Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Ақпаратты қорғаудың негізгі түсініктері мен қағидалары





Ақпаратты қорғау деген не?

Ақпаратты қорғау – бұл ақпараттың құпиялығын, тұтастығын және қолжетімділігін қамтамасыз ететін кешенді шаралар жүйесі. Ол техникалық, ұйымдастырушылық және құқықтық құралдарды біріктіреді.

Ақпаратты қорғау – неге қажет?

Құпиялылық

Ақпараттың құпиялығын, тұтастығын және қолжетімділігін сақтау арқылы ұйымдық және жеке деректерді қорғау

Қауіптерден қорғау

Құпия деректердің ұрлануы мен бұрмалануын болдырмау, кибершабуылдар мен зиянды бағдарламалардан қорғану

Заңнамалық негіз

Қазақстандағы ақпараттық қауіпсіздік заңнамасының негізі, мемлекеттік және коммерциялық құпияларды қорғау

Ақпаратты қорғау амалдары мен тәсілдері

Қорғау бағыттары

- Ақпаратты ағып кетуден қорғау
- Ұрлаудан және рұқсатсыз қолжетімділіктен қорғау
- Деректерді өзгертуден және бұрмалаудан қорғау
- Рұқсатсыз көшіру мен жоюға тосқауыл қою

Алдын алу шаралары

- Қауіптерді уақтылы анықтау және талдау
- Проактивті мониторинг жүйелерін енгізу
- Қауіпсіздік саясатын әзірлеу және енгізу
- Қызметкерлерді оқыту және хабардар ету



Ақпарат ағынының схемасы: қауіптер мен қорғаныс механизмдері

Ақпарат көзі

Деректер базалары, құжаттар, электрондық файлдар

Тасымалдау

Желілер, каналдар, бұлттық жүйелер

Қорғау қабаты

Шифрлау, аутентификация, бақылау

Қолданушы

Рұқсатты қолжетімділік, қауіпсіз пайдалану



Ақпараттық жүйе және ақпараттық ресурстар

1

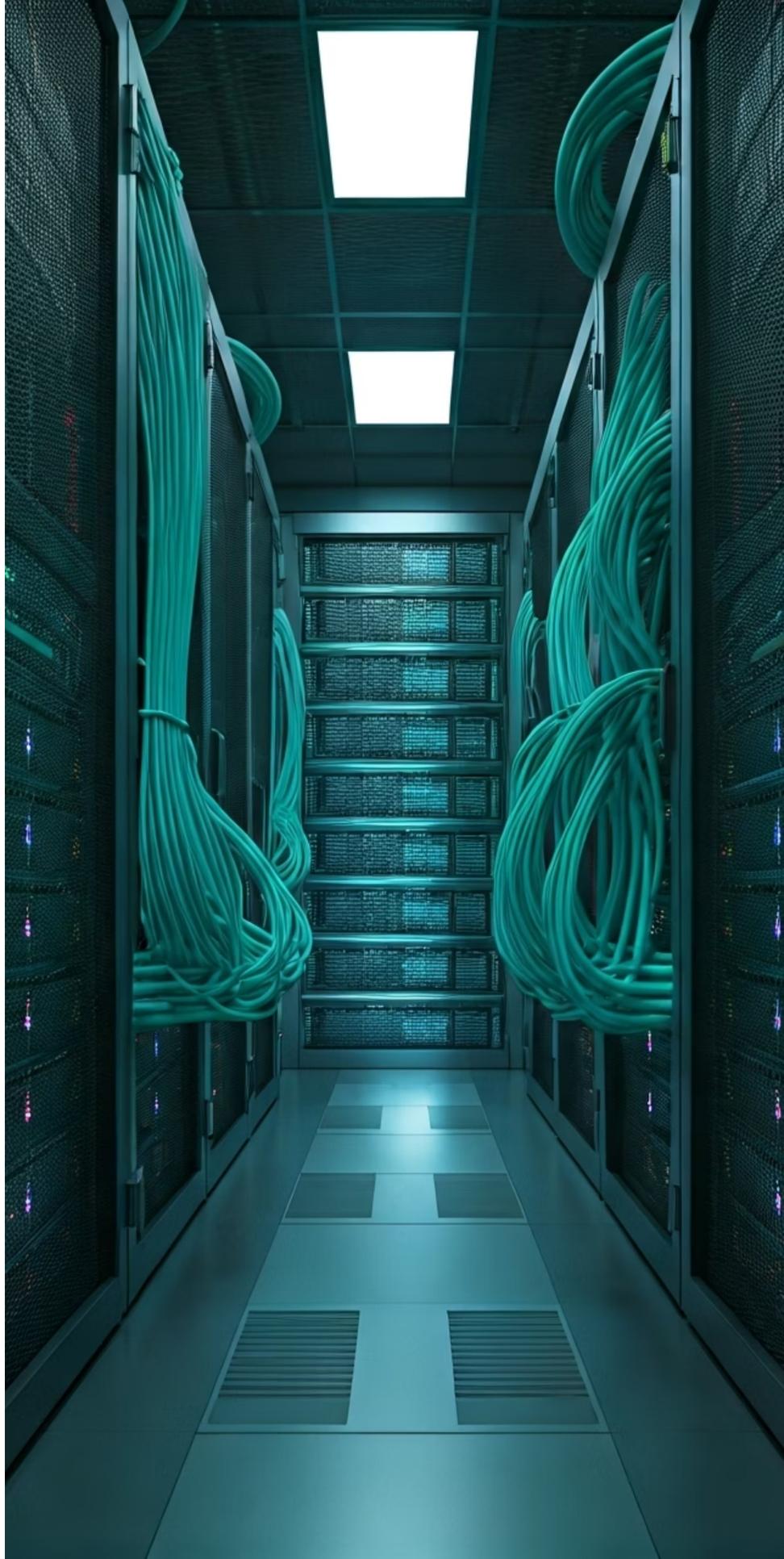
Ақпараттық жүйе

Технологиялар, желілер және бағдарламалық қамтамасыз ету кешені. Бұл дербес компьютерлер, серверлер, желілік жабдықтар, қауіпсіздік құралдары және басқа да техникалық инфрақұрылымды қамтиды.

2

Ақпараттық ресурстар

Деректер базалары, құжаттар, электрондық ақпарат. Мұнда ұйымның барлық цифрлық активтері – іскерлік деректер, жеке мәліметтер, құжаттама және зияткерлік меншік кіреді.



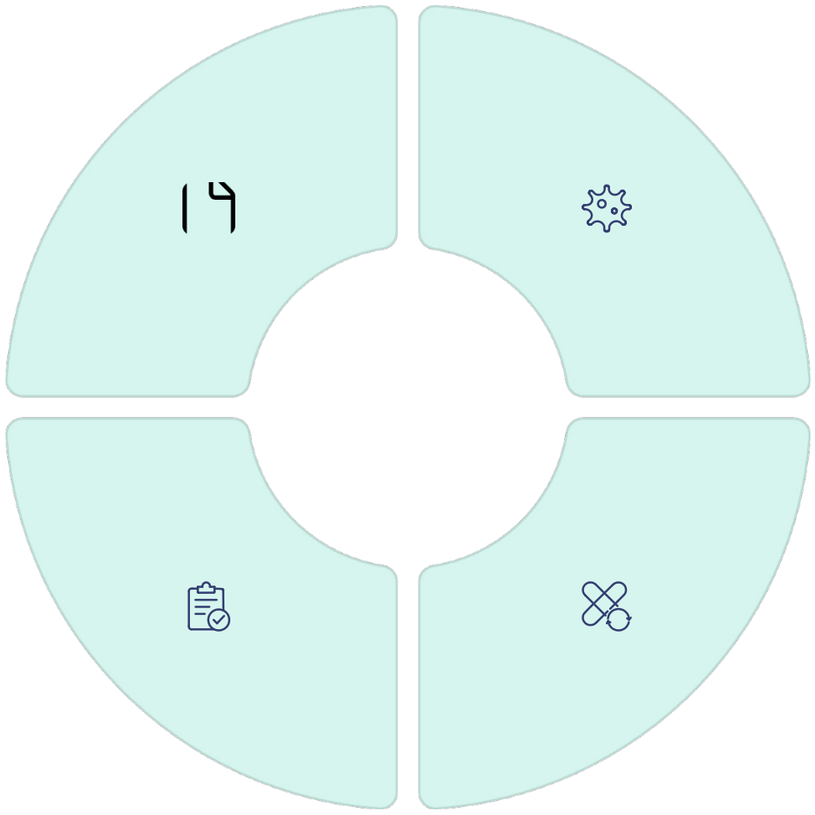
Ақпараттық қорғаудың мақсаты

Үздіксіздік

Жүйенің үздіксіз жұмыс істеуін қамтамасыз ету, бизнес-процестердің тоқтамауы

Сәйкестік

Заңнамалық талаптар мен стандарттарға сәйкестікті сақтау



Қорғаныс

Зиянды бағдарламалар мен кибершабуылдардан сенімді қорғау

Қалпына келтіру

Ақпараттық жүйелердің жедел қалпына келуін қамтамасыз ету

Ақпаратты қорғаудың негізгі қағидалары

Тиімді ақпараттық қауіпсіздік жүйесі бірнеше іргелі қағидаларға негізделген. Бұл қағидалар заманауи қауіптерге қарсы тұрақты қорғанысты қамтамасыз етеді және ұйымның ақпараттық активтерін сенімді түрде сақтайды.





Жүйенің үзіліссіз дамуының принципі

Бастапқы қауіпсіздік

Базалық қорғау құралдарын орнату және конфигурациялау

Үнемі жаңарту

Қорғау жүйесін үнемі жаңартып, дамыту және жаңа қауіптерге бейімдеу

Қауіптерге бейімделу

Жаңа шабуыл әдістеріне жедел жауап беру және қорғаныс тактикасын өзгерту

Жетілдіру

Заманауи технологиялар мен озық тәжірибелерді енгізу

Рұқсатсыз қолжетімділікті тіркеу және бақылау

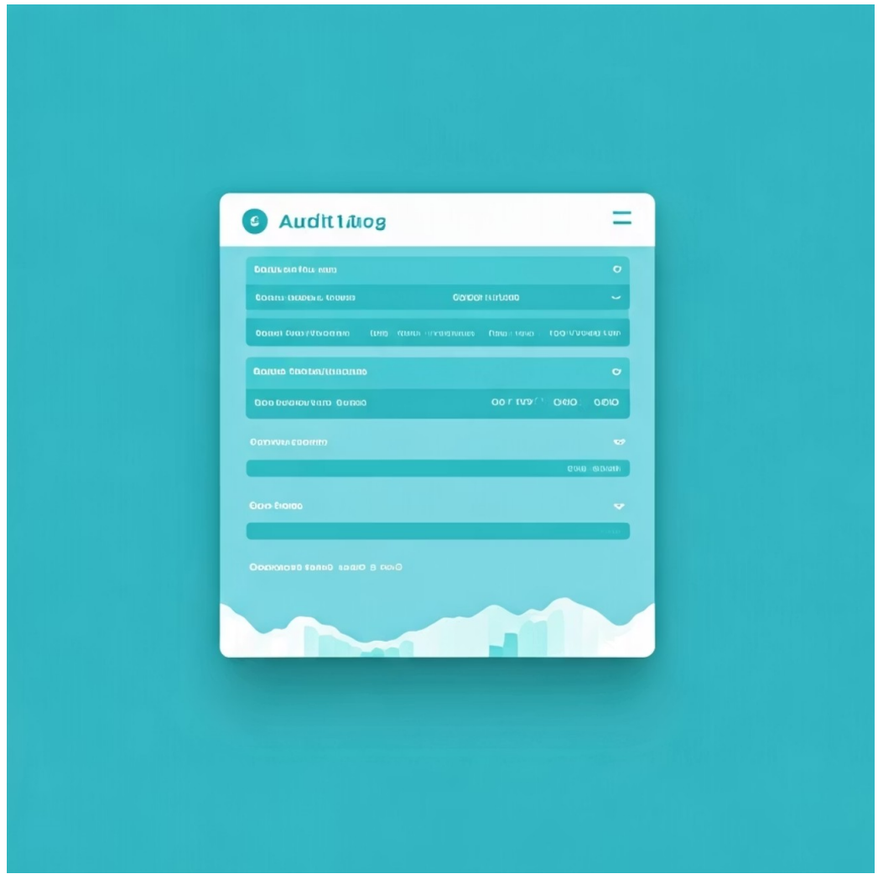
Толық аудит жүйесі

Қолданушылардың барлық әрекеттерін толық жазып отыру және сақтау қауіпсіздіктің маңызды элементі болып табылады. Әрбір қолжетімділік әрекеті, файлдармен жұмыс, жүйелік өзгерістер – барлығы дәл тіркелуі керек.

- Кіру және шығу уақытын тіркеу
- Деректерге қолжетімділік тарихы
- Өзгерістер мен әрекеттер логы
- Күдікті әрекеттерді анықтау

Есеп беру

Қауіпсіздік аудиті мен жүйелі есеп беру инциденттерді талдауға және алдын алуға көмектеседі.



Қорғаныс жүйесіне бақылау қамтамасыз ету

Жұмыс қабілеттілігін тексеру

Қорғау механизмдерінің дұрыс жұмыс істеуін үнемі бақылау. Брандмауэр, антивирус, шифрлау жүйелері мен басқа қауіпсіздік құралдарының өнімділігін тексеру.

Үнемі жетілдіру

Қауіпсіздік құралдарын үнемі жаңарту және жетілдіру. Жаңа версиялар мен патчтарды орнату, конфигурацияны оңтайландыру.

Тиімділікті бағалау

Қорғау шараларының нәтижелілігін өлшеу және талдау. Әлсіз жақтарды анықтау және жақсарту жоспарларын әзірлеу.

Зиянды бағдарламалармен күресудің барлық құралдарын пайдалану

Антивирустық қорғау

Заманауи антивирустық бағдарламалар вирустар, трояндар және басқа да зиянды кодтарды анықтап, жояды. Үнемі жаңартылатын вирустық базалар қауіпсіздікті қамтамасыз етеді.

Брандмауэр жүйелері

Желілік брандмауэрлер рұқсатсыз қолжетімділікті бұғаттайды және трафикті сүзгіден өткізеді. Кіріс және шығыс трафикті бақылау арқылы қауіпсіздікті арттырады.

Шифрлау технологиялары

Деректерді шифрлау құпиялылықты қамтамасыз етеді. SSL/TLS, AES және басқа да криптографиялық протоколдар ақпаратты қорғауда маңызды рөл атқарады.

Қызметкерлерді оқыту

Қауіпсіздік саясатын енгізу және қызметкерлерді үнемі оқыту адам факторын күшейтеді. Фишинг пен әлеуметтік инженерияға қарсы хабардарлық арттырады.

Қауіпсіздік қабаттарының визуалды көрінісі



Қауіпсіздіктің үш негізгі қабаты бір-бірін толықтырады және кешенді қорғанысты қамтамасыз етеді. Физикалық қауіпсіздік серверлер мен жабдықтарды қорғайды, техникалық шаралар киберқауіптерге қарсы тұрады, ал ұйымдастырушылық саясат адам факторын басқарады.

Ақпаратты қорғаудағы адам факторы



Қызметкерлер – бірінші қорғаныс желісі

Қызметкерлердің қауіпсіздік ережелерін сақтауы технологиялардан кем емес маңызды. Көптеген инциденттер адамның қателігінен немесе білмеушілігінен туындайды.

Негізгі шаралар:

- Үнемі оқыту және тренингтер өткізу
- Фишинг пен әлеуметтік инженерияға қарсы хабардарлық
- Күшті парольдер мен аутентификация мәдениеті
- Күдікті әрекеттерді хабарлау жүйесі



Ақпараттық қауіпсіздіктің заманауи қағидалары мен тәжірибелері

Заманауи ақпараттық қауіпсіздік жаңа технологиялар мен озық тәжірибелерді қолдануды талап етеді. Бұл бөлімде біз ақпаратты қорғаудың үш негізгі бағанасын, қазіргі заманғы қауіптерді және олармен күресу әдістерін қарастырамыз.

Құпиялылықты сақтау қағидасы

Жеке деректерді қорғау

Жеке деректерді қорғау және рұқсатсыз жариялаумау қазіргі заманның басты талабы. Қолданушылардың жеке өміріне құрметпен қарау және деректерді қауіпсіз сақтау міндетті.

Екі факторлы аутентификация

Екі факторлы аутентификацияны (2FA) қолдану қауіпсіздік деңгейін айтарлықтай арттырады. SMS-коды, аутентификатор қосымшалары немесе биометрия арқылы қосымша растау қабатын қосу парольдердің ұрлануынан қорғайды.

Деректерді минималдау

Тек қажетті деректерді ғана жинау және сақтау принципі. Артық ақпаратты жинамау қауіптерді азайтады және заңнамалық талаптарға сәйкестікті қамтамасыз етеді.



Қолжетімділікті қамтамасыз ету қағидасы

Үздіксіз жұмыс	Резервтік көшірмелер	Қалпына келтіру
Ақпараттық жүйелердің 24/7 қолжетімді болуын қамтамасыз ету	Деректердің жүйелі резервтік көшірмелерін жасау және сақтау	Апаттан кейін жедел қалпына келтіру жоспарларын әзірлеу

Ақпараттық жүйелер үнемі қолжетімді болуы керек. Бұл резервтік серверлер, қосарланған жабдықтар, жүйелі резервтік көшірмелер және апаттан қалпына келтіру жоспарларын талап етеді. Орташа есеппен, үлкен компаниялар жүйенің бір сағаттық тоқтауынан миллиондаған шығындар шегуі мүмкін.

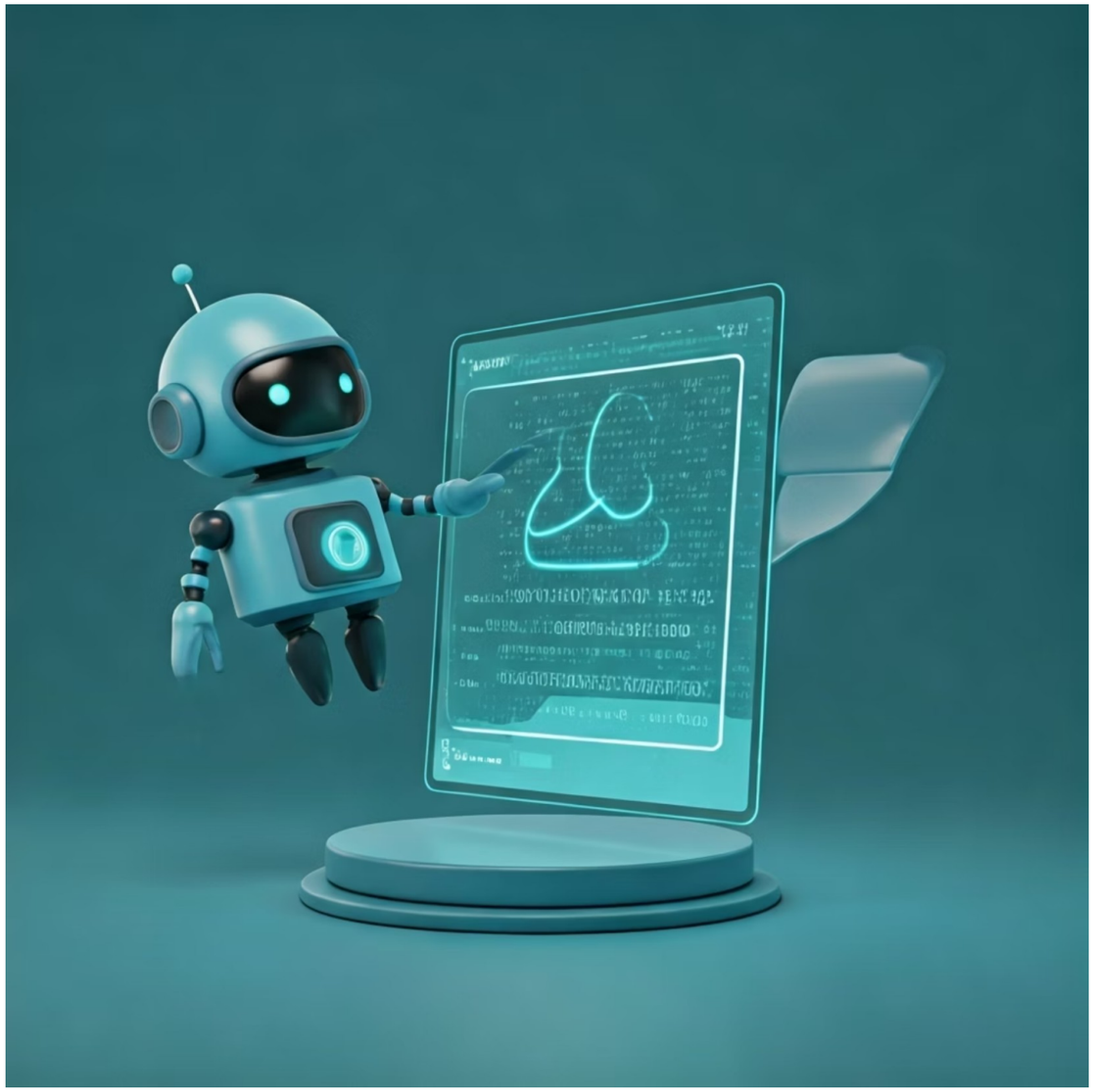
Ақпараттың тұтастығын сақтау

Деректердің өзгермегенін қамтамасыз ету

Мәліметтердің өзгермегенін, толық екенін және сенімді екенін қамтамасыз ету өте маңызды. Тұтастық бұзылған кезде деректер дұрыс емес шешімдер қабылдауға және заңды проблемаларға әкелуі мүмкін.

Негізгі әдістер:

- Хэш-функцияларды қолдану (MD5, SHA-256)
- Цифрлық қолтаңба технологиялары
- Блокчейн технологиясын пайдалану
- Өзгерістерді нұсқалау және аудит



Шифрлау әдістері

Деректерді тасымалдау және сақтау кезінде шифрлау өзгертулерді болдырмайды және тұтастықты қорғайды.

Интернет алаяқтықтан қорғану

Email фишингі

Жалған электрондық хаттар арқылы құпия мәліметтерді ұрлау. Банк немесе танымал қызметтер атынан жіберіледі.

Vishing (дауыстық фишинг)

Телефон арқылы алаяқтық. Қауіпсіздік қызметкері немесе банк өкілі болып көрсетеді.

Pharming

Пайдаланушыларды жалған сайттарға бағыттау. URL мекенжайын мұқият тексеру керек.

Әлеуметтік инженерия

Адамдардың сенімін пайдалану арқылы ақпарат жинау. Әлеуметтік желілерде абайлау керек.

Есте сақтаңыз: Сенімді сайттарды таңдау және күмәнді сілтемелерден сақтану – қауіпсіздіктің алғашқы қадамы. Егер хат немесе сілтеме күдік тудырса, оны ашпай-ақ жойыңыз!

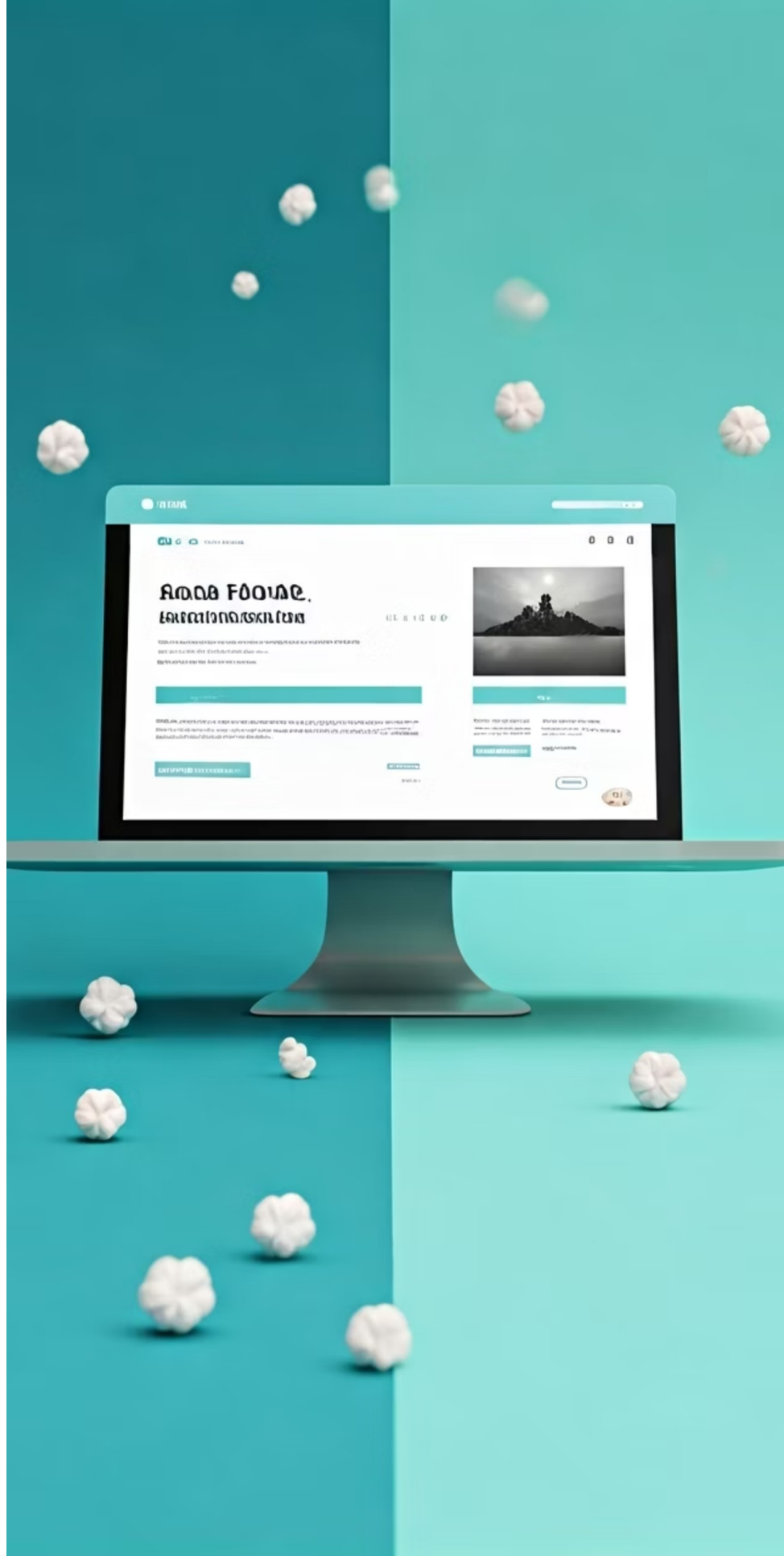
Фишинг шабуылдарының мысалы

Жалған сайттың белгілері

- Күдікті домен атауы (мысалы, amazon-security.com)
- HTTPS қосылымының болмауы
- Грамматикалық қателер және нашар дизайн
- Шұғыл әрекет етуге үндейтін хабарламалар
- Жеке деректерді сұрайтын күдікті формалар

Шынайы сайттың белгілері

- Дұрыс домен атауы
- Қауіпсіз HTTPS қосылымы (құлып белгісі)
- Кәсіби дизайн және мазмұн
- Ресми байланыс ақпараты
- Куәландырылған қауіпсіздік сертификаттары



Ақпараттық қауіпсіздік саясатының маңызы

01

Саясатты әзірлеу

Ұйымдағы қауіпсіздік ережелерін анықтау және құжаттау. Барлық процедуралар мен жауапкершіліктерді нақты белгілеу.

02

Бекіту және енгізу

Басшылықтың бекітуі және барлық қызметкерлерге жеткізу. Саясатты ұйымның барлық деңгейлерінде енгізу.

03

Оқыту бағдарламасы

Қызметкерлерді оқыту және ақпараттандыру. Үнемі тренингтер өткізу және хабардарлықты арттыру.

04

Мониторинг және бағалау

Саясаттың орындалуын бақылау. Тиімділікті өлшеу және қажет болған жағдайда түзетулер енгізу.

05

Жаңарту және жетілдіру

Саясатты жаңа қауіптер мен технологияларға сәйкес үнемі жаңарту. Озық тәжірибелерді енгізу.

Қазақстандағы ақпараттық қауіпсіздік заңнамасы

2018 жыл

ҚР Үкіметінің қаулылары мен негізгі нормативтер қабылданды

2020 жыл

Жеке деректерді қорғау туралы заңға өзгерістер енгізілді

2022 жыл

Кибершабуылдарға қарсы іс-қимылдың жаңа шаралары енгізілді

2024 жыл

Цифрлық дамуға сәйкес заңнама жаңартылды

Қазақстанда мемлекеттік құпияларды қорғау, жеке деректерді өңдеу, киберқауіпсіздік және электрондық құжат айналымы бойынша кешенді заңнамалық база қалыптасқан. Барлық ұйымдар осы талаптарды сақтауы тиіс.

Ақпараттық жүйелерді интеграциялау қағидалары

Электрондық үкімет

Электрондық үкіметтің ақпараттық жүйелерін біріктіру азаматтарға қызметтерді тиімді көрсетуге мүмкіндік береді. Бірақ интеграция кезінде қауіпсіздік талаптарын сақтау өте маңызды.



Қауіпсіздік талаптары

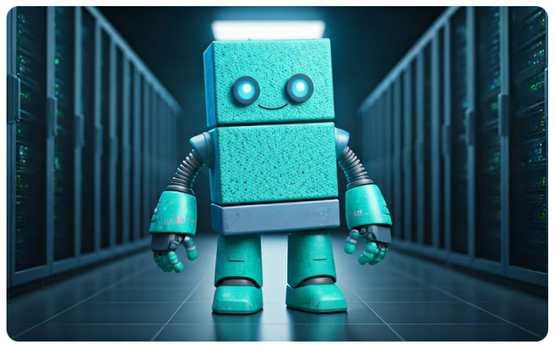
- Жүйелер арасында қауіпсіз деректер алмасу
- Бірыңғай аутентификация және авторизация
- Деректердің шифрлануы және тұтастығы
- Аудит және мониторинг жүйелері
- Апаттан қалпына келтіру механизмдері

Ақпараттық қауіпсіздікті қамтамасыз етудегі технологиялар



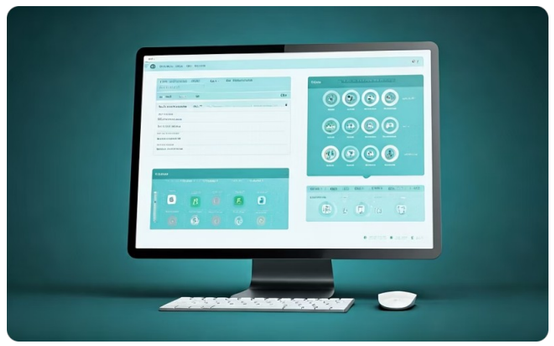
Шифрлау технологиялары

AES, RSA, ECC және басқа криптографиялық алгоритмдер деректерді қорғаудың негізі болып табылады. Симметриялық және асимметриялық шифрлау әдістері.



Брандмауэр жүйелері

Желілік және қосымша деңгейіндегі брандмауэрлер рұқсатсыз трафикті сүзеді. Next-Generation Firewall (NGFW) жаңа буын қауіпсіздік мүмкіндіктерін ұсынады.



IDS/IPS жүйелері

Intrusion Detection/Prevention Systems шабуылдарды анықтап, бұғаттайды. Желілік трафикті талдау және күдікті әрекеттерге жедел жауап беру.



Биометриялық аутентификация

Саусақ ізі, бет тану, көз торы сканерлері қауіпсіздікті арттырады. Заманауи құрылғылардың көпшілігінде біріктірілген.

Қауіпсіздік инциденттерін басқару

Анықтау

Инциденттерді уақтылы анықтау үшін мониторинг жүйелері

Тіркеу

Барлық инциденттерді толық құжаттау және тіркеу

Талдау

Инциденттің себебін және әсерін талдау

Жауап әрекеті

Жедел әрекет ету және зардапты азайту

Қалпына келтіру

Жүйелерді қалпына келтіру және сабақ алу

Тиімді инцидентке жауап беру жоспары шығындарды азайтады және қалпына келтіру уақытын қысқартады. Әрбір ұйым өзінің инцидентке жауап беру командасын дайындауы керек.

Ақпараттық қауіпсіздік аудиті және мониторинг

Қауіпсіздік аудиті

Қауіпсіздік деңгейін жүйелі бағалау кемшіліктерді анықтауға және жою жоспарын әзірлеуге көмектеседі.

1 Техникалық аудит

Жүйелер мен желілерді сканерлеу

2 Әкімшілік аудит

Саясат пен рәсімдерді тексеру

3 Физикалық аудит

Қолжетімділік бақылауын тексеру

Үздіксіз мониторинг

24/7 мониторинг қауіптерді уақтылы анықтауға мүмкіндік береді. SIEM (Security Information and Event Management) жүйелері барлық қауіпсіздік оқиғаларын жинайды және талдайды.



- Нақты уақыт режимінде қауіптерді анықтау
- Аномалияларды автоматты түрде табу
- Инциденттерге жедел жауап беру

Қолданушының қауіпсіздік жауапкершілігі

Күшті парольдер

Кемінде 12 таңба, әріптер, сандар және арнайы белгілер қоспасы. Әр қызмет үшін әртүрлі пароль қолдану. Пароль менеджерін пайдалану.

Құпиялықты сақтау

Құпия ақпаратты жарияламау, әсіресе әлеуметтік желілерде. Жұмыс құжаттарын қоғамдық орындарда қалдырмау.

Бағдарламаларды жаңарту

Операциялық жүйе мен қосымшаларды үнемі жаңартып отыру. Қауіпсіздік патчтарын дереу орнату.

Сақ болу

Күмәнді сілтемелерді ашпау, белгісіз қосымшаларды орнатпау. Фишинг хаттарын тану және есеп беру.



Мобильді құрылғылар мен бұлттық қызметтер қауіпсіздігі

1

Мобильді қауіпсіздік

Қашықтан жұмыс істеу қауіптері артып келеді. Смартфондар мен планшеттерде құпия деректер сақталады, сондықтан оларды қорғау өте маңызды.

- Құрылғыларды құлыптау (PIN, биометрия)
- Жоғалған құрылғыларды қашықтан өшіру мүмкіндігі
- Тек ресми қосымша дүкендерін қолдану
- Қоғамдық Wi-Fi желілерінде VPN пайдалану

2

Бұлттық қауіпсіздік

Бұлттық деректерді қорғау әдістері әртүрлі болуы керек. Деректер провайдер серверлерінде сақталатындықтан, сенімді қызмет таңдау маңызды.

- Екі факторлы аутентификацияны міндетті қосу
- Деректерді шифрлау (тыныштық және тасымалдау кезінде)
- Қолжетімділік құқықтарын дұрыс баптау
- Үнемі резервтік көшірмелер жасау

Мобильді құрылғыда қауіпсіздік шаралары

Биометриялық қауіпсіздік

Саусақ ізі немесе бет тану арқылы құрылғыны қорғау

Антивирус қорғанысы

Мобильді антивирус орнату және үнемі сканерлеу

Жүйені жаңарту

OS және қосымшаларды үнемі жаңартып отыру

Резервтік көшірме

Деректердің автоматты резервтік көшірмесін баптау





Кибершабуылдардың түрлері мен мысалдары

Вирустар

Өздігінен көбейетін зиянды код. Файлдар мен жүйелерді зақымдайды, деректерді жояды немесе өзгертеді.

Трояндар

Пайдалы бағдарлама болып көрсетеді, бірақ жүйеге кіргеннен кейін зиян келтіреді. Деректерді ұрлайды немесе бақылауды береді.

Ransomware

Деректерді шифрлап, оларды қайтару үшін төлем талап етеді. Соңғы жылдары кеңінен таралды.

DDoS шабуылдары

Серверлерді шамадан тыс сұраныстармен басып, қызметті тоқтатады. Ірі компаниялар үшін үлкен қауіп.

2023 жылы WannaCry, Petya және басқа да ірі ransomware шабуылдары әлемдік компанияларға миллиардтаған доллар шығын келтірді. Colonial Pipeline шабуылы АҚШ-та отын жеткізілімін тоқтатты.

Қазақстандағы ақпараттық қауіпсіздік саласындағы оқиғалар

2019 жыл

Мемлекеттік порталдарға бағытталған DDoS шабуылдары тіркелді. Қауіпсіздік шаралары күшейтілді.

2021 жыл

Банк секторына кибершабуылдар жасалды. Қаржы ұйымдарының қауіпсіздік жүйелері жаңартылды.

2022 жыл

Ransomware шабуылдары жеке компанияларға бағытталды. Қауіпсіздік хабардарлығы арттырылды.

2023 жыл

Ұлттық киберқауіпсіздік орталығы құрылды. Инциденттерге жауап беру жүйесі жақсартылды.

Қазақстан соңғы жылдары ақпараттық қауіпсіздікті күшейтуге үлкен назар аударуда. Мемлекеттік және жеке секторда қауіпсіздік инфраструктурасы дамытылуда, халықаралық тәжірибе енгізілуде.

Ақпараттық қауіпсіздік саласындағы халықаралық стандарттар

ISO/IEC 27001

Ақпараттық қауіпсіздікті басқару жүйесінің (ISMS) халықаралық стандарты. Ұйымдарға қауіпсіздік саясатын құрылымдауға және енгізуге көмектеседі.



Негізгі элементтер:

- Қауіптерді бағалау әдістемесі
- Қауіпсіздік бақылау шаралары
- Үздіксіз жетілдіру процесі

NIST Framework

АҚШ-тың Ұлттық стандарттар және технологиялар институты әзірлеген киберқауіпсіздік негіздері. Әлемдік деңгейде танымал.

Бес негізгі функция:

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

Қазақстан да осы стандарттарды бейімдеп, өз нормативтерін әзірлеуде.

Ақпараттық қауіпсіздікті қамтамасыз етудің болашағы

Жасанды интеллект

AI және машиналық оқыту қауіптерді болжау мен анықтауда революция жасауда. Аномалияларды автоматты түрде табу және проактивті қорғану.

Кванттық шифрлау

Кванттық компьютерлер қазіргі шифрлауды бұзуы мүмкін, бірақ кванттық криптография жаңа деңгейдегі қауіпсіздікті ұсынады.

Блокчейн технологиясы

Орталықсыздандырылған деректерді сақтау және транзакциялардың өзгермейтін жазбасы қауіпсіздікті арттырады.

Zero Trust архитектурасы

"Ешкімге сенбе, бәрін тексер" қағидасы болашақтың қауіпсіздік моделі болып табылады.



Ақпараттық қауіпсіздік бойынша үздік тәжірибелер

Үздіксіз оқыту және тренингтер

Қызметкерлерді жыл сайын оқыту жеткіліксіз. Жаңа қауіптер мен әдістер туралы үнемі хабардар етіп отыру керек. Симуляцияланған фишинг тесттері, қауіпсіздік викториналары және практикалық тренингтер тиімділікті арттырады.

Қауіпсіздік мәдениетін қалыптастыру

Қауіпсіздік – бұл тек IT бөлімінің міндеті емес, әрбір қызметкердің жауапкершілігі. Ұйымдық мәдениетке қауіпсіздікті енгізу үшін басшылықтың қолдауы, ашық коммуникация және үнемі еске салу маңызды.

- Қызметкерлерді марапаттау бағдарламалары
- Қауіпсіздік чемпиондарын әрбір бөлімде тағайындау
- Инциденттерді есеп беру үшін жеңіл тәсілдер
- Озық тәжірибелерді бөлісу платформалары



Қорытынды: Ақпаратты қорғау – әркімнің міндеті

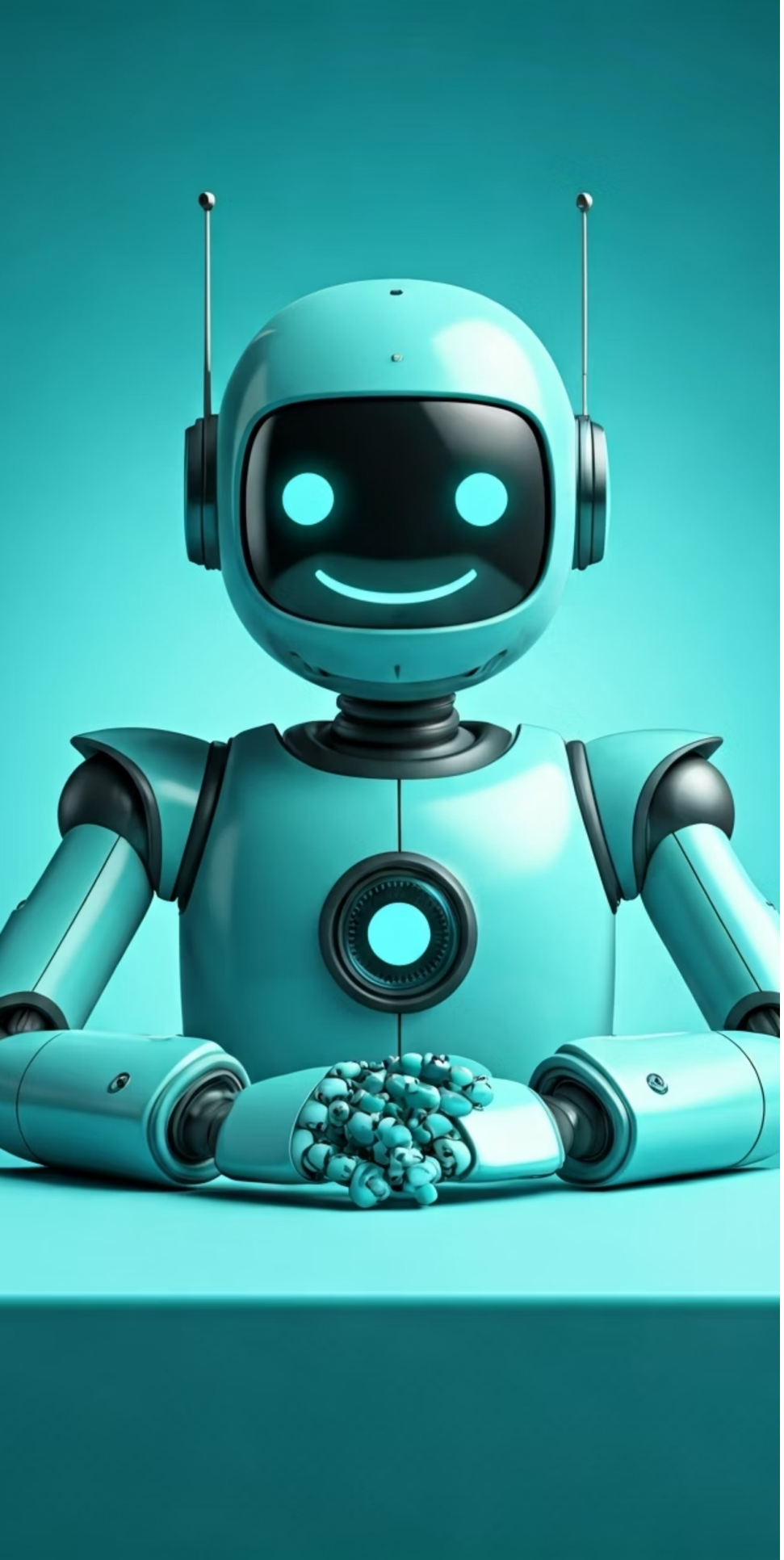


Технология + Адам = Қауіпсіздік

Заманауи қауіпсіздік жүйелері күшті болса да, адам факторы әлі де ең маңызды элемент болып қала береді. Ең жақсы технология да қызметкерлердің абайсыздығынан құлап түсуі мүмкін.

> "Қауіпсіздік – бұл өнім емес, процесс. Бір рет орнатып қоюға болмайды, оны үнемі қолдап отыру керек."

Әрбір қызметкер, әрбір қолданушы ақпараттық қауіпсіздік тізбегінің маңызды буыны. Бірге әрекет етіп, үздіксіз үйреніп, сақ болып жүрсек ғана заманауи киберқауіптерден қорғана аламыз.



Сұрақтар мен жауаптар

Неліктен парольдер әртүрлі болуы керек?

Бір пароль бұзылса, барлық аккаунттар қауіп астында қалмас үшін. Пароль менеджері барлық парольдерді қауіпсіз сақтауға көмектеседі.

Резервтік көшірме қаншалықты жиі жасалуы керек?

Критикалық деректер үшін – күн сайын, қалған деректер үшін – апта сайын. Автоматты резервтік көшірме қатені азайтады.

Фишинг хатты қалай тануға болады?

Күдікті жөнелтуші, грамматикалық қателер, шұғыл әрекет етуге үндейтін тілі, күдікті сілтемелер – бұлар фишингтің негізгі белгілері.

Қоғамдық Wi-Fi қауіпті ме?

Иә, шифрлаусыз қоғамдық желілер қауіпті. VPN қолдану арқылы деректеріңізді қорғаңыз немесе сенімді мобильді интернетті пайдаланыңыз.

Қосымша ресурстар мен оқулықтар

Заңнамалық ресурстар

- ҚР "Жеке деректер және оларды қорғау туралы" заңы
- ҚР "Мемлекеттік құпиялар туралы" заңы
- ҚР "Байланыс туралы" заңы
- Қазақстан Республикасының Үкіметінің қаулылары

Халықаралық ұйымдар

- ISO (International Organization for Standardization)
- NIST (National Institute of Standards and Technology)
- ISACA (Information Systems Audit and Control Association)
- $(ISC)^2$ (International Information System Security Certification Consortium)

Пайдалы ресурстар

- OWASP (Open Web Application Security Project)
- SANS Institute киберқауіпсіздік материалдары
- Kaspersky, Symantec блогтары және есептері
- Coursera, Udemy онлайн курстары