УТВЕРЖДАЮ
Заведующий Муниципального
бюджетного дошкольного
образовательного учреждения «Детский
сад комбинированного вида №30»

_____
(подпись)

Л.Д. Расинская

«11» января 2021 г.

ИНСТРУКЦИЯ

пользователя сегмента региональной информационной системы доступности дошкольного образования в Ставропольском крае Муниципального бюджетного дошкольного образовательного учреждения «Детский сад комбинированного вида №30»

1. Общие положения

Настоящая Инструкция разработана для обеспечения защиты персональных данных (конфиденциальной информации), обрабатываемых в сегменте региональной информационной системы доступности дошкольного образования в Ставропольском крае Муниципального бюджетного дошкольного образовательного учреждения «Детский сад комбинированного вида №30».

Персональные данные относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации являются:

- несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с конфиденциальной информацией (в том числе со служебными документами ограниченного распространения, персональными данными и т.д.) строится на следующих принципах:

принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник;

принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах;

2. Обязанности сотрудников, имеющих доступ к персональным данным (конфиденциальной информации).

Сотрудники, получившие доступ к персональным данным (конфиденциальной информации), обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки конфиденциальной информации немедленно информировать руководителя Учреждения.

Персональные данные (конфиденциальная информация) не подлежат разглашению (распространению). Прекращение доступа к такой информации

не освобождает сотрудника от взятых им обязательств по неразглашению сведений ограниченного распространения.

Сотрудники Учреждения при работе с персональными данными (конфиденциальной информацией) обязаны:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами автоматизированных рабочих мест;

выполнять требования Ответственного за обработку персональных данных (защиту информации), касающиеся защиты информации;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

хранить в тайне логин и пароль своей учётной записи, а также информацию о системе защиты, установленной на автоматизированном рабочем месте;

использовать для работы, только учтенные съемные носители информации;

контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления Ответственному за защиту персональных данных;

Немедленно ставить в известность руководителя Учреждения:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах автоматизированных рабочих мест или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищенному автоматизированному рабочему месту;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств автоматизированного рабочего места.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию персонального компьютера, выхода из строя или неустойчивого функционирования периферийных устройств (принтера, сканера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированном рабочем месте средств защиты, немедленно ставить в известность Ответственного за обработку персональных данных (защиту информации).

Ставить в известность Ответственного за обработку персональных данных (защиту информации) при:

- необходимости обновления антивирусных баз;

- обновлении программного обеспечения;

- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации автоматизированного рабочего места;

- необходимости вскрытия системных блоков персональных компьютеров, входящих в состав автоматизированного рабочего места;

- резервном копировании информации;

- и т.д.

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос аппаратных средств автоматизированного рабочего места, на котором проводилась обработка персональных данных, за пределы Учреждения с целью их ремонта, замены и т.п. без согласования с руководителем Учреждения и ответственным за обработку персональных данных (защиту информации) **запрещен**. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за обработку персональных данных (защиту информации). В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

Автоматизированные рабочие места, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана монитора, не имеющими отношения к обрабатываемой информации сотрудниками.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно конфиденциальную информацию;

- использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

- выполнять работы с конфиденциальной информацией на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя Учреждения;

- накапливать ненужные для работы персональные данные;

- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища;

- использовать компоненты программного и аппаратного обеспечения автоматизированных рабочих мест в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств автоматизированных рабочих мест или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить персональные данные на неучтенных носителях информации (USB-накопителях, CD, DVD дисках, гибких магнитных дисках и т.п.);

- оставлять автоматизированное рабочее место без блокировки входа в учётную запись (экрана монитора);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению инцидента информационной безопасности. Об обнаружении такого рода ошибок необходимо – ставить в известность ответственного за обработку персональных данных (защиту информации).

3. Ответственность

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты конфиденциальной информации (персональных данных).

За разглашение конфиденциальной информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной, административной или уголовной ответственности, предусмотренной законодательством Российской Федерацией.