Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт общественных наук
Кафедра права и методики его преподавания

Защита персональных данных в общеобразовательной школе

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
Зав. кафедрой права и МП
ИОН УрГПУ
к.и.н., доцент
Ильченко В.Н.

_____ _____
дата подпись

Исполнитель:
Ульяницкий Сергей Сергеевич
обучающийся группы БП-41

_____
подпись

Руководитель:
Зав. кафедрой права и МП
ИОН УрГПУ
к.и.н., доцент
Ильченко В.Н.

_____
подпись

Екатеринбург 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В ходе развития цивилизации у человечества появлялось множество новых объектов, составляющих общественную жизнь, которым потребовалась защита путем закрепления в законе соответствующих норм. Основным таким объектом сегодня является информация, а это значит, что персональная информация, непосредственно затрагивающая частную жизнь человека должна быть под надежной защитой государства.

Как осуществляется защита персональных данных в общеобразовательной школе? Данная работа посвящена раскрытию **этой проблемы** как с теоретической, так и с практической сторон.

В современном обществе всё больший объем личной информации требует профессиональной, качественной и безопасной обработки. Каждый человек находится под угрозой последствий недобросовестного обращения с его персональными данными, а равно вмешательства в его частную жизнь. Вопрос того, кому и какой перечень информации о себе предоставлять стоит остро в связи с участившимися случаями всевозможных утечек персональных данных, мошеннических действиях, связанных с ними. Каким образом эту сферу общественной жизни регулирует государство? Насколько подвержено угрозе в этой сфере подрастающее поколение? Как гражданин может обезопасить себя и своих близких? Возрастающая общественная значимость этих вопросов обуславливает **актуальность** выбранной темы.

Законодательство в области защиты персональных данных активно развивается совместно с множеством исследований в этой области. Так в закон о персональных данных только за последние 5 лет изменения вносились 11 раз, 4 из которых в 2017 году. Это обусловлено появлением новых способов хранения и передачи подобной информации, вследствие чего возникновением новых правоотношений в данной сфере, что

подтверждает высокую **степень разработанности** выбранной темы, ее существенное **место и значение** в науке и практике.

Персональные данные работника и обучающегося в образовательной организации, и защита этих данных являются **объектом и предметом исследования**, соответственно.

Цель исследования – рассмотреть особенности защиты персональных данных в общеобразовательной школе. В **задачи исследования** входит обзор способов защиты персональных данных и предложение мер по повышению их эффективности.

В процессе изучения предмета ВКР использовались международные нормативные акты, законодательство Российской Федерации, труды Мазурова В.А., Полякова В.В., Смольковой И.В., Комковой Г.Н. и других.

Работа основывается, в первую очередь, на нормативно-правовой базе: международных декларациях и конвенциях; Конституции Российской Федерации; кодексах и комментариях к ним; федеральных законах РФ. Для раскрытия положений приведенных НПА используются учебники; программы научных конференций, журналы; электронные сайты; локальные нормативные документы МАОУ СОШ №48.

Выпускная квалификационная работа состоит из введения, двух глав, заключения, списка источников и литературы (33 источника), и 3 приложений.

ГЛАВА 1. СУЩНОСТЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ. ИСТОРИЧЕСКИЙ, ТЕОРЕТИЧЕСКИЙ АСПЕКТЫ

1.1. Становление института персональных данных в России и мире. Его выражение в нормативных документах. Основные термины

Для рассмотрения теоретических аспектов защиты персональных данных необходимо изучить нормативные акты, касающиеся предмета исследования, историю возникновения и развития данного института права, его место и значение в общественной жизни, и в деятельности образовательной организации. На основании полученных знаний требуется сформировать представление о предмете исследования, связанных с ним процессах и тенденциях развития.

Институт персональных данных является достаточно молодым по правовым меркам. В первую очередь, его становление очень тесно связывают с развитием прав и свобод человека, его правом на неприкосновенность частной жизни.

Английский термин «privacy» обозначает все стороны частной жизни и не имеет буквального эквивалента в русском языке. Известные американские юристы Сэмюэл Уоррен и Луис Брандейс в конце 19 века одними из первых попытались сформулировать суть понятия «privacy» и определили его как «the right to be alone» - право быть оставленным в покое. Они сделали вывод, что приватность ставится под угрозу посредством новейших изобретений в своей статье «Право на приватность», выпущенной в журнале о праве в Гарварде. Тем самым обозначили необходимость создания специального «права приватности». В дальнейшем в 20 веке, судами в США была сформирована так называемая «концепция прайвеси», ставшая основой формирования права человека на неприкосновенность частной жизни. После, была принята Всеобщая Декларация прав человека, которая провозгласила «никто не может подвергаться произвольному вмешательству в его личную и семейную

жизнь…». Так выражено право на тайну личной жизни, корреспонденции, неприкосновенность чести и репутации, сообразно с правом на неприкосновенность жилища. Помимо этого обозначено право на защиту законом от такого вмешательства [**Error! Reference source not found.**]. А так же в статье 8 Европейской конвенции о защите прав человека и основых свобод: «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции[0]. Данные документы закрепили право на неприкосновенность частной жизни в качестве неотъемлемого права каждого человека.

В российском законодательстве еще в дореволюционный период были закреплены некоторые элементы права на неприкосновенность частной жизни. Например, Телеграфный устав 1876г. закреплял тайну корреспонденции, Уголовное Уложение 1903г. устанавливало запрет на вмешательство должностных лиц в личную и семейную жизнь человека при отправлении правосудия. После революции 1917 года и до начала политической оттепели конца 1950-1960-х гг. в законодательстве СССР закрепление прав и свобод граждан в нормативно-правовых актах носило скорее формальный характер, и, напротив вмешательство в частную жизнь людей оправдывалось мерами, необходимыми для обеспечения государственной безопасности.

Во 70-х годах XX века в Гессене, принимается первый специальный закон о защите персональных данных, в последствии в течении 30 лет такие законы были приняты практически во всех европейских государствах. В них закреплялись реальные механизмы регулирования оборота персональных данных.

В Российской федерации Первоначальный проект такого разрабатывался в 1998 г. Законопроект носил рабочее название «Об информации персонального характера». Но в тот период данный законопроект до рассмотрения Государственной Думой не дошел. По прошествии двух лет Советом безопасности Российской Федерации была

сформирована другая рабочая группа, подготовившая окончательный вариант впоследствии принятого Федерального закона «О персональных данных» от 27.07.2006г. №152-ФЗ, который и является основным регулятором отношений в данной сфере[32,с.33-38].

«**Персональные данные** – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация». Обеспечение конфиденциальности персональных данных, при помощи которых можно идентифицировать лицо – главное требование закона. Для идентификации необходимо дополнение ФИО гражданина иными персональными данными, такими как номер телефона, адрес, дата рождения. Например ФИО совместно с датой рождения или ФИО вместе с номером телефона будут являться персональными данными, при помощи которых можно идентифицировать лицо, а сочетание даты рождения и номера телефона – нет, потому что их принадлежность к определенному лицу не установлена.

Рассмотрим **термины**, касающиеся защиты персональных данных, приведенные в соответствующем федеральном законе(определения данных терминов приведены в **приложении 3**):

- персональные данные;
- оператор;
- обработка персональных данных;
- автоматизированная обработка персональных данных;
- распространение персональных данных;
- блокирование персональных данных;
- уничтожение персональных;
- обезличивание персональных данных;
- информационная система персональных данных;

- трансграничная передача персональных данных.

В юридической литературе представлена неоднозначная классификация охраняемой законом информации (сведений). Рассмотрим несколько классификаций, приводящихся в исследованиях Копылова, Смольковой, Мазурова.

В.А. Копылов приводит классификацию на основании доступа к информации, т.е. открытая информация и информация ограниченного доступа [20].

Открытая информация согласно Копылову: массовая информация, информация о выборах, официальные документы, обязательно представляемая (экземпляры документов, регистрационная и другая), научно-юридическая и пр.

Информация ограниченного доступа согласно В.А.Копылову – составляющая коммерческую тайну, государственная тайна, персональные данные и др. В.А. Копылов поясняет, что персональные данные и другая личная информация производятся в процессе повседневной деятельности, осуществлением гражданами их права на труд, медицинскую помощь, свободу слова и др. в процессе которого они предоставляют сведения о себе другим субъектам персональных данных.

Согласно И.В. Смольковой классификация защищаемой инфорамции выглядит так[25]:

- государственная (в том числе военная) тайна;
- конфиденциальная информация (в которую входят личная, семейная, профессиональная, служебная и коммерческая тайны).

В.А. Мазуров приводит следующую классификацию[22]:

- информация, находящаяся в открытом доступе;
- информация с ограниченным доступом (к ней можно отнеститайну частной жизни, профессиональную тайну, служебную тайну, государственную тайну).

Рассмотрев несколько мнений ученых юристов на классификацию информации, требующей защиты мы можем сделать вывод, что правовое регулирование данной сферы общественных отношений находится в процессе развития. Углубленное изучение проблем, встающих перед учеными обеспечивает наиболее тщательную проработку вопроса защиты персональных данных, получение более полных знаний о способах такой защиты, видах информации, нуждающихся в ней. Впоследствии на основе полученных в ходе таких исследований знаниях формируется законодательство, обеспечивающее эффективную защиту незыблемых прав человека, защиту информации имеющей определяющее значение для государственной безопасности и других ее видов. К сожалению, на данный момент нельзя утверждать, что потребности современного общества по защите личных данных удовлетворяются в полной мере. Законодательство, регулирующее эту сферу отношений развивается, отвечая на новые вызовы, диктуемые бурной модернизацией информационных технологий, возникновением новых правоотношений между субъектами защиты персональных данных.

Персональными данными считается информация о конкретном человеке, по которой он может быть идентифицирован и которая зафиксирована на материальном носителе. Сегодня к защите такой информации предъявляется все больше требований ведь в нее входят личная характеристика, финансовое положение, образование, профессия, сведения о состоянии здоровья и многое другое. Учитывая важность перечисленных данных к защите информации подобного рода и гараниям из сохранности предъявляются все более серьезные требования.

А.Г. Саидов в своих работах рассматривал правовое обеспечение безопасности в информационной сфере, ее законодательное регулирование. Предметом своего исследования Саидов выбрал содержание и значение правовых норм, на основании которых строится информационная безопасность Российской федерации[24]. Автор принял участие в

исследовании защиты персональных данных и обеспечения информационной безопасности в Российской Федерации с точки зрения права. Так же А.Г. Саидов утверждает, что, поскольку защита персональных данных является относительно новой областью деятельности, законодательство Российской Федерации должно ориентироваться на зарубежный опыт и иметь скорее позитивную направленность, нежели определение широкого комплекса штрафных санкций за его нарушение в качестве единственного механизма, обеспечивающего исполнение. В данном случае скорее нужно «разъяснить и научить нежели запретить и наказать».

Саидов видит необходимость в принятии Федерального закона «О неприкосновенности частной жизни», который бы наиболее полно определил случаи, когда допускается ограничение прав в сфере защиты персональных данных, в соответствии с Конституцией и решениями ЕСПЧ. Саидов утверждает, что Российская Федерация для обеспечения защиты персональных данных всех граждан должна создать все необходимые условия в строгом соответствии с международными договорами и обеспечить исполнение этих условий в полном объеме.

В.Я. Ярочкин в своей работе «Информационная безопасность» персональные данные к типу информации, которому требуется строгая правовая защита[26]. Он доказывает важность сохранности личной информации человека, необходимость ее правовой защиты. Так же в работе обозначаются угрозы персональным данным, виды угроз направленных на утечку такой информации, а так же приводятся рекомендации по защите от них. Помимо этого приводится перечень правовых актов, обеспечивающих регулирование отношений в данной сфере и в заключении некоторые технические аспекты защиты персональных данных. На основании перечисленного выше можно отметить, что Ярочкин попытался охватить все аспекты охраны

персональных данных и других видов конфиденциальной информации, дать полное описание и характеристику указанной проблеме.

В.В. Поляков и В.А. Мазуров проведя исследование «Проблемы правовой и технической защиты информации», разработали перечень наиболее эффективных средств для обеспечения информационной безопасности[23]. Отдельно стоящим компонентом исследования можно выделить подготовку специалистов по работе с персональными данными и их защите ввиду их нехватки на рынке труда. Дефицит кадров в данной, казалось бы, перспективной сфере труда объясняется большим комплексом требований, предъявляемых к кандидатам на данную должность и высокой степенью ответственности оператора персональных данных.

Н.А. Алимова в «Большом справочнике кадровика», углубленно изучает стороны проблемы защиты персональных данных работника [19]. В своем труде Алимова дает определение и развернутое объяснение сути понятий, касающихся обработки персональных данных в организации. Приводит рекомендации по организации работы с такими данными начиная от приема на работу, заканчивая хранением и уничтожением персональных данных с соблюдением требований действующего законодательства. Так же исследование Алимовой затрагивает порядок привлечения работника к дисциплинарной ответственности в случае нарушения правил обработки персональных данных, и, соответственно, формы такой ответственности.

В работе «Уголовно-правовые аспекты информационной безопасности» В.А. Мазурова тщательно подходит к рассмотрению понятия и принципов информационной безопасности, основных направлений развития законодательства, а также правовое понятие и классификацию охраняемой законом информации[22]. Мазуров определил комплекс мероприятий по защите персональных данных, привел определение и классификацию основных угроз безопасности такой информации.. Уголовно-правовая защита персональных данных

представлена особой частью его работы, в рамках которой. В.А. Мазуров проводит изучение и характеристику объекта и предмета преступлений, направленных против неприкосновенности частной жизни. Им раскрывается объективная сторона составов преступлений, и перечисляются формы ответственности за разглашение конфиденциальной информации.

Рассмотрим **нормативно-правовые акты**, регулирующие общественные отношения в процессе накопления, обработки, хранения персональных данных граждан.

Согласно ч.1 статьи 4 ФЗ 152 «О персональных данных»: Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Основные нормативные правовые акты в области персональных данных[34]:

- «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)[5];
- «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 28.01.1981 EST № 108;
- Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 23.04.2018 N 102-ФЗ) [10];
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 29.07.2017 N 223-ФЗ) [11];
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 13.07.2015);
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Минкомсвязи РФ от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним

нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- Приказ Роскомнадзора от 5 сентября 2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Законодательство о защите персональных данных имеет чрезвычайную значимость для человека, поскольку право на защиту такой информации исходит из конституционного права человека на неприкосновенность частной жизни, личной и семейной тайны.

Принципы обработки персональных данных соответствуют требованиям ратифицированных международных актов, регулирующих использование и хранение такой информации. Особым образом закон выделяет недопустимость обработки специальных категорий персональных данных: расовая принадлежность, национальность, религиозные и философские убеждения, состояние здоровья, сведения об интимной жизни, политические взгляды. Хотя и в данном случае закон предусматривает исключения.

При определенных условиях у субъекта персональных данных есть право доступа к своим данным, право на получения сведений об источнике их получения, информации о содержании, целях и способах обработки. Субъект имеет право потребовать их блокирования, уничтожения или уточнения, либо дать письменное согласие на их включение в общедоступные источники.

С другой стороны, на оператора накладывается обязанность по созданию организационных и технических условий при которых обеспечивается защита персональных данных от незаконного уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

На основе всего вышеперечисленного можно отметить широкое развитие отечественного и международного законодательства в области защиты персональных данных, его постоянное совершенствование,

связанное с внедрением новых способов контроля, отслеживанием передовых технологий сбора, хранения и обработки информации. Законодатель выделяет широкий спектр прав субъекта персональных данных в отношении информации, касающейся его, и, напротив определяет строгие требования к оператору персональных данных, особенностям его работы.

1.2. Ответственность за нарушение правил работы с персональными данными в образовательной организации

Законом устанавливается гражданская, уголовная, административная и дисциплинарная ответственность. Субъект персональных данных в судебном порядке обжалует действия оператора в случае нарушения своих прав в ходе обработки конфиденциально информации. Утверждение в Российской Федерации специального органа, в полномочия которого включена защита персональных данных, породило новый для России институт общественных отношений. В сферу его деятельности входит осуществление контроля и надзор за соблюдением законодательства по защите персональных данных. В круг полномочий контрольного органа входит право обращаться в суд для защиты интересов субъектов персональных данных.

Далее подробно рассмотрим **виды ответственности** оператора персональных данных. Внутренними правилами распорядка образовательной организации устанавливается дисциплинарная ответственность. В соответствии со ст.81 ТК РФ, работнику, совершившему дисциплинарный проступок, связанный с обработкой персональных данных выносится замечание, выговор, либо увольнение по отрицательным мотивам на основаниях приведенных в данной статье[7]. В Трудовом кодексе РФ указано, что в случае нарушения правил обработки персональных данных наступает гражданская, уголовная, административная, дисциплинарная ответственность и нет четкого

определения вида дисциплинарной ответственности за нарушение порядка обработки персональных данных.

Согласно порядку гражданского судопроизводства, субъект персональных данных может в суде потребовать от оператора компенсацию морального вреда, а так же возмещения убытков, понесенных вследствие разглашения его личной информации.

Согласно статье 13.11 КоАП «административная ответственность предусмотрена за нарушение установленного Законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) в виде предупреждения или наложения на граждан административного штрафа в размере от трех до пяти минимальных размеров оплаты труда (МРОТ), от пяти до десяти МРОТ для должностных лиц и от пятидесяти до ста МРОТ для юридических лиц»[9].

Защита персональных данных человека входит в комплекс прав, гарантируемых государством и определяется как одна из составных частей института, формирующего гарантии неприкосновенности частной жизни людей. Уголовным кодексом Российской Федерации в его особенной части определяются виды наказания за нарушение данного права человека, в том числе выражающееся в несоблюдении порядка защиты персональных данных [6]. Статья 137 Уголовного Кодекса Российской федерации устанавливает уголовную ответственность за: «незаконное собирание или распространение сведений о частной жизни лица, составляющих личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации». За совершение такого преступления лицо, виновное в нем приговаривается к уплате штрафа в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до одного года, либо арестом на срок до четырех

месяцев. В случае совершения того же преступления лицом, заведомо использовавшим для этого свое служебное положение наказанием будет штраф в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арест на срок от четырех месяцев до полугода.

В целях обеспечения работы с персональными данными проводится комплекс мероприятий, закрепляемый в документах организации. В первую очередь руководителем назначается лицо или подразделение, ответственное за данный вид деятельности, и наделяется соответствующими полномочиями. Затем определяется перечень персональных данных, нуждающихся в обработке. Далее – подготавливается и утверждается приказом руководителя список лиц, которые допущены к данной деятельности.

Основным локальным документом, регулирующим защиту информации в организации является «**Положение о работе с персональными данными**» (Пример такого положения можно увидеть в **приложении 2**). В нормативных документах не установлена унифицированная форма и структура текста такого положения, поэтому зачастую оно строится исходя из строения законов, регулирующих обработку персональных данных. Нет и единого заголовка. Уже разработанные в организациях документы называются «О защите персональных данных» или «Об организации работы с персональными данными». В большинстве своем такие документы состоят из нескольких разделов, в которых раскрываются термины, перечисляется нормативная база, определяется перечень данных, подвергающихся обработке, и прилагаемого образца заявления «О согласии на обработку персональных данных» (Приложение 1). Отдельным пунктом положения обязательно

перечисляется в каких случаях согласие работника на обработку его данных не требуется.

Надлежащее исполнение правил обработки персональных данных в общеобразовательной школе обеспечивается определенной законом ответственности лиц, участвующих в данной деятельности, за нарушение соответствующих должностных инструкций.

Статья 90 Трудового Кодекса РФ за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, предусматривает дисциплинарную, административную, гражданско-правовую и уголовную ответственность[8].

Трудовой кодекс, помимо замечания, выговора и увольнения работника (предусмотренных статьей 192 ТК РФ), совершившего дисциплинарный поступок предусматривает так же специальное основание расторжения ТД в случае разглашения охраняемой законом тайны оператором персональных данных(п.п. "в" п.6 ст.81)[8].

Работники, совершившие дисциплинарный проступок несут **дисциплинарную ответственность**. Дисциплинарная ответственность - самостоятельный вид юридической ответственности работников организации. К признакам дисциплинарного проступка относят наличие субъекта проступка, субъективной стороны, а так же объекта проступка и объективной стороны.

Внутренний трудовой распорядок организации – объект дисциплинарного проступка. Объективная сторона – вредные последствия и прямая связь между ними и действием работника.

Субъектом является гражданин, находящийся в трудовых правоотношениях с конкретной организацией и нарушивший трудовую дисциплину. Субъективная сторона такого проступка - вина со стороны работника, форме умысла или по неосторожности.

На основании заключенного трудового договора работодатель требует от работника добросовестного выполнения возложенных на него

обязанностей. В соответствии со ст. 192 ТК работодатель имеет право, но не обязан привлекать к дисциплинарной ответственности работника, совершившего дисциплинарный проступок. Так же следует отметить, что в законодательстве Российской Федерации, уставами и положением о дисциплине организации определяются различные правила при совершении дисциплинарного проступка.

Разглашение персональных данных потерпевшего лица может быть совершено среди широкого круга лиц, не имеющих законного доступа к ним. Главные нарушения правил работы с персональными данными: получение конфиденциальной информации, либо ее использование без законных оснований, а так же утрата материальных носителей информации, содержащих такие сведения [27]. За данные нарушения предусмотрена дисциплинарная ответственность, не предусматривающая увольнения, но в случае, если работник совершил разглашение персональных данных какого-либо лица, то ему грозит увольнение. К дисциплинарной ответственности могут быть привлечены только сотрудники кадровой службы, взявшие на себя обязанность исполнять требования правил, обеспечивающих безопасность при работе с персональными данными. Это значит, что они взяли на себя обязанность не разглашать сведения, составляющие персональные данные, что было закреплено в их трудовом договоре, их ознакомили под подпись с локальными нормативными актами, и работодателем были предоставлены требуемые для осуществления должностных полномочий условия.

В случае отсутствия проведения перечисленных выше мероприятий, специалист, которому доверена работа с персональными данными, ответственности не несет. Факт нарушения правил работы с персональными данными может быть установлен представителем работодателя (например, начальником отдела кадров), самим работником или специалистом государственной инспекции труда.

К правам работников организации в отношении защиты своих персональных данных относятся: осуществление контроля над полноценным выполнением требований по обеспечению конфиденциальности этой информации, наличием всех предусмотренных средств защиты персональных данных; право запретить или приостановить обработку персональных данных в случае их невыполнения[14]. С целью отстаивания своих законных прав работник имеет право обжаловать в судебном порядке любые неправомерные действия (бездействие) работодателя при обработке и защите персональных данных.

Административная ответственность. Кодекс об административных правонарушениях РФ с 2017 года выделяет 7 статей (до этого - 2) за нарушение правил работы с персональными данными.

Статья 13.11 предусматривает ответственность в виде предупреждения или наложения штрафа для должностных лиц в размере от 3000 до 20000руб., ИП – от 5000 до 20000руб., организации на сумму от 15000 до 75000руб. При этом привлечение к ответственности происходит по нескольким составам правонарушений сразу. Ранее – состав нарушения был один, а максимальный штраф составлял 10000руб.

Защита конфиденциальности такого вида охраняемой законом тайны как персональные данные предусматривается в статье 13.14 КоАП РФ.

Информация, имеющая ограниченный доступ является объектом правонарушения.

Объективная сторона данного правонарушения состоит в действиях, в результате которых произошло разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Конфиденциальную информацию определяет административное, гражданское и иное отраслевое законодательство РФ.

Административную ответственность работодатель несет только в случае его привлечения к таковой государственной инспекцией труда или судом.

Далее следует рассмотреть наиболее строгий вид ответственности – **уголовная ответственность**. Статья 137 УК РФ предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, в том случае, если такие действия являлись намеренными, в целях корыстной или иной личной заинтересованности. В случае использования виновным своего служебного положения, наказание ужесточается[18].

Личную или семейную тайну составляют сведения, не подлежащие, по мнению лица, которого они касаются, оглашению, при условии, что ранее они не были опубликованы либо оглашены иным способом.

Виды нарушения неприкосновенности частной жизни (ст. 137 УК):

- незаконное собирание сведений о частной жизни;
- незаконное их распространение;
- незаконное их распространении в публичном выступлении, в СМИ.

В законодательстве не указана связь ответственности за разглашение конфиденциальной информации с конкретным способом такого распространения. Распространением считается любая передача конфиденциальной информации третьим лицам. Незаконным распространением является разглашение конфиденциальной информации лицом (работником организации), обязанным держать ее в тайне в силу трудового договора и законодательства РФ. В некоторых случаях разглашение сведений о частной жизни по УК образует одновременно состав другого преступления например, разглашение тайны усыновления (ст. 155), В таких случаях содеянное квалифицируется по совокупности со ст. 137 УК.

Обязательный элемент объективной стороны такого преступления согласно ст. 137 УК - вред правам и законным интересам.

По характеру вред разделяется на: моральный, материальный физический. Установление наличия и характера вреда, причиненного потерпевшему, производится индивидуально с учетом особенностей ситуации и личности.

Законом определено, что, преступлением, посягающим на неприкосновенность частной жизни можно считать только действия, повлекшие за собой причинение соответствующего вреда, то есть материального состава.

Корыстная или иная личная заинтересованность – основной элемент субъективной стороны (мотив). Намерение опорочить конкурента, повлиять на личное продвижение в карьере, месть, демонстрация превосходства и другие виды выгоды за счет потерпевшего называются корыстной заинтересованностью. По ч. 1 ст. 137 УК ответственность несет любое физическое вменяемое лицо, достигшее 16 лет (общий субъект), а по ч. 2 ст. 137 УК - должностное лицо либо служащий государственного или муниципального учреждения, использующий для совершения преступления свое служебное положение (специальный субъект).

Несмотря на то, что приведенное выше законодательство, и предусмотренная за его нарушение ответственность направлены на обеспечение права человека на неприкосновенность частной жизни, в силу ч. 3 ст. 55 Конституции предусматриваются определенные ограничения права на защиту информации о частной жизни в случаях, когда это является необходимой мерой, направленной на защиту конституционного строя, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

ГЛАВА 2. ПРАКТИКА ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЕ

2.1. Организация сбора, хранения и обработки персональных данных в общеобразовательной школе

Необходимость защиты персональных данных в информационную эпоху не вызывает сомнений. Сегодня, нововведения в законодательство РФ, связанные с обработкой персональных данных направлены на совершенствование методов защиты таких данных. Существует комплекс законов, обеспечивающих информационную безопасность, которые претерпевают не одно изменение ежегодно, с целью своевременной реакции на современные вызовы информационной безопасности. За последние годы в Российской Федерации был реализован обширный комплекс мер, направленный на обеспечение безопасного хранения, обработки и передачи информации. Соответствующие мероприятия были осуществлены в органах государственной власти федерального уровня, органах субъектов Российской Федерации, на коммерческих и иных предприятиях, в учреждениях и организациях независимо от формы собственности.

В рамках повышения качества обработки персональных данных Российская Федерация сотрудничает с международным сообществом и перенимает богатый заграничный опыт, что способствует политическому, экономическому, культурному и иному взаимодействию мировых держав.

В систему государственной защиты информации входят органы и исполнители, используемая ими техника защиты информации и объекты защиты, организованные по правилам, установленным соответствующими нормативно-правовыми актами в области защиты персональных данных. Так же это является составной частью системы обеспечения национальной

безопасности Российской Федерации целью которой является защита государства от угроз в информационной среде.

В данную систему входят подсистемы, занимающиеся лицензированием деятельности предприятий в области защиты информации, сертификацией средств защиты информации и аттестацией объектов информатизации.

Органы, которым поручено регулирование защиты персональных данных:

- Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
- Федеральные органы исполнительной власти
- Органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности
- Предприятия, оказывающие услуги в области защиты информации
- Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации
- Научно-исследовательские организации по проблемам защиты информации
- Органы системы сертификации средств защиты информации
- Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
- Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации

- Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации
- Органы системы лицензирования деятельности в области защиты информации
- Органы системы аттестации объектов защиты по требованиям безопасности информации

В рамках правовых мер рассматривается деятельность законодательных органов, целью которой является создание правовой базы, которая бы гарантировала должный порядок обработки информации, регулировала полномочия субъектов и определяла ответственность за соответствующие нарушения обозначенных правил.

Существует два направления правовых основ защиты конфиденциальной информации: специализированное и иное законодательство (содержащее правовые нормы, дающие гарантию неприкосновенности частной жизни лишь косвенно или отчасти). Федеральный закон «О персональных данных» от 27 июля 2006 г., Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г., Указ Президента РФ от 6 марта 1997 г. №188, утверждающий «Перечень сведений конфиденциального характера» являются основными элементами специализированного законодательства.

Глава 14 ТК Российской Федерации, содержит правовые нормы, регулирующие обработку персональных данных работника, а так же Закон «Об архивном деле в Российской Федерации» от 22 октября 2004 г. (ст.25), Законе «Об оперативно-розыскной деятельности» (ст. 3, 5, 9, 10, 12, 21), Законе «О средствах массовой информации» (ст. 41, 43, 46, 51, 57), Закон «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования», в соответствии с которым персональные данные содержатся в индивидуальном лицевом счете

застрахованного лица, нормы о защите сведений, полученных в ходе всероссийской переписи населения (персональные данные) содержатся в Законе «О всероссийской переписи населения».

В 1981 году в Страсбурге была принята Конвенция СЕ «О защите физических лиц при автоматизированной обработке персональных данных», с целью защиты интересов граждан при электронной обработке их. В России Федеральный закон о ратификации данной Конвенции был подписан Президентом РФ 19 декабря 2005 года.

В соответствии со ст. 5 Конвенции, персональные данные, подвергающиеся автоматизированной обработке:

- собираются и обрабатываются на справедливой и законной основе;
- хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями;
- являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;
- являются точными и, когда это необходимо, обновляются;
- сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных.

Основным нормативным актом, принятым с целью регулирования защиты персональных данных в РФ, является Федеральный Закон «О персональных данных». При разработке данного федерального закона в его основу были заложены принципы, утвержденные Советом Европы в рамках Конвенции «О защите физических лиц при автоматизированной обработке персональных данных», а также положения Директивы Европейского Парламента и Совета Европы 95/46/ЕС «О защите личности в отношениях обработки персональных данных и свободном обращении этих данных» и Директивы Европейского Парламента и Совета Европы 2002/58/ЕС от 12 июля 2002 г., определяющей правила защиты персональных данных в электронном коммуникационном секторе.,

Принципы обработки персональных данных в российском законодательстве сообразны с принципами в странах Совета Европы установленными в статьях 6 и 7 Директивы95/46/ЕС. Перечень принципов, установленных в статье 5 Закона «О персональных данных», защищающих персональную информацию человека:

- персональные данные собираются законно и добросовестно. Данная норма подразумевает сбор и использование конфиденциальной информация о лице только с согласия субъекта персональных данных, за исключением случаев, четко оговоренных в части 2 статьи 6 Закона, когда такое согласие не требуется, и всегда в строгом соответствии с законом. Субъект предоставляет Согласие на обработку персональных данных в письменной форме; содержание этого документа четко установлено в п. 4 статьи 9 Закона
- заранее четко определенные цели использования персональных данных не должны изменяться. Не допускается сбор и использование сведений о субъекте для иных целей, кроме тех, на которые субъект дал письменное согласие (п.2 ч. 1 ст. 5).
- объем, характер и способы обрабатываемых персональных данных должны соответствовать целям обработки персональных данных. Данная норма пресекает возможность сбора иных персональных данных, выходящих за рамки объявленных заранее.
- собираемые персональные данные обязательно должны быть достоверными, а ширина перечня собираемой персональной информации определяется целями ее сбора. В случае обнаружения в обрабатываемых персональных данных субъекта ошибки или сведений, по какой-либо причине являющихся недостоверными субъект имеет право на внесение необходимых изменений (п.3 статья 20).
- запрещается объединение баз персональных данных в единую информационную систему, если они были собраны операторами для

различных целей. Такая мера принята во избежание возможности при утечке одной базы данных, имеющей узкую направленность, получить широкий спектр сведений о субъекте, и, тем самым возникновения угрозы его безопасности.

- временные рамки хранения персональных данных субъекта, определяются целями их обработки, такие данные подлежат уничтожению по достижении обозначенных или в случае утраты необходимости в их достижении.

Теперь, рассмотрим Доктрину информационной безопасности РФ, утвержденную Президентом РФ 9 сентября 2000г. В данном документе отражены основные цели, задачи, принципы и направления обеспечения защиты информации РФ. В данной доктрине выделяются следующие составляющие национальных интересов Российской Федерации: соблюдение конституционных прав и свобод, защита информационных ресурсов, обеспечение безопасности телекоммуникационных систем. На основе данной доктрины формируются:

- направления государственной политики, касающиеся информационной безопасности РФ;
- нововведения в областях правового регулирования, научно-технических средств, организационного и методического обеспечения безопасности Российской Федерации при обработке информации разного;
- целевые программы, в задачи которых входит обеспечение информационной безопасности Российской Федерации.

Доктрина информационной безопасности развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере. В данной доктрине уделяется особое внимание особенностям общественных отношений, возникающих при обработке информации, сферам деятельности государства, обеспечение безопасности которых является вопросом сохранности конституционного строя.

Обеспечение защиты конфиденциальной информации достигается вследствие использования таких средств, которые исключают случайный, или несанкционированный доступ, который может повлечь за собой уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (пункт 2 Положения об обеспечении безопасности персональных данных). При обработке персональных данных в информационной системе должно быть обеспечено:

- недопущение фактов несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов такого доступа
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, результатом которого может стать нарушения их функционирования;
- постоянный контроль обеспечения уровня защищенности персональных данных.
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных из-за несанкционированного доступа к ним.

С правовой точки зрения, законодательное закрепление взаимоотношений школы и государства в области защиты персональных данных, заключается в нормах информационного права и предполагает правомерность использования конфиденциальной информации работниками образовательного учреждения, соблюдение предусмотренных мер защитного характера, трудового распорядка, правил ведения документации и несение оператором персональных данных ответственности, в случае нарушения правил их обработки. Данные правила включают:

- наличие в организационных документах школы, правилах внутреннего трудового распорядка, трудовых договорах, в

должностных инструкциях положений и обязательств по защите конфиденциальной информации;

- формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
- разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

В правовом плане основными подсистемами защиты считаются::

- установление на объекте режима конфиденциальности;
- разграничение доступа к информации;
- правовое обеспечение процесса защиты информации;
- четкое выделение конфиденциальной информации как основного объекта защиты.

На базе каждой общеобразовательной школы разрабатываются собственные нормативные документы (инструкции, руководства, положения), цель которых – обеспечение информационной безопасности учреждения. Создание данных документов ведется в рамках действующего законодательства Российской федерации.

Первое с чем приходится столкнуться при обработке персональных данных – это цель обработки и ее законность. Именно постановка цели обработки является очень важной задачей при организации защиты персональных данных. Если обработка полученных данных ведется не в соответствии с поставленными целями, то такую обработку необходимо немедленно прекратить или потребовать уточнения целей обработки. Для организации законной обработки и защиты персональных данных необходимо выполнять требования законодательства в данной области, определенные в ФЗ "О персональных данных", постановлениями

Правительства Российской Федерации и рядом других подзаконных актов органов исполнительной власти.

Принципы, в соответствии с которыми строится обработка персональных данных:

- законная и справедливая основа обработки персональных данных;
- обработка конфиденциальной информации должна ограничиваться конкретными, определенными заранее законными целями. Обработка такой информации вразрез заявленным целям недопустима;
- исключено объединение баз персональных данных, имеющих различные цели создания и использования;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны строго ограничиваться в соответствии заявленным целям. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных должно осуществляться в форме, при которой возможно определить субъекта лишь в той мере, в которой этого требуют заявленные цели обработки данных.

Для того, чтобы выполнять требования законодательства и не нарушать основополагающие принципы обработки и защиты персональных данных, а также в целях урегулирования отношений в данной области, затрагивающие вопросы сбора, работы со сведениями, составляющими персональных данных, порядок учета и хранения

носителей и уничтожения хранимой информации, должно быть принято положение о персональных данных.

Помимо положения о порядке обработки и защиты персональных данных, необходимо разработать перечень должностных лиц, которые имеют доступ к данным работников, обучающихся и их родителей. Перечень состоит из списка специально уполномоченных лиц, которым в связи с исполнением должностных обязанностей могут понадобиться персональные данные. Данный список лиц утверждается приказом. Работников, имеющих доступ к персональным данным, необходимо проинформировать об ответственности при обработке таких данных. Кроме того, с сотрудников нужно взять расписку о неразглашении конфиденциальной информации, если такого пункта нет в трудовом договоре.

Для того чтобы сотрудники знали, как сохранить безопасность доверенных им сведений следует разработать инструкцию о порядке обеспечения конфиденциальности при обработке персональных данных. Данный документ определяет порядок защиты информации при получении, формировании, ведении, хранении и передаче личных дел субъектов персональных данных. Инструкция вводится в действие соответствующим приказом.

Это начальный этап обеспечения правовой защиты персональных данных, охватывающий основы, которых вполне достаточно для формирования системы разграничения доступа. Приступим теперь к рассмотрению следующего этапа защиты информации - инженерно-технической защите.

Основная идея технической защиты – это система взглядов на защиту информации с помощью инженерных и технических средств. А задачи инженерно-технической защиты представляют собой противоборства органов информационной безопасности, с одной стороны, и злоумышленников, с другой. Для успешного решения любой задачи, в том

числе технической защиты информации, необходимо иметь четкую постановку задачи и определенные принципы ее решения. Содержание этих двух условий составляет основу концепции технической защиты информации. Однако, этого зачастую оказывается недостаточно для того чтобы полностью гарантировать надежность защиты. На сегодня за плечами специалистов по информационной безопасности есть большой опыт в сфере защиты информации при помощи различных инженерно-технических средств. И развитие точных наук не стоит на месте. Ведется разработка новых средств и технологий защиты информации для обеспечения более высокого коэффициента безопасности данных. Но как бы ни развивалась наука и как бы хитры не были специалисты по информационной безопасности – не все зависит от стабильной работы технического средства или технологии. Успешное решение задачи состоит из множества факторов, одним из которых является деятельность людей. Человек – не машина и его нельзя запрограммировать. Следовательно, как бы ни эволюционировал технический аспект защиты информации, нельзя гарантировать формализованных, законных действий человека, его поведения. Такую проблему возможно решить лишь частично и типичные модели, подходы здесь не всегда действенны. Стоит отметить некую не формальность в решении подобных вопросов, то есть отсутствие стандартного решения задачи. При столкновении с подобной проблемой необходим полноценный анализ и, в каком-то смысле, индивидуальный подход.

Личные/персональные данные ребенка содержатся в основном в **личном деле обучающегося**. На каждого ребенка, зачисленного в организацию, осуществляющую образовательную деятельность, заводится личное дело, в котором хранятся все сданные документы. Таким образом, на начальном этапе обучения ребенка в общеобразовательной организации его личное дело будет состоять из следующих данных: фамилия, имя,

отчество, дата и место рождения ребенка, адрес места жительства родителей, контактные телефоны.

В процессе обучения личное дело о будет пополняться документами о состоянии здоровья ребенка, данными о результатах промежуточной и итоговой аттестаций, какими-либо персональными данными, документами, подтверждающими достижения в учебе, спорте, иных видах деятельности, а также иными документами.

Универсального шаблона личного дела законодательство об образовании не предусматривает. Поэтому каждая образовательная организация должна самостоятельно выработать структуру личного дела обучающегося (с учетом обязательных элементов) и закрепить положение о личном деле локальным нормативным актом.

Личное дело обучающегося подлежит выдаче ему или его законным представителям в случае перевода в другую организацию, осуществляющую образовательную деятельность.

Если родители отказываются подписывать согласие на обработку персональных данных, то в этом случае школа действует в рамках законодательства и предполагается, что минимум персональных данных для обработки родитель предоставить обязан.

Страхи родителей, связанные с обработкой персональных данных ребенка и семьи чаще всего необоснованны. Ребенок все равно будет находиться школьной базе, и школа будет получать на него финансирование. Но учета его участия в школьной жизни может не быть. Обработка персональных данных нередко подразумевает ведения учета успеваемости в электронном журнале, передача данных ребенка для участия в олимпиадах и конкурсах.

2.2. Планирование мероприятий по защите персональных данных в общеобразовательной школе. Надзор за их надлежащим исполнением

В ходе организации мероприятий по защите персональных данных в общеобразовательной школе рекомендуется привлекать юристов, специалистов отдела кадров, консультироваться по поводу правильности и точности формулировок, используемых в положениях и приказах.

Обязательным элементом такой деятельности общеобразовательной школы должна стать правовая составляющая, т.к. необходима:

- разработка комплекса нормативных и правовых актов, в которых определяется не только организационная и правовая составляющие, но и технические подробности защиты персональных данных;
- формирование механизмов, путей совместной проработки вопросов, возникающих в ходе деятельности по защите персональных данных с контролирующими органами, профсоюзами, управлением в сфере образования и др..
- четкая регламентация обязанностей работников образовательной организации, разработка понятных должностных инструкций, в полной мере отражающих суть и порядок действий сотрудника-оператора персональных данных. Контроль за ведением документов, дел, картотек и т.д.

Затем требуется оценить наличие законных оснований для обработки персональных данных, а в случае отсутствия таковых – получение согласия субъекта на такую обработку. При этом согласно Закону № 152-ФЗ доказать добровольное согласие субъекта персональных данных должен доказать оператор (работодатель).

Несмотря на то, что в данной главе речь идет преимущественно о защите персональных данных работников, хотелось бы в контексте обратить внимание на то, что персональные данные обучающихся и их родителей обрабатываются в общеобразовательной школе по тем же правилам и на основании той же законодательной базы. Образовательной организации предварительно нужно получить письменное согласие родителей на обработку персональных данных (в котором подтверждается

согласие, как на обработку их собственных данных, так и данных их детей).

Отдельное внимание необходимо уделить процедуре передачи персональных данных третьим лицам. При осуществлении такой процедуры требуется наличие:

- законных оснований передачи персональных данных, которые указываются в заявлении или, к примеру перечисляются договором об оказании услуг;
- договора с этим третьим лицом, в котором главное условие – взятая оператором персональных данных обязанность обеспечить тайну и безопасность этих данных в процессе их обработки. С особой внимательностью следует подходить к размещению информации, содержащей персональные данные, на интернет-сайте ОУ, с точки зрения соблюдения прав и интересов субъекта в лице работника общеобразовательной школы, обучающегося или его родителей.

Деятельность организации, направленная на защиту персональных данных работника, строится поэтапно и состоит из: выяснения полного перечня ситуаций, в которых необходимо использование персональных данных; определения процессов, в ходе которых персональные данные подвергаются обработке; построение системы аналитики на основании ограниченного числа таких процессов; определение перечня информационных систем и комплекса персональных данных, участвующих в обработке; разделение персональных данных на категории и начальная классификация информационных систем; создание системы положений, приказов, актов, инструкций и иных локальных организационно-распорядительных документов, обеспечивающих защиту персональных данных; внедрение информационно-технических средств защиты персональных данных.

Получается, **защита персональной информации в общеобразовательной школе заключается в разработке и исполнении особого режима обработки такой информации**, в который входят:

- создание внутренней документации по работе с персональными данными;
- организация системы защиты персональных данных;
- внедрение технических мер защиты персональных данных.

Согласно ст. 85 ТК РФ к персональным данным работника относится информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Какая информация, имеющая конфиденциальный характер, требуется работодателю, он решает самостоятельно, основываясь на действующем законодательстве, привлекая к участию в такой деятельности самих работников образовательной организации и их представителей[8].

Статья 87 ТК РФ гласит, что работодатель самостоятельно устанавливает мероприятия, касающиеся сбора, хранения, обработки и уничтожения персональных данных работников с учетом действующего законодательства, и подразумевает регламентирование данного порядка локальными нормативными и иными актами.

На базе образовательной организации принимается «Положение о защите персональных данных работников», разрабатываемое с учетом требований муниципальных органов, профсоюзной организации, в порядке, предусмотренном ст.372 ТК РФ[15].

Данный документ включает в себя все необходимые в процессе обработки персональных данных положения, обеспечивает защиту прав и свобод работников образовательной организации при обработке их данных, определяет ответственность лиц за невыполнение правовых норм в процессе обработки персональных данных.

Принятие такого положения носит обязательный для всех образовательных учреждений характер, его отсутствие квалифицируется как нарушение трудового законодательства работодателем.

Так же, совместно с разработкой и принятием Положения о защите персональных данных работника в образовательном учреждении требуется наличие следующих документов:

- в процессе получения персональных данных – согласие работника на получение работодателем персональных данных от третьих лиц и уведомление работника о получении его персональных данных от третьих лиц;
- при обработке персональных данных – согласие работника на обработку его персональных данных; персональных данных работников;
- при хранении персональных данных – приказ об утверждении списка лиц, имеющих доступ к персональным данным работников, и обязательств о неразглашении;
- при передаче персональных данных работников – согласие работника на передачу его персональных данных третьим лицам.

Ввиду того, что работодатель должен обеспечить конфиденциальность персональных данных, в его обязанности входит организация таких процедур как: ведение журналов учета, их выдача и передача другим лицам либо представителям различных организаций, правоохранительным органам, органам надзора и контроля.

В «Журнале учета внутреннего доступа к персональным данным» следует отмечаются: дата выдачи и возврата документов; срок пользования; цели выдачи; наименование выдаваемых документов. Лицо, которое возвращает документ, содержащий персональные данные, должно обязательно присутствовать при проверке наличия всех имеющихся документов по описи, если выданные документы составлены более чем на одном листе.

Не допускается, чтобы лицо, на законных основаниях получившее личное дело работника или обучающегося в рамках рабочей деятельности оставляло в нем какие-либо знаки, не отвечающие заявленным целям, пометки, исправления, вносило новые записи, извлекало документы из личного дела или помещало в него новые.

Кроме журнала учета внутреннего доступа к персональным данным требуется вести «Журнал учета выдачи персональных данных работников организациям и государственным органам», где регистрируются: поступающий запрос, сведения о лице, направившем запрос; дата передачи персональных данных или уведомления об отказе в их предоставлении; характер переданной информации.

Такая система учета персональных данных, подразумевает проведение регулярных и внеочередных проверок и ревизий направленных на контроль наличия документов и других носителей информации, содержащих персональные данные. Исходя из этого требуется ведение журнала таких проверок.

В общеобразовательной школе рекомендуется ведение следующих документов, осуществляющих учет движения персональных данных:

- Журнал учета внутреннего доступа к персональным данным в учреждении;
- Журнал учета выдачи персональных данных организациям и государственным органам (Журнал учета внешнего доступа к персональным данным работников);
- Журнал проверок наличия документов, содержащих персональные данные.

Так же, дополнительно, поскольку защита персональных данных осуществляется посредством использования разных типов носителей информации, а такие носители подлежат регулярной проверке, появляется необходимость ведения так же «Журнала учета применяемых работодателем носителей информации».

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника в соответствии со ст. 86 ТК РФ обязаны соблюдать необходимые требования. В соответствии со ст. 21 Закона № 152-ФЗ оператор (работодатель) также обязан:

- блокировать персональные данные, имеющие отношение к субъекту, с момента обращения его или законного представителя, либо получения запроса уполномоченного органа (если было выявлено наличие недостоверных данных или неправомерные действия оператора с ними). В случае подтверждения данных фактов оператор обязан уточнить персональные данные и снять их блокирование;
- устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными;
- незамедлительно прекратить обработку персональных данных и уничтожить их по достижения цели обработки и уведомить об этом субъекта;
- прекратить обработку персональных данных и уничтожить их, в случае отзыва субъектом персональных данных согласия на их обработку.

Персональные данные работника не могут быть переданы работодателем третьей стороне за исключением:

- самостоятельного предоставления субъектом письменного согласия на передачу персональных данных третьей;
- необходимости передачи персональных данных в целях предупреждения угрозы жизни и здоровью субъекта;
- других случаев, установленных федеральным законом.

При передаче персональных данных работника работодатель должен соблюдать следующие обязательные требования, предусмотренные ст. 88 ТК РФ:

- 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 других случаях, предусмотренных ТК РФ или иными федеральными законами;
- 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;
- передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
- Поскольку персональные данные относятся к категории конфиденциальной информации, лица, получившие персональные данные работника на законном основании, обязаны использовать их исключительно в целях, которые заявлялись при запросе соответствующей информации, а также не разглашать такую информацию (исключения из данного правила определяются только федеральными законами).

Получателями персональных данных работника на законном основании являются:

- органы социального страхования, органы пенсионного обеспечения, а также иные органы, организации и граждане (ФЗ «Об основах обязательного социального страхования»);
- налоговые органы (ст. 24 НК РФ);
- органы прокуратуры и другие правоохранительные органы (ст. 23 ФЗ № 152);

- федеральная инспекция труда (ст. 357 ТК РФ);
- профессиональные союзы (ФЗ "О профессиональных союзах, их правах и гарантиях деятельности" и ТК);
- другие органы и организации в случаях, предусмотренных федеральным законом.

В соответствии с п. 8 ст. 86 ТК РФ работники и их представители должны быть ознакомлены под подпись с документами, устанавливающими порядок обработки и защиты персональных данных, а также их права и обязанности в этой области. Работники в соответствии со ст. 89 ТК РФ имеют право[7]:

- на полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты персональных данных;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

В обязанности работников входит информирование работодателя об изменении персональных данных.

В соответствии со ст. 24 Закона № 152-ФЗ оператор персональных данных, нарушивший требования данного федерального закона, несет гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Неисполнение требований Закона № 152-ФЗ операторами баз данных может повлечь:

- гражданские иски со стороны работников;
- репутационные риски;
- приостановление или прекращение обработки персональных данных, осуществляемой с нарушением требований Закона № 152-ФЗ;
- направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных;
- привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях.

В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

За нарушение работником образовательного учреждения данной статьи работодатель имеет право применить к нему одно из дисциплинарных взысканий по ст. 192 ТК Российской Федерации. Либо может расторгнуть трудовой договор по своей инициативе по подп. "в" п. 6

ч. 1 ст. 81 ТК РФ в случае разглашения охраняемой законом тайны [14]. Кроме того, работникам грозит материальная и уголовная ответственность.

Помимо исполнения работниками своих обязанностей, четкая организация работы трех органов-регуляторов обеспечивает эффективность государственного надзора и контроля обработки персональных данных. Каждому из данных регуляторов отведена определенная область деятельности в сфере персональных данных.

Осуществление контроля и надзора за соответствием сбора, хранения и обработки информации, составляющей персональные данные субъектов, правилам, указанным в законодательстве Российской Федерации поручено уполномоченному органу по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), его территориальные органы действуют во всех субъектах Российской Федерации. Данный орган, в соответствии со ст. 23 Закона № 152-ФЗ включает в зону своей ответственности и область проверок все организационные мероприятия, проводимые в школе для обеспечения эффективной обработки персональных данных. Его права и обязанности устанавливаются в соответствующем положении. Обязанности Роскомнадзора включают:

- организацию защиты прав субъектов персональных данных в соответствии с действующим законодательством;
- принятие решений по результатам обращений физических или юридических лиц связанных с нарушением их прав в области обработки персональных данных;
- ведение реестра операторов персональных данных;
- разработку мер, совершенствующих защиту прав субъектов персональных данных;
- выполнение иных обязанностей, предусмотренных законодательством Российской Федерации.

Второй регулятор - Федеральная служба по техническому и экспортному контролю (ФСТЭК) и ее территориальные органы. В обязанности данного органа входит техническая защита информационных систем, осуществляющих обработку конфиденциальной информации. Сфера ответственности и область проверок – технические средства защиты информации, использующие некриптографические методы и способы защиты персональных данных.

Последним основным органом, регулирующим исполнение законодательства является федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, – Федеральная служба безопасности Российской Федерации (ФСБ России), устанавливающая, согласно действующего законодательства особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах и осуществляет контроль в этой области.

Так же, согласно ст. 354 ТК Российской Федерации Федеральная инспекция труда, состоящая из федерального органа исполнительной власти и его территориальных органов (государственных инспекций труда), осуществляет надзор и контроль за соблюдением законодательства, содержащего нормы трудового права, в которые входят и вопросы защиты персональных данных работников.

Администрация школы в первую очередь отвечает за обеспечение защиты персональных данных, а контролируют его, помимо уполномоченных на это органов, родители обучающихся. Наиболее распространенным примером ситуации, при которой происходит столкновение интересов школы и родителей, можно выделить размещение на информационных стендах, сайте школы или иной способ опубликования изображения обучающегося вместе с персональной информацией. В данном случае будет не важно какие педагогические или иные цели

преследовал педагог, если родители ребенка не давали письменного согласия на такие действия. Органы-регуляторы приводят пример такой ситуации в качестве наиболее распространенного нарушения. Для того, чтобы избежать конфликта на данной почве, требуется всего лишь воздержаться от указания полных фамилии имени и отчества обучающегося, либо иметь письменное разрешение от родителей на публикацию таких сведений. Так же стоит заранее получить от родителей согласие на размещение изображений их детей в материалах на школьном сайте или бумажных изданиях, даже в том случае, если не планируется публикация вместе с указанием ФИО. Наиболее простым способом получения такого согласия является включение соответствующего пункта в заявление о приеме в общеобразовательную школу. Так же конфликт может возникнуть отнюдь не в случае публикации изображений детей совместно с их именами, но и со стороны самих учителей. Администрация школы может быть обвинена в том, что, в то время, как на использование персональных данных обучающихся налагаются строгие запреты и для всех видов такого использования требуются специальные согласия и разрешения, данные о самих учителях открыто размещают на нескольких информационных ресурсах сразу. Различия подобного рода обусловлены тем, что часть данных об учителе, включающая его квалификационные характеристики, должна быть открыта и опубликована по закону. В то же время, необходимо отметить, что это строго определенный перечень данных и он не предусматривает, например указание домашнего адреса педагога или номер его мобильного телефона.

Следует упомянуть о том, что некоторые учителя видят своеобразную угрозу в своих, более продвинутых в техническом плане, подопечных, которые, по их мнению, могут легко взламывать электронные журналы и тем самым влиять на течение образовательного процесса. Очевидно, что чаще всего школьники применяют более надежные психологические приемы, например, подделывая данные, препятствуют

получению информации технически на их домашних компьютерах (меняют настройки почты или отправляют сообщения от имени родителей в адрес администрации с различными просьбами и даже требованиями) [33]. С точки зрения получения реального доступа к данным электронного журнала, намного проще воспользоваться информационной неграмотностью учителей, которые используют простые пароли (их легко подобрать), пишут их на бумажках и приклеивают к мониторам, заходят в журнал на глазах учеников, оставляют технику после входа в аккаунт без присмотра.

Рассматриваемые в главе вопросы сегодня имеют особенную актуальность в связи с практически повсеместным использованием компьютерной техники и сети Интернет, в т.ч. и в школе, развитием информационно-обрабатывающих технологий и увеличившимся объемом информации, что вызывает появление новых правовых проблем, и сложностей технического характера, требующих от работодателей принятия адекватных мер реагирования [31].

Министерство образования и науки России разрабатывает законопроект о создании базы данных с подробной информацией об учениках и их родителях, согласно которому, сведения об успеваемости, здоровье и семьях миллионов школьников и студентов будут доступны широкому кругу федеральных ведомств, а также региональным и муниципальным властям. В Министерстве образования и науки предлагают собирать данные о детях с момента их рождения в специальной базе, где будут собраны сведения об образовательных учреждениях и успеваемости, победах в конкурсах, олимпиадах, а также там должны содержаться сведения о родителях и ситуации в семье.

Внесением таких данных предлагается заниматься региональным и муниципальным структурам. За Министерством же предлагается закрепить «методологическое и методическое обеспечение системы». В рамках проекта предполагается предоставить право обработки персональных

данных детей такими ведомствами как: Министерство здравоохранения, Министерство труда, налоговые и пенсионные органы, муниципальные и региональные образовательные структуры. Большую озабоченность правозащитных организаций вызывает то, что в законопроекте не указан даже примерный круг лиц, которым будет предоставлен доступ к такой базе данных, не разработан и перечень видов ответственности за неправомерное использование конфиденциальной информации обучающихся, среди которых большинство – несовершеннолетние. В контексте данных пробелов в предлагаемом законопроекте необходимо напомнить о том, что наша система образования уже сталкивалась с несовершенством законодательства и механизмов защиты персональных данных. Еще в 2014 году были наказаны руководители более двух тысяч школ за нарушение действующего законодательства, а именно за публикации на сайтах образовательных учреждений список детей, содержащих информацию персонального характера. Делалось это, невзирая на наличие согласия родителей на размещение такой информации. Тогда выяснилось, что запрещается даже публикация списков победителей олимпиад и соревнований без соответствующего разрешения. Самый резонансный повод судить о недостаточной защищенности персональных данных в школе возник в мае 2015 года, в связи с массовыми утечками в открытый доступ персональных данных из электронных дневников. В СМИ тогда упоминалось, что некая кипрская компания получила доступ к данным как минимум 5,6 млн. российских обучающихся, зарегистрированных в системе электронного дневника и журнала «Дневник.ру». Последовавшие вслед за этим проверки Роскомнадзора, каких-либо серьезных нарушений в работе компании «Дневник.ру» не выявили..

В контексте вышеизложенного предлагаю обратить внимание на **приложение 1**, где приводится пример так называемого «согласия на

обработку персональных данных», которое необходимо подписать каждому родителю, законному представителю обучающегося.

Сперва отметим, что исключениями из правила согласия являются ситуации, когда интересующая информация общедоступна, ее передача предусмотрена федеральными законами, либо необходима в целях защиты жизни и здоровья граждан.

В любом случае, независимо от статуса лица, запрашивающего у оператора персональные данные работников или обучающихся школы, ему необходимо убедиться в законности такого запроса. Любая передача данных, в соответствии с законом, должна быть запротоколирована, что бы в случае разбирательств, связанных с утечкой, инициированных родителями или контролирующими органами, у образовательной организации имелись четкие сведения о движении конфиденциальной информации. Это значит, что любая передача такой информации за пределы общеобразовательной школы должна быть согласована с администрацией. Если со стороны оператора персональных данных нет четкой уверенности в правомочности запроса, он вправе потребовать предъявления законных оснований в письменной форме. Так же в случае проведения внеурочных или иных мероприятий, которые подразумевают движение персональных данных обучающихся за пределы образовательной организации, учитель так же должен убедиться в наличии таких оснований. В подобной ситуации письменное согласие родителей на обработку персональных данных является самым надежным документом, обеспечивающим законность обработки персональных данных. Поскольку обычно в ходе организации различных мероприятий в школе издается приказ, стоит указать в нем наличие таких оснований, при которых ответственность за доказательство необходимости передачи данных не лежала бы на учителе.

Подводя итог главы, в которой было рассмотрено практическое применение законодательства, мероприятия по защите персональных

данных в общеобразовательной школе, риски, связанные с возможностью утечки таких данных, пути их утечки, можно сделать вывод: законодательство Российской федерации стремится своевременно отвечать современным вызовам в сфере защиты информации и обеспечивать контроль ее обработки. С другой стороны, при использовании этой законодательной базы наблюдается откровенная халатность и безответственность. Оператор персональных данных далеко не всегда осознает значимость мероприятий по их защите, пренебрегает должностной инструкцией, вследствие чего допускает утечку персональных данных и иной информации, приводящую к срыву образовательного процесса, либо иному недобросовестному их применению.

ЗАКЛЮЧЕНИЕ

Результатом исследования проблемы, поставленной в выпускной квалификационной работе, стали выводы, сделанные в ходе изучения, структурирования и объединения сведений о действующем законодательстве, исследований правовой, моральной и материально-технической составляющих процесса сбора, обработки, хранения и использования персональных данных в общеобразовательной школе.

Вывод первый – нельзя утверждать об окончательной сформированности и высоком качестве законодательства в сфере регулирования защиты персональных данных в силу относительной новизны таких правоотношений, и их постоянного активного развития в последние годы. Скорость и эффективность внесения изменений в нормативные документы уступает разработке новых способов обработки информации, видов ее применения.

Вывод второй – в обществе не сложилось однозначного мнения о том, как распоряжаться персональными данными в общеобразовательной школе. Например, далеко не все родители обучающихся допускают возможность размещения каких-либо данных о своих детях на информационных порталах школы, даже если это направлено на поддержание интереса ребенка к обучению, положительную оценку его успехов, признание заслуг педагогического коллектива школы в образовательном процессе.

Вывод третий – несмотря на несовершенство законодательства, главной причиной утечки персональных данных чаще всего является халатность работников образовательной организации в процессе обработки информации, требующей защиты. Нарушения присутствуют на всех стадиях обработки, начиная от некорректного составления/заполнения согласия на обработку персональных данных, пренебрежение ведением отчетной и сопроводительной документации, заканчивая банальным

безответственным отношением к логинам и паролям электронных журналов и иных программ, содержащих персональные данные обучающихся и работников школы.

В заключении хочется отметить, что заявленная в начале работы **цель исследования:** «рассмотреть особенности защиты персональных данных в общеобразовательной школе» - достигнута. В силу особенности законодательной базы тема освещена даже несколько шире заданной, поскольку обработка и защита персональных данных, как в школе, так и в других организациях проходит по одним правилам и преследует общую цель – не допустить неправомерное использование конфиденциальной информации.

Результаты данной работы рекомендуется использовать в общеобразовательных школах и иных организациях, которым, в ходе их деятельности, необходимо обеспечить защиту персональных данных.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Всеобщая декларация прав человека : [принята 10 дек. 1948 г. резолюцией 217А Генеральной Ассамблеи ООН] // Действующее международное право. В 2 т. Т. 2 / сост. Ю.М. Колосов, Э.С. Кривчикова. – Москва : Междунар. отношения, 2007. – 223с.

2. Конвенция о защите прав человека и основных свобод (заключена в г. Риме 04.11.1950) // Собрание законодательства РФ. – 2001. – № 2. – Ст. 163.

3. Международный пакт о гражданских и политический правах (Нью-Йорк, 16.12.1966 г.) Статья. 2. // Международная защита прав и свобод человека. Сборник документов. М.: Юридическая литература, 1990. С. 53-57.

4. Конвенция о правах и основных свободах человека

5. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)// «Конституция Российской Федерации» СПб, ООО «Виктория плюс», 2014. – 48с.

6. Уголовный кодекс Российской Федерации : [федеральный закон: принят Гос. Думой 24 мая 1996 г.: с изм. от 25.04.2018– Москва : ЭКСМО, 2018. – 176 с.

7. Гражданский кодекс РФ (1-4 части) [Электронный ресурс]/ — Электронно-библиотечная система IPRbooks, 2016.— 608 c.— URL: http://www.iprbookshop.ru/1246 (дата обращения: 04.02.2018)

8. Трудовой кодекс Российской Федерации (по сост. на 20.01.2018) / Новосибирск: Норматика 2018г. 223с.

9. Шитова М.А. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: lEXT-справочник/ Шитова М.А.— М.: Эксмо, 2010.— 665 c.— Режим доступа: http://www.iprbookshop.ru/1827 (дата обращения: 01.04.2018)

10.Федеральный закон N 24-ФЗ "Об информации, информатизации и защите информации" от 20.02.1995 г. (СЗ РФ. 1995. №8.). [Электронный ресурс] / - URL: http://kremlin.ru/acts/bank/7559/page/1 (дата обращения: 15.05.2018)

11.Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (от 29.07.2017 N 223-ФЗ) [Электронный ресурс] / - URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 22.03.2018)

12.Доктрина информационной безопасности от 9 сентября 2009 г. [Электронный ресурс] / СПС Консультант плюс, 2009г. - URL: http://www.consultant.ru/document/cons_doc_LAW_28679/ (дата обращения: 29.01.2018)

13.Перечень сведений конфиденциального характера (утв. Указом Президента Российской Федерации от 6 марта 1997 г. N 188) [Электронный ресурс] / URL: http://base.garant.ru/10200083/ (дата обращения: 04.02.2018).

14.Комментарий к Трудовому кодексу Российской Федерации под ред. К.Н. Гусова. - ООО "ТК Велби", ООО "Издательство Проспект", 2003.

15. Комментарий к Трудовому Кодексу Российской Федерации / Коршунов Ю.Н., Коршунова Т.Ю., Кучма М.И., Шеломов Б.А. – Спарк 2002 г.

16.Комментарий к Кодексу Российской Федерации об административных Правонарушениях. - Проспект,2009. – 1136с.

17.Комментарий к Уголовному кодексу Российской Федерации / Грачева Ю.В., Ермакова Л.Д., Боженюк С.А.. – "Проспект", 2016. – 912с.

18.Постатейный Комментарий к Уголовному кодексу РФ 1996 г. / Безлепкин Б.Т. - ООО "Проспект", 2018. – 608с.

19.Алимова Н.А. Большой справочник кадровика. – М.: Издательско-торговая корпорация «Дашков и К°», 2007. – 536 с.

20.Копылов В.А. Информационное право. М.: Юристъ, 2005. – 512 с.

21.Магнитская Е.В. Правоведение: учебник, Е.В. Магнитская, Е.П. Евстигнеев: Питер, 2003. - 512с.

22.Мазуров В.А. Уголовно-правовые аспекты информационной безопасности: учебное пособие – Барнаул: Изд-во Алт. Ун-та, 2004. – 288с.

23.Поляков В.В., Мазуров В.А. Проблемы правовой и технической защиты: сб. науч. ст./ АлтГУ, 2008. – 179 с.

24.Саидов А.Г. Конституционно-правовые основы обеспечения информационной безопасности Российской Федерации: Махачкала, 2004. – 26 с.

25.Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе. – М.: 1999. – 346 с.

26.Ярочкин В.И. Информационная безопасность: учебник для ВУЗов. - М.: Гаудеамус, 2004. - 544с.

27.Корольков А.Е. Практические проблемы разграничения трудовых и гражданско-правовых отношений // Трудовое право. – 2011. - № 4. – С. 21 – 40.

28.Комкова Г.Н., Колесников Е.В., Липчанская М.А. Конституционное право Российской Федерации. – М.: Юрайт, 2013. – 464 с.

29.Кротов А.В. Свобода информации и право на информацию человека // Адвокатская практика. - М.: Юрист, 2007, № 2. - С. 2-5

30.Конституционное право и международное право: взаимодействие и развитие в современную эпоху [Электронный ресурс] / под ред. И. Конюховой. - М.: Российская академия правосудия, 2010. - 128 с. - URL: http://biblioclub.ru/index.php?page=book&id=142657 (дата обращения 15.02.2018)

31.«Особенности защиты персональных данных в образовательных учреждениях» С.Б. Хмельков [Электронный ресурс] // Журнал "Нормативные документы образовательного учреждения" № 3, 2011 года URL: http://usperm.ru/content/osobennosti-zashchity-personalnyh-dannyh/ (дата обращения 15.05.2018)

32.Важорова М. А. История возникновения и становления института персональных данных [Текст] // Государство и право: теория и практика: материалы Междунар. науч. конф. — Челябинск: Два комсомольца, 2011. — С. 33-38. — URL https://moluch.ru/conf/law/archive/37/365/ (дата обращения: 03.05.2018).

33.«Вне закона? Что нужно знать учителю и директору школы при работе с персональными данными». 31.08.2015. Зоя Алексеева. [Электронный ресурс] // Учительская газета URL: http://ug.ru/article/852 (дата обращения 31.04.2018)

34.Правовая информация. Нормативные акты в области защиты персональных данных. [Электронный ресурс] // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций URL: https://77.rkn.gov.ru/law/p4735/ (дата обращения: 15.05.2018)

Приложение 1

СОГЛАСИЕ на обработку персональных данных
МАОУ СОШ № 48

«_____» _____20 ____г.

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», со статьей 152.1 Гражданского кодекса Российской Федерации я,_____,
(ФИО законного представителя)
паспорт_____выдан_____
(серия, номер, код подразделения, наименование органа, выдавшего паспорт, число, месяц, год)
зарегистрированный по адресу:_____
являюсь родителем (законным представителем) несовершеннолетнего_____
_____
ФИО ребенка, число, месяц, год рождения
(далее - Обучающийся) в Муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 48, на основании пункта 1 статьи 64 Семейного кодекса Российской Федерации, что подтверждается
_____
(документ, подтверждающий, что субъект является законным представителем несовершеннолетнего)
настоящим даю свое согласие на обработку персональных данных моего ребенка в образовательной организации МАОУ СОШ № 48 г. Екатеринбурга расположенной по адресу: 620131, г. Екатеринбург, ул. Крауля,91 (далее - учреждение) с использованием средств автоматизации или без использования таких средств с целью осуществления индивидуального учета результатов освоения Обучающимся образовательных программ, а также хранения в архивах данных об этих результатах.

Я предоставляю учреждению право осуществлять следующие действия (операции) с персональными данными Обучающегося: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение.

Учреждение вправе размещать обрабатываемые персональные данные Обучающегося в информационно-телекоммуникационных сетях с целью предоставления доступа к ним ограниченному кругу лиц: обучающемуся, родителям (законным представителям) обучающегося, а также административным и педагогическим работникам учреждения. Учреждение вправе включать обрабатываемые персональные данные учащегося в списки (реестры) и отчетные формы, предусмотренные нормативными документами федеральных и муниципальными органов управления образованием, регламентирующими предоставление отчетных данных.

Перечень персональных данных, на обработку которых я даю согласие, включает:
Данные о детях:

1. Сведения личного дела обучающегося: фамилия, имя, отчество; дата рождения; пол; номер свидетельства о рождении, дата выдачи и кем выдано свидетельство; родной язык; дата поступления в учреждению, в какой класс поступил, номер и дата приказа о зачислении; дата отчисления из учреждения, из какого класса отчислен, номер и дата приказа об отчислении, причины отчисления, метка о выдаче личного дела; где воспитывался и обучался до поступления в первый класс; сведения о переходе из одной школы в другую, в том числе наименование школы и класса из которой прибыл Обучающийся, а также наименование школы и класса, в которые зачислен Обучающийся; домашний адрес; фамилия, имя, отчество родителей (законных представителей), контактные телефоны; состояние здоровья, включая данные о медицинской группе.
2. Сведения об учебном процессе и занятости Обучающегося: перечень изученных, изучаемых предметов и факультативных и элективных курсов; успеваемость, в том числе

результаты текущего контроля успеваемости, промежуточной и итоговой аттестации; данные о посещаемости уроков, причины отсутствия на уроках; поведение в учреждении; награды и поощрения; состояние физической подготовленности; расписание уроков, расписание школьных звонков; содержание уроков, занятий; содержание домашних заданий; фамилии, имена, отчества педагогов, ведущих обучение; занятость в кружках, секциях, клубах, группах продленного дня, внешкольных и внеклассных мероприятиях.

3. Согласие на размещение фотографий и иной личной информации моего ребенка на сайте (http://школа48.екатеринбург.рф) МАОУ СОШ № 48 г.Екатеринбурга, расположенной по адресу: 620131, г. Екатеринбург, ул. Крауля,91.

Я даю согласие на размещение персональных данных моего ребенка только при условии соблюдения принципов размещения информации на Интернет-ресурсах учреждения, а именно: соблюдения действующего законодательства Российской Федерации, интересов и прав граждан; защиту персональных данных; достоверность и корректность информации.

Уведомлен о том, что в информационных сообщениях о мероприятиях, размещенных на сайте учреждения без получения моего согласия, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество родителя. Представителем учреждения при получении согласия на размещение персональных данных мне разъяснены возможные риски и последствия опубликования персональных данных в сети Интернет и то, что учреждение не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

Обязуюсь предоставить информацию об изменении персональных данных в течение месяца со дня получения документов об этих изменениях. Подтверждаю, что ознакомлен с документами учреждения, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Настоящие согласие дано мной « ____ » _____ 20 ___ г. и действует на период обучения моего ребенка _____

ФИО ребенка,

в учреждении.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес учреждения по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю учреждения.

Подпись _____ / _____

Расшифровка

Приложение 2

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ ГОРОДА ЕКАТЕРИНБУРГА
ОТДЕЛ ОБРАЗОВАНИЯ ВЕРХ – ИСЕТСКОГО РАЙОНА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 48
620131, г. Екатеринбург, ул. Крауля,91 Тел./факс (343) 242-32-44

Принято
Педагогическим советом
МАОУ СОШ № 48
Протокол № 1
от 28.08.2015г

Утверждаю:
Директор МАОУ СОШ № 48
_____ Н.Б. Пичугина
Приказ № 86/1
«28» августа 2015 г.

Положение о порядке обработки и защите персональных данных в Муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 48

I. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных в Муниципальном автономном учреждении средней общеобразовательной школе № 48 (далее – Положение) регулирует порядок получения, обработки, использования, хранения и обеспечения конфиденциальности персональных данных в образовательной организации (далее - учреждение) на основании Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон № 152- ФЗ). Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", а также в соответствии с Уставом МАОУ СОШ № 48.

1.2. Основной задачей учреждения в области защиты персональных данных является обеспечение в соответствии с законодательством РФ обработки персональных данных работников учреждения, обучающихся и их родителей (законных представителей), а также персональных данных, содержащихся в документах, полученных из других организаций, обращениях граждан и иных субъектов персональных данных.

1.3. В настоящем Положении используются следующие термины и определения:

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информация — сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - учреждение, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Работник - физическое лицо, вступившее в трудовые отношения с учреждением.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Субъекты персональных данных учреждения (далее - субъекты) - носители персональных данных, в т.ч. работники учреждения, обучающиеся и их родители (законные представители), передавшие свои персональные данные учреждению на добровольной основе и в рамках выполнения требований нормативно-правовых актов для их обработки.

Съемные носители данных - материальные объекты или устройства с определенными физическими свойствами, позволяющими использовать их для записи, хранения и считывания персональных данных.

Типовая форма документа - документ, позволяющий упорядочить, типизировать и облегчить процессы подготовки документов.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и в результате которых уничтожаются материальные носители персональных данных.

1.4. Должностные лица учреждения, в обязанности которых входит обработка персональных данных субъектов, обеспечивают каждому субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Порядок обработки персональных данных в учреждении утверждается руководителем учреждения. Все работники учреждения должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на момент ознакомления.

II. Организация получения и обработки персональных данных

2.1. Получение персональных данных осуществляется в соответствии с нормативными правовыми актами РФ в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, настоящим Положением в случае согласия субъектов на обработку их персональных данных.

2.2. Оператор персональных данных не вправе требовать от субъекта предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и частной жизни.

2.3. Без согласия субъектов осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных). Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Обработка не совместимая с целями сбора персональных данных не допускается.

2.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по

отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
2.5. В случае увольнения или отчисления субъекта оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством РФ либо договором с субъектом.
2.6. Персональные данные хранятся в бумажном и (или) электронном виде централизованно с соблюдением предусмотренных нормативными правовыми актами РФ мер по защите персональных данных.
2.7. Оператор назначает лицо, ответственное за организацию обработки персональных данных.
2.8. Право на обработку персональных данных предоставляется работникам учреждения, которые обязаны сохранять их конфиденциальность.
2.9. Персональные данные при их неавтоматизированной обработке обособляются от иной информации, в частности путем фиксации их на отдельных материальных (бумажном или электронном) носителях персональных данных, в специальных разделах или на полях форм (бланков).
2.10. При фиксации персональных данных на материальных носителях не допускается размещение на одном материальном носителе персональных данных, цели, обработки которых заведомо не совместимы.

Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, используются отдельные материальные носители для каждой категории.
2.11. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, информируются руководителями:
- о факте обработки ими персональных данных;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ.

2.12. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма) (приложение), должны соблюдаться следующие условия:
- типовая форма документа содержит сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; наименование учреждения; адрес учреждения; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых в учреждении способов обработки персональных данных;
- при необходимости получения письменного согласия на обработку персональных данных типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;
- типовая форма составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных субъектов персональных данных.

2.13. При ведении журналов (классные журналы, журналы регистрации, журналы посещений и др.), содержащих персональные данные субъектов, следует учитывать, во-

первых, что необходимость их ведения предусмотрена федеральными законами и локальными актами учреждения, содержащими сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журналов, сроках обработки персональных данных, и, во-вторых, что копирование содержащейся в них информации не допускается.

2.14. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

2.15. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

2.16. Если персональные данные субъекта можно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него необходимо получить письменное согласие. Учреждение должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их получение.

III. Меры по обеспечению безопасности персональных данных при их обработке

3.1. При обработке персональных данных в отношении каждой категории персональных данных определяются места хранения, а также устанавливается перечень лиц, осуществляющих их обработку либо имеющих к ним доступ (как с использованием средств автоматизации, так и без них).

3.2. Оператором обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности образовательной организации.

3.4. Порядок конкретных мероприятий по защите персональных данных с использованием средств автоматизации или без использования таких средств определяется приказами руководителя учреждения.

IV. Права, обязанности и ответственность субъекта персональных данных и оператора при обработке персональных данных

4.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Законом № 152-ФЗ за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

- на получение сведений об операторе, о месте его нахождения, наличии у него персональных данных, относящихся к нему (т.е. субъекту персональных данных), а также на ознакомление с такими данными;
- требование 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;
- получение при обращении или запросе информации, касающейся обработки его персональных данных.

4.2. Оператор обязан:

- безвозмездно предоставлять субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных;
- вносить в персональные данные субъекта необходимые изменения;
- уничтожать или блокировать соответствующие персональные данные при предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- уведомлять субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах;
- в случае выявления неправомерной обработки персональных данных, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора;
- в случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение;
- уведомлять субъекта персональных данных или его законного представителя об устранении допущенных нарушений или об уничтожении персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ.
- уведомить субъекта персональных данных об уничтожении его персональных данных.

4.3. Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством РФ.

4.4. Ответственность за соблюдение требований законодательства РФ при обработке и использовании персональных данных возлагается на руководителей структурных подразделений и конкретных должностных лиц, обрабатывающих персональные данные, в приказе об утверждении настоящего Положения и в других соответствующих приказах.

V. Заключительные положения

5.1. Изменения в Положение вносятся согласно установленному в учреждении порядку. Право ходатайствовать о внесении изменений в Положение имеет директор и заместители директора учреждения.

Приложение 3

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017)

"О персональных данных"

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.