ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ЦИФРЛЫҚ ДАМУ,ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

КИБЕРҚАУІПСІЗДІКТІ САҚТАУ НЕГЕ МАҢЫЗДЫ?

2020 жылдың қыркүйек айында жүргізілген социологиялық зерттеулер негізінде дайындалған

«ХАЛЫҚТЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІ ТУРАЛЫ ХАБАРДАР БОЛУЫ» (КИБЕРҚАУІПСІЗДІК)

Ақпараттық қауіпсіздікті қамтамасыз ету және дербес деректерді қорғау уәкілетті орган Ақпараттық қауіпсіздік комитетінің жұмысының маңызды құрамдас бөлігі болып табылады.

Жаһандық киберқауіпсіздік индексінде (GCI) Қазақстан өз позициясын қарқынды түрде жақсартуда. Мысалы, соңғы есепте Қазақстан бірден 42 тармаққа — 40-орынға көтерілді. Бұл мемлекеттік органдар, үкіметтік емес ұйымдар мен бизнестің бірлескен жұмысының нәтижесі.

БІРАЗ МАҢЫЗДЫ АҚПАРАТ

Ақпараттық қауіпсіздік біздің өміріміздің ажырамас бөлігі болып табылады. Ақпараттық қауіпсіздік дегеніміз, әдетте, үш маңызды қағиданы сақтауды білдіреді:

Құпиялылық

Қолжетімділік

Тұтастық

Бұл не?

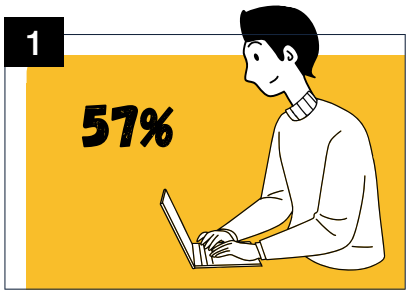
- Ақпаратқа тек оған құқығы бар адам ғана қол жеткізе алады.
- Ақпарат қажет болған кез келген уақытта қол жетімді болуы керек.
- Ақпарат сенімді болуы керек.

Принциптің біреуін бұзу басқалардың бұзылуына әкелуі мүмкін.

ДЕРЕКТЕР ҚАУІПСІЗДІГІНІҢ ҚАТЕРЛЕРІ

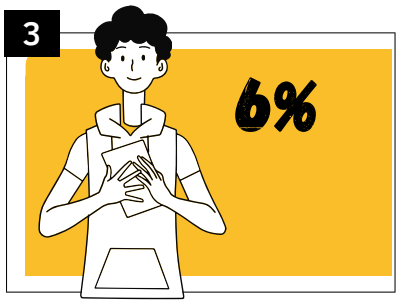
Ақпараттандыру саласындағы ақпараттық қауіпсіздік (киберқауіпсіздік) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық – коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жағдайы.

СОЦИОЛОГИЯЛЫҚ САУАЛНАМА НӘТИЖЕЛЕРІ:



Респонденттердің көпшілігі интернет арқылы ақпарат алады

Интернет және телевизор арқылы



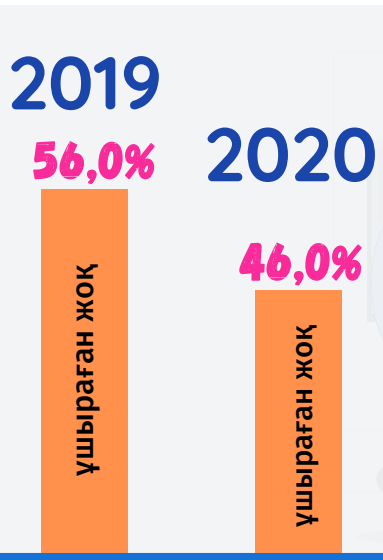
Мобильді қосымшалар арқылы

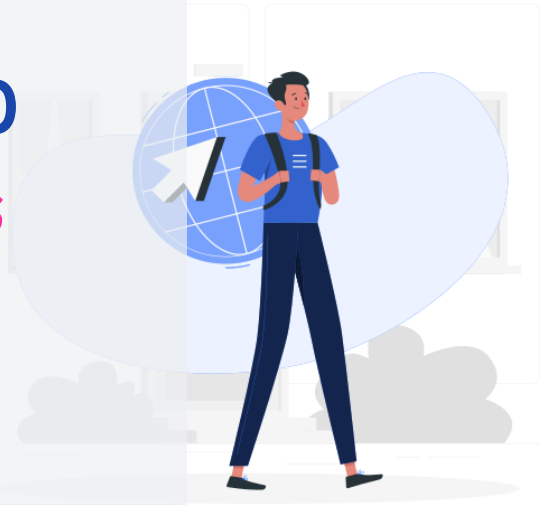
СІЗ СОҢҒЫ ЖЫЛЫ КИБЕРШАБУЫЛДАРДЫҢ ҚАНДАЙ ТҮРЛЕРІНЕ ҰШЫРАДЫҢЫЗ?

Сауалнамаға сәйкес, соңғы жылы ел тұрғындары кибершабуылдардың келесі түрлеріне ұшырады:

	2020	2019	2018
Компьютерлік вирустар шабуылы	32.1%	8.1%	8.7%
Зиянды спам	13.4%	12.1%	11%
Әлеуметтік желілердегі аккаунттарды бұзу	3.9%	6.7%	7.4%

2020 жылғы сауалнама нәтижелері бойынша респонденттердің 46% - ы кибершабуылдарға ұшырамағандарын айтты. Өткен жылмен салыстырғанда бұл көрсеткіш біршама төмен. Сонымен, 2019 жылы респонденттердің 56% - ы оларда кибершабуыл оқиғалары болмағандығын атап өтті.

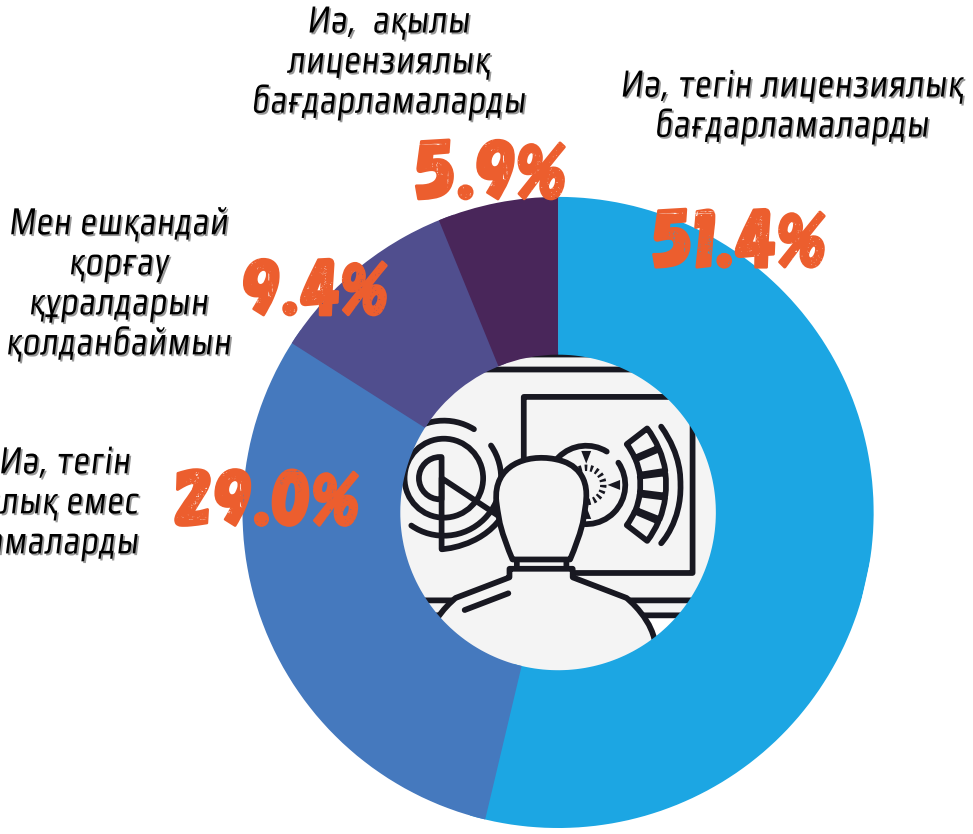




СІЗ КИБЕРШАБУЫЛҒА ҰШЫРАДЫҢЫЗ БА?

СІЗ КОМПЬЮТЕРЛІК ШАБУЫЛДАРДАН ҚОРҒАНАТЫН ҚҰРАЛДАРДЫ ПАЙДАЛАНАСЫЗ БА?

2019 ЖЫЛҒЫ МӘЛІМЕТТЕР БОЙЫНША, ЛИЦЕНЗИЯЛЫҚ ӨНІМДІ ТЕК 36% ПАЙДАЛАНДЫ

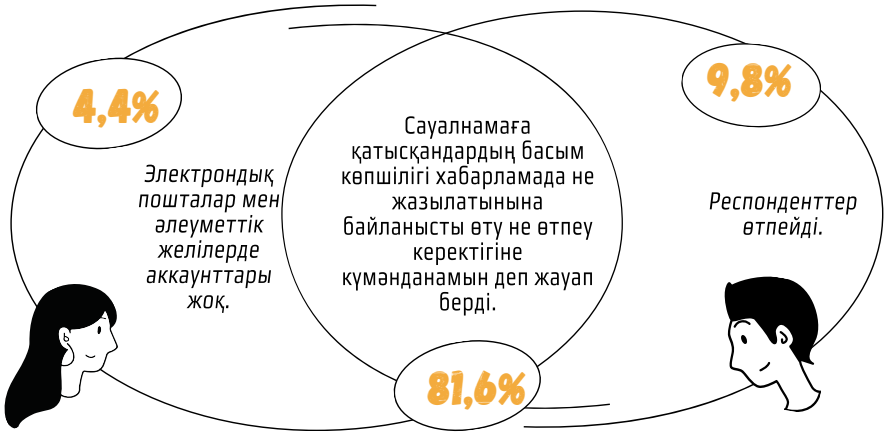


Ақпараттық қауіпсіздік деректерді, оның ішінде дербес деректерді қорғауды қамтамасыз ету негізгі міндеттердің бірі болып табылады және респонденттердің пікірінше, оны арттыру шаралар қабылдауды талап етеді.

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ АЛДЫН-АЛУ ШАРАЛАРЫ

«СІЗ ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ЖІБЕРІЛГЕН БЕЙТАНЫС СІЛТЕМЕЛЕР АРҚЫЛЫ ӨТЕСІЗ БЕ?»

Әлеуметтік сауалнама нәтижелері:



РЕСПОНДЕНТТЕР ӨЗДЕРІ РҰҚСАТ БЕРГЕН САЙТТАРДА АҚПАРАТТЫ ТЕКСЕРЕ МЕ?

63,3% – Сайтты тексеру кейде ресурс күмән тудырған кезде жүзеге асырылады.

Респонденттердің осынша пайызы сайттарда ақпаратты сирек тексереді. – **27,3%**

5,3% – Респонденттердің осынша пайызы сайттарда ақпаратты мүлдем тексермейді.

ҰСЫНЫМДАР

Ақпараттық қауіпсіздіктің алдын алу шаралары (ұсынымдар)

Бағдарламалық қамтылым – операциялық жүйелер, қосымшалар бағдарламалары, антивирустық және басқа бағдарламалар үшін жаңартуларды үнемі орнатыңыз.

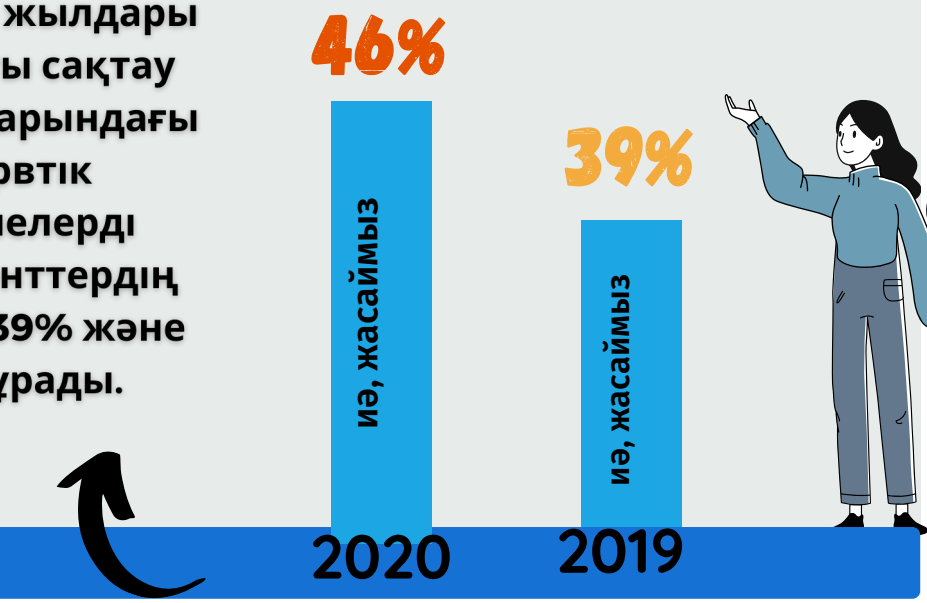
Қол жетімді болған кезде бағдарламалық қамтылымды автоматты түрде жаңарту мүмкіндіктерін қосыңыз.

Пайдаланбаған немесе әзірлеуші жаңартуларын алмаған кезде бағдарламалық қамтылымды жойыңыз.

Лицензиясы жоқ бағдарламалық қамтылымды орнатудан немесе тексерілмеген көздерден бағдарламалық қамтылымды алудан аулақ болыңыз.

Басқа құрылғыларда Сіз үшін маңызды деректерге көшірмені үнемі жасаңыз.

2019-2020 жылдары ақпаратты сақтау құрылғыларындағы резервтік көшірмелерді респонденттердің тиісінше 39% және 46% құрады.



СІЗ МАҢЫЗДЫ ДЕРЕКТЕР БОЙЫНША САҚТЫҚ КӨШІРМЕ ЖАСАЙСЫЗ БА?

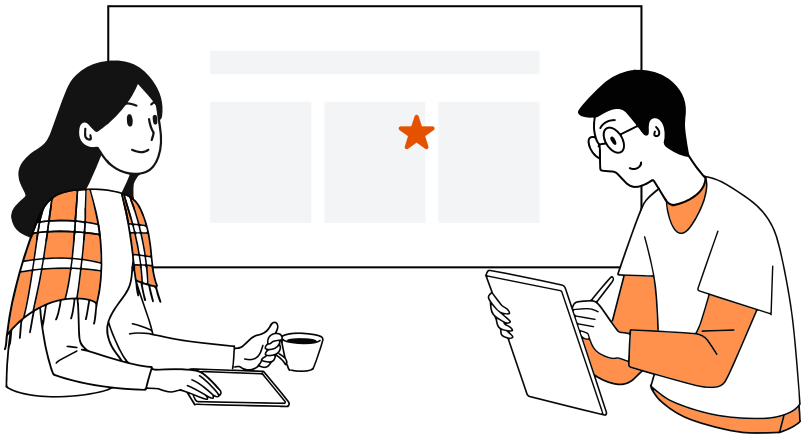
Сақтық көшірме жасау-бұл ақпаратты сақтау құрылғыларында деректердің көшірмесін жасау процедурасын білдіретін деректерді сақтаудың сенімді әдісі.

Респонденттердің пікірінше, киберқауіпсіздікті бұзуға күдік туындаған кездегі негізгі шара:

- IT-маманға жүгіну — 73,5%
- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға жүгіну — 4,8%
- кибершабуылдың салдарын өз бетінше жою — 1,6%
- ешқайда жүгінбеу — 1,5%

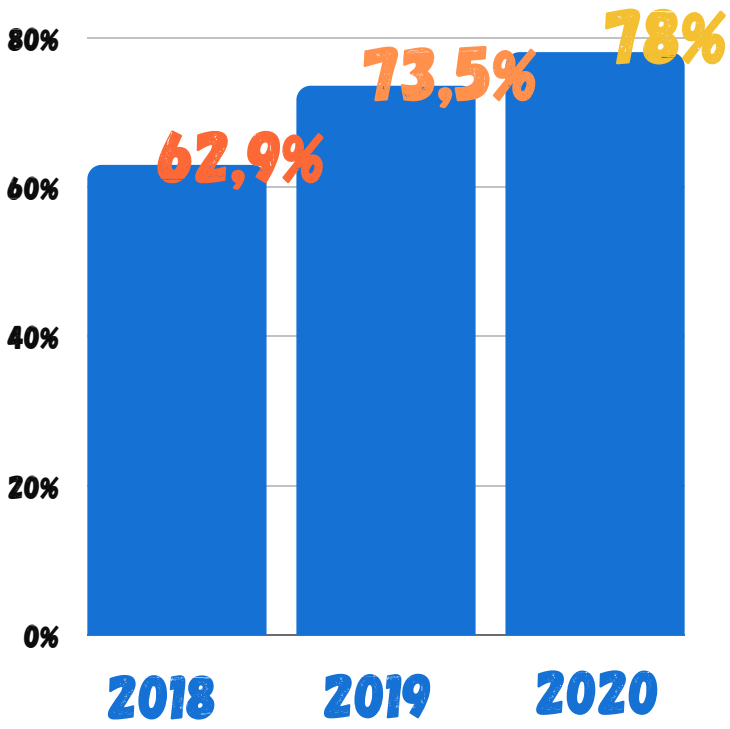
Кез келген стандартты емес немесе ақпараттық қауіпсіздікті бұзуға күдік болған жағдайда дереу жауапты мамандарға жүгініңіз;
-сондай-ақ мына телефон нөмірі бойынша компьютерлік инциденттерге әрекет ету қызметіне хабарласуға болады:
1400 немесе
+7 (7172) 55-99-97,
эл.пошта: info@kz-cert.kz

Әдістемелік ұсынымдар білім беру ұйымдарының іс-шаралар жүйесін іске асыруы, қатысушыларды интернет кеңістікте қауіпсіз жұмыс жасау ережелеріне оқытуға бағыттауды қамтамасыз ету мақсатында әзірленді



САУАЛНАМА:

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІ ТУРАЛЫ ХАЛЫҚТЫҢ ХАБАРДАР БОЛУЫ



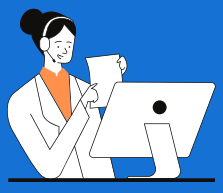
Осы хабардарлық көрсеткіші 2018 және 2019 жылдары тиісінше 62,9%-ды және 73,5%-ды құрады. Бұл 2020 жылы 2018 және 2019 жылдармен салыстырғанда халықтың хабардарлығы сәйкесінше 15%-ға және 4,5% - ға артқанын көрсетеді.

26,3% **01** Лицензиялық вирусқа қарсы бағдарламалық қамтылымды пайдалану

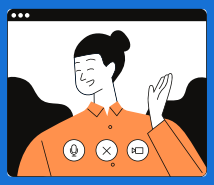
22,7% **02** Барлық сайттарда бірдей құпия сөз қолданбау

12,8% **03** Құпия сөзді өзгертіп отыру

9,8% **04** Құпия сөздерді ашпау



9,7% **05** Лицензиясыз бағдарламаларды қолданбау



КИБЕРҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫМДАР

01 ПАРОЛЬДІК САЯСАТ

- ✗ Жұмыс үстелінде құпия сөздерді электронды түрде сақтамаңыз.
- ✓ Өндірістік қажеттілік жағдайында парольдің мәнін ашуға рұқсат етіледі.
- ✓ Парольдер кемінде 8 таңбадан тұруы керек және тоқсан сайын жаңартылуы қажет.

02 ПОШТА

- ✗ Бейтаныс адамдардан электрондық хаттар мен күдікті тіркемелерді ашпаңыз.
- ✓ Электрондық пошта арқылы кез-келген күдікті анықтау мақсатында адресаттан сұрауды растау үшін балама байланыс арнасын (мысалы, телефон) пайдалану керек.
- ✓ Жіберуші мен алушының мекенжайын әрдайым тексеріп отыру қажет.

03 ВИРУСҚА ҚАРСЫ БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУ

- ✓ Лицензияланған вирусқа қарсы бағдарламалық қамтылым етуді пайдалану қажет.
- ✓ Компьютерге қосылған кезде кез-келген тасымалдаушыны вирустардан тексеруді ұмытпаңыз.
- ✓ Автоматты тексеруді орнату арқылы кіріс электрондық поштадағы барлық файлдарды вирустарға тексеріңіз.

04 ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

- ✗ Үшінші тұлғаларға IP-мекенжайларын және логин мен парольдің үйлесімін хабарлауға тыйым салынады.
- ✗ Бағдарламалық қамтылымды өз бетінше орнатуға тыйым салынады.

05 ИНТЕРНЕТ ЖӘНЕ ӘЛЕУМЕТТІК ЖЕЛІ

- ✗ Белгісіз жіберушіден сілтемелер бойынша өтуге жол берілмейді.
- ✗ Террористік, экстремистік, конституцияға қарсы және өзге де деструктивті бағыттағы материалдары бар веб-сайттарға кіруге тыйым салынады.
- ✗ Мағынасын түсінбейтін сайттарға кірген кезде келісімдер қабылдауға тыйым салынады.
- ✗ Жергілікті желіге кіру паролін басқа бағдарламалар мен сайттарда пайдалануға тыйым салынады.
- ✓ Cookies-ті (көлемі шағын файлдар) пайдаланумен байланысты қатерлерді болдырмау үшін сақталған cookies-ті кезең-кезеңімен талдау жүргізу ұсынылады.

МЕМЛЕКЕТТІК ҚЫЗМЕТШІЛЕР ҮШІН КИБЕРҚАУІПСІЗДІК БОЙЫНША ҚОСЫМША ҰСЫНЫМДАР

- ✗ МО ішкі желілерін Интернетке қосуға тыйым салынады.
- ✓ Интернет желісіне қосылуды Интернетке қол жеткізудің бірыңғай шлюзі арқылы ғана жүргізу қажет.
- ✗ Интернет желісінің ресурстарымен және электрондық поштамен жұмыс істеу кезінде қызметкерге қызметтік қажеттілік бойынша не өзге де жолмен белгілі болған мемлекеттік, қызметтік және коммерциялық ақпаратты жария етуге тыйым салынады.
- ✓ МО-ның, ЖАО-ның қызметшілері қызметтік міндеттерін орындау кезінде қызметтік хат алмасуды электрондық нысанда жүзеге асыру кезінде ведомстволық электрондық поштаны ғана пайдаланады.
- ✗ Компьютерлер мен Интернет-желілерді қараусыз қалдыруға тыйым салынады. Егер сіз жұмыс орнын қалдырсаңыз, компьютерді міндетті түрде бұғаттауыңыз керек (- Windows+L пернелер тіркесімі).
- ✗ МО БКО-ға, МО-ның локальдық желісіне сымсыз желілер, сымсыз қолжетімділік, модемдер, радиомодемдер, ұялы байланыс операторлары желілерінің модемдері және басқа да сымсыз желілік құрылғылар арқылы қосылуға тыйым салынады.

ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ БОЙЫНША ҰСЫНЫМДАР:

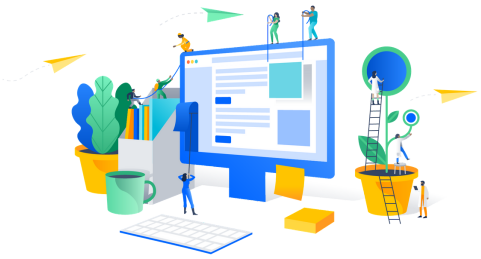
Келісімге қол қою кезінде келесіге назар аударыңыз:

- оператор жинайтын дербес деректердің тізбесі;
- дербес деректерді жинау мақсаттары мен мерзімдері;
- жиналған дербес деректерді үшінші тұлғаларға беру мүмкіндігі;
- деректерді трансшекаралық беру.

Дербес деректерді қайда болса да ұсынған кезде жеке тұлғаның келісімінің болуы міндетті талап болып табылады.

Сіздің келісіміңізсіз оператор дербес деректерді басқа тұлғалар мен ұйымдарға бере алмайды.

Сондай-ақ, жеке деректерді заңсыз таратудан қорғау үшін ұйымның жеке деректерінің құпиялылығын сақтау саясатымен танысу, сондай-ақ оларды өңдеу шарттарына мұқият назар аудару ұсынылады.



СІЗДІҢ ҚҰҚЫҚТАРЫҢЫЗ ЗАҢМЕН ҚОРҒАЛҒАН

"Дербес деректер және оларды қорғау туралы" Қазақстан Республикасы Заңының 20-бабының 2-тармағына сәйкес":

дербес деректерді жинау және өңдеу олардың қорғалуы қамтамасыз етілген жағдайларда ғана жүзеге асырылады.

дербес деректерді қамтитын базаның меншік иесі және (немесе) операторы, сондай-ақ үшінші тұлғалар

осы Заңға сәйкес оларды қорғау жөнінде шаралар қолдануға міндетті,

Сонымен қатар,

"Ақпараттандыру туралы" ҚР Заңының 56-бабына сәйкес дербес деректерді қамтитын электрондық ақпараттық ресурстарды алған ақпараттық жүйелердің меншік иелері мен иеленушілері,

Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасымен және Қазақстан Республикасының аумағында қолданылатын стандарттармен реттеледі. Бұл міндет дербес деректерді қамтитын электрондық ақпараттық ресурстарды алған кезден бастап және олар жойылғанға не иесіздендірілгенге дейін туындайды.

НЕ ІСТЕУ КЕРЕК?

Жеке деректерді заңсыз жинау және жария ету фактілері анықталған жағдайда азаматтар бұзушылықтардың жолын кесу бойынша шаралар қабылдау үшін ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетіне жүгіне алады.

Мұны электрондық пошта мекенжайына жазу арқылы жасауға болады kib@mdai.gov.kz, не "электрондық үкімет" порталы ("Электрондық өтініштер" бөлімі) арқылы, сондай-ақ болады Төрағаның жеке блогына жазуға (https://dialog.egov.kz/blogs/3932160/welcome)

ӨТІНІШТЕР МЫНАЛАРДЫ ҚАМТУЫ ТИІС:

01 Өтініш берушінің аты-жөні, байланыс деректері;

02 Бұзушылық жасалған жағдайдың сипаттамасы;

03 Бұзушылық жасау кезеңі мен мерзімдері;

04 Бұзушылықты растайтын сенімді материалдар

05 Құқық бұзушылыққа жол берген ұйымның атауы.

Егер Сіз біреудің Сіздің келісіміңізсіз дербес деректеріңізді жинауды және өңдеуді жүзеге асыратынын байқасаңыз, Сіз осы тұлғаға/ұйымға заңсыз жиналған деректерді жоюды талап етуге құқылысыз. Сонымен қатар, Сіз өзіңіздің жеке деректеріңізді жинауға және өңдеуге бұрын берілген келісімді қайтарып алуға құқығыңыз бар. Оператор әрекет етпеген немесе деректерді жоюдан бас тартқан жағдайда, Сіз дербес деректерді қорғау жөніндегі уәкілетті орган – Ақпараттық қауіпсіздік комитетіне шағымдана аласыз. Өтініштерді кез келген ыңғайлы және қолжетімді тәсілмен беруге болады.

ПАНДЕМИЯҒА БАЙЛАНЫСТЫ ЖАҢА ҰСЫНЫМДАР

Терминалдық қолжетімділік

Үй компьютерлерімен жұмыс істеу кезінде корпоративтік ақпараттық жүйелерге терминалды қол жетімділікті немесе барлық орнатылған ақпаратты қорғау құралдары бар виртуалды жұмыс орындарын пайдалану ұсынылады.

Қашықтан қолжетімділік

Ұйым желісіне қашықтан қол жеткізуді қатаң түрде екі факторлы аутентификациямен пайдаланыңыз.

Құқықтары

Желіні сегменттеу және қатынасу құқығын бөлу. Тіпті қашықтан пайдаланушылардың белсенділігі ұйымның периметрлік қорғаныс құралдарымен жабылған жөн.

Пошта

Электрондық поштаның екі факторлы аутентификациямен қорғалғанын тексеріңіз. Бұдан басқа, зиянды кодты детонациялау үшін (песочница) оқшауланған ортаға "күмәнді" хаттарды жіберу үшін электрондық поштамен жұмыс істеу бойынша шешімді енгізу қажет.

Қашықтағы әрекеттер

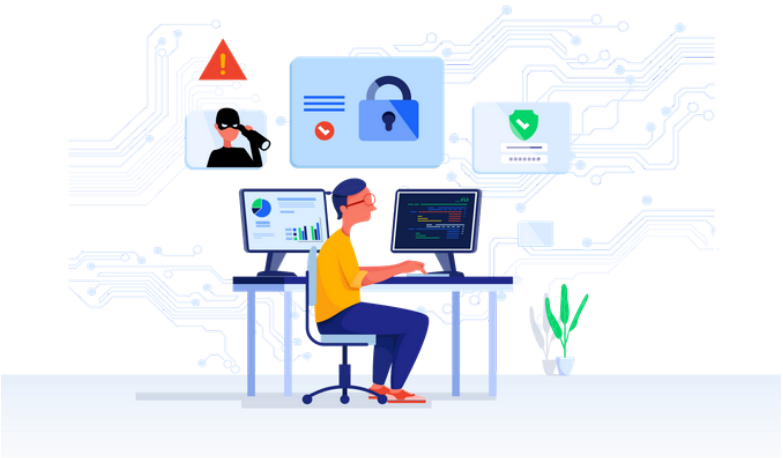
Пайдаланушылардың қашықтан әрекет ету журналдарының болуын және мерзімін, сондай-ақ қайта аутентификация талабымен белсенді емес қашықтан қосылу үзілісінің болуын тексеріңіз.

Тексеру

Қашықтан қол жеткізу үшін пайдаланылатын барлық қызметтер мен жабдықтарды жаңартылған микробағдарламалар мен қауіпсіздік патчтарының бар-жоғын тексеріңіз. Тағы бір нұсқа-бұл қызметтерге тек екі факторлы аутентификациямен қорғалған VPN арқылы қол жеткізу.

Бөгде қызметтер

Корпоративтік желіге кіру үшін аралық серверлер арқылы қосылатын және авторизация мен аутентификацияны дербес жүргізетін үшінші тарап сервистерін пайдаланбау.



АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ САЛАСЫНДАҒЫ УӘКІЛЕТТІ ОРГАН

Ақпараттық қауіпсіздік комитетінің өкілеттілігі

Қазақстан Республикасы Президентінің 2016 жылғы 16 қазандағы №350 Жарлығының аясында Ақпараттық қауіпсіздік комитеті құрылды.

01 Әзірлеу
Ақпараттық қауіпсіздікті қамтамасыз ету саласында шаралар әзірлеу (мемлекеттік құпияларды қоспағанда).

02 Бақылау
Бірыңғай талаптарды сақтауды мемлекеттік бақылау және алдын алу.

03 Қалыптастыру
Аса маңызды ақпараттық-коммуникациялық инфрақұрылымның тізбесін қалыптастыру және мониторингілеу.

04 Басқару
Интернеттің қазақстандық сегментінің кеңістігінде домендік атауларды басқару және бөлу.

05 Беру
Ақпараттық қауіпсіздік талаптарына сәйкестікке сынақтар нәтижелері бойынша акт беру.

06 Үйлестіру
2020 жылға дейінгі "Қазақстан киберқалқаны" киберқауіпсіздік тұжырымдамасын ведомствоаралық үйлестіру.

07 Ұйымдастыру
Ақпараттық қауіпсіздік инциденттеріне әрекет етудің ұлттық жоспарын орындауды ұйымдастыру.

08 Қарастыру
Жеке деректер саласындағы бұзушылықтарды қарау және жауапкершілікке тарту.

09 Жүзеге асыру
Куәландырушы орталықтарды аккредиттеуді жүзеге асыру.

10 Хабардар ету
Ақпараттық қауіпсіздік қатерлері туралы азаматтардың хабардарлығын арттыру.

11 Қатысу
Білім беру бағдарламаларын іске асыруға қатысу.

12 Жәрдемдесу
Кәсіби стандарттарды қалыптастыруға жәрдемдесу.

13 Қолдау
Ақпараттық қауіпсіздік саласындағы ғылыми зерттеулерді қолдау.

14 Өзара әрекеттесу
Халықаралық ұйымдармен, ұлттық реттеушілермен және киберқауіпсіздік орталықтарымен өзара іс-қимыл жасау.

КӘСІБИ МАМАНДАРҒА АРНАЛҒАН БӨЛІМ

Егер Сіз бизнес иесі, жауапты қызметкер, IT-маман, ақпараттық қауіпсіздік жөніндегі маман болсаңыз - келесі ұсынымдарды орындаңыз:

10 КИБЕРҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН АЗАЙТУ ҚАДАМДАРЫ

1 Ақпараттық қауіпсіздік саясатын әзірлеу

Бұл ұйымның бастапқы құжаты-Сіздің ақпараттық қауіпсіздік саласындағы конституцияңыз. Бірақ Конституциядан да басқа заңдар қажет. Мұндай заңдар" Екінші деңгейдегі құжаттар " деп аталады және саясаттың талаптарын егжей-тегжейлі сипаттайды. Респонденттердің 86,1% - ы деректер қауіпсіздігі стандарттарын пайдаланбайды.

МАҢЫЗДЫ!

Ұйымда ақпараттық қауіпсіздік жөніндегі бөлімше немесе ақпараттандыру объектілерін құру, сүйемелдеу және дамыту мәселелерімен айналысатын бөлімшеден оқшауланған ақпараттық қауіпсіздікке жауапты қызметкер болуы тиіс.

2 Пайдаланушыларды оқыту және хабардар ету

Қызметкерлерді даярлау бағдарламасын әзірлеу. Барлық қызметкерлерді ақпараттық қауіпсіздік нормаларына оқыту жүйесін енгізу. Пайдаланушылардың кибер қауіптер туралы хабардарлығын сақтау. Респонденттердің 31,4% - ы ақпараттық қауіпсіздік қатерлері туралы хабардар деп санайды.

3 Оқыс оқиғаларды басқару

Мынадай шаралар қажет: Ақпараттық қауіпсіздік оқиғаларын тіркеу, АҚ оқыс оқиғаларын басқару, АҚ оқыс оқиғалары туралы жауаптыларды хабардар ету, АҚ оқыс оқиғаларын ҚР ҰҚК "Мемлекеттік техникалық қызмет" АҚ компьютерлік инциденттерге әрекет ету қызметінде тіркеу. Респонденттердің 73,5%-ы IT-мамандарға жүгінуге ниетті.

Тәуекелдерді басқару 4

Ақпараттық қауіпсіздік тәуекелдерін бағалау нұсқаулығын немесе әдістемесін әзірлеу қажет. Сіз өзіңіздің ұйымыңызға не қауіп төндіретінін білуіңіз қажет. Респонденттердің 62,8%-ы кейде ресурс күмән тудырған кезде, олар рұқсат етілген сайттар туралы ақпаратты тексереді.

Пайдаланушы артықшылықтарын басқару 5

Тіркеулік жазбаларды басқару процестерін орнату және артықшылық берілген жазбалардың санын шектеу. Пайдаланушы артықшылықтарын шектеу және пайдаланушының әрекеттерін бақылау. Іс-шараларға және оқиғаларды тіркеу журналдарына қол жеткізуді бақылау.

Алынбалы тасымалдағыштарды басқару элементтері 6

Алынбалы тасымалдаушыларға қолжетімділікті басқару саясатын құру. Тасымалдаушы типтерін және оларды пайдалануды шектеу. Корпоративтік жүйеге импорттау алдында барлық тасымалдаушыларды зиянды бағдарламаларының бар жоғын тексеру үшін сканерлеу.

Мониторинг 7

Мониторинг стратегиясын, қосалқы саясатты әзірлеу. Ақпараттық-коммуникациялық технологияларының барлық жүйелері мен желілерін үнемі мониторингілеу. Журналдарды компьютерлік шабуылды көрсете алатын ерекше белсенділікке талдау.

Қауіпсіз конфигурация 8

Қауіпсіздік жамауларын (патчаларды) қолданыңыз және АКТ-ның барлық жүйелерін қауіпсіз конфигурациялау сақталғандығына көз жеткізіңіз. Түгендеу жүйесін құру және АКТ-ның барлық құрылғылары үшін базалық құрастыруды анықтау.

Зиянды бағдарламалардан қорғау 9

Зиянды бағдарламалардан өзекті қорғауды (лицензиялық антивирус) орнату және оларды үнемі жаңартып отыру. Респонденттердің 32,1% - на компьютерлік вирустар, 13,4% - на зиянды спам шабуыл жасады.

Желілік қауіпсіздік 10

Желіні ішкі және сыртқы шабуылдардан қорғау. Желі периметрін басқару. Рұқсатсыз кіру және зиянды элементтерді сүзгілеу. Қауіпсіздікті басқару элементтерін мониторингілеу және тестілеу. Респонденттердің 61,1% - ы өздерінің жеке деректері толық қауіпсіз деп санайды.

КОМПЬЮТЕРЛІК ИНЦИДЕНТТЕР КЕЗІНДЕ ҚАЙДА ЖҮГІНУ КЕРЕК?

қысқа телефон нөмірі арқылы Компьютерлік инциденттерге әрекет ету қызметіне хабарласыңыз: 1400 немесе +7 (7172) 55-99-97, **электрондық пошта:** info@kz-cert.kz

Компьютерлік инциденттерге әрекет ету қызметі-бұл компьютерлік қауіпсіздік қатерлерінің алдын алуда пайдаланушыларға кеңес беру және техникалық қолдауды, компьютерлік инциденттер бойынша ақпаратты жинау мен талдауды қамтамасыз ететін, Ұлттық ақпараттық жүйелер мен Интернет сегментінің пайдаланушыларына арналған бірыңғай орталық.

КЕЛЕСІ КОМПЬЮТЕРЛІК ИНЦИДЕНТТЕРДІ ӨҢДЕУ

Компьютерлік инциденттерге әрекет ету қызметінің құзыретіне оларды анықтау және бейтараптандыру мақсатында келесі компьютерлік инциденттерді өңдеу кіреді:

- **Ақпараттық ресурстарға рұқсатсыз қол жеткізу**
- **Зиянды бағдарламалық қамтылым етуді, талап етілмеген хат-хабарларды (спам) тарату**
- **Желілік инфрақұрылым тораптары мен серверлік ресурстарға шабуылдар**
- **Парольдер мен басқа да аутентификациялық ақпаратты ұрлау**
- **Ақпараттық желілерді қорғау жүйелерін бұзу**
- **Ақпараттық желілер мен хосттарды сканерлеу**

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
ЦИФРЛЫҚ ДАМУ,ИННОВАЦИЯЛАР ЖӘНЕ
АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

ҰСЫНЫМДАР

Нұр-Сұлтан қаласы -2020 жыл.