МУНИЦИПАЛЬНОЕ
БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 35 ГОРОДСКОГО ОКРУГА САМАРА

«Утверждаю»
Директор МБОУ СОШ № 35
г.о. Самара
Н.С.Мушкат
«__1__» __сентября__2014 г.

ИНСТРУКЦИЯ ДЛЯ ОПЕРАТОРОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1. Настоящая инструкция определяет порядок организации работ операторов по обеспечению защиты персональных данных сотрудников **МБОУ СОШ № 35**, обрабатываемых и хранимых в информационных системах персональных данных (ИСПДн) и определяет правовые последствия за нарушение правил информационной безопасности согласно Российского законодательства.

2. В своей работе субъекты доступа к персональным данным сотрудников **МБОУ СОШ № 35** должны руководствоваться требованиями настоящей инструкции, приказом Министерства образования Российской Федерации 343-55-148 ИН/СМИ от 03.07.02 г., ст. 24 Конституции РФ, главы 14 Трудового Кодекса РФ, Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., а также другими документами, определяющими порядок доступа и защиты персональных данных.

3. **Под персональными данными сотрудников** понимается информация, необходимая для трудовых (иных) отношений и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни, позволяющие идентифицировать его личность. Персональные данные **всегда являются конфиденциальной**, строго охраняемой информацией. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом. Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который изъявил желание вступить в трудовые (иные) отношения с **МБОУ СОШ № 35**. Субъект персональных данных самостоятельно решает вопрос передачи своих персональных данных. Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. **МБОУ СОШ № 35** выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

4. Состав персональных данных работника:

- анкета;
- автобиография;
- сведения– и копии документов об образовании;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места– жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

5. Защите подлежат персональные данные, обрабатываемые техническими средствами, а также представленные в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

6. Безопасность персональных данных при их обработке обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных. Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

7. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

8. Термины и определения, употребляемые в настоящей инструкции:

Автоматизированная информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Программное обеспечение (**ПО**) – совокупность компьютерных программ, описаний и инструкций по их применению на ЭВМ.

Информационные ресурсы (ИР) – отдельные документы и отдельные массивы документов, документы и массивы документов в АИС.

Информационное обеспечение (ИО) – совокупность единой системы классификации и кодирования технико-экономической информации, унифицированной системы документации и информационных ресурсов.

База данных (БД) – объективная форма представления и организации совокупности данных (например, статей, расчётов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Администратор сетевых ресурсов - лицо, ответственное за администрирование школьных серверов, на которых хранятся информационные ресурсы, согласно приказам по школе.

Объект ЭВТ – электронно-вычислительная техника (ЭВМ, принтер и т.п.), группа ПЭВМ в одном помещении, выполняющая одну задачу, локальная сеть ЭВМ.

Подразделение-пользователь (также субъект доступа) - пользователь, получивший разрешение (доступ) к БД и информационным ресурсам.

Субъект доступа (пользователь) – лицо, непосредственно осуществляющее доступ к информационным ресурсам.

Собственник информационных ресурсов, автоматизированных информационных систем, технологий и средств обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия владения, пользования, распоряжения указанными объектами. Собственник ИР имеет право устанавливать в пределах своей компетенции режим и правила обработки, защиты автоматизированных ИР и доступа к ним, определять условия расположения документами при их копировании и распространении.

Ответственный за защиту информации – лицо, осуществляющее контроль за соблюдением информационной безопасности, назначенное приказом по **МБОУ СОШ № 35**.

2. Основные положения.

2.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и

конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе деятельности **МБОУ СОШ № 35**.

2.2 В целях обеспечения прав и свобод человека и гражданина операторы при обработке персональных данных сотрудника обязаны соблюдать следующие общие требования:

- Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

2.3. Основными видами угроз безопасности информационных систем являются:

- противоправные действия третьих лиц;
- ошибочные действия пользователей и обслуживающего персонала АИС;
- отказы и сбои технических средств АИС, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

2.4. Целью защиты информации является:

- Предотвращение от утечки по техническим каналам, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства.
- Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.
- Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.

2.3. Обработка персональных данных **включает в себя** их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, обеспечения сохранности имущества. Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных

законодательством РФ. При принятии решений относительно сотрудника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

2.4. При обработке персональных данных сотрудников директор **МБОУ СОШ № 35** вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников на базе современных информационных технологий.

2.5 Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри **МБОУ СОШ № 35** исключительно для обработки и использования в работе.

2.6 К числу массовых потребителей персональных данных вне МБОУ СОШ № 35 можно отнести государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения муниципальных органов управления. Внутри **МБОУ СОШ № 35** к разряду потребителей персональных данных относятся сотрудники, которым эти данные необходимы для выполнения должностных обязанностей.

3. Порядок допуска к обработке персональных данных и проведению контрольных проверок программного обеспечения.

3.1. Основанием для допуска к работе с базами персональных данных и проведению контрольных проверок программного обеспечения, допуска к другим информационным ресурсам является приказ директора **МБОУ СОШ № 35**. При этом указанные лица должны иметь право получать только те персональные данные сотрудников, которые необходимы для выполнения конкретных функций.

3.2. Субъекты доступа, получающие доступ к базам персональных данных, должны изучить настоящую инструкцию и **оставить письменное подтверждение (подпись)** о неразглашении ими информации, к которой они имеют доступ, паролей, а также в том, что за нарушение правил информационной безопасности и данной инструкции они несут персональную ответственность в соответствии с законодательством Российской Федерации.

3.3. Ответственность за соблюдение требований по защите и обработке персональных данных, надлежащего порядка проводимых контрольных проверок программного обеспечения, возлагается на субъекты доступа к персональным данным, лиц, ответственных за защиту информации **МБОУ СОШ № 35, заместителей** руководителя, секретаря, администратора сети, в соответствии с назначенными им правами.

4. Порядок обработки персональных данных.

4.1. Оператор обязан **предоставлять доказательство** получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки

общедоступных персональных данных - доказательства того, что обрабатываемые персональные данные являются общедоступными;

4.2. Оператор обязан **не допускать использование** оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных;

4.3. В случае выявления оператором недостоверных персональных данных или неправомерных действий с ними, при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных обязан **осуществить блокирование** персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки и в срок, не превышающий **трех рабочих дней** с даты такого выявления, обязан устранить допущенные нарушения. В **случае невозможности устранения** допущенных нарушений оператор в срок, не превышающий **трех рабочих дней** с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор **обязан уведомить** субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4.4. В случае достижения цели обработки персональных данных, оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий **трех рабочих дней** с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий **трех рабочих дней с даты поступления указанного отзыва**, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

4.6. Оператор вправе осуществлять без уведомления субъекта персональных данных обработку его персональных данных в следующих случаях:

1) если сведения относятся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) если сведения, полученные оператором, являются связанными с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) если сведения являются общедоступными персональными данными;

5) если сведения включают в себя только фамилии, имена и отчества субъектов персональных данных;

6) если сведения необходимы для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор;

7) если сведения включены в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные

информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
8) если сведения обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
9) если обработка данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных не возможно;
10) если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
11) если обработка персональных данных осуществляется в целях научной, литературной или иной творческой деятельности, при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4.7. Согласие субъекта персональных данных обязательно должно быть дано в письменной форме, если:

1) персональные данные (**фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные добровольно субъектом персональных данных**) включаются в общедоступные источники;
2) оператором обрабатываются специальные (раса, национальность, политические взгляды, религиозные убеждения, состояние здоровья, интимной жизни), биометрические персональные данные (характерные физиологические особенности);
3) при любой передаче (распространении) его персональных данных;
4) при запрашивании любых персональных данных субъекта у третьего лица;
5) при принятии оператором решения, порождающего юридические последствия в отношении субъекта персональных данных;
6) при передаче персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных.

4.8. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

Для обработки персональных данных, содержащихся в согласии в письменной форме (например, в трудовом договоре) субъекта на обработку его персональных данных, дополнительное согласие не требуется.

4.9. Перед началом обработки персональных данных оператор обязан **на основании обращения** субъекта персональных данных представить информацию, касающуюся обработки его персональных данных:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных.

4.10. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

4.11. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

4.12. Обработка **специальных категорий** персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением **защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.**

4.13. Обработка специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Обработка **биометрических персональных данных** может осуществляться **без согласия** субъекта персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством РФ о безопасности, законодательством РФ об оперативно-розыскной деятельности, законодательством РФ о государственной службе, уголовно-исполнительным законодательством РФ, законодательством РФ о порядке выезда и въезда в РФ.

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

4.14. Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

5. Обработка персональных данных на компьютере

5.1. При обработке персональных данных при помощи компьютера необходимо принимать организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Оператор обязан:

- использовать сведения о персональных данных, содержащиеся в электронных документах только в служебных целях. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации;
- поручать обработку персональных данных другому лицу на основании договора, при чём существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке;
- приступать к работе по обработке персональных данных после обязательной своей идентификации и проверки подлинности доступа;
- не использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111» и им подобные, 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;
- не записывать пароли на бумаге, в файл, электронной записной книжке и других носителях информации, в том числе на предметах;
- удаление учётной записи и замену пароля производить в случае прекращения своих полномочий (увольнение, переход на другую работу внутри **МБОУ СОШ № 35)** полномочий администратора ИР и других сотрудников, которым по роду деятельности были предоставлены права доступа к персональным данным и полномочия по управлению подсистемой защиты информации, других функций в части защиты информации;
- использовать сертифицированные серийно выпускаемые в защищённом исполнении технические средства обработки персональных данных;
- производить необходимое количество резервных копий документов в соответствии с документацией на использование накопителей информации;
- надёжно хранить бумажные и машинные носители информации, ключи (ключевую документацию), не допускать их хищение, утрату, подмену или уничтожение;
- не разглашать пароли, IP-адреса, адреса сетевого адаптера, другие сетевые настройки;
- использовать сертифицированные средства защиты информации;
- иметь доступ только к тем ИР, которые разрешены для него согласно приказа руководителя **МБОУ СОШ № 35**;
- при получении персональных данных по электронной почте - использовать средства идентификации электронной подписи отправителя;
- в случае сбоя в работе компьютера, восстановление производить в соответствии с документацией на программное обеспечение с составлением акта восстановления**;**

- иметь на компьютере установленные лицензионные средства антивирусной защиты;
- периодически проверять систему на наличие в ней программ-вирусов, программных закладок;
- исключать возможность считывания информации с дисплеев компьютера посторонними лицами;
- не сообщать персональные данные третьей стороне без письменного согласия сотрудника, за исключением случаев, установленных федеральным законом;
- не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;
- не копировать обработанные персональные данные на жёсткий диск личного компьютера.

6. Доступ к персональным данным.

6.1. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать **номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя**. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

6.2. Внутренний доступ к персональным данным сотрудника имеют:

- руководитель **МБОУ СОШ № 35**, заместители руководителя, секретарь, системный администратор
- сотрудники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;
- сам сотрудник, носитель данных.

Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Субъект персональных данных **имеет право на получение** при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
2) способы обработки персональных данных, применяемые оператором;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
4) перечень обрабатываемых персональных данных и источник их получения;
5) сроки обработки персональных данных, в том числе сроки их хранения;
6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Право субъекта персональных данных на доступ к своим персональным данным **ограничивается** в случае, если:

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

6.3. Другие организации.

- Сведения о работающем или уже уволенном сотруднике могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления сотрудника.

6.4. Родственники и члены семей.

- Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника . В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

7. **Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника**

Операторы, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудников, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами (см. приложение).

Приложение

КОДЕКС ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц – от сорока до пятидесяти минимальных размеров оплаты труда.

ГРАЖДАНСКИЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 139. Служебная и коммерческая тайна

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения,

которые не могут составлять служебную или коммерческую тайну, определяются законом или иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок

от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия, -
наказывается лишением свободы на срок до четырех лет.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:
1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;
3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;
6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом;
8) работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
9) работники не должны отказываться от своих прав на сохранение и защиту тайны;
10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников
Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением требований настоящего Кодекса.

Статья 88. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законам.

С инструкцией ознакомлены:

Зам. директора по УВР	Т.В. Казурова
Зам. директора по ВР	О.В. Буянова
Зам директора по начальной школе	С.К. Бординова
Зам. директора по НМР и безопасности	Т.С. Милоенко
Зам. директора по питанию	Н.Е. Титова
Зам. директора по дошкольному отделению	Е.В. Тринбачёва
Зам. директора по АХЧ	Е.Г. Кузнецова
Главный бухгалтер	С.В. Ситникова
Секретарь школы	Н.Ю. Водовских
Системный администратор	А. Ю.Ситников