

ФЕДЕРАЛЬНАЯ
СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)
УФСБ РОССИИ
ПО РЕСПУБЛИКЕ КАРЕЛИЯ

27.02.2024 № 64/106-434
г. Петрозаводск, 185035

Экз. № 2
Директору МОУ «Райватальская
СОШ»

Корхонен С.Ф.

Республика Карелия, п. Хийтола,
ул. Ленина, д. 16

ПРЕДСТАВЛЕНИЕ

об устранении причин и условий, способствовавших
совершению административного правонарушения

Руководствуясь статьей 29.13 Кодекса Российской Федерации об административных правонарушениях, Управление Федеральной службы безопасности Российской Федерации по Республике Карелия:

1. Обращает Ваше внимание на то, что сотрудниками отделения в г. Лахденпохья УФСБ России по Республике Карелия выявлены нарушения при организации работы МОУ «Райватальская СОШ» с информационными системами персональных данных (ИСПДн), в нарушение ст. 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», п. 3 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи - с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ России от 13.06.2001 №152, п. 5, п. 6 «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», утвержденных приказом ФСБ России от 10.07.2014 г. № 378 выраженное в несоблюдении требований к защите персональных данных при их обработке в ИСПДн, что создало предпосылки получения неконтролируемого доступа к информационным системам иных лиц¹ и могло повлечь нарушение порядка

¹ В соответствии с пп. «а», «б» п. 13 Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее - Постановление Правительства РФ от 1 ноября 2012 г. N 1119) определяется перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

доступа к информации, воздействие на технические средства обработки информации, в результате которого нарушается их функционирование и могут наступить иные негативные последствия, предусмотренные ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

По факту выявленного нарушения 16 февраля 2024 г. составлен протокол об административном правонарушении по части 6 статьи 13.12 КоАП РФ (Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации) возбуждено дело об административном правонарушении № 106/10-24АП. Согласно постановлению № 106/10-24АП от 27 февраля 2024 г., директор Корхонен С.Ф. признана виновной в совершении административного правонарушения по части 6 статьи 13.12 КоАП РФ, ей назначено наказание в виде административного штрафа в размере 1000 рублей.

Причиной совершения административного правонарушения явилось ненадлежащее исполнение должностным лицом ст. 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», а условиями отсутствие нормативных документов, определяющих перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, отсутствие ответственных лиц за обеспечение безопасности персональных данных в информационных системах, не выполнение требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119, нарушение требований «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ России от 13.06.2001 №152, а также не выполнение необходимых мер, утвержденных приказом ФСБ России от 10.07.2014 г. № 378².

2. Информирует, что для устранения причин и условий, способствовавших совершению административного правонарушения, необходимо в соответствии со ст. 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» необходимо обеспечить безопасность персональных данных посредством:

- применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

² 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;

системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- обнаружения фактов несанкционированного доступа к персональным данным и принятием 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;

- установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных и т.д.;

В соответствии с пп. «а», «б» п.13 Постановления Правительства РФ от 1 ноября 2012 г. № 1119 необходимо нормативно определить перечень мероприятий, необходимых для обеспечения безопасности помещений, в которых размещена информационная система, исключающих неконтролируемое проникновение или пребывание в этих помещениях лиц, не имеющих права доступа в эти помещения, а также необходимых для обеспечения сохранности носителей персональных данных

В соответствии с инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ России от 13.06.2001 №152 необходимо обеспечить безопасность персональных данных посредством:

- организации хранения дистрибутивов СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в надежных металлических хранилищах, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин;

- в соответствии с п. 52 Приказа ФАПСИ № 152 окна выделенного спецпомещения, расположенного на втором этаже здания, где обрабатывается информация, содержащая персональные данные, необходимо оборудовать охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению;

- в соответствии с п. 30,64 Приказа ФАПСИ № 152 обеспечить хранение в шкафах (ящиках, хранилищах) оборудованных приспособлениями для опечатывания замочных скважин устанавливающих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ, ключевых документов, исключающее возможность бесконтрольного доступа к ним, а также их непреднамеренное уничтожение;

- в соответствии с п. 31 Приказа ФАПСИ № 152 аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудовать средствами контроля за их вскрытием;

- в соответствии с п. 51, 53 Приказа ФАПСИ № 152 оборудовать выделенное спецпомещение прочными входными дверями с замками, гарантирующими надежное закрытие спецпомещения в нерабочее время. Размещение, специальное оборудование, охрана и организация режима в спецпомещении должны исключить возможность неконтролируемого проникновения или пребывания посторонних, а также просмотра посторонними лицами ведущихся там работ;

- в соответствии с п. 55 Приказа ФАПСИ № 152 ключи от входных дверей спецпомещений пронумеровать, учесть установленным порядком, организовать выдачу ключей под роспись в журнале учета. Хранение ключей вне помещений Учреждения не допускается;

- в соответствии с п. 57 Приказа ФАПСИ № 152 спецпомещения обеспечить охранной сигнализацией, связанной со службой охраны Учреждения или другими средствами, препятствующими неконтролируемому проникновению и пребыванию в этих спецпомещениях;

- в соответствии с п. 59 Приказа ФАПСИ № 152 организовать хранение и выдачу ключей от спецпомещений установленным порядком;

3. Разъясняет о необходимости информирования УФСБ России по Республике Карелия о фактах возникновения объективных обстоятельств, препятствующих устранению причин и условий, способствовавших совершению административного правонарушения.

4. Предупреждает, что непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения, может повлечь ответственность, предусмотренную законодательством Российской Федерации.

5. Предлагает рассмотреть представление и в течение месяца с момента получения сообщить в УФСБ России по Республике Карелия по адресу: 185035, Республика Карелия, г. Петрозаводск, ул. Андропова, д. 5 об устранении выявленных причин и условий, способствовавших совершению административного правонарушения.

Начальник отделения в г. Лахденпохья
УФСБ России по Республике Карелия



А.С. Сагайда

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 176382614773150070335747769939328150673109021982

Владелец Корхонен Светлана Федоровна

Действителен с 11.04.2023 по 10.04.2024