УТВЕРЖДАЮ
Заведующий МОУ детским садом № 377
_____ Т.М. Жирова
«07» 09 2022г.

ИНСТРУКЦИЯ № 1
пользователя автоматизированной системы обработки конфиденциальной информации

1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты конфиденциальной информации в МОУ детского сада № 377.

Конфиденциальная информация относится к категории информации ограниченного распространения.

1.2.Наиболее вероятными каналами утечки информации для автоматизированных систем (АС) 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»).

1.3.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 и т.д.) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;

принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.);

2. Обязанности работников, имеющих доступ к конфиденциальной информации.

2.1.Работники, получившие доступ к 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 структурного подразделения, специалиста по защите информации.

2.2.Конфиденциальная информация не подлежит разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3.В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а

также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Правительства области, полученные в течение срока работы.

2.4.Работники при работе с конфиденциальной информацией обязаны:

Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

Выполнять требования администратора безопасности, касающиеся защиты информации;

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

Хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС;

Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

Контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы;

2.5.Немедленно ставить в известность руководителя подразделения, специалиста по отдела по защите информации:

- в случае утери носителя с конфиденциальной информацией 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 ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АС;

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

2.6.В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

2.7.Ставить в известность администратора безопасности структурного подразделения при:

- необходимости обновления антивирусных баз;

- обновлении программного обеспечения;

- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации АС;

- необходимости вскрытия системных блоков персональных компьютеров входящих в состав АС;

- резервном копировании информации;

- и т.д.

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

2.9.Вынос ПЭВМ, на которой проводилась обработка конфиденциальной информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.10.ПЭВМ, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

2.11.Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;
- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- накапливать ненужную для работы конфиденциальную информацию;
- передавать или принимать без расписки документы ограниченного распространения;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера.
- использовать компоненты программного и аппаратного обеспечения АС подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения, , ответственного за техническое и (или) программное обеспечение, начальника отдела защиты информации.

3. Ответственность

3.1.Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

3.2.За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Прошнуровано, пронумеровано
и скреплено печатью на 3 листах
Заведующий МОУ детский сад № 377
Т.М. Жирова МОУ