**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
ҚОРҒАНЫС ЖӘНЕ АЭРОҒАРЫШ
ӨНЕРКӘСІБІ МИНИСТРЛІГІ**

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

**Қазақстан Республикасының
Қорғаныс және аэроғарыш өнеркәсібі министрлігі**

Ақпараттық қауіпсіздік комитеті

Астана қ., Мәңгілік ел даңғылы 8, «Министрліктер Үйі», 1-кіреберіс
тел.: +7 (7172) 74-99-80, e-mail: kib@mdai.gov.kz

ҰСЫНЫМДАР

Киберқауіпсіздікті қамтамасыз ету мәселелері

Құрастырушы авторлар:
Р.К. Абдикаликов, Б.Б. Атамқұлов,
Д.В. Голобурда, Т.С. Мустагулов, Т.Т. Шаймергенов

20 жылдан астам уақыт бойы ақпараттық технологиялар біздің өмірімізді күн сайын өзгертіп келеді: интернет пен мобильді байланыс коммуникацияның жаңа нысандары, экономикалық белсенділік пен ойын-сауықтар үшін негіз болды.

Жаңа техникалық мүмкіндіктерді мемлекеттік органдар өз процестерін оңтайландыру және азаматтарға неғұрлым сапалы қызмет көрсету үшін пайдаланады.

«Электрондық үкімет» термині көптеген «онлайн» іс-шараларды қамтиды және нәтижесінде мемлекеттік мекемелерге бару қажетсіз болып қалды.

Алайда, адамның бір негізгі қажеттілігін елемеуге болмайды, ол – қауіпсіздікті қамтамасыз ету қажеттілігі.

Әсіресе, бұл ақпарат қауіпсіздігіне қатысты, себебі бұл қатерлер әрқашан бір қарағаннан байқалмайды және жиі бағаланбай жатады. Оны қамтамасыз ету үшін АКТ-ны пайдалануға тартылған әрбір адамнан білім мен іс-әрекет талап етіледі. Барлық пайдаланушылар «оффлайн» сияқты «онлайн» да сақ болуы тиіс.

Ақпараттық технологиялар мен интернет ұсынатын мүмкіндіктерді сақтау үшін тәуекелдерді азайту маңызды. Қауіпсіздік оған барлық қатысушылар өз үлестерін қосқан кезде ғана мүмкін болмақ.

Ақпараттық қауіпсіздік жөніндегі орган ретінде Министрлік дайындаған ұсынымдар Қазақстанда АКТ қауіпсіздігі деңгейін арттыруға қосылған үлес болады деп үміттенеміз.

2018 жылғы қыркүйекте жүргізілген «киберқауіпсіздік қатерлері туралы халықтың хабардарлығы» атты әлеуметтік зерттеу негізінде дайындалды

Терминдер мен анықтамалар

Интернет дегеніміз не?

Электрондық ақпараттық ресурстарды сақтауға және беруге арналған біріктірілген компьютерлік желілердің дүниежүзілік жүйесі

Дербес деректер бұл

Электрондық және (немесе) материалдық тасымалдауышта айқындалған немесе олардың негізінде айқындалатын дербес деректер субъектісіне жататын мәліметтер

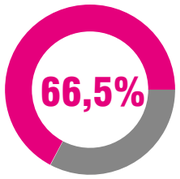
Киберқауіпсіздік дегеніміз

Электрондық нысандағы ақпараттың қорғалу деңгейімен анықталатын ақпараттық-коммуникациялық технологияларды пайдалану ортасының күйі (электрондық ақпараттық ресурстар, ақпараттық жүйелер және ақпараттық-коммуникациялық инфрақұрылым)

Киберқауіпсіздікті сақтау неліктен маңызды?

#01

Интернеттің желілік кеңістігі ақпараттық-коммуникациялық технологиялардың арқасында ақпаратты беру және тарату, сервистер мен қызметтерді қашықтықтан көрсету үшін сапалық тұрғыда жаңа орта қалыптастырады.



Қазақстан тұрғындары өздерін қызықтыратын ақпарат пен қызметтерді Интернет, оның ішінде мобильді Интернет арқылы алуды қалайды

#02

Ақпаратты қорғауға мұқтаж объектілердің өзара тәуелділігі (онлайн қызметтер мен сервистер) технологиялық іркіліс немесе компьютерлік шабуыл болған жағдайда «каскадтық әсерге» әкелуі мүмкін.

45,9%

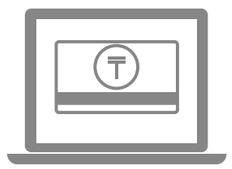
тұрғындар онлайн қызметтерді төлеу үшін мобильді қосымшаларды үнемі пайдаланады

31,6%

тұрғындар үнемі «Электрондық үкімет» порталын пайдаланады

31,1%

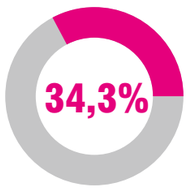
тұрғындар банк қызметтерін алу үшін Интернет-банкингті пайдаланады



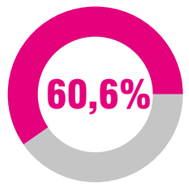
#03

Компьютерлік шабуылдар онлайн-қызметтерге деген қоғамдық сенімді бұзуға және экономикаға зиян келтіруге қабілетті.

Соңғы жылы



қазақстандықтар кибер-шабуылдарға тап болған



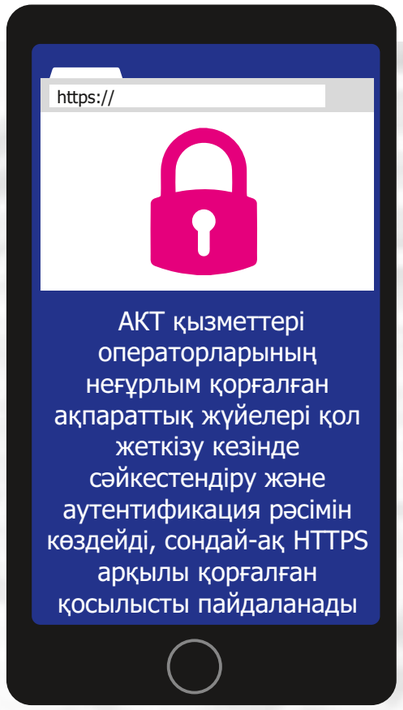
IT саласындағы сұралған мамандар қызметінде өз киберқауіпсіздік қатерлеріне тап болады

Көп жағдайда компьютерлік шабуылдар адамның салғырттығы мен абайсыздығынан сәтті іске асырылады.

Ақпараттық қауіпсіздік ақпараттың қауіпсіздігі үшін маңызды үш атрибутты қамтамасыз етуге негізделеді:

Ақпараттың құпиялылығы	оның иесі белгілеген адамдардың қатаң шектелген шеңбері ғана онымен таныса алатындығын білдіреді.
Ақпараттың бүтіндігі	ақпараттың (деректердің) бұрмаланбаған түрде сақталу қабілеті. Ақпаратты құқыққа сыйымсыз немесе иесі көздемеген түрде өзгерту тұтастықтың бұзылуына әкеп соғады.
Ақпараттың қолжетімділігі	ақпараттық жүйенің ақпаратқа тек сәйкестендірілген субъектілерге уақытылы кедергісіз қол жеткізуді ұсыну қабілеттілігімен айқындалады.

Егер мүмкіндік болса қосфакторлы аутентификацияға көшіңіз, мысалы, SMS-хабарлама арқылы ұялы телефон нөмірі бойынша



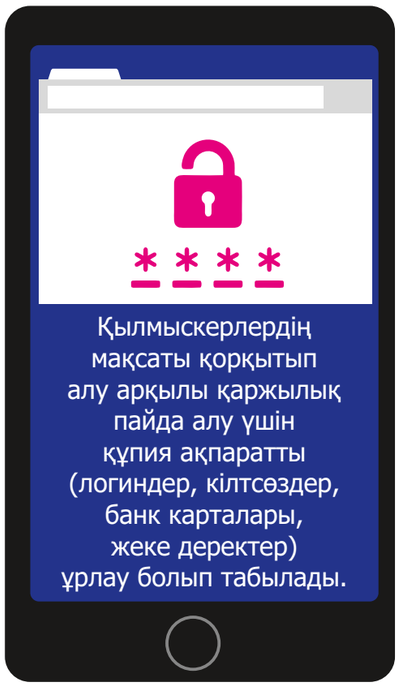
АКТ қызметтері операторларының неғұрлым қорғалған ақпараттық жүйелері қол жеткізу кезінде сәйкестендіру және аутентификация рәсімін көздейді, сондай-ақ HTTPS арқылы қорғалған қосылысты пайдаланады

Сәйкестендіру – субъектілерге түпнұсқалылықты анықтауды қамтамасыз ететін ақпараттық жүйеге немесе жеке сәйкестендіргіш электрондық ресурсына қолжетімділік беру және субъектінің ақпараттық жүйедегі өкілеттіктерін айқындау және сеанс процесіндегі әрекеттерді тіркеу.

Аутентификация – бұл бір нәрсенің түпнұсқалығын тексеру процесі. Аутентификация мысалы, пайдаланушы енгізген кілтсөзді сервер деректер базасында сақталған кілтсөзбен салыстыру болуы мүмкін. Бұндай тексеру біржақты да, өзара да болуы мүмкін - барлығы сервистің қауіпсіздік саясаты мен қорғау тәсіліне байланысты.

Деректер қауіпсіздігі қатері

Соңғы жылы сұралған қазақстандықтар кибершабуылдардың мынадай түрлеріне тап болған:



Зиянды бағдарламалық қамттылым (malware – malicious software қысқарту: **malicious** – зиянды және **software** – бағдарламалық қамтылым) – бағдарламалық қамтылымның кең санаты болып табылады – олар Сіздің рұқсатыңызсыз орнатылып, компьютеріңіздің жұмысына әсер етеді.

Ақпаратқа әсер ету тәсілі бойынша мынадай зиянды БҚ болып бөлінеді:

- эксплоиттар;
- логикалық бомбалар;
- троян және тыңшылық бағдарламалар;
- компьютерлік вирустар;
- желілік құрттар.

Зиянды бағдарламалар пайдаланушының компьютеріне қалай енеді?

Бұл қалай болады?

Зиянды бағдарламалар көбінесе компьютерге:

- электрондық пошта арқылы;
- ақпарат тасымалдауыштар арқылы (флеш-жинақтаушы);
- белгісіз сайттардан файлдарды жүктеу кезінде енеді.

Тарату әдістері

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

Қолданушыны құпия ақпаратты ашуға итермелеу үшін қасқүнемдер қолданатын тактика (зиянды тіркемесі бар жалған мекенжайлары бар хаттарды жіберу).

ФИШИНГ

(ағылш. Phishing, fishing – балық аулау, алу)

Интернет-алаяқтықтың бір түрі. Мақсаты – қолданушылардың құпия деректеріне (логиндер, кілтсөздер, банк карталарының деректері және т.б.) сырт жағынан нағыз интернет-ресурстарынан айырмашылығы жоқ жалған интернет-ресурстары арқылы қол жеткізу болып табылады.

ЗИЯНДЫ БАҒДАРЛАМАЛЫҚ ҚАМТЫЛЫМДЫ САЙТ АРҚЫЛЫ ТАРАТУ

Қаскөйлердің сайт файлдарына немесе сайтты басқару жүйесінің әкімшілендіру бөліміне рұқсатсыз қолжетімділік алуы.

Компьютердің зиянды бағдарлама жұқтыруының қандай салдарлары бар?

Зиянды бағдарламалар жүйенің қалыпты жұмыс істеуіне әсер етеді, бұл қызмет көрсетуден бас тартуға, деректерді бұғаттауға, жоюға немесе модификациялауға, сондай-ақ желінің өткізу қабілетін төмендетуге әкелуі мүмкін.

Зиянды бағдарламаны жұқтыру белгілері:

- жүйенің жұмысқа қабілеттілігінің төмендеуі;
- браузерде сұраныстарды жағымсыз сайттарға қайта бағыттау;
- қалқымалы терезелер.

Компьютерді зиянды бағдарламалардан қалай қорғауға болады?

Не істеу керек?

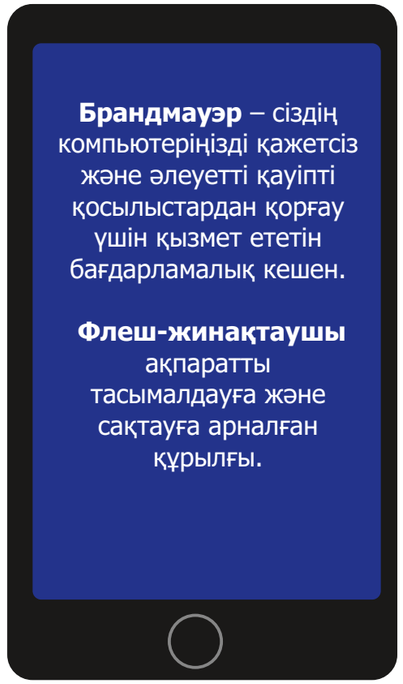
Зиянды бағдарламалар көбінесе басқа файлдармен бірге қолданылады, сондықтан Сізге белгісіз ресурстардан жіберілген электрондық пошта салымдарын ашпаңыз.

#01 операциялық жүйенің кіріктірілген брандмауэрін ешқашан өшірмеңіз.

Брандмауэр компьютер мен Интернет арасында қорғаныс тосқауылын жасайды. Брандмауэрді тіпті бір минутқа өшіру ДК зиянды бағдарламаны жұқтыру қаупін арттырады.

55%

қазақстандықтар өз компьютері үшін антивирус пайдаланбайды



#02 сіздің жүйеңізді ықтимал онлайн – қауіптерден қорғау үшін антивирустық БҚ пайдаланыңыз. Сенімді көздерден антивирустық және антишпиондық бағдарламаларды орнатыңыз.

#03 флеш-жинақтаушыларды абайлап пайдаланыңыз.

Компьютердің зиянды бағдарламалық қамтылымды жұқтыру мүмкіндігін азайтыңыз: белгісіз флеш-жинақтағыштарды (немесе USB-жинақтағыштарды) өз компьютеріңізге қоспаңыз.

37,6%

пайдаланушылар электрондық хат алған кезде бейтаныс адамнан сілтемеге өту туралы өтінішімен, көрсетілген сілтеме бойынша ауысатынын атап өтті

#04 сізге таныс емес пайдаланушылардан файлдарды қабылдамаңыз, әсіресе алынатын EXE, COM, CMD файлдарына назар аударыңыз.

#05 тексерілмеген Интернет-көздер ұсынған БҚ (Бағдарламалық қамтылым) жүктеуге келіспеңіз.

- Сіз жіберушіні білсеңіз де, электрондық пошта, жедел хабарлар немесе әлеуметтік желілердегі жарияланымдарда салынған файлдарды ашу немесе сілтемелерді басу кезінде мұқият болыңыз. Оған қоңырау шалып, оның не жасағанын біліңіз: жоқ болса, жедел хабар алмасу қызметінің терезесін жойыңыз немесе жабыңыз.
- Бағдарламалық қамтылымды тек Өзіңіз сенетін сайттардан жүктеп алыңыз.
- Электрондық пошта хабарларындағы сілтемелерге ауыспаңыз және авторлық құқықтарды бұзу арқылы тегін бағдарламалық қамтылым ұсынылатын веб-сайттан аулақ болыңыз. Белгісіз домен аймақтарынан музыка, ойын, бейне және т.б. «тегін» жүктеуден сақтаныңыз (**.ws**, **.biz** және т.б.). Олар сайттың өзінде де, жүктелетін файлдарда да зиянды бағдарламалық қамтылымды қамтуы мүмкін.

#06 егер сіз терезе қалқымалы баннер жарнамасына тап болсаңыз.

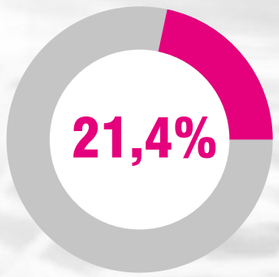
- **«Келісемін»**, **«ОК»**, **«рұқсат»**, **«Мен қабылдаймын»**, **«жүктеу»**, **«жалғастыру»** және тағы басқа **«келісім түймелері»** түймелерін баннерлік жарнамада, күтпеген қалқымалы терезелерде немесе ескертулерде, күдікті болып көрінетін сайттарда немесе тыңшылық БҚ немесе вирустарды жою ұсыныстарында баспаңыз.
- Браузер қойындысын жабу үшін пернетақтадағы **CTRL+F4** түймесін басыңыз.
- Егер терезе жабылмаса, браузерді жабу үшін пернетақтадағы **Alt+F4** түймесін басыңыз.

Егер сіз компьютеріңіз зиянды бағдарламаны жұқтырған деп күдіктенсеңіз

#07 Ақпаратты өңдеуді тоқтату үшін, сондай-ақ ақпараттың (логин, кілтсөз және басқа да құпия ақпарат) таралуын болдырмау үшін құрылғыны Интернеттен ажыратыңыз).

69,6%

кибершабуыл не компьютері зиянды бағдарлама жұқтырған жағдайда қайда жүгіну керектігін және/немесе не істеу керектігін білмейді немесе күмәнданады



сұралған пайдаланушылар ақпаратты қорғаудың барлық ықтимал әдістерін қолдануға тырысады

Ақпараттық қауіпсіздіктің алдын алу

Ескірген немесе лицензиясыз бағдарламалық қамтылым осал болып табылады

#01

Барлық бағдарламалық қамтылым – операциялық жүйелер, қосымшалар бағдарламалары, антивирустық және басқа бағдарламалар үшін жаңартуларды үнемі орнатып отырыңыз

#02

Мүмкін болса бағдарламалық қамтылымды автоматты түрде жаңарту функциясын қосыңыз

#03

Әзірлеуші жаңартуларын пайдаланбайтын немесе алмайтын бағдарламалық қамтылымды жойып отырыңыз

#04

Лицензияланбаған бағдарламалық қамтылымды немесе тексерілмеген көздерден бағдарламалық қамтылымды орнатудан аулақ болыңыз

#05

Барлық құрылғыларда деректердің сақтық көшірмесін тұрақты түрде жүзеге асырыңыз

Parol123456#!&

сенімді кілтсөздер кем дегенде 8 символдан тұруы тиіс және әріптер, сандар мен символдар (!@#$%^&*)

****

кілтсөзіңізді ешкімге ашпаңыз, ең маңыздысы, шифрланған күйде сақтаңыз

****

барлық сайттарда бірдей кілтсөздер пайдаланбаңыз. Кілтсөзді жоғалтқан жағдайда, сіздің мәліметтеріңізге кіру оңай болады

Home Wi-Fi Подключено

модем мен үйдегі сымсыз желі үшін әртүрлі сенімді құпия сөздерді жасаңыз. Оны қалай қолдану туралы құрылғы нұсқаулығынан немесе модем, роутер, маршрутизатормен қамтамасыз еткен компаниядан сұрап біліңіз

61,8%

пайдаланушылар кілтсөздерін өзгертпейді немесе оларды ұмытқан кезде ғана өзгертеді

32,2%

пайдаланушылар әлеуметтік желілерде, аккаунттарда, жеке кабинеттерде бірдей кілтсөздер пайдаланады

Интернеттегі қауіпсіз «серфинг» бойынша ұсыныстар

#01 Интернетте жұмыс істеу кезінде қорғау дәрежесін арттыру үшін өз браузеріңізді **ТЕҢШЕҢІЗ** (жарнама мен қалқымалы терезелерді бұғаттауыш, тыңшылықтан қорғау және т.б.).

#02 Әлеуметтік желілерде өз өміріңіз туралы **ӘҢГІМЕЛЕУДІҢ ҚАЖЕТІ ЖОҚ**.

#03 Қоғамдық «Wi-Fi-нүктелерін» аса қажет болмаса **ПАЙДАЛАНБАҢЫЗ**.

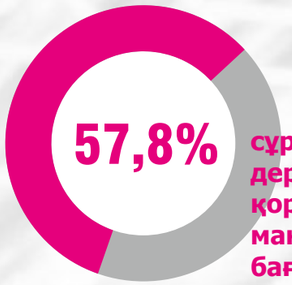
#04 Анонимді прокси-серверді (анонимайзерлерді) **ПАЙДАЛАНБАҢЫЗ**. Олар арқылы сіздің деректеріңіз үшінші тұлғаларға қолжетімді болады.

#05 Кілтсөздеріңізді шифрланған түрде сақтау үшін кілтсөздер менеджерін **ОРНАТЫҢЫЗ**.

#06 Сайттар беделін бағалау қызметтерін және сілтемелердің онлайн сканерлерін **ПАЙДАЛАНЫҢЫЗ**.

Сайттардың беделін бағалау сервистері және сілтемелердің онлайн сканерлері:

- **VirusTotal (https://www.virustotal.com)**
- **URLVoid (http://www.urlvoid.com/)**
- **2ip.ru (http://2ip.ru/site-virus-scaner)**
- **Web Inspector (http://siteinspector.comodo.com)**
- **Dr.Web Онлайн-сканері (http://vms.drweb.com/online)**
- **TrustOrg.com (http://trustorg.com/)**
- **Phishtank.com (http://www.phishtank.com/)**



сұралғандар дербес деректерді қорғаудың маңыздылығын жете бағаламайды

қазақстандықтар өз дербес деректерін қауіпсіздікте деп санамайды

Бұны білу маңызды!

Дербес деректерді жинауды, өңдеуді заңнамада көзделген жағдайларды қоспағанда, **СУБЪЕКТІНІҢ НЕМЕСЕ ОНЫҢ ЗАҢДЫ ӨКІЛІНІҢ** келісімімен меншік иесі және (немесе) оператор жүзеге асырады.

Қолжетімділігі шектеулі дербес деректерге қол жеткізе алатын меншік иелері және (немесе) операторлар, сондай-ақ үшінші тұлғалар **ОЛАРДЫҢ ҚҰПИЯЛЫЛЫҒЫН** субъектінің немесе оның заңды өкілінің келісімінсіз олардың таралуына жол бермеу не өзге де заңды негіз болған талаптарды сақтау арқылы **ҚАМТАМАСЫЗ ЕТЕДІ**.

Дербес деректерді сақтауды меншік иесі және (немесе) оператор, сондай-ақ үшінші тұлға Қазақстан Республикасының аумағында сақталатын базада жүзеге асырады.

Базаның меншік иесі және (немесе) операторы, сондай-ақ үшінші тұлға дербес деректерді қорғау жөніндегі қажетті шараларды қолдануға міндетті:

- дербес деректерге рұқсатсыз қол жеткізуді болдырмау;
- егер мұндай рұқсат етілмеген қолжетімділіктің алдын алу мүмкін болмаса, дербес деректерге рұқсатсыз кіру фактілерін дер кезінде анықтау;
- дербес деректерге рұқсатсыз қол жеткізудің жағымсыз салдарларын азайту.

Дербес деректер субъектісі құқылы

#01 базаның меншік иесінде және (немесе) операторында, сондай-ақ үшінші тұлғада өзінің дербес деректерінің болуы туралы білуге, онда мыналар қамтылады:

- дербес деректерді жинау және өңдеу фактісін, мақсатын, көздерін, тәсілдерін растау;
- дербес деректер тізбесі;
- дербес деректерді өңдеу мерзімдері, оның ішінде оларды сақтау мерзімдерін білуге;

#02 база меншік иесінен және (немесе) операторынан негіздеме болған кезде өзінің дербес деректерін өзгерістер мен толықтыруды талап етуге;

#03 дербес деректерді жинау, өңдеу шарттарының бұзылуы туралы ақпарат болған жағдайда меншік иесінен және (немесе) база операторынан, сондай-ақ үшінші тұлғадан өзінің дербес деректерін оқшаулауды талап ету;

#04 базаның меншік иесінен және (немесе) операторынан, сондай-ақ үшінші тұлғадан Қазақстан Республикасының заңнамасын бұза отырып жиналған және өңдеу жүргізілген өзінің дербес деректерін жоюды, сондай-ақ ҚР Заңында белгіленген өзге де жағдайларда «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңына және Қазақстан Республикасының өзге де нормативтік құқықтық актілеріне сәйкес талап ету;

#05 «Дербес деректер және оларды қорғау туралы» ҚР Заңының 8-бабының 2-тармағында көзделген жағдайлардан басқа, дербес деректерді жинауға, өңдеуге келісімді кері қайтарып алу;

#06 меншік иесіне және (немесе) база операторына өзінің дербес деректерін жалпыға қол жетімді дербес деректер көздерінде таратуға келісім беру (бас тарту);

#07 өзінің құқықтары мен заңды мүдделерін қорғауға, оның ішінде моральдық және материалдық зиянды өтеуге;

#08 «Дербес деректер және оларды қорғау туралы» ҚР Заңында және Қазақстан Республикасының басқа да заңдарында көзделген өзге де құқықтарды жүзеге асыру.

Прокуратура органдары дербес деректер және оларды қорғау саласында заңдылықтың сақталуын жоғары қадағалауды жүзеге асырады.

Кәсіби қызметте АКТ қолдану

сұралған IT саласының мамандары өз қызметінде киберқауіпсіздік қатерлеріне тап болады

ұйымның сұралған IT саласының қызметкерлерінде ақпараттық қауіпсіздікті басқару жүйесі жоқ

#01 **Мобильді құрылғылармен жұмыс**
Мобильді құрылғылармен жұмыс істеу саясатын жасаңыз, оны сақтау үшін персоналды таныстырыңыз. Барлық құрылғылар үшін негізгі қауіпсіздік деңгейін қолданыңыз. Деректерді тасымалдау кезінде де, сақтау кезінде де сақтаңыз.

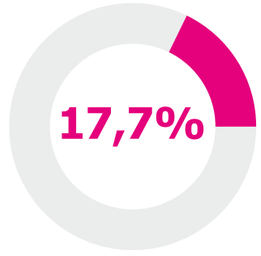
#02 **Пайдаланушыларды оқыту және хабардар ету**
Пайдаланушылардың қолайлы қауіпсіздік саясатын және Сіздің жүйелеріңізді қауіпсіз пайдалану саясатын әзірлеңіз. Бұл саясатқа персоналды оқытуды енгізіңіз. Персоналдың ақпараттық қауіпсіздік қатерлері туралы хабардарлығын қамтамасыз етіңіз.

#03 **Пайдаланушының артық құқықтарын басқару**
Басқарудың тиімді процестерін орнатыңыз және айрықша құқық берілген пайдаланушылардың санын шектеңіз. Қолданушылардың айрықша құқықтарын шектеңіз және олардың әрекетін мониторингілеуді жүзеге асырыңыз. Оқиғалар журналына қолжетімділікті бақылаңыз.

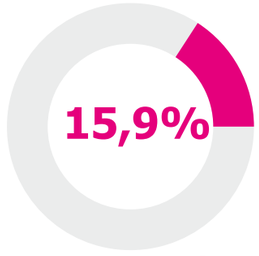
#04 **Алмалы-салмалы тасымалдаушыларды пайдалану ережесі**
Алмалы-салмалы тасымалдауыштарға қол жеткізуді бақылау ережелерін жасаңыз. Тасымалдауыш түрлері мен оларды пайдалануды шектеңіз. Корпоративтік желіге қосар алдында барлық тасымалдауыштарды зиянды бағдарламалардың бар-жоғына тексеріңіз.

#05 **Қауіпсіз конфигурация**
Қауіпсіздік жүйесін жаңартыңыз және барлық жүйелердің қауіпсіз конфигурациясы қамтамасыз етілгеніне көз жеткізіңіз. Ұйым желісіне қосылған және қосылуға болатын құрылғылар тізімін бақылаңыз.

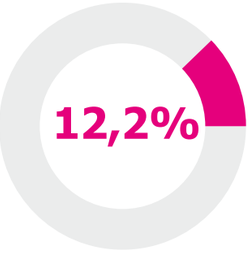
Кәсіби қызметте АКТ қолдану



желіаралық экрандарды пайдаланады



деректерді, байланыс арналарын шифрлауға жүгінеді



DLP жүйесін пайдаланады

#06 **Зиянды бағдарламалардан қорғау**
Тиісті саясат әзірлеңіз және ұйымда зиянды бағдарламалардан қорғау жүйесін орнатыңыз.

#07 **Желілік қауіпсіздік**
Желінің периметрін басқарыңыз. Желіңізді сыртқы және ішкі шабуылдардан қорғаңыз.

#08 **Мониторинг**
Мониторинг стратегиясын әзірлеңіз. Барлық жүйелер мен желілердің мониторингін үздіксіз жүргізіңіз. Белсенділікті іздеуге оқиғалар журналын талдаңыз, ол ақпараттық қауіпсіздік оқиғаларын көрсетуі мүмкін. Қауіпсіздікті басқару элементтерін мониторингілеуді және тестілеуді жүзеге асырыңыз.

#09 **Оқыс оқиғаларды басқару**
Резервтеу және авариялық қалпына келтіру мүмкіндігін ескеріңіз. Ақпараттық қауіпсіздік оқыс оқиғаларына ден қою жоспарын жасаңыз.

#10 **Өзара іс-қимыл**
Ақпараттық қауіпсіздік оқыс оқиғалары туралы Құқық қорғау органдарына және мамандандырылған ұйымдарға хабарлаңыз.

Стандартты шараларды сақтау бүгінгі күні байқалатын шабуылдардың 80%-ын ескертуі мүмкін.

Өзіңізден сұраңыз

#01 Сіз брандмауэріңіздің белсендірілгеніне және Сіздің компьютеріңізде деректерді қорғайтынына сенімдісіз бе?

#02 Сіздің компьютеріңіздегі деректерге ішкі желіден немесе қашықтықтан кім қол жеткізуі мүмкін?

#03 Сіздің желіңіздің қандай қызметтері Интернет арқылы қолжетімді екенін анық білесіз бе?

#04 Сізге сыртқы IP мекенжайы бар әрбір Сіздің желі құрылғыңыз шынымен белгілі ме?

#05 Сіз соңғы рет қашан тәуекелдерді бағалау жүргіздіңіз немесе енуге сыртқы тест жүргіздіңіз?

#06 Қаскүнем Сіздің желіңізге ене ала ма?

ҰСЫНЫМДАР

Ұйымдар, мекемелер, кәсіпорындар басшыларына, ақпараттық инфрақұрылым мен ақпараттық технологиялардың қауіпсіздігі жөніндегі кәсіби мамандарға, сондай-ақ жоғары оқу орындарының студенттеріне

«Болашақ» халықаралық бағдарламалар орталығы

Академиялық оқудан (магистратура, докторантура), әлемнің жетекші компаниялары мен университеттерінде ғылыми және өндірістік тағылымдамадан өту үшін басым гранттар береді.

«Ақпараттық (кибер) қауіпсіздік» мамандығы бойынша тағылымдамадан өту үшін ізденушінің таңдаған мамандану саласында соңғы 12 айды қоса алғанда, кемінде 3 жыл жұмыс өтілі болуы тиіс.

Мамандығы бойынша оқудан (магистратура, докторантура) өту үшін «ақпараттық қауіпсіздік» ізденушінің бакалавр немесе маман дипломының қосымшасы бойынша орташа балы GPA 3.30 (4.00/4.33-ден) немесе 5.00-ден 4.30 болуы тиіс.

Толық ақпарат:

bolashak.gov.kz

KZ-CERT

Компьютерге зиянды бағдарламалық қамтылым жұқтыру қаупі болса, компьютерлік оқыс оқиғаларға ден қою қызметіне тегін бірыңғай қысқа нөмір арқылы хабарласыңыз:
1400, +7 (7172) 55-99-97,
немесе электрондық пошта арқылы:
incident@kz-cert.kz

ЖЕДЕЛ ЖЕЛІ

Қазақстанда терроризм, экстремизм, порнография, қатыгездік пен зорлық-зомбылықты насихаттайтын құқыққа қайшы контентке қарсы іс-қимыл бойынша:

сайт: **safekaznet.kz**
телефон: **+7 (7272) 73-24-63**,
электрондық пошта: **report@iak.kz**

отандық жүйенің көмегімен
СІЗ ӨЗІҢІЗДІҢ ИНТЕРНЕТ-РЕСУРСЫҢЫЗҒА БАҒАЛАУ ЖҮРГІЗЕ АЛАСЫЗ
WebTotem интернет-ресурста:
webtotem.kz

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

Миссия – Қазақстан Республикасының орнықты дамуын қамтамасыз ететін электрондық ақпараттық ресурстардың ішкі және сыртқы қатерлерден қорғалу деңгейіне қол жеткізу және оны сақтау

Ақпараттық қауіпсіздікті қамтамасыз ету саласында **шаралар әзірлеу** (мемлекеттік құпияларды қоспағанда)

Мемлекеттік бақылау және бірыңғай талаптарды сақтау профилактикасы

2020 жылға дейін **"Қазақстанның Киберқалқаны»** киберқауіпсіздік тұжырымдамасын ведомствоаралық үйлестіру

Ақпараттық жүйелерді ақпараттық қауіпсіздік талаптарына сәйкестікке **аттестаттау және сынау** жүргізу

Азаматтардың ақпараттық қауіпсіздік қатерлері туралы **хабардарлығын** арттыру

Білім беру бағдарламаларын іске асыруға қатысу

Ақпараттық-коммуникациялық инфрақұрылымның **аса маңызды объектілерінің** тізбесін қалыптастыру және оны мониторингілеу

Кәсіби стандарттарды қалыптастыруға жәрдемдесу

Ұсынымдарды дайындау кезінде мынадай нормативтік құқықтық актілер пайдаланылды

- «Ақпараттандыру туралы» ҚР Заңы;
- «Байланыс туралы» ҚР Заңы;
- «Дербес деректер және оларды қорғау туралы» ҚР Заңы;
- «Электрондық құжат және электрондық цифрлық қолтаңба туралы» ҚР Заңы;
- «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» ҚРҮҚ.