МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2

ПРИКАЗ

от «01» 09. 2017 года **№ 72**

Об утверждении документов
по обеспечению безопасности информации,
не содержащей сведения, составляющие государственную тайну.

Руководствуясь статьей 22.1 Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по обеспечению безопасности информации, не содержащей сведений, составляющих государственную тайну (приложение 1).

2. Утвердить следующие формы журналов, используемых при обработке защищаемой информации, не содержащей сведения, составляющие государственную тайну (ЗИ), в том числе персональных данных, а также при эксплуатации технических средств защиты, согласно приложениям:

- журнал учета передачи защищаемой информации, не содержащей сведения, составляющие государственную тайну (Приложение 2);
- журнал учёта обращений субъектов персональных данных о соблюдении их законных прав в области защиты персональных данных (Приложение 3);
- журнал учета носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну (Приложение 4);
- журнал уничтожения носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну (Приложение 5);
- журнал учета мероприятий по контролю состояния защиты защищаемой информации, не содержащей сведения, составляющие государственную тайну (Приложение 6);
- журнал учета применяемых средств защиты информации, эксплуатационной и технической документации к ним (Приложение 7);
- журнал учета нарушений порядка предоставления ЗИ (Приложение 8);
- журнал сдачи, выдачи ключей от помещения (Приложение 9).

3. Назначить с 01. 09. 2017 г. лицом, ответственным за ведение журналов, используемых при обработке защищаемой информации, не содержащей сведения, составляющие государственную тайну, а также при эксплуатации технических средств защиты: учителя информатики Юкина С.В.

4. Контроль исполнения приказа оставляю за собой.

Директор МБОУ СОШ № 2 Л.Г. Пархоменко

С приказом ознакомлены С.В. Юкин

2

Приложение 1
к приказу №72 от «01» 09 2017 г.

Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам в Ростовской области

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

2016

1 Общие положения

Все должностные лица, уполномоченные на обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, в том числе персональные данные (ЗИ), а также остальные сотрудники, работающие в помещениях, в которых ведётся обработка ЗИ, должны быть ознакомлены с данной инструкцией.

Должностные лица, допущенные к обработке ЗИ, обязаны строго соблюдать установленные правила работы и несут персональную ответственность за обеспечение безопасности информации.

2 Порядок обеспечения безопасности при обработке и хранении ЗИ, осуществляемой с использованием средств автоматизации

Безопасность ЗИ при их обработке в информационных системах обеспечивается с помощью системы защиты, включающей организационные меры и средства защиты информации (СЗИ).

Допуск лиц к обработке ЗИ в региональном сегменте единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам в Ростовской области (далее - РИС) осуществляется на основании приказа «О сотрудниках, осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну».

Должна быть обеспечена сохранность носителей ЗИ и СЗИ, а также исключена возможность неконтролируемого пребывания в помещениях, в которых ведётся обработка защищаемой информации, посторонних лиц.

Компьютеры и (или) электронные папки (каталоги), в которых содержатся файлы с ЗИ, для каждого пользователя должны быть защищены

индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с ЗИ без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Сотрудникам, работающим с ЗИ, запрещается оставлять материальные носители с защищаемой информацией без присмотра в незапертом помещении.

Сотрудникам, работающим с ЗИ, запрещается сообщать ее устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения ЗИ. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (списков, картотек, файловых архивов и др.), содержащих ЗИ, запрещается.

Передача ЗИ допускается только в случаях, установленных Федеральными законами Российской Федерации, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача ЗИ по телефону, факсу, электронной почте за исключением случаев, установленных законодательством.

Все компоненты программного и аппаратного обеспечения РИС должны использоваться персоналом только в служебных целях. Использование их в других целях запрещается.

Запрещается приём посетителей в помещениях, во время осуществления обработки ЗИ, кроме случаев, возникающих при необходимости обработки ЗИ принадлежащей посетителю.

Пользователю запрещается самовольно изменять конфигурацию аппаратно-программных средств РИС или устанавливать дополнительно любые программные и аппаратные средства. Кроме того, все изменения конфигурации технических и программных средств осуществляются только с

участием администратора безопасности.

Категорически запрещается записывать и хранить ЗИ на неучтённых носителях, а также использовать носители с выявленными неисправностями.

Пересылка ЗИ без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

При обработке ЗИ пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) или съёмных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки ЗИ, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения заражённых файлов;
- незамедлительное восстановление ЗИ, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3 Порядок обеспечения безопасности при обработке и хранении ЗИ, осуществляемой без использования средств автоматизации

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ЗИ и исключающие несанкционированный к ней доступ. Лица, осуществляющие обработку ЗИ без использования средств автоматизации, должны быть проинформированы о факте обработки ими ЗИ, категориях обрабатываемой ЗИ, а также об особенностях и правилах осуществления такой обработки, в том числе (под личную подпись) с данной инструкцией.

При фиксации ЗИ на материальных носителях не допускается фиксация на одном материальном носителе защищаемой информации, цели обработки

которой заведомо не совместимы. Для обработки различных ЗИ, осуществляемой без использования средств автоматизации, для каждой категории защищаемой информации должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своём согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей,

предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путём обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путём фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путём изготовления нового материального носителя с уточнёнными персональными данными.

4 Порядок учёта, хранения и обращения со съёмными носителями, твёрдыми копиями и их утилизация

Все находящиеся на хранении и в обращении съёмные носители с ЗИ подлежат учёту. Каждый съёмный носитель с записанной на нем ЗИ должен иметь этикетку, на которой указывается его уникальный учётный номер.

Учтённый съёмный носитель получают для выполнения работ на конкретный срок. При получении делаются соответствующие записи в «Журнале учета носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну». По окончании работ пользователь сдаёт съёмный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале.

Запрещается:

- хранить съёмные носители с ЗИ вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съёмные носители с ЗИ из служебных помещений для работы с ними на дому, в гостиницах и т.д.

При отправке или передаче ЗИ адресатам на съёмные носители записываются только предназначенные адресатам данные.

О фактах утраты съёмных носителей, содержащих ЗИ, либо

разглашения, содержащихся на них сведений немедленно ставится в известность непосредственный руководитель. На утраченные носители составляется акт. Соответствующие отметки вносятся в «Журнал учета носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну».

Съёмные носители с ЗИ, пришедшие в негодность, или отслужившие установленный срок, подлежат передаче администратору безопасности для уничтожения.

5 Обязанности сотрудников по обеспечению безопасности ЗИ

В обязанности сотрудников входит:

- своевременный и точный ввод данных в РИС;
- немедленно ставить в известность администратора безопасности региональной информационной системы о случаях обнаружения непредусмотренных отводов кабелей и проводов, изменений алгоритмов функционирования технических и программных средств автоматизированного рабочего места (АРМ), нарушениях нормальной работы средств защиты, которые свидетельствуют о возможных попытках или фактах НСД к информации.
- по окончании рабочего дня сдача полученных во временное пользование съёмных носителей (гибких магнитных дисков, flash-носителей), а так же, при необходимости, индивидуальных идентификаторов, которые должны быть помещены в сейф (металлический шкаф).
- после окончания обработки ЗИ и изъятия съёмных накопителей информации необходимо выключить электропитание АРМ.

6 Ответственность

Сотрудник несёт ответственность за содержание вводимой им информации.

Сотрудник (пользователь РИС) несёт ответственность за сохранность и правильное использование получаемых в ходе выполнения работ машинных носителей и машинных документов с ЗИ. Степень конфиденциальности съемных носителей информации и документов, получаемых в ходе автоматизированной обработки информации, определяется администратором безопасности региональной информационной системы.

Сотрудники, осуществляющие обработку или хранение ЗИ, несут ответственность за обеспечение их информационной безопасности.

Лица, виновные в нарушении норм, регулирующих обработку и хранение ЗИ, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами в том числе:

- за разглашение ЗИ в процессе осуществления своей деятельности – в пределах определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.
- за причинение материального ущерба – в пределах, определённых действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

7 ЕДИНЫЙ ГЛОССАРИЙ ТЕРМИНОВ И СОКРАЩЕНИЙ

Термин, сокращение	Определение
Авторизация	Процедура предоставления определенному лицу или группе лиц прав на выполнение определенных действий
АРМ	Автоматизированное рабочее место
Аутентификация	Процедура проверки подлинности (например, «проверка подлинности пользователя путем сравнения введенного им пароля с паролем в базе данных пользователей»)
Безопасность информации	Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность
Доступ к информации	Возможность получения и использования информации
Защита информации	Деятельность, направленная на обеспечение безопасности защищаемой информации
Защищаемая информация	Информация, для которой обладателем информации определены характеристики ее безопасности
ЗИ	Защищаемая информации, не содержащая сведений, составляющие государственную тайну, в том числе персональных данных
НСД	Несанкционированный доступ
Обработка защищаемой информации	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с защищаемой информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
РИС	Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным

	программам в Ростовской области
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации