Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Заманауи кибершабуылдар және оларға қарсы әдістер





Кибершабуылдардың өсуі мен маңызы

Технологиялардың дамуымен қатар киберқылмыстар да күрделене түсуде. Қазақстан мен әлем бойынша кибершабуылдардың саны қарқынды өсіп келеді. Бұл тенденция мемлекеттік және жеке секторда жаңа қорғаныс стратегияларын қажет етеді.

Цифрлық трансформация процесінде киберқауіпсіздікке назар аудару өте маңызды. Әрбір жаңа технология жаңа қауіптерді де алып келеді, сондықтан үнемі сақ болу керек.

2024 жыл: Қазақстандағы кибершабуылдардың жаңа деңгейі

Zaimer.kz дерекқорының ұрлануы

1,9 миллион адамның жеке мәліметтері Telegram-да ашық жарияланды. Бұл – қаржы секторындағы ең ірі дерек утечкасы.

Министрлікке шпиондық шабуыл

Мемлекеттік органның серверіне жасалған шабуыл құпия ақпараттың ұрлануына әкелді. Ұлттық қауіпсіздікке тікелей қатер төнді.

Медициналық деректердің жоғалуы

Балалардың медициналық карталары мен жеке мәліметтері заңсыз қолға түсті. Бұл отбасылар үшін үлкен қауіп тудырды.

Осы оқиғалар Қазақстандағы киберқауіпсіздік жүйесінің әлсіз тұстарын ашып берді. Мұндай жағдайлар жүйелі қорғаныс шараларының қажеттігін көрсетеді.

Кибершабуылдар: цифрлық дәуірдің жаңа қауіпі

Әлемдік статистика бойынша 2024 жылы кибершабуылдар саны алдыңғы жылмен салыстырғанда 30 пайызға артты. Бұл өсім әсіресе мемлекеттік органдар мен қаржы институттарына бағытталған шабуылдарға байланысты.

Қазақстан да бұл үрдістен тыс қалмады. Мемлекеттік және жеке секторда шабуылдардың жиілігі артып, олардың салдары да ауырлай түсуде. Экономикалық шығындар миллиардтаған теңгені құрайды.

30%

Шабуылдардың өсуі

2024 жылы әлем бойынша

60%

Мемлекеттік органдар

Шабуылдардың үлесі

Кибершабуылдардың негізгі түрлері

Фишинг және әлеуметтік инженерия

Пайдаланушыларды алдап, құпия ақпаратты алу әдісі. Жалған электрондық хаттар мен сайттар арқылы жүзеге асырылады.

DDoS шабуылдары

Серверлерді үлкен трафик ағынымен шамадан тыс жүктеп, қызметін тоқтату. Бизнеске үлкен зиян келтіреді.

Зиянды бағдарламалар

Вирустар, трояндар, ransomware – жүйелерді бұзатын және деректерді ұрлайтын бағдарламалар.

Ақпарат ұрлау

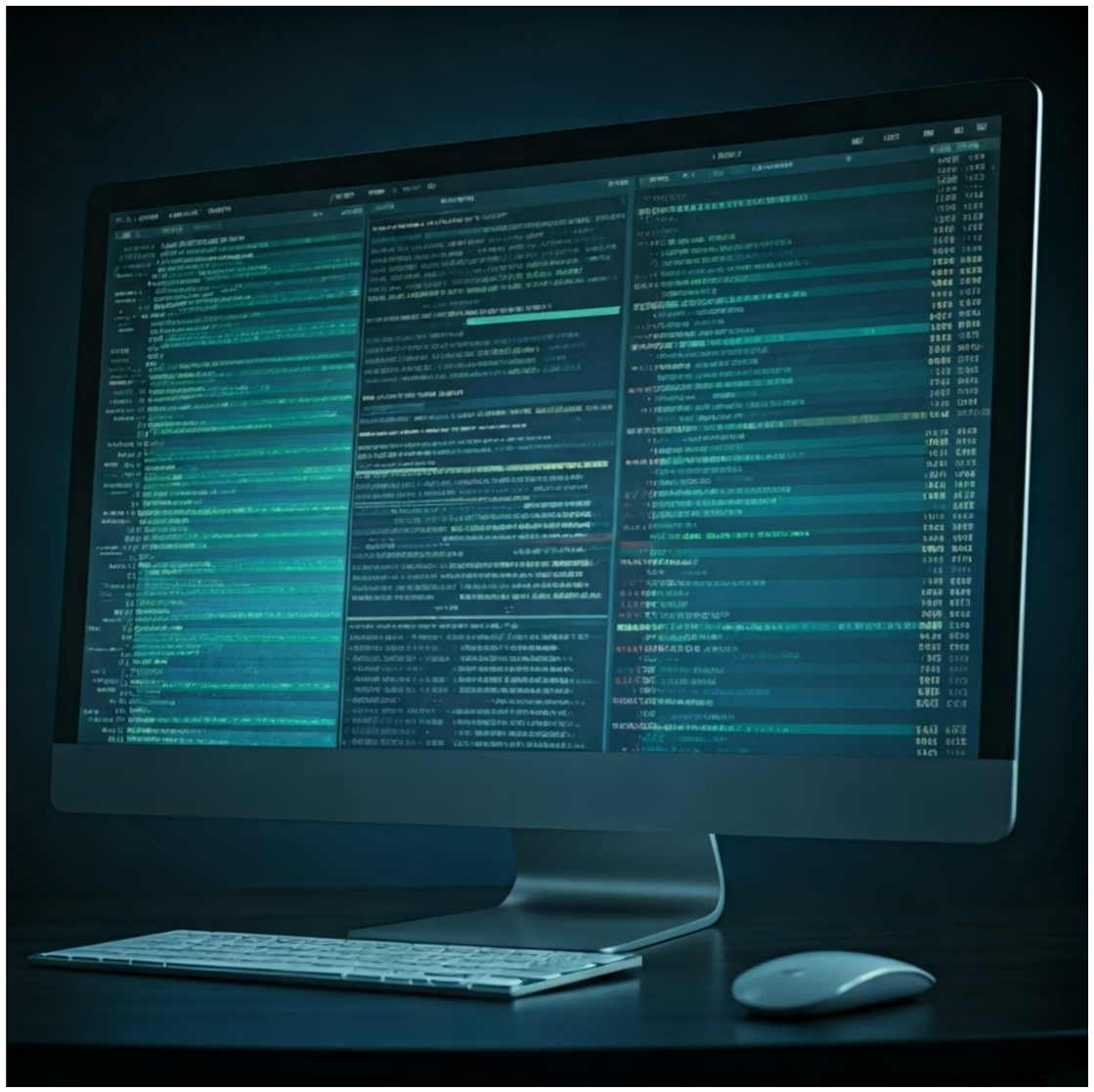
Жеке және корпоративтік деректерді заңсыз жолмен алу, қолдану және сату. Ең қауіпті түрлерінің бірі.

Қазақстандағы нақты оқиғалар

Отандық кибершабуылдар тарихындағы ең ірі инциденттер қазіргі қорғаныс жүйесінің олқылықтарын көрсетеді. Әрбір оқиға маңызды сабақ береді.



Zaimer.kz дерекқорының ірі утечкасы



Масштабы

1 947 022 адамның толық жеке мәліметтері – ЖСН, телефондар, мекенжайлар, қаржылық деректер ашық қолжетімді болды.

Салдары

Мошенниктер осы деректерді пайдаланып жалған займдар ресімдеп, клиенттердің ақшаларын ұрлады. Мыңдаған адам зардап шекті.

Себептері

Ескірген жүйелер, әлсіз шифрлау механизмдері, қауіпсіздік аудитінің жүргізілмеуі және қызметкерлердің төмен дайындығы.

Министрліктің серверіне жасалған шабуыл

2024 жылдың басында белгісіз хакерлер тобы бір министрліктің ішкі желісіне кіруге сәтті болды. Олар әлсіз парольдер мен жаңартылмаған бағдарламалық қамтамасыз етудің орнын пайдаланды.

1-қадам: Кіру

1

Қызметкердің электрондық поштасына фишинг хат жіберіліп, есептік жазбасына қол жеткізілді.

2

2-қадам: Жүйеге ену

Хакерлер ішкі желіге кіріп, басқа қызметкерлердің есептік жазбаларын да бақылауға алды.

3-қадам: Деректерді ұрлау

3

Құпия хат алмасулар, стратегиялық құжаттар және басқа да маңызды ақпарат көшіріліп алынды.

4

Салдары

Ұлттық қауіпсіздікке төнген қатер, сыртқы мемлекеттердің мүддесі, халықаралық беделдің зақымдалуы.

Медициналық ақпараттық жүйедегі деректердің ұрлануы



Қазақстанның бірыңғай медициналық ақпараттық жүйесі 2024 жылы кибершабуылға ұшырады. Нәтижесінде мыңдаған балалардың жеке және медициналық деректері заңсыз қолға түсті.

Ұрланған ақпарат: толық аты-жөні, туған күні, ЖСН, мекенжайы, ата-анасының байланыс деректері, вакцинация тарихы, медициналық диагноздар мен емдеу тарихы.

Бұл деректер әлеуметтік инженерия, таргеттік алаяқтық және тіпті баланы ұрлау қылмыстарында пайдаланылуы мүмкін. Ата-аналар қауіпті хабарламалар алып, үлкен стресс сезінді.

DDoS шабуылы: отандық интернет ресурсына шабуыл

2024 жылдың қаңтар айында Қазақстанның ірі электрондық коммерция платформасы күшті DDoS шабуылына ұшырады. Шабуылшылар әлемнің әр түкпірінен мыңдаған IP-адрестерді пайдаланды.

Ұзақтығы

Шабуыл 6 сағатқа созылды. Сайт толығымен қолжетімсіз болды, клиенттер қызметтерді пайдалана алмады.

Қарқындылығы

Секундына 500 гигабиттен астам трафик серверлерге бағытталды, бұл қалыпты жүктемеден 1000 есе көп.

Шығындар

Тікелей қаржылық залал 50 млн теңгеден асты. Беделдік шығындар одан да жоғары болды.



Кибершабуылдардың технологиялық негіздері

Кибершабуылдарды түсіну үшін олардың техникалық құрылымын білу маңызды. Қорғану стратегиясы қауіптің сипатына негізделуі керек.

Вирустар мен зиянды бағдарламалардың түрлері

1

Макровирустар

Microsoft Office құжаттарына енгізіледі. Макро функцияларын пайдаланып таралады және файлдарды бұзады.

2

Резиденттік вирустар

Компьютердің жедел жадында орналасады. Жүйе қосылған кезде белсенді болып, үнемі әрекет етеді.

3

Резиденттік емес вирустар

Жедел жадта тұрақты орналаспайды. Белгілі бір файл іске қосылған кезде ғана белсенді болады.

4

Полиморфты вирустар

Өздерінің кодын үнемі өзгертіп отырады. Антивирустық бағдарламаларға анықталмауға тырысады.

5

Троян бағдарламалары

Пайдалы бағдарлама ретінде танылады, бірақ зиянды әрекеттер жасайды. Деректерді ұрлайды, жүйені бұзады.

Вирус жұққан компьютердің белгілері

Функционалдық мәселелер

- Бағдарламалардың жұмысының нашарлауы немесе толық тоқтауы
- Жүйенің баяу жүктелуі және өшуі
- Файлдардың өздігінен жоғалуы немесе өзгеруі
- Интернет байланысының төмендеуі
- Процессордың шамадан тыс жүктелуі

Визуалды белгілер

- Экранда түсініксіз хабарламалар пайда болуы
- Бөтен символдар мен графикалық элементтердің шығуы
- Браузерде жарнама терезелерінің көбеюі
- Мәзірлердің өзгеруі немесе жаңа белгісіз бағдарламалардың пайда болуы
- Курсордың өздігінен қозғалуы

Егер осы белгілердің кем дегенде үшеуі байқалса, компьютерді дереу тексеру қажет!

Фишинг: адам психологиясына бағытталған шабуыл

Фишинг – техникалық емес, психологиялық әдіс. Хакерлер адамдардың сенгіштігі мен сақтықсыздығын пайдаланады.

1

1. Жалған хат

Танымал компаниядан немесе мемлекеттік органнан келген сияқты электрондық хат жіберіледі.

2

2. Қорқыту немесе ынталандыру

Хатта есептік жазбаны блоктау қаупі немесе сыйлық алу мүмкіндігі туралы айтылады.

3

3. Жалған сілтеме

Құрбан сілтемені басып, ұқсас сайтқа кіреді және логин мен парольді енгізеді.

4

4. Деректердің ұрлануы

Енгізілген мәліметтер хакерлердің қолына түседі және заңсыз мақсатта пайдаланылады.

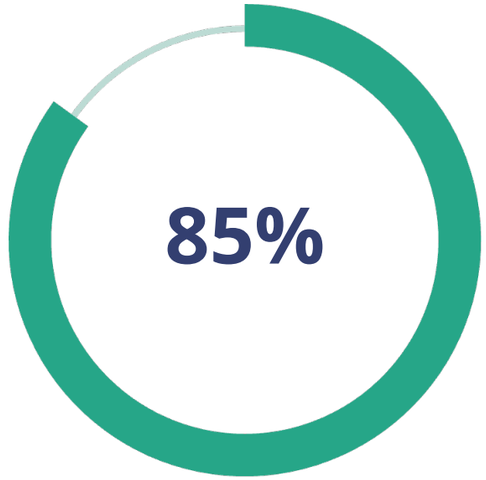
Әлеуметтік желілерде де фишинг кең таралған. Жалған профильдер арқылы достармен байланыс орнатып, құпия ақпарат сұралады.

Ransomware: деректерді кепілге алу

Ransomware – зиянды бағдарламаның ең қауіпті түрі. Ол құрбанның барлық маңызды файлдарын шифрлайды және оларды ашу үшін төлем талап етеді.

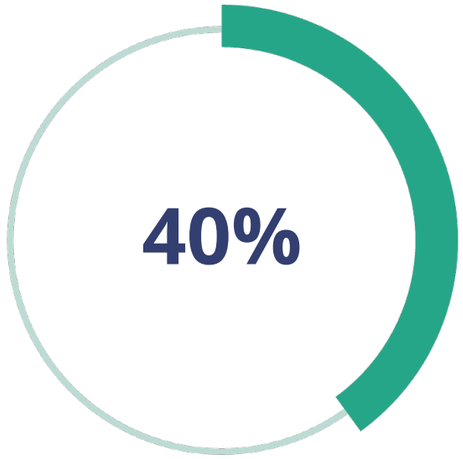
Шабуыл кезеңдері: алдымен вирус жүйеге еніп, деректерді талдайды. Содан кейін ең маңызды файлдарды – құжаттар, фотосуреттер, дерекқорлар – қатты шифрлайды. Экранда төлем талап ететін хабарлама шығады.

2024 жылы Қазақстанда бірнеше ірі ұйым ransomware зардап шекті. Олардың кейбіреуі миллиондаған теңге төлемек болды, бірақ кепілдік жоқ.



Төлеген компаниялар

Деректерін қайтармады



Қайталанған шабуылдар

Бір рет төлеген құрбандарға

Ransomware-ге төлем жасау ұсынылмайды! Бұл жаңа шабуылдарды ынталандырады.

Қорғану әдістері мен технологиялары

Тиімді қорғаныс – бұл технология, адамдар және процестердің үйлесімді жұмысы. Кешенді тәсіл қажет.



Деректерді қорғау: шифрлау және аудит



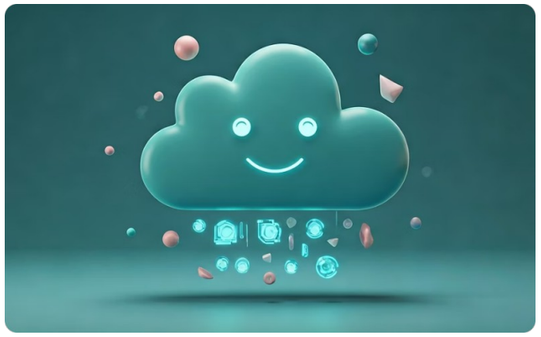
Күшті шифрлау

Дерекқорларды AES-256 немесе одан күшті алгоритммен шифрлау. Барлық құпия ақпаратқа шифрлау қолданылуы керек.



Қауіпсіздік аудиті

Жыл сайын немесе жарты жыл сайын сыртқы мамандарға жүйені тексертіп, олқылықтарды анықтау және жою.



Сақтық көшірмелер

Барлық маңызды деректердің тұрақты сақтық көшірмелерін жасау. Көшірмелерді бөлек серверлерде немесе бұлтта сақтау.

Қызметкерлерді оқыту және кибергигиена

Адам факторы – киберқауіпсіздіктегі ең әлсіз буын. Қызметкерлердің біліміне үлкен инвестиция салу қажет.

01

Қауіптер туралы хабардар ету

Қызметкерлерге фишинг, әлеуметтік инженерия және басқа қауіптер туралы түсіндіру.

02

Тұрақты тренингтер

Ай сайын немесе тоқсан сайын қауіпсіздік тренингтерін өткізу. Практикалық жаттығулар қосу.

03

Симуляция жаттығулары

Жалған фишинг хаттарын жіберіп, қызметкерлердің әрекетін тексеру және кері байланыс беру.

04

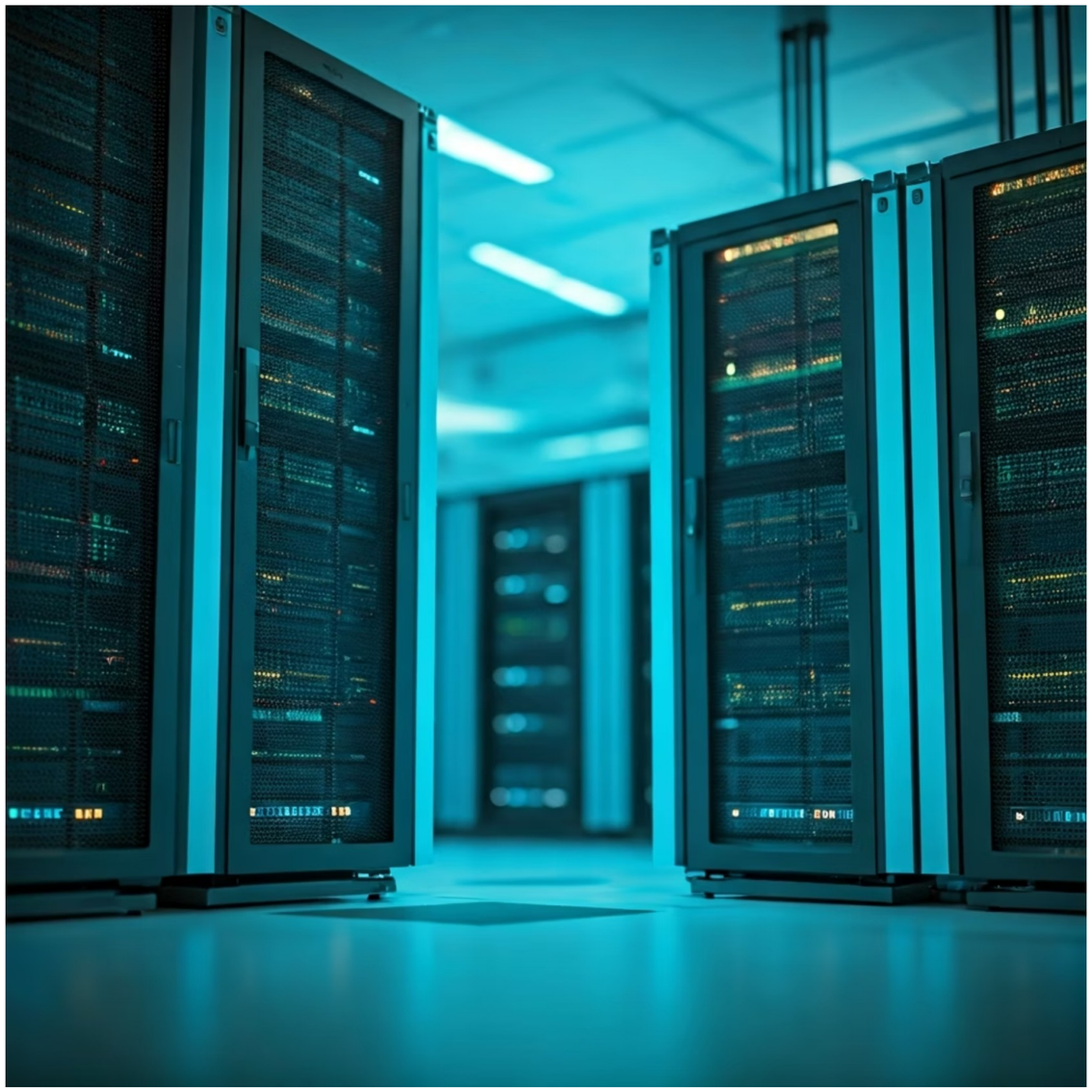
Кибергигиена ережелері

Күшті парольдер, екі факторлы аутентификация, күдікті хабарламаларды тексеру дағдыларын қалыптастыру.

Желілік қорғаныс: DDoS-қа қарсы шешімдер

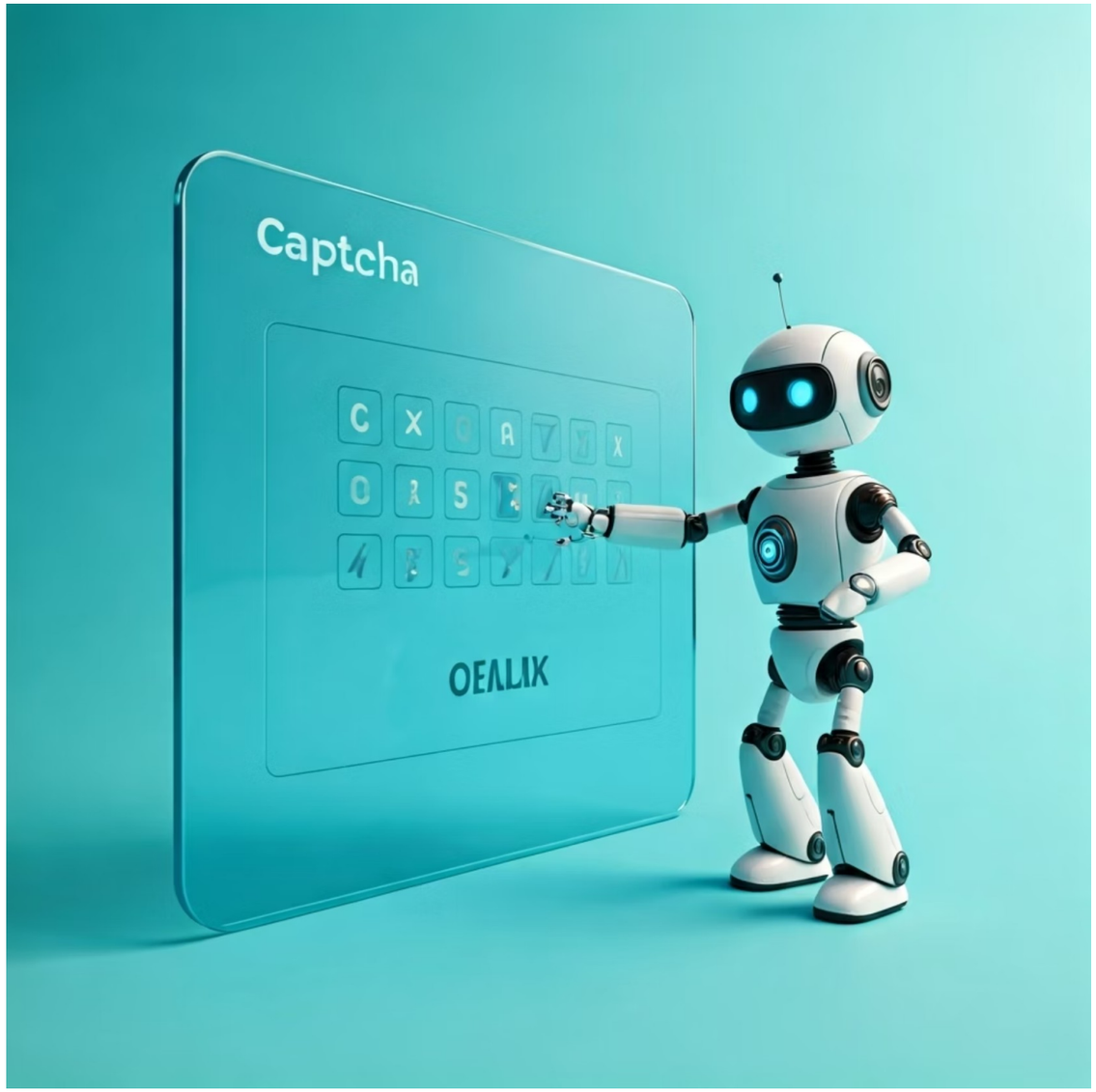
Бұлтты қорғаныс қызметтері

Cloudflare, Akamai сияқты қызметтер DDoS трафигін автоматты түрде сүзіп, заңды пайдаланушыларды өткізеді. Олар үлкен шабуылдарды тоқтата алады.



CAPTCHA және жылдамдық шектеулері

Бот трафигін адам трафигінен ажырату үшін CAPTCHA жүйелерін қолдану. Секундына сұраныстар санын шектеу.



Трафикті үнемі мониторингілеу және аномалияларды дереу анықтау жүйесін құру маңызды. Қазіргі заманғы AI технологиялары шабуылдарды бірнеше секундта анықтай алады.

Антивирус бағдарламаларының рөлі

Kaspersky

Ресейлік әзірлеме, өте күшті қорғаныс. Ransomware мен жаңа қауіптерді жақсы анықтайды.

Norton

Symantec компаниясының өнімі. Интернет қауіпсіздігін қосымша қамтамасыз етеді, VPN бар.

Microsoft Defender

Windows жүйесіне кіріктірілген. Негізгі қорғанысты тегін қамтамасыз етеді, үнемі жаңартылады.

Антивирус бағдарламасын орнату жеткіліксіз. Оны тұрақты жаңартып, толық сканерлеу жүргізу керек. Апта сайын жүйені тексеру – қауіпсіздіктің негізі.

Бір уақытта екі антивирус орнатпаңыз – олар бір-біріне кедергі жасайды!

Қауіпсіздік инциденттеріне жедел әрекет ету

Инцидентті анықтау

Күдікті белсенділік, жүйенің баяулауы, бөтен файлдар – мұның бәрі инцидент белгісі. Дереу назар аудару керек.

Оқшаулау

Зардап шеккен жүйені желіден ажырату. Вирустың таралуын тоқтату үшін барлық байланыстарды үзу.

Талдау және жою

Қауіптің түрін анықтап, антивирустық бағдарламамен немесе қолмен жою. Логтарды сақтау.

Қалпына келтіру

Таза сақтық көшірмелерден жүйені қалпына келтіру. Барлық парольдерді өзгерту.

Есеп және алдын алу

Инцидент туралы толық есеп жасау. Қайталанбауы үшін шаралар қабылдау.



Қазақстанның киберқауіпсіздік инфрақұрылымы

Ұлттық деңгейде киберқауіпсіздікті қамтамасыз ету – мемлекеттің маңызды міндеті. Қазақстанда бұл бағытта белсенді жұмыс жүргізілуде.

Құқықтық база және халықаралық ынтымақтастық

1 Қазақстандық заңнама

«Ақпараттандыру туралы» заң, Қылмыстық кодекстің киберқылмысқа қатысты баптары, деректерді қорғау стандарттары.

2 Халықаралық конвенциялар

Қазақстан киберқылмыспен күрес жөніндегі халықаралық келісімдерге қосылған. Басқа елдермен ақпарат алмасады.

3 Бірлескен операциялар

Интерпол, ТМД елдері және басқа серіктестермен бірлесіп трансұлттық киберқылмыскерлерді ұстау операциялары жүргізіледі.

Құқықтық база үнемі жаңартылып отырады. Жаңа қауіптер пайда болған сайын заңдарға түзетулер енгізіледі.



Жаһандық тәжірибе және сабақтар

Әлемдік тәжірибені зерделеу Қазақстанға өз қорғаныс жүйесін жетілдіруге көмектеседі. Басқа елдердің қателерінен және табыстарынан үйренеміз.

2024 жылғы әлемдік ірі кибершабуылдар

АҚШ: денсаулық сақтау жүйесі

Миллиондаған науқастың медициналық деректері ұрланды. Ransomware шабуылы ауруханаңың жұмысын бірнеше күнге тоқтатты.

1

Азия: мемлекеттік органдар

Оңтүстік-Шығыс Азия елдерінің бірнешеуінде мемлекеттік ақпараттық жүйелерге шабуыл жасалды. Дипломатиялық қатынастар шиеленісті.

2

Еуропа: банк секторы

Бірнеше еуропалық банк DDoS және фишинг шабуылдарының құрбаны болды. Клиенттер миллиондаған евро жоғалтты.

3

Бұл шабуылдар жаңа әдістер мен құралдарды қолданды: AI негізіндегі фишинг, кванттық криптографияны бұзуға әрекеттер, IoT құрылғылары арқылы шабуылдар.



Қазақстанға арналған сабақтар

Қауіпсіздік мәдениетін қалыптастыру

Батыс елдерінде киберқауіпсіздік – бұл мәдениеттің бір бөлігі. Балалар мектепте, қызметкерлер жұмыста, азаматтар күнделікті өмірде қауіпсіздік ережелерін сақтайды.

Қазақстанда да осындай мәдениетті қалыптастыру керек. Бұл үшін ұзақ мерзімді білім беру бағдарламалары, қоғамдық науқандар және мемлекеттік қолдау қажет.

Технологиялық жаңартулар

Ескірген жүйелер – қауіптің негізгі көзі. Қазақстандық ұйымдар мен мекемелердің көпшілігі әлі де 10-15 жыл бұрынғы технологияларды пайдаланады.

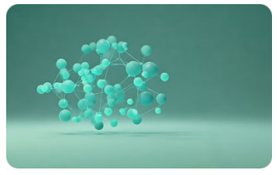
Жаңа жабдық, бағдарлама және қорғаныс жүйелеріне инвестиция салу – маңызды басымдық. Бұл қымбат, бірақ кибершабуылдардың зардаптарынан әлдеқайда арзан.



Болашаққа көзқарас

Киберқауіпсіздік өрісі тез дамуда. Жасанды интеллект, кванттық есептеу, блокчейн – мұның бәрі қорғаныстың жетілдіруге және жаңа қауіптер тудыруға әкеледі.

Киберқауіпсіздіктің дамуы: жасанды интеллект және автоматтандыру



AI негізіндегі қорғаныс

Жасанды интеллект аномалияларды адамнан мыңдаған есе жылдам анықтайды. Ол үлгілерді үйреніп, белгісіз қауіптерді болжай алады.



Автоматты жауап беру

Қауіп анықталған сәтте жүйе өзі шабуылды тоқтатады, жүйені оқшаулайды және қалпына келтіруді бастайды – адамның араласуынсыз.



Болжамды талдау

AI деректерді талдап, болашақ шабуылдарды болжайды. Бұл қауіпті алдын ала жоюға мүмкіндік береді.

Бірақ хакерлер де AI пайдаланады. Автоматтандырылған фишинг, AI-дан жасалған deepfake видеолар, интеллектуалды зиянды бағдарламалар – жаңа дәуірдің қауіптері.

Кибершабуылдарға қарсы инновациялық шешімдер

Биометриялық аутентификация	Блокчейн технологиясы	Кванттық криптография
Саусақ ізі, бет тану, радужка сканерлеуі – парольдерді толығымен алмастыруы мүмкін. Қауіпсіздік деңгейі әлдеқайда жоғары.	Деректерді орталықсыз және өзгермейтін түрде сақтау. Деректерді бұзу немесе өзгерту мүмкін емес.	Кванттық механиканың заңдарына негізделген шифрлау. Қазіргі технологиямен бұзу мүмкін емес.

Қазақстанда да осы технологияларды енгізу қажет. Бірақ бұл үшін мамандарды даярлау, ғылыми зерттеулерді қолдау және халықаралық ынтымақтастық керек.

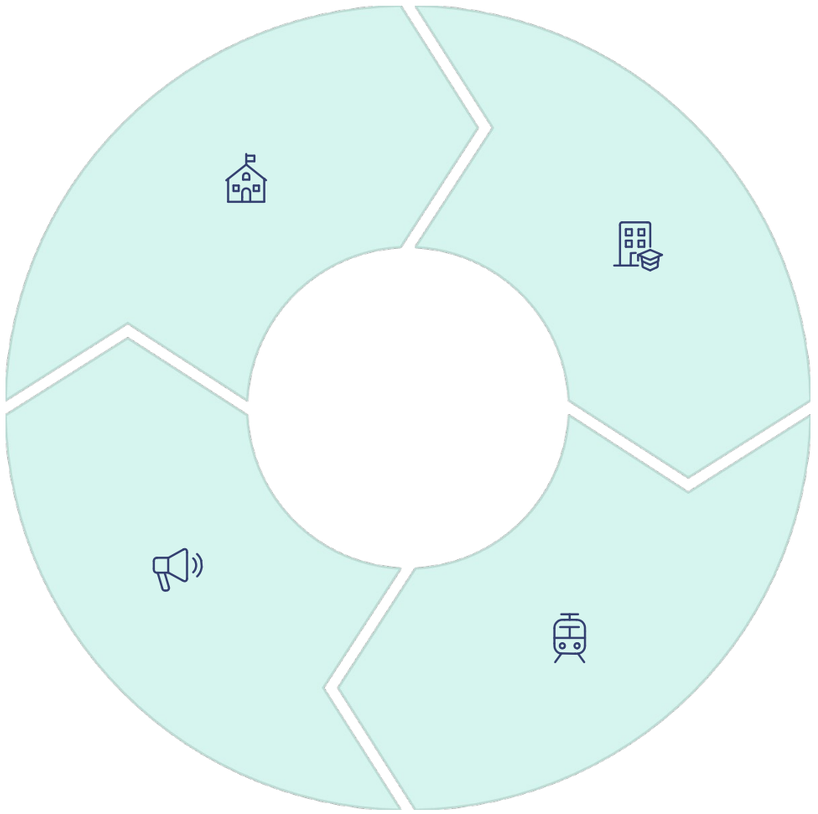
Қоғамдық сананы арттыру және білім беру

Мектептерде оқыту

Балаларды кішкентай кезінен киберқауіпсіздік ережелеріне үйрету. Информатика сабақтарына кибергигиена тақырыптарын енгізу.

Қоғамдық науқандар

БАҚ, әлеуметтік желілер, билбордтар арқылы қауіпсіздік туралы ақпарат тарату. Халықтың сауаттылығын арттыру.



Жоғары білім

Киберқауіпсіздік мамандығын дамыту. Бакалавриат пен магистратурада арнайы бағдарламалар ашу.

Кәсіби оқыту

Қызметкерлер үшін тұрақты тренингтер мен сертификаттау. Халықаралық стандарттарға сәйкес курстар.



Қорытынды

Заманауи кибершабуылдар – бұл жай технологиялық мәселе ғана емес. Бұл – ұлттық қауіпсіздіктің, экономиканың, әрбір азаматтың құқықтарын қорғаудың мәселесі.

Кибершабуылдар – қазіргі заманның шынайы қатері

Қазақстанда және бүкіл әлемде киберқауіптер тоқтаусыз өсіп келеді. 2024 жылы біз осыған тағы бір рет көз жеткіздік. Ірі дерекқорлардың ұрлануы, мемлекеттік органдарға шабуылдар, балалардың деректерінің таратылуы – мұның бәрі біздің қорғанысымыздың жеткіліксіз екенін көрсетеді.

Бірақ біз дайын болуымыз керек. Қорғану – бұл тек технология емес. Бұл білім, мәдениет және халықаралық ынтымақтастық. Әрбір азамат, әрбір ұйым, мемлекет – барлығымыз осы күреске үлесімізді қосуымыз керек.

30%

Өсім 2024

Әлемдік деңгейде

2/3

Адам факторы

Шабуылдардың себебі

85%

Алдын алуға болатын

Тиісті қорғанумен



Бірге қауіпсіз цифрлық болашаққа!

> Киберқауіпсіздік – әркімнің жауапкершілігі. Күшті пароль қою, күдікті хаттарды тексеру, жүйелерді жаңарту – қарапайым әрекеттер үлкен айырмашылық жасайды.

Қауіпсіздік – біздің ортақ міндетіміз. Тек біріккен жағдайда ғана біз цифрлық дәуірдің қауіптерінен қорғана аламыз. Білім, технология, заңдар және ынтымақтастық – бұл біздің қаруымыз.

Болашақ біздің қолымызда. Қауіпсіз цифрлық Қазақстанды бірге құрайық!