ПРИНЯТО
на заседании
Общего собрания
работников Учреждения
Протокол № 5 от 11.08.2017

УТВЕРЖДАЮ
Директор МАОУ СШ № 59
«Перспектива» г. Липецка
_____ Д.А. Гладышев
«_18_» августа_2017 г.

Инструкция пользователя
информационной системы персональных данных
в МАОУ СШ № 59 «Перспектива» г. Липецка

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность пользователей информационной системы персональных данных в МАОУ СШ № 59 «Перспектива» (далее – Организация или Оператор).

1.2. Пользователями информационной системы персональных данных, предназначенной для обработки информации, являются работники Организации, допущенные к работе в информационной системе персональных данных в установленном порядке на основании приказа Организации (далее – Пользователь).

1.3. Пользователь в своей работе должен руководствоваться настоящей инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

– Трудовой кодекс Российской Федерации (ст. 65, ст. 85-90);

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– локальные акты Организации в сфере обработки персональных данных.

1.4. Основные понятия и термины, используемые в настоящей инструкции, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.5. Пользователь получает указания от своего непосредственного руководителя и подотчетен ему.

1.6. Персональные данные (ПДн) относятся к категории информации ограниченного распространения.

1.7. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

– несанкционированный доступ к информации, обрабатываемой в ИСПДн;

– 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»).

1.8. Работа с персональными данными 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, 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.).

1.9. Пользователь несет персональную ответственность за свои действия.

2. Обязанности пользователя

2.1. Знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов, правил и инструкций Организации, регламентирующих деятельность по обработке и защите персональных данных в том числе:

– Правил обработки персональных данных;

– Порядка доступа работников в помещения, в которых ведется обработка персональных данных;

– Правил организации режима обеспечения безопасности помещений, в которых размещена информационная система;

– Правил доступа к персональным данным, обрабатываемым в информационной системе.

2.2. Знать и выполнять установленные требования по учету, хранению и использованию носителей персональных данных, обеспечению безопасности персональных данных.

2.3. Соблюдать установленную технологию обработки персональных данных.

2.4. Обеспечивать конфиденциальность персональных данных, ставших известными в результате обработки персональных данных.

2.5. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.6. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.7. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.8. 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.

2.9. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

2.10. Выполнять требования администратора безопасности, касающиеся защиты информации;

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

2.12. Хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;

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

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

2.15. При выходе в течение рабочего дня из помещения, в котором

размещается ИСПДн, пользователь обязан:

– блокировать ввод-вывод информации на своем рабочем месте ИСПДн в случаях кратковременного отсутствия (перерыв) или выключать ПЭВМ;

– блокировать вывод информации на монитор ПЭВМ;

2.16. Ставить в известность администратора ИСПДн структурного подразделения при:

– необходимости обновления антивирусных баз;

– обновлении программного обеспечения;

– проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

– необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

– резервном копировании информации т.д.

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

2.18. Вынос ПЭВМ, на которой проводилась обработка персональных данных, 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.

2.19. Соблюдать требования парольной политики.

2.20. При возникновении внештатных и аварийных ситуаций незамедлительно докладывать непосредственному руководителю и системному администратору информационных систем для приятия необходимых мер с целью ликвидации их последствий и возможного ущерба, в частности:

– 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 ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;

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

2.21. 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.

2.22. Пользователю ЗАПРЕЩАЕТСЯ:

– подключать к техническим средствам информационной системы персональных данных нештатные устройства (флэш-диски, карты памяти, жесткие диски и др.);

– самостоятельно вносить изменения в состав, конфигурацию и размещение технических средств ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИСПДн;

– разрешать работу со средствами ИС лицам, не допущенным к обработке персональных данных в установленном порядке;

– оставлять незаблокированными автоматизированные рабочие места при отсутствии на рабочем месте;

– сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн;

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

– несанкционированно открывать общий доступ к папкам на своей рабочей станции;

– отключать (блокировать) средства защиты информации;

– обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

– 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 ненужные для работы персональные данные;

– 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 ИСПДн подразделения в неслужебных целях;

– осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);

– 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, администратора безопасности.

2.23.При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован.

2.24.Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Права пользователя

3.1. Пользователь имеет право обращаться к ответственному за организацию обработки персональных данных по любым организационным вопросам, касающимся обработки и защиты персональных данных в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности персональных данных).

3.2. Пользователь имеет право обращаться к системному администратору информационных систем с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных средств защиты информации.

3.3. Пользователь имеет право обращаться к системному администратору с просьбой об оказании консультаций и технической помощи по использованию установленных в ИС программных и технических средств, в том числе средств защиты информации.

3.4.Решать в отведенное ему время поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

4. Ответственность пользователя

Пользователь информационной системы персональных данных несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией, в пределах, определенных действующим законодательством Российской Федерации, в частности:

– за соблюдение установленной технологии обработки информации;

– за соблюдение режима конфиденциальности ПДн при их обработке и хранении в ИСПДн;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

– за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с персональными данными.

Пользователи, виновные в несоблюдении настоящей инструкции, расцениваются как нарушители Федерального закона РФ 27.07.2006 № 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

5. Организация парольной защиты

5.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям администратором ИСПДн или создаются самостоятельно.

5.2. Правила формирования пароля:

– пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из 8 символов;

– в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);

➢ символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

– запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

5.3. Правила ввода пароля:

– ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

5.4. Правила хранение пароля:

– запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5.5. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

– своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

6. Правила работы в сетях общего доступа и (или) международного обмена

6.1.Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

6.2.При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус и других);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– запрещается скачивать из Сети программное обеспечение и другие файлы;

– запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);

– запрещается нецелевое использование подключения к Сети.

Разработал: ответственный за организацию обработки персональных данных _____ Е.В. Беляева

(подпись)