Утверждаю
Директор КГОБУ
Шкотовской КШИ
_____ В.С. Семенцова

Приложение 2 к приказу
от 15 мая 2017 г. № 55

ПОЛОЖЕНИЕ № 16
об обработке защищаемой информации в КГОБУ Шкотовской КШИ
в сегменте государственной информационной системе «Контингент»

1. Общие положения

Целью данного Положения является обеспечение защиты информации, в том числе и персональных данных в КГОБУ Шкотовской КШИ , от несанкционированного доступа, неправомерного использования или утраты.

Настоящее Положение разработано на основании статей Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации»; Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119.

Настоящее Положение утверждается приказом директора КГОБУ Шкотовская КШИ и является обязательным для исполнения всеми лицами, имеющими доступ к работе в сегменте государственной информационной системе «Контингент».

2. Основные определения и понятия

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

3. Основания и цели обработки защищаемой информации

Основанием для обработки защищаемой информации, в том числе и персональных данных, являются следующие нормативными актами Российской федерации:

– Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;

– Распоряжение Правительства Российской Федерации от 25 октября 2014 г. № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

Целью обработки защищаемой информации, в том числе и персональных данных, является:

– прием заявления, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную образовательную программу.

4. Состав защищаемой информации

Состав защищаемой информации, обрабатываемой в сегменте государственной информационной системе определяется в документе «Перечень информации, подлежащей защите в сегменте государственной информационной системе «Контингент».

Состав персональных данных, обрабатываемых в КГОБУ Шкотовская КШИ определяется в соответствии с пунктами приказа «О выполнении требований законодательства Российской Федерации в области защиты персональных данных в КГОБУ Шкотовская КШИ.

5. Права субъекта персональных данных

Субъект персональных данных имеет право:

– на полную информацию о своих персональных данных и обработке этих данных.

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных законодательством РФ.

– требовать об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных законодательством РФ.

– защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Порядок обработки защищаемой информации

В целях обеспечения безопасности защищаемой информации, в том числе и персональных данных, все операции по оформлению, формированию, ведению и хранению данной информации в сегменте государственной информационной системе «Контингент» должны выполняться только пользователями, допущенными к обработке защищаемой информации, в соответствии с нормативно правовыми актами оператора, регламентирующими порядок допуска сотрудников к работе в сегменте государственной информационной системе «Контингент».

Пользователи ведут обработку защищаемой информации в соответствии с «Инструкцией пользователей и технологией обработки защищаемой информации в сегменте государственной информационной системе «Контингент» под контролем Администратора безопасности информации (далее Администратор) и Ответственного за организацию обработки персональных данных (далее Ответственный).

Администратор управляет системой защиты информации, осуществляет настройку и сопровождение средств защиты информации, осуществляет методическую поддержку пользователей в вопросах обработки и защиты информации и выполняет функции ответственного пользователя криптосредств в соответствии с «Инструкцией Администратора безопасности информации в сегменте государственной информационной системе «Контингент».

Ответственный назначается приказом директора КГОБУ Шкотовская КШИ, он контролирует обработку и защиту персональных данных, доводит до сведения работников оператора требования законодательства РФ в области защиты персональных данных, контролирует прием и обработку обращений и запросов субъектов персональных данных или их представителей.

Средства криптографической защиты информации используются в соответствии с «Положением о работе со средствами криптографической защиты информации в сегменте государственной информационной системе «Контингент».

В КГОБУ Шкотовская КШИ применяются прошедшие в установленном порядке процедуру оценки соответствия (сертифицированные) средства защиты информации.

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с «Положением об обработке персональных данных без использования средств автоматизации в КГОБУ Шкотовская КШИ.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке организации и в том объеме, который позволяет не разглашать излишний объем защищаемой информации.

7. Передача защищаемой информации

При передаче защищаемой информации в КГОБУ Шкотовская КШИ должно соблюдать следующие требования:

Передавать защищаемую информацию в порядке, установленном законодательством РФ, и ограничивать передаваемую информацию только теми сведениями, которые необходимы для выполнения конкретных задач.

Разрешать доступ к защищаемой информации только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только ту информацию, которая необходима для выполнения конкретных функций.

Передавать защищаемую информацию только тем организациям, с которыми заключен договор с указанием обязанности обеспечивать защиту информации, являющейся государственным информационным ресурсом в соответствии с текущим законодательством РФ.

8. Ответственность за разглашение защищаемой информации

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

Утверждаю
Директор КГОБУ Шкотовской КШИ
Ю.В. Семенова

Приложение 14 к приказу
от 15 мая 2017 г. № 55

ПОЛОЖЕНИЕ №15
о работе со средствами криптографической защиты информации в сегменте государственной информационной системе «Контингент»
в КГОБУ Шкотовской КШИ

1. Настоящее Положение разработано на основании статей следующих нормативных документов:

– «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», утверждённые приказом ФСБ России от 10.07.2014 № 378;

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9.02.2005 № 66;

– «Инструкция 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», утвержденная приказом ФАПСИ от 13.06.2001 № 152.

Контроль за соблюдением порядка работы со средствами криптографической защиты информации (СКЗИ) осуществляет Администратор безопасности информации (далее - Администратор).

Администратор допускается к работе с СКЗИ только после соответствующего обучения.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее — режимные помещения), должны обеспечивать сохранность защищаемой информации, СКЗИ и ключевых документов к ним.

При оборудовании помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ, указанные в эксплуатационных документах.

Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

.

Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения

или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает Администратор по согласованию, при необходимости, с директором. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.

Двери помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе.

Для предотвращения просмотра извне помещений их окна должны быть защищены.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя СКЗИ. Дубликат ключа от хранилища ответственного пользователя СКЗИ в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

По окончании рабочего дня помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале Администратора безопасности информации или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.
Ключи от помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Администратор безопасности информации.

В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ, ответственным пользователем СКЗИ или оператором.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Администратором необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в «Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов в сегменте государственной информационной системе «Контингент».

Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в Техническом (аппаратном) журнале АРМ ИС.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

Уничтожение ключевой информации может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) исходной ключевой информации без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Ключевую информацию, в отношении которой возникло подозрение в компрометации, необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.