

Директору
МБОУ «Школа-интернат С(П)ОО
с. Новый Каинлык»
МР Краснокамский район РБ

Сабирьяновой Г.М.

ул. Школьная, д.30,
с. Новый Каинлык
Краснокамский район, РБ,
452945.

ПРЕДСТАВЛЕНИЕ

Об устранении нарушений
законодательства об
информационной безопасности
и защите персональных данных

В соответствии с поручением прокуратуры республики от 14.02.2024 № Исуб-69-1702-24/2340-20800001 «О проведении анализа результатов работы по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации» во исполнение задания Генеральной прокуратуры Российской Федерации прокуратурой района проведена проверка в МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ и ООШ д. Бурнюш - филиал МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ по результатам которой установлено следующее.

В силу требований ч. 4 ст. 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) обладатель информации при осуществлении своих прав обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Согласно ст. 16 Федерального закона № 149-ФЗ защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

В силу п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) персональные данные – любая информация, относящаяся прямо или косвенно

определенному, или определяемому лицу (субъекту персональных данных). Информация, предоставленная администрации образовательного учреждения родителями (законными представителями) учащихся либо обучающимися самостоятельно, относится к конфиденциальной, обработка которых не допускается без согласия субъекта персональных данных (ч. 1 ст. 6, ст. 7 Федерального закона № 152-ФЗ).

Так, ч. 1 ст. 5 Федерального закона № 152-ФЗ предусматривает, что обработка персональных данных должна осуществляться на законной и справедливой основе.

Статьей 21 данного Федерального закона регламентированы обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.

Указанные нормы обязывают нормативно регламентировать круг лиц, допущенных к обработке персональных данных, обрабатываемых в информационных системах, а также в соответствующих помещениях данных органов.

Вместе с тем, проверка показала, что в МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ и ООШ д. Бурнюш - филиал МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ не в полном объеме реализованы требования по выполнению организационных и технических мер по обеспечению безопасности персональных данных. На момент проведения проверочных мероприятий выявлены следующие нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- не назначено ответственное лицо за организацию обработки персональных данных;
- не осуществляется внутренний контроль соответствия обработки персональных данных требованиям законодательства;
- не произведена оценка вреда, который может быть причинен субъекта персональных данных в случае нарушений требований законодательства в области обработки и защиты персональных данных;
- не проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- не производится обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных, по реагированию на компьютерные инциденты в них;
- не регламентирован контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Требованиями приказа ФСТЭК России от 18.02.2013 № 21 определен состав мер по обеспечению безопасности персональных данных, реализуемых в

рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, и включает в себя: идентификацию и аутентификацию субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных); регистрацию событий безопасности; антивирусную защиту; обнаружение (предотвращение) вторжений; контроль (анализ) защищенности персональных данных; обеспечение целостности информационной системы и персональных данных; обеспечение доступности персональных данных; защиту среды виртуализации; защиту технических средств; защиту информационной системы, ее средств, систем связи и передачи данных; выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них; управление конфигурацией информационной системы и системы защиты персональных данных.

При этом в силу п. 18 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия: планирование мероприятий по защите информации в информационной системе; анализ угроз безопасности информации в информационной системе; управление (администрирование) системой защиты информации информационной системы; управление конфигурацией информационной системы и ее системой защиты информации; реагирование на инциденты; информирование и обучение персонала информационной системы; контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В нарушение п. 8 приказа ФСТЭК России от 18.02.2013 № 21 в МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ и ООШ д.Бурнюш - филиал МБОУ «Школа-интернат С(П)ОО с. Новый Каинлык» МР Краснокамский район РБ отсутствует инструкция по установке, ремонту, модернизации, модификации и техническому обслуживанию программных аппаратных, и программно-аппаратных средств на ПЭВМ, обрабатывающих информацию ограниченного распространения; отсутствует перечень персональных данных, обрабатываемых в учреждении; отсутствует приказ об определении помещений, в которых обрабатываются персональные данные.

В нарушение п. 13 Требований отсутствует инструкция по обращению с материальными носителями персональных данных; отсутствует перечень программного обеспечения, разрешенного к установке; отсутствуют правила рассмотрения запросов субъектов персональных данных; отсутствует инструкция об организации контроля состояния персональных данных, не утвержден состав комиссии по контролю состояния обработки персональных данных, план по контролю (по защите информации).

В нарушение п. 14 Требований отсутствует порядок реагирования на инциденты информационной безопасности; отсутствует инструкция по эксплуатации средств защиты информации; отсутствует перечень информационных систем; отсутствует журнал инструктажа по информационной безопасности; не размещена на информационном стенде политика обеспечения безопасности конфиденциальных данных в отношении обработки персональных данных.

Выявленные нарушения прав являются недопустимыми, требуют незамедлительного устранения и недопущения их впредь.

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

ТРЕБУЮ:

1. Рассмотреть настоящее представление с обязательным участием представителя прокуратуры района, заблаговременно уведомив о дате, времени и месте рассмотрения.

2. Принять исчерпывающие меры к устранению допущенных нарушений действующего законодательства, причин и условий им способствующих, и недопущению их впредь.

3. Рассмотреть вопрос о привлечении к установленной законом ответственности виновных должностных лиц, допустивших нарушения законодательства, в случае применения данной меры представить копию соответствующего приказа.

4. О результатах рассмотрения представления и принятых мерах сообщить в прокуратуру Краснокамского района в установленный законом месячный срок с приложением копий приказов о наложении дисциплинарных взысканий и документов, подтверждающих устранение выявленных нарушений закона.

Прокурор района

Н.А. Щербинин

