

# ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ШКОЛЕ

**Анатолий Борисович Вифлеемский,**

*директор Центра экономики образования, доктор экономических наук*

**Игорь Григорьевич Лоцицкий,**

*директор информационно-вычислительного центра «Аверс»*

В Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных» внесены кардинальные изменения, поскольку был принят Федеральный закон от 25 июля 2011 года № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных». Многие требования по обработке персональных данных и даже сами определения существенно изменились. Возникло множество спекуляций по поводу новых требований. Разберёмся, так ли страшны требования по защите персональных данных.

- оператор персональных данных • обработка • общедоступные источники
- специальные данные • письменное согласие, защита

## Новые понятия

В новой редакции под **персональными данными** понимают *любую информацию, относящуюся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)*. Тем самым термин стал более расплывчатым и неопределённым, что даёт основания для отнесения к персональным данным практически любых сведений о работниках, учащихся школ, в том числе: фамилия, имя, отчество; год, месяц, дата и место рождения; адрес; семейное, социальное, имущественное положение; образование; профессия; доходы; результаты промежуточной или текущей аттестации; сведения о пропуске учащихся уроков по болезни; другая информация.

В этот перечень можно включить практически все сведения о работнике, которые получает администрация школы в рамках трудовых отношений с работниками, а также любую информацию об учащихся и их родителях.

**Оператор персональных данных** — это государственный, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами *организующие и (или) осуществляющие обработку персональных данных*, а также определяющие цели их обработки, состав, действия (операции), совершаемые с персональными данными. Таким образом, любое образовательное учреждение осуществляет обработку персональных данных и является оператором персональных данных. Следовательно, необходимо знать и соблюдать требования, предъявляемые действующим законодательством к их обработке.

Персональные данные могут содержаться в документации, включающей: документы по анкетированию, тестированию и т.п.; приказы (распоряжения) по личному составу; документацию по аттестации сотрудников, служебным расследованиям и т.п.; учётную документацию (картотеки, книги, журналы и т.п.); аналитическую и справочную документацию, как используемую руководством, так и выдаваемую работникам для представления в заинтересованные органы; отчётную документацию, передаваемую в государственные органы статистики, налоговые органы и другие учреждения.

**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.

Как видно из определения, любое возможное действие с персональными данными подпадает под понятие «обработка», при этом некоторые действия очень близки по своему содержанию. Так, распространение персональных данных отличается от их предоставления кругом лиц, которым раскрываются персональные данные.

**Распространение** персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

**Предоставление** персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

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

**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.

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

В целях информационного обеспечения могут создаваться **общедоступные источники персональных данных** (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться: его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии; иные персональные данные, сообщаемые субъектом персональных данных.

Таким образом, практически любые персональные данные с согласия субъекта могут быть объявлены общедоступными. Однако при этом сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или других уполномоченных государственных органов.

Помимо этого, статьями 10 и 11 Федерального закона «О персональных данных» установлены **специальные данные**, в отношении которых действуют повышенные меры защиты от несанкционированной обработки и распространения. Это информация, касающаяся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Если от сбора информации о национальности работников, учащихся школы вполне могут отказаться (или уже

отказались), то информация о состоянии здоровья необходима школам (как минимум для учёта посещения, для определения возможности заниматься физкультурой и т.д.). Необходима информация о здоровье работников и для ведения табеля (если учитель отмечает пропуск ученика по болезни, это очевидно, считается обработкой «информации о здоровье»). Понятно, что школам неизбежно приходится работать со специальными данными.

Приведённое выше определение персональных данных позволяет, в частности, некоторым «специалистам» говорить о незаконности оглашения в классе оценок учащихся при отсутствии согласия на то, что оценки считаются общедоступными данными. Иными словами, если нет специально оформленного согласия на то, что оценки ученика являются общедоступными данными, учителю больше нельзя сказать «Садись, Вася, пять!», так как это станет «распространением персональных данных» об этом ученике. Получить же согласие на общедоступность данных у большинства родителей, как показывает практика, достаточно проблематично.

Однако, по нашему мнению, такое мнение не совсем верно. Действительно, получить согласие на обработку персональных данных учеников школа должна: в таком согласии, как правило, перечисляются все возможные виды обработки, включая распространение персональных данных. И здесь следует вернуться к определениям и вспомнить, что распространение — это раскрытие информации неопределённому кругу лиц, в том числе и всем ученикам в классе. Но учтём, что среди персональных данных в согласии на обработку персональных данных должны фигурировать результаты итоговой и промежуточной аттестации, прочие оценки учеников — и тогда никаких проблем с оглашением оценок учителем в классе не возникнет.

Как видим, если внимательно читать нормы права, закон всё же позволяет учителю оглашать оценки учащихся. В то же время бу-

мажной волокиты действительно не избежать без риска привлечения к ответственности проверяющими. В частности, должен быть определён перечень лиц, допускаемых в школе к персональным данным учащихся, и среди них должны быть упомянуты учителя.

### **Уведомление Роскомнадзора школой**

Знакомство с Федеральным законом «О персональных данных» для ряда школ началось с требования отослать уведомление об обработке персональных данных в территориальный орган Роскомнадзора. Многие школы так и сделали, хотя это было не обязательно. За исключением ряда определённых действующим законодательством случаев оператор, обрабатывающий персональные данные, обязан направить уведомление об обработке персональных данных уполномоченного органа. Однако школа, как правило, подпадает под какой-либо из случаев, когда направлять такое уведомление не обязательно.

**Школа вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:**

- *обрабатываемых в соответствии с трудовым законодательством;*
- *полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;*
- *сделанных субъектом персональных данных общедоступными;*

- включающих только фамилии, имена и отчества субъектов персональных данных;
- необходимых для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включённых в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Таким образом, обработка персональных данных работников школы, а также учащихся и их родителей (законных представителей) в случае заключения с ними договора и непредставления этих данных без их согласия третьим лицам не требует уведомления территориального управления Роскомсвязнадзора. Если не используются средства автоматизации (об этом ниже), то уведомление направлять также не обязательно.

### **Письменное согласие для обработки персональных данных**

Формально письменное согласие для обработки персональных данных работников, учащихся и их родителей в большинстве случаев в школе не требуется. Федеральный закон «О персональных данных» определяет, в частности, случаи, когда возможна обработка персональных данных в школе и при отсутствии такого согласия:

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных

### УПРАВЛЕНИЕ ОБРАЗОВАНИЕМ

или договора, по которому субъект персональных данных будет выгодоприобретателем или поручителем;

- обрабатываются персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (*персональные данные, сделанные общедоступными* субъектом персональных данных);
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, *если получить согласие субъекта персональных данных невозможно*;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных», при условии обязательного обезличивания персональных данных;
- обрабатываются персональные данные, подлежащие опубликованию или обязательному раскрытию в соответствии с федеральным законом;

● обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

Последний случай возможности обработки персональных данных будет конкретизироваться правоприменительной практикой, учитывая возможность субъективного толкования «прав и законных интересов». В прежней редакции закона такая возможность отсутствовала.

Для школ актуально разрешение проводить обработку персональных данных без специального согласия их субъекта в целях исполнения договора: это даёт право на обработку персональных данных работников школы (работающих на условиях трудовых договоров, а также на условиях договоров гражданско-правового характера).

Обработка специальных категорий персональных данных в соответствии со статьёй 10 Федерального закона «О персональных данных» допускается только в определённых частях второй этой статьи случаях. Среди этих случаев для образовательных учреждений актуальны следующие:

- субъект персональных данных дал **согласие в письменной форме** на обработку своих персональных данных;
- обработка персональных данных осуществляется **в соответствии с законодательством** о государственной социальной помощи, трудовым законодательством, законодательством РФ о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка персональных данных осуществляется в *медико-профилактических целях*, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется *лицом, профес-*

*сионально занимающимся медицинской деятельностью* и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;

● обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия.

Таким образом, без специального разрешения с персональными данными о состоянии здоровья учащихся может работать только медицинский работник школы в медико-профилактических целях. Для доступа других работников к таким данным требуется согласие ученика, а до его совершеннолетия — его родителей (законных представителей). При этом можно получить согласие на обработку данных, так как попытки получить согласие на признание этих данных общедоступными неизбежно столкнутся с непониманием родителей (законных представителей) учащихся. В то же время пока отсутствует правоприменительная практика, позволяющая понять, что понимается под фразой «обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц»: ведь можно трактовать и так, например, что обработка данных о здоровье ученика в школе осуществлялась для реализации его права на образование.

Учитывая, что согласно трудовому договору школа обязана начислять заработную плату, выплачивая при этом налоги на доходы физических лиц, (являясь налоговым агентом), перечислять страховые взносы в пенсионный фонд, отдельное согласие на выполнение таких обязанностей, связанных с обработкой персональных данных, не требуется. Обработка информации о здоровье работников, связанная с выполнением требований трудового законодательства, пенсионного законодательства, начислением страховых взносов во внебюджетные фонды и т.п., возможна и без получения согласия работников (так как если они не

дадут согласие, невозможно выполнить нормы законодательства).

Учитывая, что с 2011 года установлена обязательность для педагогических работников проходить аттестацию по представлению администрации, школа вправе формировать специальные базы данных педагогических работников для их аттестации, однако для передачи этих данных органам управления образованием или уполномоченным ими учреждениям необходимо получить согласие работника. Конечно, можно сослаться на то, что в этом случае данные были переданы в рамках исполнения трудового договора, однако в таком случае могут возникнуть претензии уже к органу управления образования (или методической службе), которая станет обрабатывать персональные данные, не имея ни договора, ни согласия работника.

Кроме того, из вышеприведённых требований следует, что нельзя передавать персональные данные, не связанные с необходимостью исполнения договора. Так, например, нельзя предоставлять органу управления образования данные о доходах работников школы (даже при введении новых систем оплаты труда), так как невозможно увязать передачу этих данных с необходимостью выполнять условия договора (нормативные правовые акты, которые обязывали бы предоставлять такую информацию, отсутствуют, а письмо — запрос органа управления образованием не относится к нормативным правовым актам).

Персональные данные учащихся и их родителей (за исключением специальных категорий персональных данных) школа может обрабатывать без их согласия, если с учеником или родителем (законным представителем) подписан соответствующий договор. Однако при этом нельзя передавать персональные данные учащихся и их родителей (законных представителей), если такая передача не связана с исполнением договора: в случае проверки школе придётся доказать, что переданные сведения каким-то образом связаны с исполнением договора.

Как видим, обработка персональных данных во многих случаях возможна и без получения письменного разрешения от работника, ученика (его родителей), однако в реальной деятельности школы избежать случаев, когда получить

согласие всё же необходимо, достаточно сложно. Поэтому для того, чтобы обезопасить себя при различных проверках, иметь возможность передавать определённые персональные данные по запросам органа управления образованием, а также быть уверенным в соответствии законодательству всей проводимой обработки персональных данных, согласие на обработку персональных данных следует получить и у работников, и у родителей (законных представителей учащихся), а также у самих учащихся в возрасте старше 14 лет<sup>1</sup>. Требования к согласию установлены статьёй 9 Федерального закона «О персональных данных».

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В то же время в случаях, предусмотренных федеральным законом, персональные данные обрабатываются только с согласия в письменной форме субъекта персональных данных. Равнозначным согласием в письменной форме на бумажном носителе с собственноручной подписью субъекта персональных данных признаётся согласие в форме электронного документа, подписанного, в соответствии с федеральным законом, электронной подписью.

Учитывая, что школе придётся доказывать наличие согласия на обработку, в том числе передачу персональных данных (а при обработке специальных данных речь идёт о именно письменном согласии), необходимо получать письменное согласие на их обработку. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать:

<sup>1</sup> Особенности обработки персональных данных несовершеннолетних разобраны в нашей книге «Персональные данные и информационные технологии в образовании». М., 2010.

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование образовательного учреждения, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых даётся согласие субъекта этих данных;
- наименование или фамилию, имя, отчество и адрес лица, обрабатывающего персональные данные по поручению оператора, если обработка будет поручена этому лицу (например, централизованной бухгалтерии);
- перечень действий с персональными данными, на совершение которых даётся согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

#### **Что должна сделать школа для защиты персональных данных**

Школе в обязательном порядке необходимо утвердить **положение о персональных данных**.

Трудовой кодекс РФ и ранее устанавливал обязанность утверждать такой локальный акт школы, регламентирующий обработку персональных данных работников, с которым нужно было ознакомить всех сотрудников под

подпись. Этот локальный акт должен устанавливать порядок обработки персональных данных, их передачи, а также права, обязанности сторон, ответственность за нарушение установленных правил.

При этом разработка локального нормативного акта о персональных данных работников — это обязанность работодателя, неисполнение которой может повлечь привлечение к административной ответственности по статье 5.27 КоАП РФ, а именно наложение административного штрафа на должностных лиц в размере от 500 до 5 тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, — от 500 до 5 тысяч рублей или административное приостановление деятельности на срок до 90 суток; на юридических лиц — от 30 до 50 тысяч рублей или административное приостановление деятельности на срок до 90 суток.

Теперь же утверждена обязанность школы публиковать или иным способом обеспечивать доступ к документу, определяющему её политику в отношении обработки персональных данных, сведений о реализуемых требованиях защиты персональных данных и т.п., причём в отношении не только работников, но и других лиц, персональные данные которых обрабатываются школой. В этом Положении должен быть определён перечень лиц, допускаемых в школу к персональным данным учащихся, и среди них должны быть упомянуты учителя.

Кроме того, согласно введённой Федеральным законом от 25.07.2011 № 261-ФЗ статье 22.1. в школе необходимо назначить лицо, ответственное за организацию обработки персональных данных. Этот работник (заместитель директора, как правило) должен получать указания непосредственно от директора школы и быть ему подотчётным.

На лицо, ответственное за организацию обработки персональных данных, законом возлагаются такие обязанности:

- осуществлять внутренний контроль за соблюдением школой и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников школы положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать приём и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приёмом и обработкой таких обращений и запросов.

В условиях проводимой модернизации образования во всех школах обработка персональных данных ведётся на компьютерах. Ведение электронных журналов и дневников — это вообще тема отдельного разговора (особенно различные формально «бесплатные» интернет-сервисы, к которым можно предъявить массу претензий по нарушению требований законодательства о персональных данных). Речь идёт даже о примитивной обработке в WORD персональных данных: ведь напечатать список учеников или учителей в этой или иной программе на компьютере — это уже означает «обработать персональные данные».

В Федеральном законе «О персональных данных» теперь появилось такое определение:

**Автоматизированная обработка** персональных данных — *обработка персональных данных с помощью средств вычислительной техники.*

Из этого определения вполне можно сделать вывод о том, что каждая школа занимается автоматизированной обработкой персональных данных (если, конечно, она не отказалась от использования компьютеров и не печатает все списки на печатных машинках!).

После этого пугают «страшными» требованиями, которые установлены Федеральным законом «О персональных данных» к автоматизированной обработке персональных данных, говорят о больших затратах, для того, чтобы привести свои информационные системы персональных данных в соответствие с новыми требованиями — применять достаточно дорогостоя-

щие средства защиты, строить модель угроз, разрабатывать внутренние документы. В результате делают выводы о том, что придётся или принимать на работу специалистов по безопасности, либо пользоваться специализированными услугами по защите информации. Причём, компании, которые такие услуги оказывают, должны иметь соответствующие лицензии.

Правда, пугали всем этим и до внесения поправок в закон, но о каких-то страшных последствиях нам не известно. Более того, многие директора школ вообще толком и не представляют, что от них требуется в связи с наличием Федерального закона «О персональных данных». Конечно, не совсем внятно прописанные определения усилили основания для страха, однако также как и до внесения поправок в закон, пока ещё нет оснований пугаться: достаточно более тщательно изучить действующее законодательство.

Во-первых, Федеральный закон «О персональных данных» содержит правовые нормы, определяющие возможность принимать подзаконные нормативные правовые акты для конкретизации требований законодательства о персональных данных. Так, в соответствии с частью 3 статьи 4 Федерального закона «О персональных данных» *особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами РФ с учётом положений настоящего Федерального закона.*

Постановлением Правительства РФ от 15 сентября 2008 г. № 687 было утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. В соответствии с пунктом 1 указанного Положения обработка персональных данных, содержащихся

в информационной системе персональных данных либо извлеченных из такой системы (далее — персональные данные), считается осуществлённой **без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.**

Обратим особое внимание на то, что в соответствии с пунктом 2 указанного Положения *обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из неё.*

Таким образом, можно констатировать, что с точки зрения совокупности определений, данных в действующем российском законодательстве, любая обработка персональных данных на компьютере считается автоматизированной, однако при этом, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека, то обработка считается осуществляемой без использования средств автоматизации и должна производиться в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Поэтому подавляющее большинство информационных систем в школах формально можно рассматривать как осуществляемые без использования средств автоматизации (включая ИАС «Директор» ИВЦ «Аверс», и значительную часть бухгалтерского программного обеспечения): ведь все лицевые карточки в этих системах правятся

в соответствующих окнах вручную человеком. Для уничтожения лицевых карточек оператору необходимо их выделить в списке и нажать специальную клавишу для удаления данных. Даже архивация данных осуществляется специальной программой, которая запускается человеком.

А вот различные программы, позволяющие переформатировать данные (в том числе из формата бухгалтерской программы в формат, например, программы пенсионного фонда), в рамках которых осуществляется автоматический ввод данных и дальнейшая передача без обращения к каждой конкретной записи о работнике, относятся к автоматизированной обработке данных. При этом обработка персональных данных (включая фамилию, имя, отчество, номер пенсионного свидетельства и т.п.) — неотъемлемая часть таких программ.

Если же передача данных в другие программы (в том числе для целей налогового учёта) осуществляется не полностью автоматически, а с участием человека, участвующего в диалоге с программой в обработке персональных данных, то такую обработку персональных данных также нельзя признать автоматизированной.

Школе следует привыкнуть выполнять требования Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено Постановлением Правительства РФ от 15.09.2008 № 687), тем более, что такая обработка персональных данных ещё долго гарантированно будет в школе (про отмену бумажных журналов и переход исключительно на безбумажные технологии речи никто не ведёт — распечатывать журналы приходится и тогда, когда их ведут в электронной форме).

## Меры

Согласно новой статье 18.1 Федерального закона «О персональных данных» оператор обязан принимать меры, необходимые

и достаточные для выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. При этом школа *самостоятельно определяет состав и перечень мер*, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.

Таким образом, какие конкретно принимать меры, решать школе. И только когда будут приняты подзаконные нормативные акты, которые обяжут школу принимать определённые меры по защите персональных данных, можно будет говорить об обязательности их применения (за исключением ряда мер, обязательность которых уже предусмотрена Федеральным законом «О персональных данных»).

К таким мерам **могут**, в частности, относиться:

- 1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
- 2) издание оператором, являющимся юридическим лицом, документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьёй 19 настоящего Федерального закона;
- 4) внутренний контроль и (или) аудит соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение вреда и принимаемых оператором мер, обеспечивающих выполнение обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно обрабатывающих персональные данные, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Из этого перечня меры № 1 и 2 обязательны с учётом других норм Федерального закона «О персональных данных» (выше мы об этом говорили). Мера № 4, как правило, предусматривается положением о персональных данных школы. Мера № 6 необременительна для школы и осуществляется заместителем директора, ответственным за обработку персональных данных (она прямо прописана в его обязанностях).

Проблемны меры № 3 и 5, однако их применение остаётся пока что на усмотрение самой школы. Отметим, что согласно части 3 статьи 18.1. Федерального закона «О персональных данных» Правительство РФ устанавливает перечень мер, обеспечивающих выполнение обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами. Школа — государственное или муниципальное учреждение, а не орган, поэтому когда Правительством РФ будет принят такой нормативный акт, на школу эти требования не должны распространяться.

А вот государственным и муниципальным органам управления образованием их придётся выполнять.

Согласно статье 19 Федерального закона «О персональных данных» оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий.

Обеспечение безопасности персональных данных достигается, в частности (какие из них применять — определяет сама школа):

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, мер, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищённости персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учётом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных.

Правительство РФ с учётом возможного вреда субъекту персональных данных, объёма и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

- уровни защищённости персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни их защищённости;

- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Состав и содержание необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищённости, организационных и технических мер по обеспечению безопасности персональных данных при их обработке

в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в сфере противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Здесь под **угрозами безопасности персональных данных** понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

### Уровень защищённости

Под **уровнем защищённости персональных данных** понимается комплексный показатель, характеризующий требования, исполнение которых нейтрализует определённые угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

На сегодня Правительством РФ принято лишь Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, (утверждено Постановлением Правительства РФ от 17.11.2007 № 781), в котором такие уровни и требования отсутствуют.

Пункт 6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных

данных предусматривает, что информационные системы классифицируются операторами в зависимости от объёма обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Порядок проведения такой классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности РФ и Министерством информационных технологий и связи РФ, т.е. речь идёт о совершенно иной классификации. Никаких «комплексных показателей» Правительством РФ пока не принято.

Кроме того, это Положение в пункте 1 устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных лишь с использованием средств автоматизации. И если школа обрабатывает персональные данные в порядке, подпадающем под определения, данные в Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (Положения, утверждённого Постановлением Правительства № 687, как нами было рассмотрено выше), то нет необходимости выполнять требования Положения, утверждённого Постановлением Правительства № 781. **НО**