АППАРАТ
ЗАКОНОДАТЕЛЬНОГО СОБРАНИЯ
ОРЕНБУРГСКОЙ ОБЛАСТИ

П Р И К А З

12 августа 2013 года № 150-пс

г. Оренбург

Об утверждении порядка доступа работников аппарата Законодательного Собрания Оренбургской области в помещения, в которых ведется обработка персональных данных

В соответствии с постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и, операторами, являющимися государственными или муниципальными органами»

п р и к а з ы в а ю:

1. Утвердить порядок доступа работников аппарата Законодательного Собрания Оренбургской области в помещения, в которых ведется обработка персональных данных согласно приложению (прилагается).

2. Доступ работников аппарата Законодательного Собрания Оренбургской области в помещения, в которых ведется обработка персональных данных осуществлять строго в соответствии с утвержденным порядком.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель аппарата
Законодательного Собрания
Оренбургской области Н.А.Кренделев

Разослано: руководителю аппарата Законодательного Собрания Оренбургской области, начальнику управления делами аппарата Законодательного Собрания Оренбургской области, начальнику управления организационно-документационного обеспечения и информатизации Законодательного Собрания Оренбургской области, отделу информационных технологий управления организационно-документационного обеспечения и информатизации аппарата Законодательного Собрания Оренбургской области, отделу государственной гражданской службы и кадров, отделу бухгалтерского учета управления делами аппарата Законодательного Собрания Оренбургской области.

А.А.Веселков
77 52 18

Приложение
к приказу руководителя
аппарата Законодательного
Собрания Оренбургской
области
от 12 августа 2013 года
№ 150-пс

Порядок доступа
работников аппарата Законодательного Собрания Оренбургской области в помещения, в которых ведется обработка персональных данных

Настоящий документ разработан во исполнение Федерального закона от 27.07.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных», приказа Федеральной службы безопасности Российской Федерации (ФСБ России) от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», Кодекса об административных правонарушениях от 30.12.2001 № 195-ФЗ (глава 13), Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ (глава 14 «Защита персональных данных работника»). С целью предотвращения неавторизованного доступа, повреждения и воздействия в отношении помещений и информации, определяется перечень защищаемых помещений и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составляется технический паспорт на защищаемые помещения.

Средства обработки информации должны быть размещены в зонах безопасности, обозначенных определенным периметром безопасности, обладающими соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Размещение рабочих мест и специальное оборудование помещения должны обеспечивать сохранность технических средств и информации,

исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.

Входные двери помещений должны быть оборудованы замками с контролем доступа, гарантирующими надежную защиту помещений в нерабочее время, опечатывающими устройствами и системой контроля доступа, обеспечивающими контроль и регистрацию за входом в помещения.

На каждый механический замок входной двери помещения должно быть в наличии не менее 2-х экземпляров ключей. Один ключ должен находиться у ответственного за помещение, резервный комплект ключей – у ответственного за эксплуатацию здания. В нерабочее время ключи сдаются на пост охраны.

Окна помещений должны быть оборудованы средствами сигнализации на вскрытие, разбитие стекла и шторами.

Обращается особое внимание, что при работе с информацией персональных данных двери помещений должны быть всегда закрыты.

В помещении устанавливаются сейфы (металлические шкафы), оборудованные опечатывающими устройствами, предназначенные для хранения носителей информации, в том числе ключевой информации и документов по персональным данным и других рабочих материалов.

Вскрытие и закрытие помещений осуществляется работниками, работающими в данных помещениях.

Список работников, имеющих право вскрывать и опечатывать помещения, утверждается руководителем и передаётся на пост охраны.

При отсутствии работников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

При закрытии помещений работники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в опечатываемый сейф (металлический шкаф).

При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) ответственному за защиту информации.

Одновременно принимаются меры по охране места происшествия, до прибытия должностных лиц в помещение никто не допускается.

Руководитель, ответственный за защиту информации и администратор автоматизированной системы (далее АС) организуют проверку АС на предмет несанкционированного доступа к конфиденциальной информации и наличия документов и машинных носителей информации.

При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за

помещение, или ответственному за защиту информации, или руководителю, или администратору АС. Помещения вскрывать запрещается.

Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за защиту информации в присутствии сотрудника охраны с составлением акта.

При обработке защищаемой информации в АС исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны АС, определенных соответствующим приказом.

Зона информационной безопасности защищается путем закрытия на замок самого помещения и помещений внутри физического периметра безопасности, которые могут быть заперты и иметь запираемые сейфы.

Должны выполняться следующие правила:

основное оборудование должно быть расположено в местах с ограничением доступа посторонних лиц;

оборудование (в том числе копировальные устройства и факсы), должны быть расположены соответствующим образом в пределах зоны безопасности во избежание доступа, который мог бы скомпрометировать информацию;

двери и окна необходимо запирать, когда в помещениях нет сотрудников;

служебные помещения должны быть оборудованы техническими средствами сигнализации.

Для повышения степени защиты зон информационной безопасности устанавливаются дополнительные меры по управлению информационной безопасностью. Они включают мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне безопасности, и состоять в следующем:

о существовании зоны информационной безопасности и проводимых в ней работах должны быть осведомлены только лица, которым это необходимо в силу производственной необходимости;

из соображений безопасности и предотвращения возможности действий по причинению вреда в охраняемых зонах необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала;

пустующие зоны безопасности должны быть физически закрыты, и их состояние необходимо периодически проверять;

использование фото, видео, аудио или другого записывающего оборудования должно быть разрешено только при получении специального разрешения.