



БҰЙРЫҚ

«02» 09 2026 ж.
Астана қаласы

ПРИКАЗ

№ 06-01/104
города Астана

Астана қаласы әкімдігінің «Шарапат»
әлеуметтік қызмет көрсету орталығы» МКҚК
ақпараттық қауіпсіздік бойынша
инциденттерге әрекет ету регламентін бекіту туралы

Ақпараттық қауіпсіздікті қамтамасыз ету, ақпараттық ресурстар мен дербес деректерді қорғау мақсатында **БҰЙЫРАМЫН:**

1. Осы бұйрыққа қосымшаға сәйкес Астана қаласы әкімдігінің «Шарапат» әлеуметтік қызмет көрсету орталығы» МКҚК ақпараттық қауіпсіздік бойынша инциденттерге әрекет ету Регламенті бекітілсін.

2. Комплаенс-офицер осы бұйрықты кәсіпорынның ресми сайтында орналастырсын және кәсіпорын қызметкерлерін жоғарыда көрсетілген ішкі нормативтік құжатпен таныстырсын.

3. Осы бұйрықтың орындалуын бақылауды өзіме қалдырамын.

Директордың м. а.

Н. Нұрадинов



Н. Нұрадинов

Приказ N 06-01/104
от 02.09.2026г

**Об утверждении Регламента реагирования на инциденты
по информационной безопасности
в ГККП «Центр социального обслуживания «Шарапат»
акимата г.Астаны»**

В целях обеспечения информационной безопасности, защиты информационных ресурсов и персональных данных **ПРИКАЗЫВАЮ:**

1. Утвердить Регламент реагирования на инциденты по информационной безопасности в ГККП «Центр социального обслуживания «Шарапат» акимата г.Астаны» согласно приложению к настоящему приказу.
2. Комплаенс-офицеру разместить данный приказ на официальном сайте Предприятия и ознакомить с вышеуказанным внутренним нормативным документом работников Предприятия.
3. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. директора

Н. Нурадинов



Н. Нурадинов

Приложение к приказу
№ _____
от «__» _____ 2026г

РЕГЛАМЕНТ

реагирования на инциденты информационной безопасности в в ГККП «Центр социального обслуживания «Шарапат» акимата г.Астаны»

Настоящий регламент реагирования на инциденты информационной безопасности (далее - Регламент) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности в ГККП «Центр социального обслуживания «Шарапат» акимата г.Астаны» (далее - Предприятие) при выявлении инцидента информационной безопасности, а также порядок проведения расследования инцидента информационной безопасности.

1.Основные положения

Инцидент информационной безопасности - это одно или серия событий, которое привело к уничтожению, модификации, копированию, распространению (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах Предприятия, а также блокировке доступа к ней.

Инциденты могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или отдельных события) и вызваны как техническими, так и нетехническими средствами.

Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение принятых организационно-распорядительных документов по защите информации или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к информационной безопасности.

2.Выявление инцидента

Основными источниками, от которых ответственное лицо по информационной безопасности может получить сведения об инцидентах информационной безопасности, являются:

- сообщения от работников Предприятия о выявленных фактах нарушения информационной безопасности;
- результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);

- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем и средств защиты информации.

Ответственное лицо по информационной безопасности должен регулярно информировать работников о необходимости немедленного его оповещения о возникновении инцидента с указанием контактной информации и способов предоставления информации.

3. Порядок действий при обнаружении инцидента информационной безопасности

Ответственное лицо по информационной безопасности с момента получения информации о предполагаемом инциденте информационной безопасности незамедлительно проводит первоначальный анализ полученных данных.

В случае если инцидент привел к негативным последствиям, в связи с уничтожением, модификацией, копированием, распространением информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах, а также блокировке доступа к ней, удаление файлов с информацией, имеющей резервные копии, ответственное лицо по информационной безопасности информирует руководство Предприятия для проведения служебного расследования на инциденты информационной безопасности.

Служебное расследование представляет собой получение (сбор) необходимой информации об инциденте, доказательств факта возникновения инцидента, определение обстоятельств (деталей), способствовавших совершению инцидента, в целях определения причин возникновения инцидента, виновных лиц и меры ответственности за нарушение безопасности информации.

По результатам расследования комиссия по служебному расследованию составляет заключение по расследованию инцидента, согласовывает его со всеми членами комиссии и передает руководству Предприятия для решения вопроса о привлечении виновного в инциденте к ответственности.

В служебном расследовании указывается следующая информация:

1. Дата и время совершения инцидента.
2. Источник информации, от которого ответственное лицо по информационной безопасности получил информацию об инциденте.
3. Ф.И.О. и должность лица, по вине которого произошел инцидент.
4. Описание инцидента.
5. Причины инцидента.
6. Меры, принятые для устранения причин, последствий инцидента.
7. Выработка корректирующих мероприятий.

По результатам служебного расследования принимаются меры о необходимости принятия дополнительных организационных и технических мер, направленных на предотвращение или минимизацию рисков возникновения подобных нарушений.

4. Ответственность

Каждый работник Предприятия несет персональную дисциплинарную, административную или уголовную ответственность за действия либо бездействия, повлекшие неправомерное уничтожение, блокирование, модификацию либо копирование информации, в соответствии с действующим законодательством.

Бұйрыққа қосымша

№ _____

« _____ » _____ 2026ж

РЕГЛАМЕНТ

ақпараттық қауіпсіздік инциденттеріне ден қою Астана қаласы әкімдігінің «Шарапат» әлеуметтік қызмет көрсету орталығы» МКҚК

Осы ақпараттық қауіпсіздік инциденттеріне ден қою регламенті (бұдан әрі - Регламент) ақпараттық қауіпсіздік инциденті анықталған кезде «Астана қаласы әкімдігінің Шарапат» әлеуметтік қызмет көрсету орталығы» МКҚК (бұдан әрі-кәсіпорын) ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың іс-қимыл тәртібін, сондай-ақ ақпараттық қауіпсіздік инцидентіне тергеп-тексеру жүргізу тәртібін белгілейді.

1.Негізгі ережелер

Ақпараттық қауіпсіздік оқиғасы-бұл кәсіпорынның автоматтандырылған жұмыс орындарында және (немесе) серверлерінде өңделетін ақпараттың жойылуына, өзгертілуіне, көшірілуіне, таралуына (тек қол жетімділігі шектеулі ақпаратқа қатысты), сондай-ақ оған қол жеткізуді бұғаттауға әкеп соқтырған оқиғалардың бірі немесе сериясы.

Оқиғалар қасақана немесе кездейсоқ болуы мүмкін (мысалы, кез-келген адам қателігінің немесе жекелеген оқиғалардың салдары) және техникалық және техникалық емес құралдардан туындауы мүмкін.

Ақпараттық қауіпсіздік оқиғасы-ақпаратты қорғау бойынша қабылданған ұйымдық-өкімдік құжаттардың бұзылуын немесе қорғау шараларынан бас тартуды немесе ақпараттық қауіпсіздікке қатысы болуы мүмкін бұрын белгісіз жағдайдың туындауын көрсететін жүйенің, сервистің немесе желінің белгілі бір жай-күйінің сәйкестендірілген пайда болуы.

2.Оқиғаны анықтау

Ақпараттық қауіпсіздік жөніндегі жауапты тұлға Ақпараттық қауіпсіздік оқиғалары туралы мәліметтер ала алатын негізгі көздер:

- кәсіпорын қызметкерлерінен ақпараттық қауіпсіздікті бұзудың анықталған фактілері туралы хабарламалар;

- ақпараттық қауіпсіздік мониторингі құралдарының жұмыс нәтижелері, тексеру және аудит нәтижелері (ішкі немесе сыртқы);

- серверлер мен жұмыс станцияларының операциялық жүйелерінің, антивирустық жүйенің, резервтік көшіру жүйесінің және ақпаратты қорғаудың басқа жүйелері мен құралдарының журналдары мен ескертулері.

Ақпараттық қауіпсіздік жөніндегі жауапты тұлға байланыс ақпаратын және ақпарат беру тәсілдерін көрсете отырып, инциденттің туындағаны туралы оны дереу хабардар ету қажеттігі туралы қызметкерлерді ұдайы хабардар етуге тиіс.

3. Оқиға анықталған кездегі іс-қимыл тәртібі
ақпараттық қауіпсіздік

Ақпараттық қауіпсіздік жөніндегі жауапты тұлға ақпараттық қауіпсіздіктің болжамды оқиғасы туралы ақпаратты алған сәттен бастап алынған деректерге алғашқы талдауды дереу жүргізеді.

Егер оқиға автоматтандырылған жұмыс орындарында және (немесе) серверлерде өңделетін ақпаратты жоюға, модификациялауға, көшіруге, таратуға, сондай-ақ оған қол жеткізуді бұғаттауға байланысты жағымсыз салдарға әкеп соққан жағдайда, резервтік көшірмесі бар ақпараты бар файлдарды жою, Ақпараттық қауіпсіздік жөніндегі жауапты тұлға қызметтік тергеу жүргізу үшін кәсіпорын басшылығына хабарлайды ақпараттық қауіпсіздік оқиғаларына.

Қызметтік тергеп-тексеру инцидент туралы қажетті ақпаратты, инциденттің туындау фактісінің дәлелдемелерін алуды (жинауды), инциденттің туындау себептерін, кінәлі тұлғаларды айқындау мақсатында инцидент жасауға ықпал еткен мән-жайларды (бөлшектерді) айқындауды және ақпарат қауіпсіздігін бұзғаны үшін жауапкершілік шараларын білдіреді.

Тергеп-тексеру нәтижелері бойынша қызметтік тергеп-тексеру жөніндегі комиссия инцидентті тергеп-тексеру жөніндегі қорытындыны жасайды, оны Комиссияның барлық мүшелерімен келіседі және инцидентке кінәлі адамды жауапқа тарту туралы мәселені шешу үшін кәсіпорын басшылығына береді.

Қызметтік тергеуде мынадай ақпарат көрсетіледі:

1. Оқиғаның жасалған күні мен уақыты.
2. Ақпараттық қауіпсіздік жөніндегі жауапты тұлға оқиға туралы ақпарат алған ақпарат көзі.
3. Оқиға болған адамның Т.А. Ә. және лауазымы.
4. Оқиғаның сипаттамасы.
5. Оқиғаның себептері.
6. Оқиғаның себептерін, салдарын жою үшін қабылданған шаралар.
- 7.Түзету шараларын әзірлеу.

Қызметтік тергеп-тексеру нәтижелері бойынша осындай бұзушылықтардың туындау тәуекелдерін болғызбауға немесе азайтуға бағытталған қосымша ұйымдастырушылық және техникалық шараларды қабылдау қажеттігі туралы шаралар қабылданады.

4. Жауапкершілік

Кәсіпорынның әрбір қызметкері қолданыстағы заңнамаға сәйкес ақпаратты заңсыз жоюға, бұғаттауға, модификациялауға немесе көшіруге әкеп соққан әрекеттер не әрекетсіздіктер үшін дербес тәртіптік, әкімшілік немесе қылмыстық жауаптылықта болады.