Спросите себя:

#1 Вы уверены, что Ваш брандмауэр активирован и защищает Ваши данные?

#2 Кто имеет доступ к конфиденциальным данным из внутренней сети или удаленно?

#3 Вы точно знаете, какие службы Вашей сети доступны через Интернет?

#4 Вам действительно известно каждое устройство Вашей сети, которое имеет внешний IP-адрес?

#5 Когда Вы в последний раз делали оценку риска или внешний тест на проникновение?

#6 Может ли злоумышленник проникнуть в Вашу сеть?

KZ-CERT

incident@kz-cert.kz

При подозрении на заражение вредоносным программным обеспечением обращайтесь в Службу реагирования на компьютерные инциденты по бесплатному единому короткому номеру **1400,**
+7 7172 559997, либо по электронной почте **incident@kz-cert.kz**

Нормативно-правовые акты:

- Закон РК «**Об информатизации**»;
- Закон РК «**О связи**»;
- Закон РК «**О национальной безопасности**»;

- **Единые требования** в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

- **Национальный антикризисный план** реагирования на инциденты информационной безопасности;

- **Правила и критерии отнесения** объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры;

- **Правила обмена информацией**, необходимой для обеспечения информационной безопасности между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности;

- **Правила проведения мониторинга** обеспечения **информационной безопасности** объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры;

- **Правила передачи резервных копий** электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов;

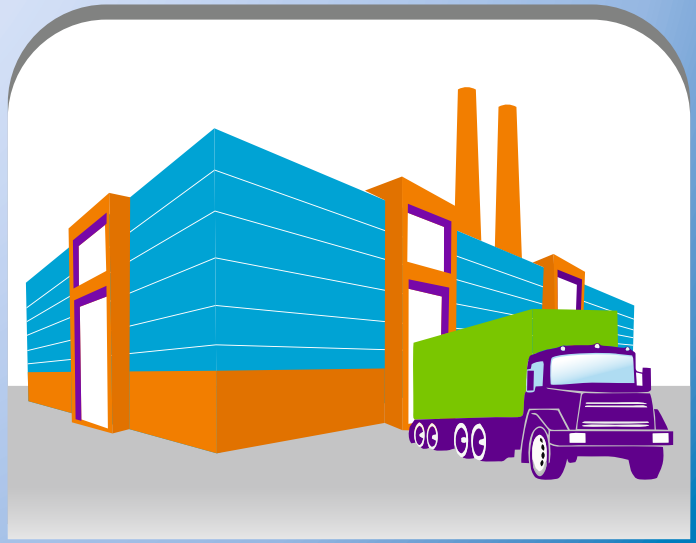
- **Профили защиты и методика** разработки профилей защиты;

- **Методика и Правила проведения испытаний** сервисного программного продукта, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности

Министерство оборонной и аэрокосмической промышленности Республики Казахстан
Комитет по информационной безопасности
г. Астана, пр. Мәңгілік ел 8, «Дом министерств», 1 подъезд тел.+77172749980, kib@mdai.gov.kz
www.mdai.gov.kz

Министерство оборонной и аэрокосмической промышленности Республики Казахстан
Комитет по информационной безопасности

Обеспечение информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры



ОПРЕДЕЛЕНИЯ

критически важные объекты информационно коммуникационной инфраструктуры – объекты информационно-коммуникационной инфраструктуры в сфере государственных услуг, связи и информатизации, транспорта, энергетики, космоса, металлургии, а также в нефтегазовой сфере.

оперативный центр информационной безопасности – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.

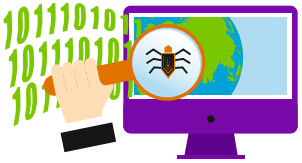
служба реагирования на инциденты информационной безопасности – юридическое лицо или структурное подразделение юридического лица, обеспечивающее анализ информации о событиях информационной безопасности в целях оказания консультативного и технического содействия в устранении последствий инцидентов информационной безопасности.

инцидент информационной безопасности – отдельно или серийно возникающие сбой в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов.

внутренний аудит информационной безопасности – объективный, документированный процесс контроля качественных и количественных характеристик текущего состояния информационной безопасности объектов информатизации в организации, осуществляемый самой организацией в своих интересах.

ОБЯЗАННОСТИ

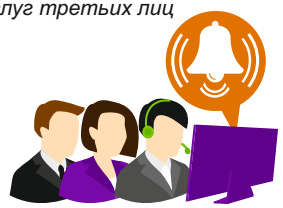
исполнение Единых требований в области ИКТ и обеспечения ИБ



осуществление мониторинга обеспечения ИБ объектов информатизации

обеспечение подключения систем мониторинга обеспечения ИБ к техническим средствам системы мониторинга обеспечения ИБ НКЦИБ.

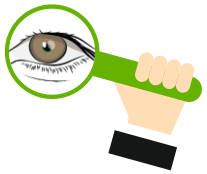
**осуществляется собственным подразделением или приобретением услуг третьих лиц*



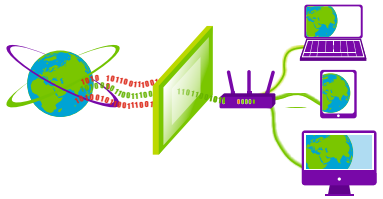
оповещение KZ-CERT об инцидентах ИБ

проведение **испытание/аттестации** на соответствие требованиям ИБ

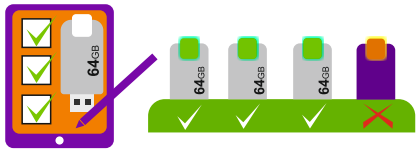
РЕКОМЕНДАЦИИ



проводите мероприятия по **оценке уровня защищенности** инфраструктуры



используйте **межсетевые экраны** для организации политики безопасности сети



организуйте **учет съемных носителей** информации

регулярно осуществляйте **резервное копирование** информации

проводите мероприятия по **осведомленности сотрудников** об угрозах информационной безопасности

Өзіңізден сұраңыз:

#1 Сіз брандмауэріңіз іске қосылған және Сіздің деректеріңізді қорғап тұрғанына сенімдісіз бе?

#2 Құпия деректерге ішкі желіден немесе қашықтықтан кім қатынай алады?

#3 Интернет арқылы Сіздің желіңіздің қандай қызметтері қолжетімді екенін нақты білесіз бе?

#4 Сізге желіңіздің сыртқы IP-мекен-жайы бар, әрбір құрылғысы шынымен де белгілі ме?

#5 Сіз қашан соңғы рет тәуекел бағасын немесе заңсыз енуге сыртқы тест жасадыңыз?

#6 Сіздің желіңізге теріс пиғылды адам кіре ала ма?

KZ-CERT
incident@kz-cert.kz

Зиянды бағдарламалық қамтылымды жұқтыру қаупі кезінде компьютерлік оқыс оқиғаларға ден қою қызметіне бірыңғай тегін қысқа **1400**,
+7 7172 559997 нөмірлері бойынша немесе **incident@kz-cert.kz** электронды поштасына хабарласыңыз.

Нормативтік-құқықтық актілер:

- «**Ақпараттандыру туралы**» ҚР Заңы;
- «**Байланыс туралы**» ҚР Заңы;
- «**Ұлттық қауіпсіздік туралы**» ҚР Заңы;

- Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы **бірыңғай талаптар**;
- Ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қоюдың **дағдарысқа қарсы ұлттық жоспары**;
- Ақпараттық-коммуникациялық инфрақұрылым объектілерін ақпараттық - коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызу **қағидалары мен өлшемшарттары**;
- Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасындағы ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті **ақпарат алмасу қағидалары**;
- «Электрондық үкіметтің» ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің **ақпараттық қауіпсіздігін** қамтамасыз етуге **мониторинг жүргізу қағидалары**;
- Электрондық ақпараттық ресурстардың **резервтік көшірмелерін** электрондық ақпараттық ресурстарды резервтік сақтаудың бірыңғай платформасына **беру қағидалары**;
- **Қорғау бейіндерін** және қорғау бейіндерін әзірлеу **әдістемесі**;
- Сервистік бағдарламалық өнімге, «электрондық үкіметтің» ақпараттық - коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне **сынақтар жүргізу әдістемесі мен қағидалары.**

Қазақстан Республикасының
Қорғаныс және аэроғарыш өнеркәсібі министрлігі

Ақпараттық қауіпсіздік комитеті

Астана қ., Мәңгілік ел даңғылы 8-үй, «Министрліктер үйі» ғимараты, 1-кіреберіс, тел.+77172749980, kib@mdai.gov.kz
www.mdai.gov.kz

Қазақстан Республикасының
Қорғаныс және аэроғарыш өнеркәсібі министрлігі

Ақпараттық қауіпсіздік комитеті

Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерін ақпараттық қауіпсіздікпен қамтамасыз ету

АНЫҚТАМАЛАР

ақпараттық – коммуникациялық инфрақұрылымның аса маңызды объектілері – мемлекеттік көрсетілетін қызмет, байланыс және ақпараттандыру, көлік, энергетика, ғарыш, металлургия, сондай-ақ мұнай-газ саласындағы ақпараттық-коммуникациялық инфрақұрылымның объектілері.

ақпараттық қауіпсіздіктің жедел орталығы – электрондық ақпараттық ресурстарды, ақпараттық жүйелерді, телекоммуникация желілері мен ақпараттандырудың басқа да объектілерін қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі.

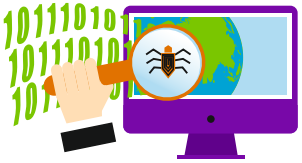
ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою қызметі – ақпараттық қауіпсіздіктің оқыс оқиғаларының салдарын жоюға консультациялық және техникалық жәрдем көрсету мақсатында ақпараттық қауіпсіздік оқиғалары туралы ақпаратты талдауды қамтамасыз ететін заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі.

ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жекелей немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қатер төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшірмесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер.

ішкі ақпараттық қауіпсіздік аудиті – ұйым өзі, өз мүдделерінде жүзеге асыратын ұйымдағы ақпараттандыру объектілерінің ақпараттық қауіпсіздігінің ағымдағы жай-күйінің сапалық және сандық сипаттамаларын бақылаудың әділ, құжатталған процесі.

МІНДЕТТЕР

АКТ және АҚ қамтамасыз ету саласындағы бірыңғай талаптарды **орындау**



Ақпараттандыру объектілерін АҚ-ты қамтамасыз етуді **мониторингілеуді жүзеге асыру**

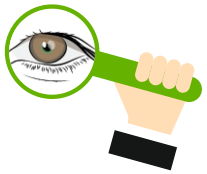
АҚҰҰО АҚ қамтамасыз етуді мониторингілеу жүйесінің техникалық құралдарына АҚ-ты қамтамасыз ету мониторингілеу жүйесіне **қосылуын қамтамасыз ету**

**меншікті бөлімшемен немесе үшінші тұлғаларға көрсетілетін қызметті сатып алумен жүзеге асырылады*

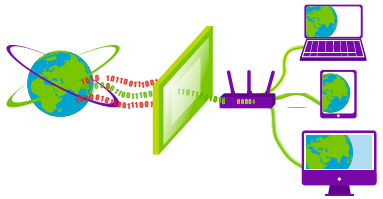
АҚ оқыс оқиғалары туралы KZ-CERT **хабардар ету**

АҚ талаптарына сәйкестікке **сынақ/аттестация** өткізу

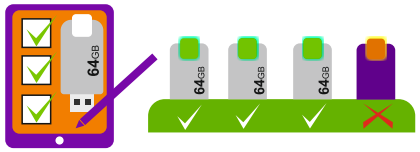
ҰСЫНЫМДАР



инфрақұрылымның **қорғаныс деңгейін бағалау жөнінде** іс-шара өткізіңіз



желінің қауіпсіздік саясатын ұйымдастыру үшін **желіаралық экрандарды** қолданыңыз



ақпараттың **алмалы тасығыштың есебін** ұйымдастырыңыз

ақпараттың **резервтік көшірмесін** ұдайы жүзеге асырыңыз

ақпараттық қауіпсіздік қауіптері туралы **қызметкерлердің хабардар болуы** болу жөнінде іс-шаралар өткізіңіз