С.Н.Краева Подписано цифровой подписью: С.Н.Краева

Инструкция

ответственного лица за организацию обработки персональных данных муниципального автномного общеобразовательного учреждения муниципального образования город Краснодар гимназии № 25

1. Общие положения

1.1 Инструкция лица, ответственного за обработку персональных данных (далее – Инструкция) определяет в муниципальном автономном общеобразовательном учреждении муниципального образования город Краснодар гимназии № 25имени Героя Советского Союза Петра Гаврилова (МБОУ гимназия № 25) обязанности, права и ответственность.

1.2 Пользователями информационных систем персональных данных являются сотрудники МАОУ гимназии № 25, допущенные к обработке персональных данных в информационных системах персональных данных (ИСПД) в соответствии с утвержденным МАОУ гимназией № 25 перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных необходим для выполнения ими трудовых обязанностей.

1.3 Ознакомление сотрудников МАОУ гимназии № 25 с требованиями настоящей инструкции проводит администратор информационной безопасности информационных систем под подпись с выдачей копии Инструкции.

1.4 Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращения**
АРМ	Автоматизированное рабочее место
ИСПД	Информационная система персональных данных
ПД	Персональные данные
ПК (ноутбук)	Персональный компьютер

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014

Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде	

Термин	Определение	Источник
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных",

постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",

приказ ФСБ России от 10.07.2014 №378 Об утверждении Состава и содержания 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 требованиям к защите персональных данных для каждого из уровней защищенности",

приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

1.4. Работники, ответственные за обработку ПД должны быть ознакомлены с настоящей Инструкцией до начала работы. Обязанность по организации ознакомления с настоящей Инструкцией возлагается на ответственного за организацию обработки ПД.

2. Обязанности

2.1. Лицо, ответственное за организацию обработки ПД обязан знать и выполнять требования законодательства Российской Федерации и локальных актов МБОУ гимназии № 23, устанавливающих правила обработки и защиты персональных данных в информационных системах персональных данных

2.2. При эксплуатации ИСПД с целью защиты ПД пользователь обязан**:**

- руководствоваться требованиями организационно-распорядительной документации по организации обработки и защиты ПД;
- соблюдать установленную технологию обработки и защиты ПД;
- знать свои идентификаторы и пароли, осуществлять ввод паролей в условиях, исключающих их просмотр;
- не записывать значения паролей на бумагу, электронные носители, иные предметы и не разглашать (не сообщать или любым другим способом не доводить до кого либо, включая работников МБОУ гимназии № 23, в т. ч. директора, администратора безопасности значения действующих паролей;
- осуществлять смену пароля не реже, чем через 60 дней;

- ежедневно вести антивирусный контроль на непосредственных средствах ПК (ноутбуках);
- проверять вложения электронной почты перед началом работы на предмет наличия вредоносного программного обеспечения (далее – ПО);
- использовать для записи ПД только машинные носители информации, учтенные в установленном порядке;
- хранить машинные и материальные носители персональных данных в служебных помещениях, утвержденных Перечнем мест хранения персональных данных, исключающих несанкционированный доступ к ним;
- использовать для вывода на печать документов, содержащих информацию, находящуюся в ИСПД, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам ИСПД посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на ПК (ноутбуках) работ.

В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются ПК (ноутбуки) ИСПД и материальные носители ПД, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить ПК (ноутбуки), блокировать доступ к материальным носителям.

Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Докладывать администратору безопасности и руководителю:

- о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, ПК (ноутбуки) ИСПД, помещениям, в которых располагаются ПК (ноутбуки) ИСПД, и хранилищам;
- об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка ПД и хранилищ;
- об обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), при иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.), а также при нетипичном поведении ИСПД (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбои в работе);
- о попытках получения информации лицами, не имеющими к ней допуска;
- о попытках неконтролируемого проникновения посторонних лиц в помещения контролируемой зоны ИСПД;
- об иных внештатных ситуациях, связанных с угрозой безопасности ИСПДн.

2.5. **Пользователю запрещается**:

- подключать к ПК (ноутбукам) ИСПД нештатные устройства;
- применять в ИСПД незарегистрированные машинные носители

информации либо использовать учтенные машинные носители информации в неслужебных целях;

- при работе в сети Интернет:

использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

использовать информационные ресурсы сети Интернет, для целей, не связанных с областью производственной деятельности пользователя;

- выносить материальные носители ПД, машинные носители информации, мобильные технические средства данных за пределы контролируемой зоны МАОУ СОШ № 101 без письменного разрешения директора;
- несанкционированно вносить незарегистрированные машинные носители информации, мобильные технические средства;
- блокировать, изменять настройки и выгружать антивирусное ПО на своих ПК (ноутбуках);
- самостоятельно осуществлять подключение (отключение) ПК (ноутбуков) к локальной вычислительной сети;
- продолжать работы на ПК (ноутбуках) при обнаружении вредоносного ПО в процессе обработки информации;
- самостоятельно вносить изменения в состав, конфигурацию и размещение ПК (ноутбуков) ИСПД;
- самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИСПД;
- самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) ИСПД;
- сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к ИСПД;
- разрешать работу с ПК (ноутбуком) ИСПД лицам, не допущенным к обработке ПД в установленном порядке;
- находиться в нерабочее время в помещениях, где размещено оборудование ИСПД и СЗИ без служебной записки (или иного вида разрешающего документа), подписанного директором МАОУ ГИМНАЗИЯ №25.

3. Права пользователя информационной системы персональных данных

3.1. Пользователь ИСПД имеет право:

- обращаться к администратору безопасности ИСПД и ответственному за организацию обработки ПД по любым вопросам, касающихся обработки и защиты информации в ИСПД (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации ИСПД);
- обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИСПД информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);
- обращаться к системному администратору ИСПД и администратору

безопасности с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств ИСПД.

4. Ответственность

4.1. Ответственность за соблюдение требований настоящей инструкции пользователями возлагается на всех сотрудников МАОУ гимназии № 25, участвующих в обработке защищаемой информации (в том числе персональных данных).

4.2. На пользователя ИСПД возлагается персональная ответственность:

- за соблюдение установленной технологии обработки ПД;
- за соблюдение режима конфиденциальности информации;
- за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПД;
- за соблюдение требований локальных актов по вопросам обработки и защиты ПД в ИСПД.

4.3. Работники МАОУ ГИМНАЗИЯ № 25несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

4.4. Ответственность за организацию контрольных и проверочных мероприятий возлагается на администратора информационной безопасности информационных систем.

Лист ознакомления с инструкцией ответственного лица за организацию обработки персональных данных

№ п/п	**Ф.И.О. сотрудника**	**Дата ознакомления**	**Подпись сотрудника в ознакомлении**
