпсіздік шараларын жетілдіру. Циклдік процесс ретінде жүзеге асырылады.

Ақпараттық қауіпсіздік бойынша үздік тәжірибелер

Көп деңгейлі қорғаныс

Defense in Depth стратегиясы бірнеше қорғаныс қабаттарын қамтиды: желілік қауіпсіздік, қосымшалар қауіпсіздігі, деректер қауіпсіздігі және физикалық қауіпсіздік. Бір қабаттың бұзылуы жүйені толық қорғаусыз қалдырмайды.

Тұрақты аудит

Жүйелерді тұрақты тексеру, осалдықтарды іздеу және қауіпсіздік конфигурацияларын бағалау. Пентестинг және Red Team жаттығулары нақты қорғаныс деңгейін көрсетеді.

Үздіксіз тестілеу

Қауіпсіздік шараларының тиімділігін тексеру үшін тұрақты симуляциялар мен жаттығулар өткізу. Vulnerability scanning және penetration testing кезеңдік түрде орындалуы керек.

Ақпаратты қорғауда кешенді тәсілдің маңызы

Техникалық және бағдарламалық кешендер

Ақпараттық қауіпсіздіктің техникалық және бағдарламалық кешендері – бұл заманауи цифрлық экономиканың тірегі. Олар ұйымдардың деректерін, процестерін және репутациясын қорғайды.

Кешенді тәсіл мыналарды біріктіреді:

- Озық аппараттық және бағдарламалық шешімдер
- Жақсы ұйымдастырылған процестер мен процедуралар
- Білімді және жауапты қызметкерлер
- Үздіксіз мониторинг және жетілдіру

Қазақстанның жетістіктері

Қазақстандағы ұлттық ақпараттық қауіпсіздік жүйелері мен инновациялар сенімді болашақтың кепілі болып табылады.

> Тек технологиялар емес, сонымен қатар адамдар мен процестердің үйлесімі ақпараттық қауіпсіздіктің табысын қамтамасыз етеді.

