"ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЕҢБЕК ЖӘНЕ ХАЛЫҚТЫ ӘЛЕУМЕТТІК ҚОРҒАУ МИНИСТРЛІГІНІҢ ЕҢБЕКТІ ҚОРҒАУ ЖӨНІНДЕГІ РЕСПУБЛИКАЛЫҚ ҒЫЛЫМИ-ЗЕРТТЕУ ИНСТИТУТЫ" ШАРУАШЫЛЫҚ ЖҮРГІЗУ ҚҰҚЫҒЫНДАҒЫ РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК КӘСІПОРНЫ

РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ "РЕСПУБЛИКАНСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПО ОХРАНЕ ТРУДА МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ РЕСПУБЛИКИ КАЗАХСТАН"

БҰЙРЫҚ

ПРИКАЗ

2026ж. «18» тамыз
Астана қаласы

№ 01-3/113 ө/к
город Астана

Кейбір ішкі нормативтік құжаттарды бекіту туралы ақпараттық қауіпсіздік, сондай-ақ «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК-да талап-арыз жұмысын ұйымдастыру мәселелері бойынша

Ақпараттық қауіпсіздікті қамтамасыз ету, ақпараттық ресурстар мен дербес тдеректерді қорғау, сондай-ақ талап-арыз жұмысын ұйымдастыру мақсатында, сондай-ақ «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК Жарғысының 22-тармағының 6-тармақшасына сәйкес, **БҰЙЫРАМЫН:**

1. «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК Ақпараттық қауіпсіздік саясаты бекітілсін.
2. «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК Ақпараттық қауіпсіздік инциденттеріне ден қою регламенті бекітілсін.
3. Наразылық-талап жұмысын жүргізу тәртібі туралы ереже бекітілсін.
4. Комплаенс-офицер мен әкімшілік-бақылау жұмысы және цифрландыру бөлімі қызметкерлерді жоғарыда көрсетілген ішкі нормативтік құжатпен таныстырсын, «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК-ның интернет-ресурсында орналастырылуын қамтамасыз етсін.
5. Осы бұйрықтың орындалуын бақылауды өзіме қалдырамын.
6. Осы бұйрық қол қойылған сәттен бастап күшіне енеді.

Бас директордың м.а. **А. Бекмагамбетов**

004659

№ 01-3/113 и/л
от 18.08.2026г

Об утверждении некоторых внутренних нормативных документов по вопросам информационной безопасности, а также организации претензионно-исковой работы в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан»

В целях обеспечения информационной безопасности, защиты информационных ресурсов и персональных данных, а также организации претензионно-исковой работы, а также в соответствии с подпунктом 6 пункта 22 Устава РГП на ПХВ «Республиканского научно-исследовательскиого института по охране труда Министерства труда и социальной защиты населения Республики Казахстан», **ПРИКАЗЫВАЮ:**

1.Утвердить Политику информационной безопасности РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан».

2. Утвердить Регламент реагирования на инциденты информационной безопасности РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан».

3. Утвердить Положение о порядке проведения претензионно-исковой работы.

4. Комплаенс-офицеру и Отделу административно-контрольной работы и цифровизации ознакомить с вышеуказанным внутренним нормативным документом работников, обеспечить размещение на интернет-ресурсе РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан».

5. Контроль за исполнением настоящего приказа оставляю за собой.

6. Настоящий приказ вступает в силу с момента его подписания.

И.о. Генерального директора **А. Бекмагамбетов**

Согласовано:

Руководитель юридического отдела Ж.Ж. Уралбаева
И.о. Руководителя административного отдела Н.С. Бухаров
Комплаенс-офицер А. К. Мухамбетова

Приложение к приказу
№ 01-3/113 ч/т
от «18» 02 2026г

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан»

Настоящий регламент реагирования на инциденты информационной безопасности (далее - Регламент) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан» (далее - Институт) 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 Института, а также блокировке доступа к ней.

Инциденты могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или отдельных событий) 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 Института 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 должно 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 Института 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 Института 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 Института несет ответственность за действия либо бездействия, повлекшие неправомерное уничтожение, блокирование, модификацию либо копирование информации, в соответствии с действующим законодательством Республики Казахстан.

«18» 08 2026 г
№01-3/113 н/к
бұйрыққа қосымша

«Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК-дағы ақпараттық қауіпсіздік инциденттеріне ден қою

РЕГЛАМЕНТ

Осы ақпараттық қауіпсіздік инциденттеріне ден қою регламенті (бұдан әрі - Регламент) «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК-да ақпараттық қауіпсіздікті қамтамасыз етуге жауапты адамдардың іс-қимыл тәртібін белгілейді (бұдан әрі-Институт) ақпараттық қауіпсіздік инциденті анықталған кезде, сондай-ақ ақпараттық қауіпсіздік инцидентіне тергеу жүргізу тәртібі.

1.Негізгі ережелер

Ақпараттық қауіпсіздік оқиғасы-бұл институттың 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:

- Институт қызметкерлерінің ақпараттық қауіпсіздікті бұзудың анықталған фактілері туралы хабарламалары;
- ақпараттық қауіпсіздік мониторингі құралдарының жұмыс нәтижелері, тексеру және аудит нәтижелері (ішкі немесе сыртқы);

Приложение к приказу
№ 01-3/113 н/к
от «18» 08 2026г

Политика информационной безопасности
в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан»

г.Астана, 2026 г

1.Общие положения

Настоящая Политика информационной безопасности (далее - Политика) представляет собой организационный документ в области защиты информации в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан» (далее - Институт) и определяет общие направления обеспечения информационной безопасности.

Основной целью, на достижение которой направлены все положения настоящей Политики является защита информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Задачи обеспечения информационной безопасности сводятся к прогнозированию и предотвращению таких воздействий, а также к минимизации ущерба от их реализации.

Требования к безопасности, используемые процедуры и структура непосредственно влияют на цели и задачи, стоящие перед системой информационной безопасности.

2.Область применения

Настоящая Политика устанавливает процедуру управления процессами обеспечения информационной безопасности.

Требования настоящей Политики распространяются на все структурные подразделения, а также работников, имеющих доступ к информационным системам Института.

3.Определения и сокращения

В настоящей Политике применяются термины в соответствии с законами Республики Казахстан «Об информатизации», «Об электронном документе и электронно-цифровой подписи» и иного действующего законодательства, а также следующие термины с соответствующими определениями:

информация - сведения, находящиеся на электронном или бумажном носителях, при необходимости, удостоверяемые печатью, рукописной либо электронной цифровой подписью;

безопасность - состояние защищенности от внутренних и внешних условий, процессов и факторов, ставящих под угрозу ее устойчивое развитие и экономическую независимость;

информационная безопасность (ИБ) - состояние защищенности информационных ресурсов и интересов в информационной сфере;

информатизация - организационный, социально-экономический и научно-технический процесс, направленный на формирование и развитие

электронных информационных ресурсов, информационных систем на основе использования информационных технологий;

информационная система - аппаратно-программный комплекс, предназначенный для реализации информационных процессов;

информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, передачи, использования и распространения электронных информационных ресурсов с использованием информационных технологий;

информационные технологии (ИТ) - совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации;

администратор - к администраторам относятся уполномоченные работники, обеспечивающие функционирование соответствующих механизмов;

пользователь - работники, имеющие доступ к информационным ресурсам, обращающиеся к информационным системам за получением необходимых электронных информационных ресурсов и пользующиеся ими.

4.Общие положения

В настоящей Политике определяются принципы, цели, задачи и основные положения обеспечения информационной безопасности Института.

Настоящая Политика обеспечивает процессы информационной безопасности и ответственность за их выполнение, а также определяет развивающие ее процессы обеспечения информационной безопасности.

Принципы построения комплексной системы защиты:

законность – предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством Республики Казахстан;

системность – системный подход к построению системы защиты информации и предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

комплексность – комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

непрерывность защиты – непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем;

своевременность – предполагает упреждающий характер мер для обеспечения безопасности информации;

преемственность и совершенствование – предполагают постоянное совершенствование мер и средств защиты информации;

конфиденциальность, достоверность, разграничение ответственности и контроля.

Основной целью защиты информационных ресурсов и информационных систем является защита субъектов информационных отношений от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем, или несанкционированного доступа к циркулирующей в них информации и ее незаконного использования.

Основными задачами системы обеспечения безопасности информации являются:

обеспечение необходимой доступности информационных ресурсов в целях обеспечения непрерывности бизнеса;

обеспечение целостности информационных ресурсов в целях обеспечения требуемой поддержки деятельности в информационной сфере, включая задачи принятия решений;

обеспечение конфиденциальности информации, отнесенной к закрытым сведениям;

обеспечение достоверности и актуальности обрабатываемой информации;

утверждение единой корпоративной этики в вопросах информационной безопасности, поддерживающей осведомленность работников;

защиту законных прав и работников, в случаях неправомерного использования или злоупотребления информационными активами;

защиту от несанкционированных действий в процессах функционирования информационных систем;

разграничение прав доступа к информации, серверам и рабочим станциям, средствам защиты.

5. Распределение обязанностей за обеспечение ИБ

Ответственный за информационную безопасность:

-обеспечивает выбор и приобретение средств информационной безопасности Института и поддержки для них;

-контролирует сервер логов и постоянно мониторинг работы систем и подсистем;

-производит внутренний аудит структуры информационных систем и контролирует соблюдение политики информационной безопасности;

Пользователи обязаны придерживаться политики «чистого стола» в соответствии с категориями документов, с которыми они работают, и дополнительно – специальными мерами безопасности, предусмотренными

нормативной документацией для отдельных категорий документов и отдельных категорий пользователей.

6. Способ осуществления

Объектами информационной безопасности являются:

информационные ресурсы с ограниченным доступом, составляющие коммерческую или служебную тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления.

7. Безопасность системных файлов

Системными файлами рабочих станций и серверов являются исполняемые файлы, динамически загружаемые модули, конфигурационные файлы отдельных сервисов и реестра, а также временные файлы сервисов и файлы подкачки.

Для повышения безопасности системных файлов, помимо применения других методов обеспечения безопасности, описанных в нормативной документации, соответствующие системные администраторы обязаны:

- не устанавливать сервисы и приложения, не связанные с реально используемой функциональностью системы;
- не хранить предыдущие версии программных продуктов в той же системе.
- производить резервное копирование системных файлов перед установкой обновлений в систему. Следить за корректностью работы антивирусного программного обеспечения на сервере хранения патчей, сервис-паков и обновлений.

8. Безопасность носителей данных

Важные документы, принадлежащие Институту, должны иметь информационную защиту от утраты, повреждения и фальсификации. Некоторые документы должны храниться с соблюдением норм безопасности для того, чтобы обеспечить соответствие требованиям законов и нормативных актов, а также поддержать важные области деятельности.

Все криптографические ключи, относящиеся к зашифрованным архивам или цифровым подписям, должны храниться в секрете и при необходимости предоставляться авторизованным лицам.

9. Меры защиты информационных ресурсов и информационных систем

Безопасное функционирование должно основываться на своевременности обнаружения проблем в сфере информационной безопасности, выявлении причинно-следственных связей возможных проблем и создании на этой основе точного прогноза их развития.

Меры по физической защите информационно-технических ресурсов:

- элементы информационной системы, потенциально подверженные ущербу, размещаются в защищенных зонах;
- уровень защищенности зоны должен соответствовать потенциальным угрозам в отношении информационно-технических ресурсов внутри неё.

10. Данные, документация и программное обеспечение

Политика информационной безопасности запрещает несанкционированный доступ к информации, получаемой, разработанной, обрабатываемой, хранимой и передаваемой в информационных системах Института, ее раскрытие, передача, копирование, изменение, удаление, ненадлежащее использование, а также неправомерное обращение с носителями этой информации.

Каждый работник Института несет персональную ответственность за нарушения требований настоящей Политики.

«18» 08 2026 ж.
№ 01-3/113 ө/қ
бұйрыққа қосымша

«Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК
Ақпараттық қауіпсіздік саясаты

1.Жалпы ережелер

Осы ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми - зерттеу институты» ШЖҚ РМК-да (бұдан әрі-Институт) ақпаратты қорғау саласындағы ұйымдастыру құжатын білдіреді және ақпараттық қауіпсіздікті қамтамасыз етудің жалпы бағыттарын айқындайды.

Осы саясаттың барлық ережелері қол жеткізуге бағытталған негізгі мақсат ақпаратты және оны қолдайтын инфрақұрылымды ақпараттың өзіне, оның иелеріне немесе қолдаушы инфрақұрылымға зиян келтіруі мүмкін кез келген кездейсоқ немесе зиянды әсерлерден қорғау болып табылады.

Ақпараттық қауіпсіздікті қамтамасыз ету міндеттері мұндай әсерлерді болжауға және алдын алуға, сондай-ақ оларды іске асырудан болатын залалды азайтуға дейін азаяды.

Қауіпсіздік талаптары, қолданылатын процедуралар мен құрылым ақпараттық қауіпсіздік жүйесінің мақсаттары мен міндеттеріне тікелей әсер етеді.

2.Қолдану саласы

Осы Саясат ақпараттық қауіпсіздікті қамтамасыз ету процестерін басқару рәсімін белгілейді.

Осы Саясаттың таралу саласы Институт иесі болып табылатын автоматтандырылған және ақпараттық жүйелер мен ресурстар болып табылады.

Осы Саясаттың талаптары барлық құрылымдық бөлімшелерге, сондай-ақ институттың ақпараттық жүйелеріне қол жеткізе алатын қызметкерлерге қолданылады.

3.Анықтамалар мен қысқартулар

Осы Саясатта «Ақпараттандыру туралы», «Электрондық құжат және электрондық-цифрлық қолтаңба туралы» Қазақстан Республикасының заңдарына және өзге де қолданыстағы заңнамаға сәйкес терминдер, сондай-ақ тиісті анықтамалары бар мынадай терминдер қолданылады:

ақпарат-қажет болған жағдайда мөрмен, қолжазбамен немесе электрондық цифрлық қолтаңбамен куәландырылатын электрондық немесе қағаз жеткізгіштердегі мәліметтер;

қауіпсіздік-оның тұрақты дамуы мен экономикалық тәуелсіздігіне қауіп төндіретін ішкі және сыртқы жағдайлардан, процестерден және факторлардан қорғалу жағдайы;

ақпараттық қауіпсіздік (АҚ) - Ақпараттық ресурстар мен ақпараттық саладағы мүдделердің қорғалу жағдайы;

ақпараттандыру-ақпараттық технологияларды пайдалану негізінде электрондық ақпараттық ресурстарды, Ақпараттық жүйелерді қалыптастыруға және дамытуға бағытталған ұйымдастырушылық, әлеуметтік-экономикалық және ғылыми-техникалық процесс;

ақпараттық жүйе-ақпараттық процестерді іске асыруға арналған аппараттық-бағдарламалық кешен;

ақпараттық процестер-ақпараттық технологияларды пайдалана отырып, электрондық ақпараттық ресурстарды құру, жинау, өңдеу, жинақтау, сақтау, іздеу, беру, пайдалану және тарату процестері;

Ақпараттық технологиялар (ат) - ақпаратты жинауды, жасауды, сақтауды, жинақтауды, өңдеуді, іздеуді, шығаруды, көшіруді, беруді және таратуды қамтамасыз ететін технологиялық кешенге біріктірілген әдістердің, өндірістік процестердің және бағдарламалық-техникалық құралдардың жиынтығы;

әкімші-әкімшілерге тиісті тетіктердің жұмыс істеуін қамтамасыз ететін уәкілетті қызметкерлер жатады.

пайдаланушы-ақпараттық ресурстарға қолжетімділігі бар, қажетті электрондық ақпараттық ресурстарды алу үшін ақпараттық жүйелерге жүгінетін және оларды пайдаланатын қызметкерлер.

4.Жалпы ережелер

Осы Саясатта институттың ақпараттық қауіпсіздігін қамтамасыз етудің принциптері, мақсаттары, міндеттері мен негізгі ережелері айқындалады.

Осы Саясат ақпараттық қауіпсіздік процестерін және олардың орындалуына жауапкершілікті қамтамасыз етеді, сондай-ақ оны дамытатын ақпараттық қауіпсіздікті қамтамасыз ету процестерін айқындайды.

Осы саясат негізінде институттың ақпараттық қауіпсіздігін қамтамасыз ету процестері.

Кешенді қорғаныс жүйесін құру принциптері:

заңдылық-қорғау іс-шараларын жүзеге асыруды және Қазақстан Республикасының қолданыстағы заңнамасына сәйкес Ақпарат қауіпсіздігі жүйесін әзірлеуді көздейді;

жүйелілік-ақпаратты қорғау жүйесін құруға жүйелі көзқарас және ақпараттың қауіпсіздігін қамтамасыз ету мәселесін түсіну және шешу үшін маңызды барлық өзара байланысты, өзара әрекеттесетін және уақыт бойынша өзгеретін элементтерді, жағдайлар мен факторларды ескеруді көздейді;

кешенділік-компьютерлік жүйелерді қорғаудың әдістері мен құралдарын кешенді пайдалану қауіптерді іске асырудың барлық маңызды (маңызды) арналарын жабатын және оның жекелеген компоненттерінің түйіскен жерлерінде әлсіз жерлері жоқ тұтас қорғаныс жүйесін құру кезінде гетерогенді құралдарды келісілген қолдануды қамтиды.

қорғаудың үздіксіздігі-ақпараттық жүйелердің өмірлік циклінің барлық кезеңдерінде тиісті шаралар қабылдауды көздейтін үздіксіз, мақсатты процесс;

уақтылығы-ақпараттың қауіпсіздігін қамтамасыз ету шараларының белсенді сипатын болжайды;

сабақтастық және жетілдіру – ақпаратты қорғау шаралары мен құралдарын үнемі жетілдіруді көздейді;

құпиялылық, сенімділік, жауапкершілік пен бақылауды ажырату.

Ақпараттық ресурстар мен ақпараттық жүйелерді қорғаудың негізгі мақсаты ақпараттық қатынастар субъектілерін ақпараттық жүйелердің жұмыс істеу процесіне кездейсоқ немесе қасақана рұқсатсыз араласу немесе оларда айналымдағы ақпаратқа рұқсатсыз қол жеткізу және оны заңсыз пайдалану арқылы оларға материалдық, физикалық, моральдық немесе өзге де залал келтіруден қорғау болып табылады.

Ақпарат қауіпсіздігін қамтамасыз ету жүйесінің негізгі міндеттері:

ақпараттық ресурстардың қажетті қолжетімділігін қамтамасыз ету

бизнестің үздіксіздігін қамтамасыз ету мақсатында;

шешім қабылдау міндеттерін қоса алғанда, ақпараттық саладағы қызметті талап етілетін қолдауды қамтамасыз ету мақсатында ақпараттық ресурстардың тұтастығын қамтамасыз ету;

жабық мәліметтерге жатқызылған ақпараттың құпиялылығын қамтамасыз ету;

өңделетін ақпараттың дұрыстығы мен өзектілігін қамтамасыз ету;

қызметкерлердің хабардарлығын қолдайтын ақпараттық қауіпсіздік мәселелерінде бірыңғай корпоративтік этиканы бекіту;

ақпараттық активтерді заңсыз пайдалану немесе теріс пайдалану жағдайларында қызметкерлердің заңды құқықтары мен құқықтарын қорғау;

ақпараттық жүйелердің жұмыс істеу процестеріндегі рұқсат етілмеген әрекеттерден қорғау;

ақпаратқа, серверлерге және жұмыс станцияларына, қорғаныс құралдарына қол жеткізу құқықтарын ажырату.

5. АҚ қамтамасыз ету міндеттерін бөлу

Ақпараттық қауіпсіздікке жауаптылар:

- институттың ақпараттық қауіпсіздік құралдарын таңдауды және сатып алуды және оларға қолдау көрсетуді қамтамасыз етеді;

- лог серверін бақылайды және жүйелер мен ішкі жүйелердің жұмысын үнемі бақылайды;

- Ақпараттық жүйелер құрылымына ішкі аудит жүргізеді және ақпараттық қауіпсіздік саясатының сақталуын бақылайды;

Пайдаланушылар өздері жұмыс істейтін құжаттардың санаттарына сәйкес «таза үстел» саясатын және құжаттардың жекелеген санаттары мен пайдаланушылардың жекелеген санаттары үшін нормативтік құжаттамада көзделген қосымша – арнайы қауіпсіздік шараларын ұстануға міндетті.

6. Жүзеге асыру тәсілі

Ақпараттық қауіпсіздік объектілері:

коммерциялық немесе қызметтік құпияны құрайтын қолжетімділігі шектеулі ақпараттық ресурстар, кездейсоқ және санкцияланбаған әсерлерге және олардың қауіпсіздігінің бұзылуына қатысты өзге де сезімтал ақпараттық ресурстар, оның ішінде оларды ұсынудың нысаны мен түріне қарамастан құжаттар және ақпарат массивтері түрінде ұсынылған ашық (жалпыға қолжетімді) ақпарат.

7. Жүйелік файлдардың қауіпсіздігі

Жұмыс станциялары мен серверлердің жүйелік файлдары - орындалатын файлдар, динамикалық жүктелетін Модульдер, жеке қызметтер мен тізілімнің конфигурациялық файлдары, уақытша қызмет файлдары мен своп файлдары.

Жүйелік файлдардың қауіпсіздігін арттыру үшін, нормативтік құжаттамада сипатталған қауіпсіздікті қамтамасыз етудің басқа әдістерін қолданумен қатар, тиісті жүйелік әкімшілер:

- жүйенің нақты қолданылатын функционалдығына байланысты емес қызметтер мен қосымшаларды орнатпаңыз;
- бағдарламалық өнімдердің алдыңғы нұсқаларын сол жүйеде сақтамаңыз.

Жүйеге жаңартуларды орнатпас бұрын жүйелік файлдардың сақтық көшірмесін жасаңыз. Патчтарды, сервистік пакеттерді және жаңартуларды сақтау серверінде антивирустық бағдарламалық қамтамасыз етудің дұрыс жұмыс істеуін қадағалау.

8.Деректер тасымалдаушыларының қауіпсіздігі

Институтқа тиесілі маңызды құжаттардың жоғалудан, зақымданудан және бұрмаланудан ақпараттық қорғанысы болуы керек. Кейбір құжаттар заңдар мен ережелердің сәйкестігін қамтамасыз ету, сондай-ақ маңызды қызмет салаларын қолдау үшін қауіпсіздік ережелеріне сәйкес сақталуы керек.

Шифрланған мұрағаттарға немесе цифрлық қолтаңбаларға қатысты барлық криптографиялық кілттер құпия сақталуы және қажет болған жағдайда уәкілетті тұлғаларға ұсынылуы тиіс.

9.Ақпараттық ресурстар мен ақпараттық жүйелерді қорғау шаралары

Қауіпсіз жұмыс істеу Ақпараттық қауіпсіздік саласындағы проблемаларды уақтылы анықтауға, ықтимал проблемалардың себеп-салдарлық байланыстарын анықтауға және осы негізде олардың дамуының нақты болжамын жасауға негізделуі керек.

Ақпараттық-техникалық ресурстарды физикалық қорғау жөніндегі шаралар:

- зақымдануы ықтимал ақпараттық жүйенің элементтері қорғалған аймақтарда орналастырылады;

- аймақтың қорғалу деңгейі оның ішіндегі ақпараттық-техникалық ресурстарға қатысты ықтимал қатерлерге сәйкес келуі тиіс.

10. Деректер, құжаттама және бағдарламалық қамтамасыз ету

Ақпараттық қауіпсіздік саясаты институттың ақпараттық жүйелерінде алынған, әзірленген, өңделетін, сақталатын және берілетін ақпаратқа рұқсатсыз қол жеткізуге, оны ашуға, беруге, көшіруге, өзгертуге, жоюға, тиісінше пайдаланбауға, сондай-ақ осы ақпаратты тасымалдаушылармен заңсыз жұмыс істеуге тыйым салады.

Институттың әрбір қызметкері осы саясаттың талаптарын бұзғаны үшін дербес жауапты болады.

Приложение к приказу
от «18» 08 2026 года
№ 01-3/113 о/д

Положение
о порядке проведения
претензионно-исковой работы

1. Общие положения

1.1. Положение о порядке проведения претензионно-исковой работы в РГП на ПХВ «Республиканский научно-исследовательский институт по охране труда Министерства труда и социальной защиты населения Республики Казахстан» (далее – Институт) определяет единый порядок организации, ведения и контроля претензионной и исковой работы, взаимодействия юридического отдела со структурными подразделениями Института.

1.2. Настоящее Положение разработано в соответствии с законодательством Республики Казахстан, регулирующим гражданские, трудовые, административные процедурно-процессуальные и иные правоотношения.

1.3. Целью претензионно-исковой работы является защита имущественных и иных законных интересов Института, обеспечение договорных и иных правоотношений Института.

1.4. Основными задачами претензионно-исковой работы являются:

предупреждение и минимизация имущественных потерь и иных негативных последствий для Института;

своевременное выявление и устранение нарушений обязательств;

обеспечение надлежащего судебного представительства и защиты интересов Института.

1.5. Претензионно-исковая работа осуществляется на принципах законности, обоснованности заявляемых требований и возражений, своевременности, документальной подтвержденности, эффективности досудебного урегулирования и защиты интересов Института.

1.6. Структурные подразделения Института в пределах своей компетенции обеспечивают своевременное выявление нарушений, подготовку и представление в юридический отдел достоверных документов, расчетов, сведений и иных материалов, необходимых для претензионной и исковой работы.

1.7. Общее руководство организацией претензионно-исковой работы осуществляет юридический отдел.

2. Организация претензионной работы

2.1. Претензионная работа включает:

установление фактических обстоятельств возникновения спора;

анализ договорных и иных обязательств сторон;

определение характера и размера нарушенных прав и законных интересов Института;

сбор и анализ подтверждающих документов;

определение правовой позиции Института;

предъявление требований нарушившей обязательство стороне;

рассмотрение поступивших в адрес Института претензий;

принятие мер по досудебному урегулированию спора.

2.2. При выявлении факта неисполнения или ненадлежащего исполнения договорных обязательств, причинения имущественного ущерба либо возникновения иных обстоятельств, ответственное структурное подразделение незамедлительно представляет руководству Института служебную записку о выявленном нарушении с

изложением обстоятельств и предложением о необходимости принятия мер досудебного урегулирования.

2.3. Подготовка претензионных писем, проектов ответов на претензии, поступившие в адрес Института, осуществляется юридическим отделом с участием соответствующих структурных подразделений.

2.4. Претензия подписывается руководителем Института либо иным лицом, уполномоченным на ее подписание в установленном порядке.

2.5. При осуществлении претензионно-исковой работы юридический отдел вправе:

запрашивать у структурных подразделений Института документы и сведения, необходимые для правового анализа;

получать письменные и устные пояснения специалистов структурных подразделений;

требовать предоставления расчетов, актов, договоров, переписки и иных документов, подтверждающих обстоятельства спора;

давать структурным подразделениям рекомендации по устранению выявленных нарушений и досудебному урегулированию споров;

привлекать специалистов соответствующих структурных подразделений к подготовке материалов для суда;

при необходимости инициировать проведение сверки взаиморасчетов, экспертизы, обследования или иных мероприятий в пределах компетенции Института.

2.6. Структурные подразделения обязаны своевременно предоставлять юридическому отделу запрошенные документы и сведения.

2.7. Документы, необходимые для предъявления претензии, передаются в юридический отдел с приложением документов, имеющих значение для разрешения спора.

2.8. Юридический отдел осуществляет правовую проверку представленных материалов, в том числе проверяет:

наличие правовых оснований для предъявления требований;

соблюдение условий договора;

наличие доказательств нарушения обязательств;

правильность определения размера требований;

соблюдение сроков исковой давности и иных юридически значимых сроков;

необходимость соблюдения обязательного досудебного порядка;

иные обстоятельства, имеющие значение для разрешения спора.

2.9. При необходимости юридический отдел запрашивает дополнительные документы, сведения и пояснения.

2.10. Претензионные письма регистрируются в установленном в Институте порядке делопроизводства.

2.11. Юридический отдел ведет учет претензий, направленных Институтом и поступивших в его адрес, и осуществляет контроль сроков их рассмотрения.

2.12. Копия направленной претензии и документы, подтверждающие ее направление, хранятся в материалах претензионного производства.

2.13. После полного исполнения сторонами достигнутых договоренностей спор признается урегулированным в досудебном порядке.

2.14. Спор, по которому в целом или его части не достигнуто согласие между сторонами, передается на рассмотрение суда.

2.15. Решение о целесообразности обращения в суд принимается с учетом правовой перспективы дела, размера требований, имеющихся доказательств, сроков исковой давности, необходимости соблюдения досудебного порядка, размера государственной пошлины и иных судебных расходов, а также возможных последствий судебного разбирательства.

3. Организация исковой работы

3.1. Основаниями для подачи исков в суд являются поручения руководства Института, служебные записки структурных подразделений, либо иные документы, содержащие предложение о необходимости обращения в суд.

3.2. Документы, необходимые для предъявления претензии, передаются в юридический отдел с приложением:

договора и дополнительных соглашений к нему;

документов, подтверждающих исполнение или нарушение обязательств;

актов выполненных работ, оказанных услуг, приема-передачи товаров и иных документов;

переписки сторон;

расчетов задолженности, неустойки, убытков и иных требований;

документов, подтверждающих возникновение и размер задолженности;

иных документов, имеющих значение для разрешения спора.

3.3. До обращения в суд юридический отдел проверяет:

наличие правовых оснований для обращения в суд;

соблюдение срока исковой давности;

подведомственность и подсудность дела;

необходимость соблюдения досудебного порядка урегулирования спора;

размер и состав исковых требований;

наличие и достаточность доказательств;

размер государственной пошлины и иных судебных расходов;

необходимость привлечения к участию в деле третьих лиц, экспертов и иных участников процесса;

иные обстоятельства, имеющие значение для рассмотрения дела.

3.4. Юридический отдел запрашивает от структурных подразделений дополнительные документы, сведения, расчеты и пояснения, необходимые для подготовки и ведения судебного дела.

3.5. Исковое заявление и иные процессуальные документы подготавливаются юридическим отделом и подписываются руководителем Института либо иным уполномоченным лицом в соответствии с законодательством и внутренними документами Института.

3.6. Судебное сопровождение включает:

подготовку и подачу исковых заявлений;

подготовку отзывов, возражений, объяснений, ходатайств и иных процессуальных документов;

участие в судебных заседаниях;

представление доказательств и правовой позиции Института;

заявление необходимых ходатайств;

контроль процессуальных сроков;

получение и анализ судебных актов;

подготовку предложений по вопросу обжалования судебных актов;
подготовку проектов апелляционных и кассационных жалоб и иных документов об обжаловании судебных актов;
участие в процедурах примирения и досудебного урегулирования;
подготовку проектов мировых соглашений и иных соглашений о примирении;
передачу исполнительных документов для исполнения и взаимодействие с судебными исполнителями;
контроль взыскания задолженности и поступления денежных средств;
осуществление иных действий, необходимых для защиты прав и законных интересов Института.

3.7. Юридический отдел представляет интересы Института в судах первой, апелляционной и кассационной инстанций, а также при рассмотрении иных судебных процедур в пределах предоставленных полномочий.

3.8. Процессуальные документы направляются в суд посредством Единого портала судебных органов.

3.9. Вопрос о заключении мирового соглашения, соглашения о примирении, отказе от иска, признании иска, изменении предмета или основания иска, а также обжаловании судебного акта выносится юридическим отделом на рассмотрение руководства Института с представлением соответствующего правового обоснования.

3.10. При необходимости к участию в судебных заседаниях привлекаются работники структурных подразделений Института, располагающие специальными знаниями и сведениями по предмету спора.

3.11. Юридический отдел обеспечивает учет судебных дел Института, контроль процессуальных сроков и сроков вступления судебных актов в законную силу.

3.12. Исполнительные документы, подлежащие предъявлению к исполнению, передаются юридическим отделом судебному исполнителю в установленном законодательством порядке.

3.13. Юридический отдел обеспечивает своевременное и качественное внесение сведений по судебным делам в цифровую систему «Бақылау» и их актуализацию в соответствии с установленным порядком.

4. Особенности претензионно-исковой работы по закупкам

4.1. Претензионно-исковая работа по договорам, заключенным в рамках государственных и научных закупок, осуществляется с учетом законодательства Республики Казахстан о государственных закупках, соответствующих правил закупок, условий заключенных договоров и Правил взаимодействия структурных подразделений при осуществлении государственных и научных закупок, утвержденных приказом Института от 27 июня 2025 года № 01-3/82 н/к.

4.2. Инициатор закупок при выявлении факта неисполнения или ненадлежащего исполнения договорных обязательств поставщиком либо возникновения иных обстоятельств, требующих принятия мер, информирует отдел закупок и юридический отдел не позднее 5 рабочих дней с момента, когда ему стало известно или должно было стать известно о соответствующем нарушении.

4.3. Информация о нарушении договорных обязательств предоставляется в форме служебной записки с приложением подтверждающих документов, включая договор, дополнительные соглашения, акты, переписку, расчеты и иные материалы.

4.4. Юридический отдел подготавливает проекты претензий, исковых заявлений и иных документов, связанных с нарушением договорных обязательств, с учетом материалов, представленных инициатором закупки и отделом закупок.

4.5. Вступивший в законную силу судебный акт о признании поставщика недобросовестным участником государственных закупок направляется юридическим отделом в отдел закупок для принятия предусмотренных законодательством мер, в том числе для обеспечения внесения соответствующих сведений в Реестр недобросовестных участников государственных закупок в установленном порядке.

4.6. При взыскании задолженности, неустойки, убытков и иных денежных сумм по договорам закупок юридический отдел взаимодействует с бухгалтерией, отделом закупок и инициатором закупки.

5. Ответственность работников

5.1. Руководители структурных подразделений несут ответственность в пределах своей компетенции за своевременное выявление нарушений обязательств. полноту и достоверность предоставляемых документов и сведений, правильность представленных расчетов.

5.2. Юридический отдел несет ответственность за:

своевременную подготовку и направление претензий, исковых заявлений, отзывов, ходатайств и иных процессуальных документов;

соблюдение процессуальных сроков, находящихся в зоне его контроля;

надлежащее правовое сопровождение судебных дел;

осуществление контроля исполнения судебных актов в пределах предоставленных полномочий;

своевременное внесение и актуализацию сведений по судебным делам в цифровой системе «Бақылау».

5.3. Работники Института несут ответственность за неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящим Положением, в соответствии с законодательством Республики Казахстан и актами работодателя.

6. Заключительные положения

6.1. Вопросы, не урегулированные настоящим Положением, регулируются законодательством Республики Казахстан и внутренними актами Института.

2026 жылғы «18» 08
№ 01-3/113 н/к
бұйрыққа қосымша

Наразылық-талап жұмысы өткізу тәртібі туралы
Ереже

1. Жалпы ережелер

1.1. «Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрлігінің Еңбекті қорғау жөніндегі республикалық ғылыми-зерттеу институты» ШЖҚ РМК-да (бұдан әрі – Институт) Наразылық-талап жұмысы өткізу тәртібі туралы Ереже наразылық және талап қою жұмысын ұйымдастырудың, жүргізудің және бақылаудың, заң бөлімінің Институттың құрылымдық бөлімшелерімен өзара іс-қимылының бірыңғай тәртібін айқындайды.

1.2. Осы Ереже азаматтық, еңбек, әкімшілік рәсімдік-процестік және өзге де құқықтық қатынастарды реттейтін Қазақстан Республикасының заңнамасына сәйкес әзірленді.

1.3. Наразылық-талап қою жұмысының мақсаты Институттың мүліктік және өзге де заңды мүдделерін қорғау, Институттың шарттық және өзге де құқықтық қатынастарын қамтамасыз ету болып табылады.

1.4. Наразылық-талап қою жұмысының негізгі міндеттері:

Институт үшін мүліктік шығындар мен өзге де жағымсыз салдардың алдын алу және азайту; міндеттемелердің бұзылуын уақтылы анықтау және жою;

Институттың тиісті сот өкілдігін және мүдделерін қорғауды қамтамасыз ету.

1.5. Наразылық-талап қою жұмысы заңдылық, мәлімделген талаптар мен қарсылықтардың негізділігі, уақтылығы, құжаттамалық расталуы, сотқа дейінгі реттеудің тиімділігі және Институт мүдделерін қорғау қағидаттарында жүзеге асырылады.

1.6. Институттың құрылымдық бөлімшелері өз құзыреті шегінде бұзушылықтарды уақтылы анықтауды, талап қою және талап қою жұмысы үшін қажетті сенімді құжаттарды, есептерді, мәліметтер мен өзге де материалдарды дайындауды және заң бөліміне ұсынуды қамтамасыз етеді.

1.7. Наразылық-талап қою жұмысын ұйымдастыруға жалпы басшылықты заң бөлімі жүзеге асырады.

2. Талап қою жұмысын ұйымдастыру

2.1. Шағым жұмысы мыналарды қамтиды:

даудың нақты жағдайларын анықтау;

тараптардың шарттық және өзге де міндеттемелерін талдау;

Институттың бұзылған құқықтары мен заңды мүдделерінің сипаты мен мөлшерін анықтау;

растайтын құжаттарды жинау және талдау;

Институттың құқықтық ұстанымын анықтау;

міндеттемені бұзған тарапқа талаптар қою;

Институт атына келіп түскен шағымдарды қарау;

дауды сотқа дейін реттеу жөнінде шаралар қабылдау.

2.2. Шарттық міндеттемелерді орындамау немесе тиісінше орындамау, мүліктік залал келтіру не өзге де мән-жайлар туындау фактісі анықталған кезде жауапты құрылымдық бөлімше мән-жайларды баяндай отырып және сотқа дейінгі реттеу шараларын қабылдау қажеттігі туралы ұсыныспен анықталған бұзушылық туралы қызметтік жазбаны Институт басшылығына дереу ұсынады.

2.3. Институт атына келіп түскен шағымдарға шағым хаттарын, жауап

жобаларын дайындауды тиісті құрылымдық бөлімшелердің қатысуымен заң бөлімі жүзеге асырады.

2.4. Шағымға Институт басшысы не оған белгіленген тәртіппен қол қоюға уәкілетті өзге тұлға қол қояды.

2.5. Талап қою-талап қою жұмысын жүзеге асыру кезінде заң бөлімі:

Институттың құрылымдық бөлімшелерінен құқықтық талдау үшін қажетті құжаттар мен мәліметтерді сұрату;

құрылымдық бөлімшелер мамандарының жазбаша және ауызша түсіндірмелерін алу;

есеп айырысуларды, актілерді, шарттарды, хат алмасуды және даудың мән-жайын растайтын өзге де құжаттарды ұсынуды талап ету;

құрылымдық бөлімшелерге анықталған бұзушылықтарды жою және дауларды сотқа дейін реттеу жөнінде ұсыныстар беру;

тиісті құрылымдық бөлімшелердің мамандарын сот үшін материалдар дайындауға тарту; қажет болған жағдайда Институттың құзыреті шегінде өзара есеп айырысуларды, сараптаманы, тексеруді немесе өзге де іс-шараларды салыстырып тексеруді жүргізуге бастамашылық жасау.

2.6. Құрылымдық бөлімшелер заң бөліміне сұратылған құжаттар мен мәліметтерді уақтылы ұсынуға міндетті.

2.7. Талап қою үшін қажетті құжаттар дауды шешу үшін маңызы бар құжаттарды қоса бере отырып, заң бөліміне беріледі.

2.8. Заң бөлімі ұсынылған материалдарды құқықтық тексеруді жүзеге асырады, оның ішінде:

талап қою үшін құқықтық негіздердің болуы;

шарт талаптарын сақтау;

міндеттемелерді бұзу туралы дәлелдердің болуы;

талаптардың мөлшерін анықтаудың дұрыстығы;

талап қою мерзімдерін және өзге де заңды маңызы бар мерзімдерді сақтау;

сотқа дейінгі міндетті тәртіпті сақтау қажеттілігі;

дауды шешу үшін маңызы бар өзге де мән-жайлар.

2.9. Қажет болған жағдайда заң бөлімі қосымша құжаттарды, мәліметтер мен түсіндірмелерді сұратады.

2.10. Шағым хаттары Институтта белгіленген іс жүргізу тәртібімен тіркеледі.

2.11. Заң бөлімі Институт жіберген және оның атына келіп түскен талаптардың есебін жүргізеді және оларды қарау мерзімдерін бақылауды жүзеге асырады.

2.12. Жіберілген шағымның көшірмесі және оның бағытын растайтын құжаттар шағым өндірісінің материалдарында сақталады.

2.13. Тараптар қол жеткізілген уағдаластықтарды толық орындағаннан кейін дау сотқа дейінгі тәртіппен реттелді деп танылады.

2.14. Жалпы немесе оның бір бөлігі Тараптар арасында келісімге қол жеткізілмеген дау соттың қарауына беріледі.

2.15. Сотқа жүгінудің орындылығы туралы шешім істің құқықтық перспективасы, талаптардың мөлшері, қолда бар дәлелдемелер, талап қою мерзімдері, сотқа дейінгі тәртіпті сақтау қажеттілігі, мемлекеттік баждың және өзге де сот шығыстарының мөлшері, сондай-ақ сот талқылауының ықтимал салдары ескеріле отырып қабылданады.

3. Талап қою жұмысын ұйымдастыру

3.1. Институт басшылығының тапсырмалары, құрылымдық бөлімшелердің қызметтік жазбалары немесе сотқа жүгіну қажеттілігі туралы ұсынысты қамтитын өзге де құжаттар сотқа талап қою үшін негіз болып табылады.

3.2. Шағым беру үшін қажетті құжаттар заң бөліміне қосымшамен бірге беріледі:

шарт және оған қосымша келісімдер;

міндеттемелердің орындалғанын немесе бұзылғанын растайтын құжаттар;

орындалған жұмыстар, көрсетілген қызметтер актілері, тауарларды қабылдау-беру және өзге де құжаттар;

тараптардың хат-хабарлары;

берешекті, тұрақсыздық айыбын, залалды және өзге де талаптарды есептеу;

берешектің пайда болуын және мөлшерін растайтын құжаттар;

дауды шешу үшін маңызы бар өзге де құжаттар.

3.3. Сотқа жүгінгенге дейін заң бөлімі тексереді:

сотқа жүгіну үшін құқықтық негіздердің болуы;

ескіру мерзімін сақтау; істің ведомстволық бағыныстылығы және соттылығы;

дауды реттеудің сотқа дейінгі тәртібін сақтау қажеттілігі;

талап қою талаптарының мөлшері мен құрамы;

дәлелдемелердің болуы және жеткіліктілігі;

мемлекеттік баждың және өзге де сот шығыстарының мөлшері;

іске қатысуға үшінші тұлғаларды, сарапшыларды және процестің өзге де қатысушыларын тарту қажеттілігі;

істі қарау үшін маңызы бар өзге де мән-жайлар.

3.4. Заң бөлімі құрылымдық бөлімшелерден сот ісін дайындау және жүргізу үшін қажетті қосымша құжаттарды, мәліметтерді, есептеулер мен түсіндірмелерді сұратады.

3.5. Наразылық-талап қою және өзге де процестік құжаттарды заң бөлімі дайындайды және оған Институттың заңнамасына және ішкі құжаттарына сәйкес Институт басшысы не өзге де уәкілетті тұлға қол қояды.

3.6. Сот сүйемелдеуіне мыналар кіреді:

наразылық-талап қоюы дайындау және беру;

пікірлер, қарсылықтар, түсініктемелер, өтініштер және өзге де іс жүргізу құжаттарын дайындау;

сот отырыстарына қатысу;

Институттың дәлелдемелері мен құқықтық ұстанымын ұсыну;

қажетті өтініштерді беру;

іс жүргізу мерзімдерін бақылау;

сот актілерін алу және талдау;

сот актілеріне шағымдану мәселесі бойынша ұсыныстар дайындау;

апелляциялық және кассациялық шағымдардың жобаларын және сот актілеріне шағымдану туралы өзге де құжаттарды дайындау;

татуласу және сотқа дейінгі реттеу рәсімдеріне қатысу;

бітімгершілік келісімдерінің және татуласу туралы өзге де келісімдердің жобаларын дайындау;

атқарушылық құжаттарды орындау үшін беру және сот орындаушыларымен өзара іс-қимыл жасау;

берешекті өндіріп алуды және ақша қаражатының түсуін бақылау;

Институттың құқықтары мен заңды мүдделерін қорғау үшін қажетті өзге де әрекеттерді жүзеге асыру.

3.7. Заң бөлімі бірінші, апелляциялық және кассациялық сатылардағы соттарда, сондай-ақ берілген өкілеттіктер шегінде өзге де сот рәсімдерін қарау кезінде Институттың мүдделерін білдіреді.

3.8. Процестік құжаттар сотқа сот органдарының Бірыңғай порталы арқылы жіберіледі.

3.9. Бітімгершілік келісімін, татуласу, талап қоюдан бас тарту, талап қоюды тану, талап қоюдың нысанасын немесе негізін өзгерту, сондай-ақ сот актісіне шағым жасау туралы мәселені заң бөлімі тиісті құқықтық негіздемені ұсына отырып, Институт басшылығының қарауына шығарады.

3.10. Қажет болған жағдайда сот отырыстарына қатысуға даудың мәні бойынша арнайы білімі мен мәліметтері бар Институттың құрылымдық бөлімшелерінің қызметкерлері тартылады.

3.11. Заң бөлімі Институттың сот істерін есепке алуды, сот актілерінің заңды күшіне енуінің іс жүргізу мерзімдері мен мерзімдерін бақылауды қамтамасыз етеді.

3.12. Орындауға ұсынылуға жататын атқарушылық құжаттарды заң бөлімі заңнамада белгіленген тәртіппен сот орындаушысына береді.

3.13. Заң бөлімі сот істері бойынша мәліметтерді «Бақылау» цифрлық жүйесіне уақтылы және сапалы енгізуді және оларды белгіленген тәртіпке сәйкес өзектендіруді қамтамасыз етеді.

4. Сатып алу бойынша наразылық-талап қою жұмысының ерекшеліктері

4.1. Мемлекеттік және ғылыми сатып алу шеңберінде жасалған шарттар бойынша Наразылық-талап қою жұмысы Институттың 2025 жылғы 27 маусымдағы № 01-3/82 н/қ бұйрығымен бекітілген Қазақстан Республикасының мемлекеттік сатып алу туралы заңнамасын, сатып алудың тиісті қағидаларын, жасалған шарттардың талаптарын және мемлекеттік және ғылыми сатып алуды жүзеге асыру кезінде құрылымдық бөлімшелердің өзара іс-қимыл жасау қағидаларын ескере отырып жүзеге асырылады.

4.2. Сатып алу бастамашысы өнім берушінің шарттық міндеттемелерді орындамау немесе тиісінше орындамау не шаралар қабылдауды талап ететін өзге де мән-жайлар туындау фактісі анықталған кезде сатып алу бөлімін және заң бөлімін ол тиісті бұзушылық туралы белгілі болған немесе белгілі болуы тиіс сәттен бастап 5 жұмыс күнінен кешіктірмей хабардар етеді.

4.3. Шарттық міндеттемелерді бұзу туралы ақпарат шартты, қосымша келісімдерді, актілерді, хат алмасуды, есеп айырысуларды және өзге де материалдарды қоса алғанда, растайтын құжаттарды қоса бере отырып, қызметтік жазба нысанында беріледі.

4.4. Заң бөлімі сатып алу бастамашысы мен сатып алу бөлімі ұсынған материалдарды ескере отырып, шарттық міндеттемелерді бұзуға байланысты шағымдардың, наразылық-талап қоюдың және өзге де құжаттардың жобаларын дайындайды.

4.5. Өнім берушіні мемлекеттік сатып алуға жосықсыз қатысушы деп тану туралы заңды күшіне енген сот актісін заңдарда көзделген шараларды қабылдау үшін, оның ішінде белгіленген тәртіппен мемлекеттік сатып алуға жосықсыз

қатысушылардың тізіліміне тиісті мәліметтерді енгізуді қамтамасыз ету үшін заң бөлімі сатып алу бөліміне жібереді.

4.6. Сатып алу шарттары бойынша берешекті, тұрақсыздық айыбын, залалды және өзге де ақшалай сомаларды өндіріп алу кезінде заң бөлімі бухгалтериямен, сатып алу бөлімімен және сатып алу бастамашысымен өзара іс-қимыл жасайды.

5. Қызметкерлердің жауапкершілігі

5.1. Құрылымдық бөлімшелердің басшылары өз құзыреті шегінде міндеттемелердің бұзылуын уақтылы анықтағаны үшін жауапты болады. ұсынылатын құжаттар мен мәліметтердің толықтығы мен дұрыстығы, ұсынылған есептердің дұрыстығы.

5.2. Заң бөлімі жауапты:

шағымдарды, талап арыздарды, пікірлерді, өтініштерді және өзге де іс жүргізу құжаттарын уақтылы дайындау және жолдау;

оның бақылау аймағындағы іс жүргізу мерзімдерін сақтау;

сот істерін тиісті құқықтық сүйемелдеу;

берілген өкілеттіктер шегінде сот актілерінің орындалуын бақылауды жүзеге асыру;

«Бақылау» цифрлық жүйесінде сот істері бойынша мәліметтерді уақтылы енгізу және өзектендіру.

5.3. Институт қызметкерлері Қазақстан Республикасының заңнамасына және жұмыс берушінің актілеріне сәйкес осы Ережеде көзделген міндеттерді орындамағаны немесе тиісінше орындамағаны үшін жауапты болады.

6. Қорытынды ережелер

6.1. Осы Ережемен реттелмеген мәселелер Қазақстан Республикасының заңнамасымен және Институттың ішкі актілерімен реттеледі.