ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ПРЕЗИДЕНТІНІҢ ЖАНЫНДАҒЫ
МЕМЛЕКЕТТІК БАСҚАРУ АКАДЕМИЯСЫ

КИБЕРҚАУІПСІЗДІК МӘСЕЛЕЛЕРІ БОЙЫНША МЕМЛЕКЕТТІК ҚЫЗМЕТШІЛЕРГЕ АРНАЛҒАН ӘДІСТЕМЕЛІК ҰСЫНЫСТАР

2018

МЕМЛЕКЕТТІҢ КИБЕРҚАУІПСІЗДІГІ – БҰЛ ӘР МЕМЛЕКЕТТІК ҚЫЗМЕТШІНІҢ ЖАУАПКЕРШІЛІГІ

Киберқауіпсіздік – электрондық нысандағы ақпараттың және оның өңдеу, сақтау, беру (электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымды) ортасының сыртқы және ішкі қауіп-қатерлерден қорғалу жағдайы.

НЕЛІКТЕН КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МАҢЫЗДЫ?

1. Мемлекеттердің қызмет етуі үшін, сондай-ақ азаматтарға мемлекеттік көрсетілетін қызметтер ұсыну үшін киберкеңістіктің күннен-күнге маңызы артып келеді.

2. Кибершабуылдар экономикалық зиян шектіреді, онлайн-қызметтерге қоғамдық сенімді кетіреді және азаматтарға, олардың меншіктері мен құпиялығына залал келтіреді.

3. Кибершабуылдар оңай құпиясөздер, жеке деректерді жариялау сынды адами немқұрайлылық пен абайсыздықтардан туындайды.

ТЕРМИНДЕР МЕН АНЫҚТАМАЛАР

Ақпараттық қауіпсіздіктің классикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: **құпиялық, тұтастық және қолжетімділік.**

Ақпараттың **құпиялығы** онымен өзінің иесі белгілеген қатаң шектелген адамдар тобы ғана таныса алады дегенді білдіреді.

Ақпараттың **тұтастығы** – ақпараттың (деректердің) бұрмаланбаған түрде сақталу қабілеті. Ақпараттың заңсыз және иесі көздемеген өзгеруі (оператор қатесінің немесе уәкілеттігі жоқ адамның қасақана іс-әрекетінің нәтижесінде) тұтастықтың бұзылуына алып келеді.

Ақпараттың **қолжетімділігі** ақпараттық жүйенің тиісті өкілеттіктері бар субъектілерге ақпаратқа дер кезінде бөгетсіз рұқсат беру қабілетімен анықталады. Ақпаратты жою немесе бұғаттау (қателіктің немесе қасақана іс-әрекеттің нәтижесінде) қолжетімділіктің жойылуына алып келеді.

НЕГІЗГІ ПРОБЛЕМАЛАР

- тұрғындардың, АКТ саласы қызметкерлерінің және ұйымдар басшыларының ақпараттық қауіпсіздік мәселелері жөніндегі құқықтық сауаттылығының төмендігі;
- ақпараттандырудың мемлекеттік және мемлекеттік емес субъектілерінің және АКТ саласында көрсетілетін қызметтерді пайдаланушылардың белгіленген талаптарды, техникалық стандарттар мен ақпаратты электрондық түрде жинау, өңдеу, сақтау және беру регламенттерін бұзуы;
- ақпараттық жүйелерге, бағдарламалық жасақтама және ақпараттық-коммуникациялық инфрақұрылымның басқа да элементтеріне теріс ықпал ететін персоналдың әдейі жасамаған қателері және технологиялық іркілістер;
- халықаралық қылмыстық топтардың, қоғамдастықтардың және жеке тұлғалардың қаржы- банк саласындағы ұрлауды, өнеркәсіптің, энергетиканың, байланыс және ақпараттық- коммуникациялық қызметтер саласының технологиялық процестерін басқарудың автоматтандырылған жүйесінің жұмысын бұзу мақсатында зиянды ықпалды жүзеге асыру бойынша іс-қимылы;
- ақпараттық-коммуникациялық инфрақұрылымға барлау және зиянкестік әрекет жасау арқылы Қазақстан Республикасы мүдделеріне қарсы бағытталған саяси, экономикалық, террористік құрылымдардың, шет мемлекеттердің барлау және арнайы қызметтерінің қызметі.

КИБЕРҚАУІПСІЗДІК ҚАУІП-ҚАТЕРЛЕРІНІҢ ТИПТЕРІ

1. **Күшпен алушы-бағдарлама** – сатып алуға дейін компьютерлік жүйенің файлдарына кіруді бұғаттау арқылы ақшаны алып алу үшін зиянды бағдарламалық қамтамасыз етудің әртүрлілігі. Сатып алуды аудару файлдарды қалпына келтіруге немесе жүйенің жұмыс істеп кетуіне кепілдік бермейді.

2. **DDoS - шабуыл** (ағылш. Distributed Denial of Service – «қызмет көрсетуден бас тарту») – кең таралған және қауіпті желілік шабуылдардың бірі болып табылатын қызмет көрсетуден бас тарту түріндегі үлестірілген шабуыл. Шабуыл нәтижесінде заңды пайдаланушыларға, желілерге, жүйелер мен өзге де ресурстарға қызмет көрсету бұзылады немесе толық істен шығарылады. DDoS-шабуыл нәтижесінде сайтқа қызмет көрсететін серверлерге үлкен көлемдегі жалған сұратуларды өңдеуге тура келеді және сайт қарапайым пайдаланушы үшін қолжетімсіз болып қалады.

3. **Әлеуметтік инженерия** – құпия ақпаратты ашу үшін пайдаланушыны тартуға зиянкестер қолданатын тактика.

4. **Фишинг** (ағылш. phishing, fishing – балық аулау, іліктіру) – компьютерлік айлакерліктің түрі, оның негізгі мақсаты – алдау арқылы құрбанды алаяққа қажетті ақпаратты ұсынуы үшін еріксіз көндіру. Бұл заңмен қудаланатын компьютерлік қылмыс.

5. **Сайтты бұзу** – бұл зиянкестің сайттың файлдарына немесе сайтты басқару жүйесін әкімшілендіру бөліміне рұқсатсыз қол жеткізуі.

ЗИЯНДЫ БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУ

Зиянды бағдарламалық қамтамасыз ету (malware - malicious software сөздерінен қысқартылған: **malicious** - зиянды және **software** - бағдарламалық қамтамасыз ету) – жеке компьютерге, серверге немесе компьютерлік желіге зиян келтіру үшін арнайы жасалған кез келген бағдарламалық қамтамасыз етуді белгілеу үшін пайдаланылатын жалпыға бірдей қабылданған термин.

Зиянды бағдарламалар бағдарламалық қамтамасыз етудің күрделі санатын білдіреді. Олар Сізден рұқсат сұрамай орнатылады және компьютердің жұмысына әсер етеді.

Тарату тәсілі бойынша келесі зиянды бағдарламалық қамтамасыз етулер ерекшеленеді: эксплоиттар, логикалық бомбалар, троян және тыңшы бағдарламалар, компьютерлік вирустар мен желілік зиянкестер. Зиянды бағдарламалардың ең кең тараған түрлері трояндар, зиянкестер мен вирустар болып табылады.

Троян – зиянкестер ақпаратты жинау, оны бұзу немесе түрлендіру, компьютердің жұмыс қабілетін бұзу немесе оның ресурстарын жағымсыз мақсаттарда пайдалану үшін пайдаланылатын зиянды бағдарлама.

Компьютерлік вирус – көбею (репликациялану) қабілеті айрықша ерекшеленген компьютерлік бағдарламаның бір түрі. Оған қоса оның атынан зияндалған бағдарлама жіберілген пайдаланушының бақылауындағы мәліметтерді зақымдау немесе толық жою мүмкіндігі бар.

Желілік зиянкес – компьютерлік бағдарламаның ұдайы өздігінен қалпына келтірілетін локалдық және жаһандық компьютерлік желілерде таралатын түрі. Компьютерлік вирустарға қарағанда зиянкес дербес бағдарлама болып табылады. Trackware – компьютерде жүргізілетін іс-қимылдарды бақылайтын және тіркейтін зиянды бағдарламаның жаңа вариациясы.

ЗИЯНДЫ БАҒДАРЛАМАЛАР ПАЙДАЛАНУШЫНЫҢ КОМПЬЮТЕРІНЕ ҚАЛАЙ ЕНЕДІ?

Зиянды бағдарламалар компьютерге көбіне Интернет арқылы немесе электрондық пошта бойынша енеді. Егер Сіз URL-адресте қателік жіберсеңіз немесе кездейсоқ белгісіз сілтемені бассаңыз, «агрессиялық» мазмұндағы немесе зиянды бағдарламалары бар қауіпті сайттарға түсуіңіз мүмкін. Пайдаланушылар файлдарды бір компьютерден тікелей екіншіге жібере алатын P2P (peer-to-peer) желілер компьютерді зиянды және жарнамалық БҚ зақымдауға елеулі қауіп төндіреді.

ЗИЯНДЫ БАҒДАРЛАМАЛАР КОМПЬЮТЕРДІҢ ЖҰМЫСЫНА ҚАЛАЙ ӘСЕР ЕТЕДІ?

Жүйенің жұмыс қабілетінің төмендеуі, қалқып шығатын бос аралықтар немесе браузерде сұрау салуларды жағымсыз сайттарға жіберу зиянды бағдарламамен зақымдалудың белгілері болып табылады. Зиянды бағдарламалар жүйенің қалыпты қызмет етуіне әсер етеді, бұл жүйенің қызмет көрсетпей қалуына, деректердің алмастырылуына және өткізу қабілетінің төмендеуіне әкеп соғуы мүмкін. Бұдан басқа, компьютерді өшіру немесе қайта жүктеу мүмкін болмайды.

КОМПЬЮТЕРДІ ЗИЯНДЫ БАҒДАРЛАМАЛАРДАН ҚАЛАУ ҚОРҒАУҒА БОЛАДЫ?

Зиянды бағдарламалар көбіне басқа файлдармен қоса беріліп таратылады, сондықтан Сізге белгісіз ресурстардан жіберілген электрондық поштадағы хабарламаларды ашпаңыз. Сіздерге таныс емес пайдаланушылардан келген файлдарды ешқашан қабылдамаңыз, сондай-ақ AVI, EXE немесе JPG кеңейтулері бар файлдарды ашқанда абайлаңыздар.

ЕГЕР СІЗ КОМПЬЮТЕРІҢІЗ ЗИЯНДЫ БАҒДАРЛАМАМЕН ЗАҚЫМДАЛДЫ ДЕП КҮДІКТЕНСЕҢІЗ:

Логиндерді, парольдерді және басқа құпия ақпаратты пайдаланумен байланысты қандай болсын қызметті тоқтатыңыз. Жүйеңізді ықтимал онлайн-қатерлерден қорғау үшін вирусқа қарсы БҚ қолданыңыз. Сенімді әзірлеушілердің вирусқа қарсы және тыңшылыққа қарсы бағдарламаларды орнатыңыз. Сіздің вирусқа қарсы бағдарламаңыздың жаңартылғанына, компьютерді сканерлеуді жүргізетініне және зиянды ретінде белгіленетін барлық бағдарламаларды жоятынына көз жеткізіңіз. Көбіне, компьютерді тексеруді аяқтау және зиянды бағдарламаларды айқындау туралы дұрыс емес ақпаратты қамтитын қалқымалы хабарламаны асығыста зейінсіз оқуға болады. Мұндай хабарламада зиянды бағдарламаларды тарату үшін кеңінен пайдаланылатын жалған бағдарламалық қамтамсыз етуді жүктеу ұсынылады. Сіздің компьютерді қорғауды немесе вирустарды жоюды ұсынатын Сіз орнатпаған немесе Сізге таныс емес бағдарламаның ескертуіне жауап ретінде ешқашан ештеңе жүктемеңіз. Вирустармен зақымдалу мүмкіндігі аса үлкен болады.

БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУДІ ҮНЕМІ ЖАҢАРТЫҢЫЗ

Киберқылмыскерлер осалдықтарды бағдарламалық қамтамасыз етуде пайдалану әрекеттерін жасауда тапқырлық танытады. Сол себепті:

- Барлық Сіздің бағдарламалық қамтамасыз етуге – вирусқа қарсы және тыңшылыққа қарсы бағдарламаларға, операциялық жүйелерге, мәтіндерді өңдеу бағдарламалары мен өзге де бағдарламаларға арналған жаңартуларды үнемі орнату;
- Қол жетімді болса, бағдарламалық қамтамасыз етуді автоматты түрде жаңарту функцияларын қосу;
- Сіз пайдаланбайтын бағдарламалық қамтамасыз етуді жою қажет.

СЕНІМДІ ПАРОЛЬДЕРДІ ПАЙДАЛАНЫП, ОЛАРДЫ ҚҰПИЯ САҚТАҢЫЗ

- Сенімді парольдер кем дегенде 8 символдан құрылып, әріптерден, сандар мен символдардан тұратын тіркестерді қамтуға тиіс.
- Өз паролыңізді ешкімге ашпаңыз.
- Барлық сайттарда бірдей парольді қолданбаңыз. Оны ұрлаған болса, барлық ақпаратқа қауіп-қатер төнеді.
- Маршрутизаторға арналған түрлі сенімді парольдер мен сымсыз қосу кілтін үйде құрыңыз. Оны қалай істеуге болатындығын маршрутизаторды ұсынушы

БРАНДМАУЭРДІ ЕШҚАШАН АЖЫРАТПАҢЫЗ

Брандмауэр Сіздің компьютер мен Интернеттің арасында қорғау қалғанын құрайды. Брандмауэрді бір минутқа болсын ажырату ДК зиянды бағдарламамен зияндау тәуекелін жоғарылатады.

ФЛЕШ-ЖИНАҚТАҒЫШТАРДЫ ПАЙДАЛАНҒАНДА АБАЙ БОЛЫҢЫЗ

Компьютерді зиянды БҚ зақымдау мүмкіндігін барынша төмендетіңіз:

- Өз компьютеріңізге белгісіз флеш-жинақтағыштарды (немесе USB-жинақтағыштарды) қоспаңыз.
- Жинақтағышты компьютерге қосқан кезде SHIFT клавишасын басыңыз. Егер Сіз оны істеуді ұмытсаңыз, флеш-жинақтағыштың қалқымалы бос терезелерін жабу үшін жоғарғы оң жақ бұрыштағы X басыңыз.
- Жинақтағыштағы белгісіз файлдарды ашпаңыз.

ЗИЯНДЫ БҚ ҰСЫНАТЫН ЖҮКТЕМЕГЕ КЕЛІСІМ БЕРМЕҢІЗ

- Жіберушіні білсеңіз де – электрондық поштадағы, шұғыл хабарламалардағы немесе әлеуметтік желілердегі жарияланымдардағы файлдарды ашқан немесе сілтемелерді басқан кезде өте ұқыпты болыңыз. Жолдасыңыз жіберген болса, оған телефон шалып ол жібергеніне көз жеткізіңіз; жоқ болса, шұғыл хабарламалармен алмасу қызметінің терезесін жойыңыз немесе жабыңыз.
- Баннер жарнамасындағы, кенеттен қалқып шығатын терезелердегі немесе ескертулердегі, заңды емес деп көрінетін сайттардағы немесе тыңшылық БҚ не вирустарды жою ұсыныстарындағы «Келісемін», «ОК» және «Мен қабылдаймын» деген түймелерді баспаңыз.
- Пернетақтада CTRL + F4 басыңыз.
- Егер терезе жабылмаса, браузерді жабу үшін пернетақтада Alt + F4 басыңыз.
- Қажет болса, барлық қосымша парақтарды жабыңыз және браузерді келесі жолы қосуға арналған қосымша парақтарды сақтамаңыз.
- Бағдарламалық қамтамасыз етуді тек өзіңіз сенетін сайттарда ғана жүктеңіз.
- Тегін бағдарламалық қамтамасыз ету – әсіресе тегін вирусқа қарсы БҚ ұсынылатын электрондық пошта хабарламаларындағы сілтемелер бойынша кірмеңіз және веб-сайттардан аулақ болыңыз. Музыканы, ойындарды, видео мен басқаларды «тегін» жүктеулерден сақтаныңыз. Оларды жүктеген кезде зиянды БҚ болуы мүмкін.

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ БОЙЫНША ҰСЫНЫМДАР

Құпиясөз (пароль) саясаты

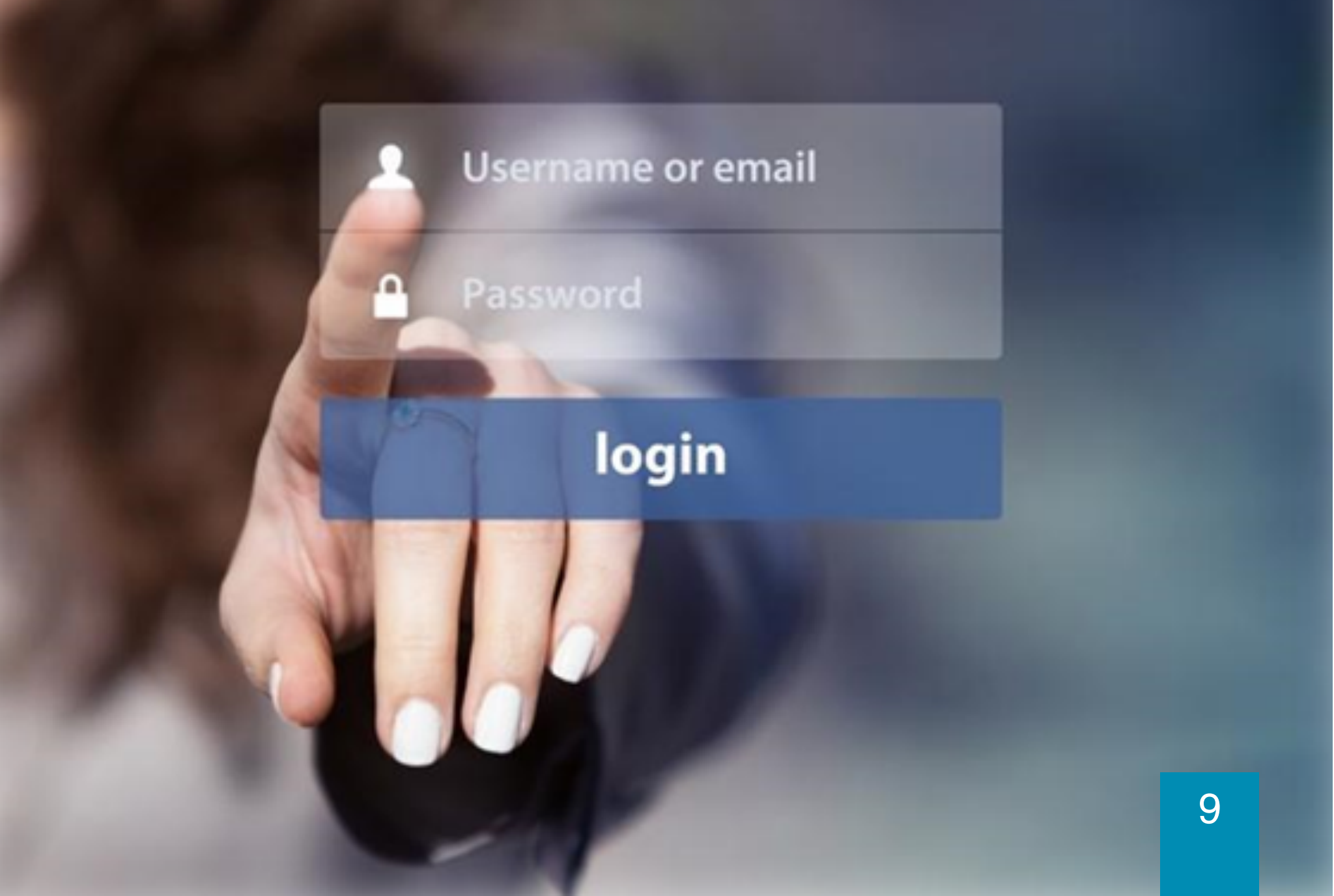
1. Құпиясөздерді жұмыс орнында электрондық түрде сақтамау, жазылған құпиясөздерді көпшілікке қолжетімді орындарда сақтамау, құпиясөздерді үшінші тұлғаға айтпау.

2. Өндірістік қажеттілік жағдайында құпиясөздің мәнін ашуға жол беріледі, одан кейін құпиясөзді МІНДЕТТІ ТҮРДЕ ауыстыру керек.

3. Құпиясөздер кемінде 8 символдан болуы тиіс және тоқсан сайын жаңартылып отыру тиіс.

Электрондық цифрлық қолтаңба

ЭЦҚ-ны компьютерде сақтауға болмайды.



КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ БОЙЫНША ҰСЫНЫМДАР

Пошта

1. Бейтаныс адамдардан келген электрондық хаттамалар мен күмәнді жүктемелерді, әсіресе егер ол мұрағаттар немесе атқарылатын файлдар (.exe) болса ашпау. Егер Сіз хатты маңызды деп санасаңыз, онда жолдаушылармен телефон арқылы байланысу қажет және хаттың тақырыбы мен жолдау себебін нақтылап алу керек.

2. Электрондық пошта арқылы кез келген күмәнді өтінімге адресаттан өтінімді растау үшін балама байланыс арнасын (мысалы, телефон) пайдалану керек.

3. Жолдаушы мен алушының адресінің дұрыс жазылуын үнемі тексеріп отыру қажет (тіпті күн сайын хат алмасатын адамдардың да).

4. Мемлекеттік органдар мен жергілікті атқару органдарының қызметшілері өз міндеттерін орындау мақсатында қызметтік жазысу барысында ведомстволық электрондық поштаны ғана пайдалануы тиіс.

Вирусқа қарсы бағдарламалық қамтамасыз ету

1. ЛИЦЕНЗИЯЛЫҚ вирусқа қарсы бағдарламалық қамтамасыз етуді пайдалану қажет. Вирусқа қарсы базаларды жаңарту тәулігіне кемінде 1 рет жүргізілуі тиіс.

2. Кез келген тасығышты компьютеріңізге қосу барысында вирусқа міндетті түрде тексеру қажет.

3. Электрондық поштадағы кіріс барлық файлдарға вирусті автоматты тексеруді баптау арқылы тексеріс жүргізу керек.

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ БОЙЫНША ҰСЫНЫМДАР

Интернет және әлеуметтік желілер

1. Интернет желілеріне қосылуды Интернетке қолжетімділіктің бірыңғай шлюзі арқылы ғана жүзеге асыру қажет.
2. Компьютерді МО БКО[1] Интернет желісіне қосуға тыйым салынады. Әр желіге жеке компьютерлерді пайдалану қажет.
3. МО БКО-ға, МО-ның жергілікті тораптарына сымсыз желілер, сымсыз кіру, модемдер, радиомодемдер, ұялы байланыс операторларының желі модемдері, ұялы байланыстың абоненттік құрылғылары және өзге де сымсыз желілік құрылғылар арқылы қосылуға тыйым салынады.
4. Бейтаныс жолдаушыдан электрондық пошта арқылы алынған бағдарламаны іске қосуға және сілтемелер бойынша өтуге тыйым салынады.
5. Лаңкестік, экстремистік, конституцияға қарсы және өзге де деструктивті бағыттағы материалдары бар веб-сайттарға кіруге тыйым салынады.
6. Күмәнді және зиян келтіретін сайттарға, сондай-ақ ақпараты функционалдық міндеттерді орындаумен байланысты емес сайттарға кіруге тыйым салынады.
7. Мәнін түсінбейтін сайттарға кіру кезінде келісімді қабылдауға тыйым салынады.
8. Жергілікті торапқа кіру құпиясөзін тіркеу талап етілетін басқа бағдарламалар мен сайттарға пайдалануға тыйым салынады.
9. Интернет ресурстары мен электрондық поштамен жұмыс жасау барысында қызметшілерге жұмыс қажеттілігіне орай немесе өзгеше жолмен белгілі болған мемлекеттік, қызметтік және коммерциялық ақпараттарды жария етуге тыйым салынады.
10. Cookie файлдарын пайдаланудан туындауы мүмкін қауіп-қатерлерді болдырмау үшін олардағы құнды, құпия ақпараттардың барын анықтау үшін жиі жиі сараптап тұруға кеңес беріледі.

---

[1]**Мемлекеттік органдардың бірыңғай көліктік ортасы (бұдан әрі – МО БКО) – «электрондық үкіметтің» ақпараттық-коммуникациялық инфрақұрылымына кіретін және ақпараттық қауіпсіздіктің талап етілетін деңгейін сақтай отырып, мемлекеттік органдардың, олардың ведомстволық бағынысты ұйымдары мен жергілікті өзін-өзі басқару органдарының, сондай-ақ уәкілетті орган айқындаған өзге де ақпараттандыру субъектілерінің оқшауланған (Интернетке қолжетімділігі бар жергілікті желілерді қоспағанда), ведомстволық**

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ БОЙЫНША ҰСЫНЫМДАР

Әлеуметтік инженерия

1. МО БКО мен Интернет-желілеріне қосылған компьютерлерді қараусыз ашық күйде қалдыруға тыйым салынады. Жұмыс орнын міндетті тәртіпте қалдыру жағдайында компьютерді бұғаттау (компьютерді бұғаттаудың жылдам әдісі – Windows+L клавишін басу) қажет.

2. Үшінші тұлғаға IP-адрестер мен логин және құпиясөзді айтуға тыйым салынады.

3. Жеке бағдарламалық қамтамасыз етуді орнатуға және лицензиясы немесе лауазымдық міндеттеріңізді орындауға қатысы жоқ бағдарламалық қамтамасыз етуді іске қосуға тыйым салынады.

Кез келген әдеттен тыс жағдайлар орын алған немесе киберқауіпсіздіктің бұзылуына күдік келтірілген жағдайда МО-ның ақпараттық қауіпсіздік жөніндегі жауапты мамандарына және Компьютерлік оқиғаларға жауап қату қызметіне +7 (7172) 55-99-97 телефон нөмірі, info@kz-cert.kz адресі арқылы жүгіну қажет.

НОРМАТИВТІК ЖӘНЕ ҚҰҚЫҚТЫҚ АКТІЛЕР

«Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы Қазақстан Республикасының аумағында, ақпараттандыру объектілерін құру, дамыту және пайдалану кезінде, сондай-ақ ақпараттық-коммуникациялық технологиялар саласын дамытуды мемлекеттік қолдау кезінде мемлекеттік органдар, жеке және заңды тұлғалар арасында туындайтын ақпараттандыру саласындағы қоғамдық қатынастарды реттейді. 2017 жылғы 28 желтоқсандағы № 128-VI Қазақстан Республикасының Заңына сәйкес өзгерістер мен толықтырулар енгізілді.

«Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды реттейді. Ақпараттық коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы талаптарды айқындайды.

Киберқауіпсіздік тұжырымдамасы (Қазақстанның киберқалқаны) Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына енуі бойынша «Қазақстан-2050» Стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді. Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын белгілейді.

ҚР Қорғаныс және аэроғарыш өнеркәсібі министрілігі және «Орталық Азия киберқауіпсіздік кәсіпқойлар қоғамы» ҚҰ-ның қатысуымен әзірленді.