Прокуратура
Российской Федерации

Рыбинская межрайонная
прокуратура

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

27.04.2023 № 7-01-2023

337726 701317

Директору МБОУ «Большеключинская ООШ № 4»

Тетериной Ж.С.

ПРЕДСТАВЛЕНИЕ

Об устранении нарушений законодательства
о информационной безопасности и защите
персональных данных

На основании решения от 28.03.2023 г. № 68 в образовательном учреждении проведена проверка соблюдения требований законодательства об информационной безопасности и защите информации, о персональных данных в части, касающейся информационных технологий, в ходе которой выявлены нарушения, требующие устранения.

Так, в ходе проверки установлено, что МБОУ «Большеключинская ООШ № 4» 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).

Обработка в информационных системах персональных данных образовательным учреждением осуществляется с использованием средств криптографической защиты информации, класс которой и сертификация в ходе проверки Вами не подтверждены.

Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяется работа всех информационных систем в Российской Федерации. Статья 13 данного закона даёт понятие информационных систем.

Федеральный закон от 27.07.2006 г. № 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,

ВТ № 009155

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).

В соответствии со ст. 16 Федерального закона от 27.07.2006 г. № 149-ФЗ защита информации обеспечивается, в частности:

1) предотвращением несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременным обнаружением фактов несанкционированного доступа к информации;

3) предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущением воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможностью незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянным контролем за обеспечением уровня защищенности информации.

К операторам государственных информационных систем, в которых ведётся обработка информации ограниченного доступа (не содержащей сведений, составляющих государственную тайну), предъявляются требования, изложенные в Приказе ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

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 г. N 1119 (п. 5 Требований).

При этом согласно ч. 4 Требований, утверждённых постановлением Правительства Российской Федерации от 01.11.2012 г. 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 г. 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 г. N 378 требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и их выполнение зависит от уровня защищенности персональных данных при их обработке в информационных системах.

Кроме того, согласно ст. 18.1, ст. 19 Федерального закона от 27.07.2006 г. 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 учетом уровня защищенности (ч. 4 ст. 19 Федерального закона от 27.07.2006 г. N 152-ФЗ). Под уровнем угроз понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ч. 11 ст. 19 Федерального закона от 27.07.2006 г. N 152-ФЗ).

Во исполнение ч. 4 ст. 19 Федерального закона от 27.07.2006 г. N 152-ФЗ «О персональных данных» приказом ФСТЭК России от 18.02.2013 г. N 21 утверждены состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

В зависимости от информационных систем, к которым обеспечивается доступ образовательного учреждения, определены угрозы безопасности.

Так, в соответствии с ч. 5 ст. 19 Федерального закона от 27.07.2006 г. N 152-ФЗ Приказом Минобрнауки России от 07.09.2021 г. N 840 определены угрозы безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством науки и высшего образования Российской Федерации, приведен перечень возможных угроз безопасности, в т.ч. угрозы нарушения безопасности защищаемых с использованием средств криптографической защиты информации персональных данных.

Однако, вопреки требованиям действующего законодательства о защите информации и о персональных данных, образовательным учреждением допущены следующие нарушения:

- работники, непосредственно осуществляющие обработку персональных данных, не ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных;

- не исполнена обязанность опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных, в том числе публикация политики организации и сведений о реализуемых требованиях к защите персональных данных на сайте образовательного учреждения в информационно-телекоммуникационной сети «Интернет»;

- классы защищенности используемых информационных систем, тип угроз персональных данных, модели угроз учреждением не установлены (не определены) и в ходе проверки не подтверждены, в связи с чем не представляется возможным подтвердить обоснованность установления учреждением уровня защищенности «3» (акт от 06.04.2023 г. №б/н);

- Вами не подтверждена достаточность навыков в сфере обеспечения безопасности персональных данных в информационной системе работников, ответственных за обеспечение безопасности персональных данных в информационной системе, что является одним из требований приказа ФСБ России от 10.07.2014 г. N 378 к защите персональных данных для 3 уровня защищенности;

- не изданы локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, в т.ч. по обнаружению фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- не обеспечена регистрация и учет действий, совершаемых с персональными данными в информационной системе персональных данных;

- не обеспечен учет машинных носителей персональных данных, их защита, сохранность носителей персональных данных,

- не организован должный режим обеспечения безопасности помещений, в которых размещены информационные системы с использованием СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, в т.ч. не обеспечен режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, лиц, не имеющих права доступа в Помещения (в число которых входит правовое, организационное и техническое обеспечение 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; утверждения правил доступа в Помещения в рабочее и

нерабочее время, а также в нештатных ситуациях; утверждения перечня лиц, имеющих право доступа в Помещения) и иные меры криптографической защиты.

Предоставленный Вами в ходе проверки Порядок доступа работников в помещения, в которых ведется обработка информации ограниченного доступа, и расположены средства криптографической защиты информации от 06.04.2023 г. №б/н носит формальный характер.

Меры по криптографической защите подлежат приведению в соответствие с приказом ФСБ России от 10.07.2014 г. N 378, в т.ч. в соответствии с определенным в установленном порядке уровнем защищенности, соответствующим классам защиты каждой из используемых учреждением информационных систем, который Вами в ходе проверки, как достоверный, как и класс средств криптографической защиты информации, не подтверждены.

Таким образом, в результате упущений в регулировании вопросов, связанных с трудовыми правами и обязанностями работников учреждения в сфере защиты информации и о персональных данных, наличия пробелов в локальном нормативном регулировании, а также при фактической организации работы, не исключается неправомерный доступ, копирование, предоставление или распространение информации из доступных образовательной организации информационных систем; неправомерное блокирование, нарушение целостности и достоверности информации в них, атаки на информационные системы и иные несанкционированные действия.

Причинами и условиями допущенных нарушений является ненадлежащее исполнение обязанностей ответственным за обработку персональных данных в образовательном 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