Прокуратура
Российской Федерации

Рыбинская межрайонная
прокуратура

ул. 40 лет Октября, 44, г. Заозёрный,
Красноярский край, 663960

15.02.2024 № 7-01-2024

Директору КГБУСО «КЦСОН «Рыбинский»

Ураловой Т.В.

ул. Фабричная, 11, г. Заозерный, Рыбинский район, Красноярский край, 663960
e-mail: volfvi@krasmail.ru

ПРЕДСТАВЛЕНИЕ

Об устранении нарушений законодательства о информационной безопасности и защите персональных данных

На основании решения от 20.02.2024 г. № 37 в КГБУСО «КЦСОН «Рыбинский» проведена проверка соблюдения требований законодательства об информации, информационных технологиях и о защите информации, о персональных данных в части, касающейся их обработки с использованием информационных систем и технологий, а также соблюдение требований законодательства о порядке рассмотрения обращений граждан Российской Федерации, в ходе которой выявлены нарушения, требующие устранения.

Так, в ходе проверки установлено, что КГБУСО «КЦСОН «Рыбинский» в силу своей деятельности имеет доступ к персональным данным как работников учреждения, так и лиц, получающих в учреждении услуги, является пользователем информационных систем, доступ к которым осуществляется посредством интернет-ресурсов, имеет возможность входа в информационные системы, внесения и получения из них информации, не относящейся к общеизвестным сведениям, и иной информации, доступ к которой как ограничен, так и не ограничен, в т.ч. к размещённым в информационных системах персональным данным - информации, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Согласно ст. 18.1, ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» установлено, что оператор обязан принимать меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, и меры по обеспечению безопасности персональных данных при их обработке.

При этом состав и содержание необходимых для выполнения требований к защите персональных данных, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, должен быть обеспечен с

ВХОД No. 419
«02» 04 2024 г.
ПОДПИСЬ

ВТ № 010071

учетом уровня защищенности (ч. 4 ст. 19 Федерального закона от 27.07.2006 г. N 152-ФЗ).

В силу п. 1 и 5 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 г. N 152-ФЗ к таким мерам относятся назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных, а также оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом.

Требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» утверждены приказом Роскомнадзора от 27.10.2022 N 178.

Однако, КГБУСО «КЦСОН «Рыбинский» данные требования законодательства не исполнил, ответственного за организацию обработки персональных данных, не назначил, оценку вреда в соответствии с приказом Роскомнадзора от 27.10.2022 N 178, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», не провел, соотношение указанного вреда и принимаемых учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом, не оценил.

Помимо этого, Федеральный закон от 27.07.2006 № 149-ФЗ обязывает не только владельца информации, но и оператора информационной системы (гражданина или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных), обеспечить защиту информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий, соблюдать конфиденциальность информации ограниченного доступа путём принятия правовых, организационных и технических мер (ч. 1 ст. 16).

При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 01.11.2012 N 1119 (п. 5 Требований).

При этом согласно ч. 4 Требований, утверждённых постановлением Правительства Российской Федерации от 01.11.2012 N 1119, выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утверждены Приказом ФСБ России от 10.07.2014 N 378. Приказом определено, что эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и требованиями, установленными в настоящем приказе, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области (п. 4).

Согласно приказа ФСБ России от 10.07.2014 N 378 требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 N 1119, и их выполнение зависит от уровня защищенности персональных данных при их обработке в информационных системах.

Обработка в информационных системах персональных данных учреждением осуществляется с использованием средств криптографической защиты информации КС2 (СКЗИ класса КС2). Согласно актам от 17.04.2023 г., являющихся приложением к приказу директора КГБУСО «КЦСОН «Рыбинский», установлен 4 уровень защищенности.

Однако, в нарушение требований подп. «а» п. 5 и п. «а», «б», «в» п. 6 приложения к приказу ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» учреждением надлежащим образом не организован режим обеспечения безопасности помещений, в которых размещены информационные системы, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения путем утверждения правил доступа в Помещения в рабочее и нерабочее время (с учетом оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений) и утверждения перечня лиц, имеющих право доступа в эти Помещения.

Таким образом, в результате упущений в регулировании вопросов, связанных с защитой информации и персональных данных, наличия пробелов в локальном нормативном регулировании, при фактической работе не исключается неправомерный доступ, копирование, предоставление или распространение информации из доступных организации информационных государственных

систем; неправомерное блокирование, нарушение целостности и достоверности информации в них, атаки на информационные системы и иные несанкционированные действия, а также доступ к персональным данных третьих лиц и несанкционированные действия с ними.

Причинами и условиями допущенных нарушений является ненадлежащее исполнение обязанностей ответственным за информационную безопасность в учреждении и упущения в работе с Вашей стороны.

На основании изложенного и руководствуясь ст. ст. 6, 7, 22, 24 Федерального закона от 17.01.1992 г. № 2202-1 «О прокуратуре Российской Федерации»,

ТРЕБУЮ:

1. Безотлагательно рассмотреть настоящее представление с участием представителя Рыбинской межрайонной прокуратуры.

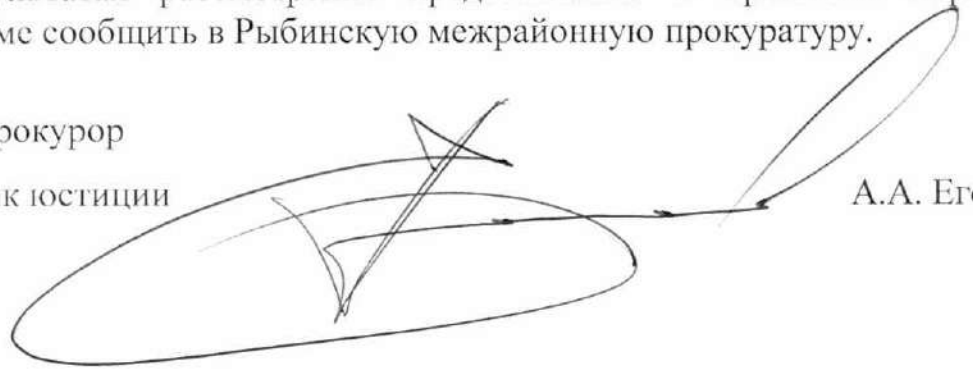
2. В течение месяца со дня внесения представления принять конкретные меры по устранению допущенных нарушений закона, причин и условий им способствующих, недопущению их впредь.

3. Рассмотреть вопрос о привлечении лиц, по чьей вине стали возможны данные нарушения, к дисциплинарной ответственности.

4. О результатах рассмотрения представления и принятых мерах в письменной форме сообщить в Рыбинскую межрайонную прокуратуру.

Межрайонный прокурор

старший советник юстиции А.А. Егоров



О.И. Костицкая, тел. 2-06-86