Хранение и использование персональных данных

Анатолий Борисович Вифлеемский

Новым веянием времени стали так называемые «облака», куда в некоторых городах органы управления образованием захотели поместить персональные данные всех работников школ. Однако не задумались о том, какие условия должны быть соблюдены, что привело к массовым нарушениям законодательства о защите персональных данных.

Депутаты против офшорного дневника

По сообщениям СМИ, первый заместитель председателя Комитета Госдумы по образованию, депутат от Челябинской области В.В. Бурматов направил обращение на имя вице-премьера Правительства РФ О.Ю. Голодец, в котором обозначил, по его мнению, недостаточные меры Министерства образования по обеспечению безопасности персональных данных школьников. Депутат обратил внимание на тот факт, что доступ к данным как минимум 5,6 млн российских учащихся получила офшорная компания, зарегистрированная на Кипре.

«*Частная компания собирает и обрабатывает персональные данные школьников, учителей и их родителей на протяжении нескольких лет, подключив к системе более 30 тыс. школ и более 5,6 млн учеников. При этом изучение порядка базового (бесплатного) подключения школ и школьников к системе «Дневник.ру» показало, что данные несовершеннолетних имеют примитивную систему защиты и не предусматривают использования программного-аппаратных средств шифрования при передаче данных через открытые каналы (сеть Интернет) при коммуникациях с пользователями и имеют минимальную защиту только на стороне ООО «Дневник.ру*». При этом **единственным 100% учредителем «Дневник.ру» является кипрский офшор «I.AR.EICH. EDU REVOLYUSHN KHOLDINGZ LTD»**, зарегистрированный в Никосии, а руководит обществом выпускник Колумбийского университета в Нью-Йорке Г.Д. Леви 1982 года рождения. Считаю необходимым выяснить, каким образом персональные данные как минимум 5,6 млн российских школьников оказались в распоряжении компании с учредителем в виде кипрского офшора, *стратегическим партнёром которой официально указывается Министерство образования и науки Российской Федерации*» — сказано в депутатском запросе[1]. Кроме того, ООО «Дневник.ру» обвинялось в незаконной трансграничной передаче персональных данных.

[1] http://www.nakanune.ru/news/2015/5/19/22399938/ #sthash.zZYQi0ER.dpuf

Естественно, что ООО «Дневник.ру» незамедлительно стало опровергать обвинения депутата-единоросса. Ответ этого общества сводился к трём позициям:

1. На стороне ООО «Дневник.ру» достаточно средств защиты персональных данных, а школы пусть сами позаботятся о защите;

2. Многие IT-компании учреждены офшорными компаниями;

3. Персональные данные российских школьников хранятся и обрабатываются ООО «Дневник.ру» в России, что можно подтвердить сервисом Who.is.

«Следует отметить, что офшорные учредители присутствуют у многих крупных ИТ и телекоммуникационных компаний России, которые ежедневно обрабатывают огромные массивы персональных данных. Такая практика обусловлена тем, что российское законодательство пока не позволяет быстро структурировать сложные инвестиционные сделки. Однако этот юридический аспект не означает, что компания — оператор персональных данных — занимается трансграничной передачей данных: это запрещено законодательством Российской Федерации» — так дословно сказано в релизе ООО «Дневник.ру»[2].

Таким образом, из обвинений ООО «Дневник.ру»признало лишь наличие иностранного учредителя. Конечно, это отрицать было бы совершенно бессмысленно, так как выписку из ЕГРЮЛ в современных условиях можно получить практически моментально.

Однако такое признание отнюдь не освобождает от ответа на поставленные депутатом вопросы Минобрнауки России: возможно ли в современных условиях борьбы с офшорными компаниями в России иметь в качестве стратегического партнёра федеральному министерству коммерческую дочку «офшорки»? Не даёт ли такое партнёрство оснований для подозрений в наличии коррупционной составляющей у ответственных работников министерства?

Впрочем, необходимо дождаться разъяснений Минобрнауки касательно наличия факта «стратегического партнёрства». Пока что мы видели заявление лишь одной стороны, тогда как другая сторона может и не посчитать себя «стратегическим партнёром». Точно также как «партнёры» МММ по прошествии некоторого времени стали считать себя обманутыми вкладчиками.

А вот насчёт хранения и обработки персональных данных российских школьников в России сервис Who.is даёт неутешительный для ООО «Дневник.ру» ответ. Когда-то, в прошлом десятилетии, действительно, сайт dnevnik.ru располагался на серверах в России, теперь же — далеко за пределами границ России.

Пройдя по ссылкам, можно легко установить местонахождение серверов, на которых расположены данные «Дневник.ру» и среди них нет ни одного российского адреса. Например, **Domain awsdns-10.org** имеет IP 205.251.196.83, IP Location Mount Pearl, NL, CA.

Таким образом, обвинения депутата В.В. Бурматова совершенно справедливы, а вот руководителям учреждений, использующим в качестве ЭКЖ сервисы dnevnik.ru, следует задуматься о переходе на использование другого электронного дневника.

Федеральным законом от 21 июля 2014 г. № 242-ФЗ было установлено, что при сборе персональных данных операторы персональных данных (включая операторов информационных систем) должны обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории России. Такие обязанности возложены и на школы, неизбежно являющиеся операторами персональных данных и обрабатывающие их, в частности,

[2] Там же.

при ведении ЭКЖ. Федеральным законом от 31 декабря 2014 г. № 526-ФЗ установлено, что требование о хранении персональных данных на серверах, расположенных в России, начинает действовать с 1 сентября 2015 г.

Запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ должны осуществляться с использованием баз данных, находящихся на территории России. Исключение из этого правила составят случаи, когда обработка персональных данных необходима, например, для достижения предусмотренных международным договором РФ или законом целей, а также некоторых других (пункты 2, 3, 4, 8 части 1 статьи 6 Закона о персональных данных). Обеспечить нахождение на территории РФ баз данных должны будут обладатели информации, операторы информационной системы. А это, в данном случае, прямо относится к ООО «Дневник.ру».

Полномочия по контролю реализации новых требований законодательства о персональных данных возложены на Роскомнадзор. Сведения о месте нахождения таких баз данных оператор обязан сообщать в Роскомнадзор в уведомлении об обработке персональных данных.

Таким образом, и школам, в случае использования «облачных» дневников, придётся узнать место нахождения базы данных и сообщить Роскомнадзору. При этом такой адрес с 1 сентября 2015 г. не может быть за пределами России.

Требования Минобрнауки России к электронным дневникам

Хотя депутат В.В. Бурматов и полагает, что Министерство образования и науки РФ принимает недостаточные меры по обеспечению безопасности персональных данных школьников, сказать, что министерство бездействует, нельзя.

Письмом от 21 октября 2014 г. № АК-3358/08 Минобрнауки России направило уточнения в методические рекомендации по внедрению систем ведения журналов успеваемости в электронном виде, предусмотрев организацию дополнительных работ по исполнению Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». И эти новые требования Минобрнауки России касаются всех школ, использующих сервис Дневник.ру.

Электронные журналы, обрабатывающие данные вне образовательной организации, согласно Требованиям Минобрнауки России, предусматривают необходимость:

- *уведомить уполномоченный орган по защите прав субъектов персональных данных о своём намерении осуществлять обработку персональных данных»* (п. 1 ст. 22 Закона № 152-ФЗ) и декларировать изменения «в течение десяти рабочих дней с даты возникновения» (п. 7 ст. 22 Закона № 152-ФЗ), в том числе при смене варианта используемого электронного журнала;
- контролировать возможность трансграничной передачи персональных данных;
- получить и соответствующим образом хранить письменные согласия субъектов на обработку персональных данных, в том числе на передачу их в организацию, обслуживающую внешний электронный журнал;
- обеспечить соответствие целей обработки данных, указанных в согласии на обработку, с целями обработки данных у организации, которой эти данные передаются;
- заключить договор с организацией, обслуживающей электронный журнал, об ответственности за обработку переданных ей персональных данных в соответствии с заявленными целями.

Учитывая, что ООО «Дневник.ру» отрицает очевидную трансграничную обработку персональных данных, контроль со стороны школы обещает быть не простым. Согласия о передаче на обработку персональных данных ООО «Дневник.ру», как правило, в школах отсутствуют.

Обеспечить соответствие целей обработки персональных данных целям ООО «Дневник.ру», связанным с рекламой и различными маркетинговыми акциями, школе вообще невозможно. Даже заключить договор с ООО «Дневник.ру» можно лишь на условиях, которые организация сочтёт для себя выгодными. При этом основные цели деятельности любой коммерческой организации, включая ООО «Дневник.ру» уже определены гражданским законодательством — извлечение прибыли (ст. 50 ГК РФ). Общеизвестно, что офшорные учредители нужны для того, чтобы при этом заплатить как можно меньше налогов с полученной прибыли.

Поэтому Минобрнауки России обратило особое внимание на то, что *«при использовании электронных журналов, обрабатывающих данные внутри образовательной организации, ряд перечисленных выше мероприятий может быть сокращён и (или) облегчён при соответствующей подготовке локальной нормативной базы».*

Вместе с тем в любом случае образовательная организация должна обеспечить организационно-технические меры по защите персональных данных, находящихся в её информационных системах, включая электронный журнал, в соответствии с требованиями закона и инструкций по информационной безопасности. В обоих случаях необходимо соблюдать условие пункта 1 статьи 9 Федерального закона № 152-ФЗ «О персональных данных» о том, что *согласие на обработку персональных данных даётся субъектом с соблюдением его интересов.*

Министерство предупреждает, что *«если обработка персональных данных субъекта диктуется интересами организации, а не интересами субъекта, то согласие может быть признано ничтожным и аннулировано, а обработка данных — нарушающей требования законодательства».* А это означает, что, если родителям учеников не нужен электронный журнал и дневник, то они вправе не давать или отозвать своё согласие. В этом случае никаких данных ученика, родители которого не дали согласие на обработку персональных данных, в ЭКЖ Дневника.ру быть не должно.

ГИА и персональные данные

Минобрнауки России уделяет вопросам соблюдения законодательства о персональных данных всё больше и больше внимания. Письмом от 4 марта 2015 г. № 03–155 были направлены Разъяснения о порядке действий в случае отсутствия согласия на обработку персональных данных, совершеннолетними участниками государственной итоговой аттестации (далее — ГИА) или родителями (законными представителями) несовершеннолетних участников ГИА, в которых обратило внимание на то, что доступ к персональным данным, содержащимся в ФИС и РИС, а также обработка указанных данных осуществляются в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». При этом министерство обратило внимание на то, что *обработка персональных данных учащихся осуществляется, в том числе для внесения информации в ФИС. В случае отказа от обработки персональных данных учащегося они не будут внесены в ФИС и РИС.*

Хранение и обработка информации, содержащейся в ФИС и РИС, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации, предусмотренных нормативными правовыми актами Российской Федерации в области защиты информации. Доступ к персональным данным, содержащимся в ФИС и РИС, и обработка указанных данных осуществляются в строгом соответствии с Федеральным законом № 152-ФЗ.

Минобрнауки сделало вывод о том, что *«...без согласия субъекта персональных данных или его представителя (в случае, если речь идёт о несовершеннолетнем гражданине), внесение сведений в ФИС и РИС запрещено».*

Каким же образом в таком случае проводить государственную итоговую аттестацию? Можно ли отказать в её прохождении учащемуся? Ведь ФИС и РИС предусмотрены Законом «Об образовании в РФ». Неужели нельзя заставить дать согласие на обработку персональных данных?

Ответы на эти вопросы содержатся в письме Рособрнадзора от 17 марта 2015 г. № 02–91.

С целью соблюдения конституционных прав граждан на получение основного общего и среднего общего образования необходимо обеспечить возможность прохождения ГИА учащимися, отказывающимися дать согласие на обработку персональных данных, без внесения их персональных данных в федеральную информационную систему обеспечения проведения государственной итоговой аттестации учащихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приёма граждан в образовательные организации для получения среднего профессионального и высшего образования (ФИС) и региональные информационные системы обеспечения проведения государственной итоговой аттестации учащихся, освоивших основные образовательные программы основного общего и среднего общего образования (РИС).

Для сдачи ГИА названные выше лица подают заявление в государственную экзаменационную комиссию субъекта РФ (ГЭК) с просьбой предоставить возможность пройти ГИА без обработки их персональных данных.

ГЭК принимает решение о допуске данного учащегося к сдаче ГИА без внесения персональных данных о нём в РИС и ФИС, а также определяет для него пункт проведения экзамена (далее — ППЭ), аудиторию и место. Решение ГЭК оформляется протоколом. Данный протокол направляется в ППЭ.

Рособрнадзор обращает внимание на то, что для указанной категории граждан экзамен проводится в штатном режиме за исключением того, что в бланке регистрации не указываются данные о документе, удостоверяющем личность. Все сопроводительные документы при этом оформляются вручную.

Особенности в проведении ГИА учащихся, в отношении которых нет согласия на обработку персональных данных, имеются и после проведения экзамена.

После проведения экзамена работу учащегося упаковывают в отдельный конверт и доставляют в ГЭК. ГЭК направляет в Рособрнадзор письмо с просьбой проверить экзаменационную работу учащегося и прикладывает к письму конверт, содержащий индивидуальный комплект указанного учащегося (все экзаменационные материалы, контрольный измерительный материал). Вскрывать запечатанный в ППЭ конверт с экзаменационными материалами запрещается.

После проверки экзаменационной работы Рособрнадзор направляет результаты в ГЭК для утверждения и выдачи учащемуся. Рособрнадзор при этом отметил, что результаты ГИА такого учащегося будут отсутствовать в ФИС и РИС, что повлечёт за собой ограничение его прав при поступлении на обучение по образовательным

программам высшего образования — программам бакалавриата и специалитета. Однако представляется, что в случае обращения таких учащихся с жалобами на нарушение конституционных прав на образование, и эти проблемы будут разрешены без необходимости внесения персональных данных в информационные системы.

Аутсорсинг бухучёта, персональные данные и «облака»

Точно так же, как и персональные данные учащихся, требуют защиты и персональные данные работников школы. При этом в отношении обработки этих персональных данных проверяющих даже больше — ещё и государственная трудовая инспекция может проверить соблюдение норм трудового законодательства, также устанавливающего требования в части обработки персональных данных работников школы.

Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»[3] дают ответы на некоторые злободневные вопросы, возникающие в рамках трудовых отношений образовательных учреждений со своими работниками.

В частности, Роскомнадзор указывает на то, что «...при привлечении сторонних организаций для ведения кадрового и бухгалтерского учёта работодатель обязан соблюдать требования, установленные ч. 3 ст. 6 Федерального закона «О персональных данных», в том числе получить согласие работников на передачу их персональных данных».

Содержание согласия работника должно быть конкретным и информированным, т.е. содержать информацию, позволяющую однозначно сделать вывод о целях, способах обработки с указанием действий, совершаемых с персональными данными, объёме обрабатываемых персональных данных.

Согласие работника может быть оформлено как в виде отдельного документа, так и закреплено в тексте трудового договора и отвечать требованиям, предъявляемым к содержанию согласия, согласно ч. 4 ст. 9 Федерального закона «О персональных данных».

Это означает, что согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) 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);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых даётся согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

[3] Опубликованы на сайте http://www.rsoc.ru

7) перечень действий с персональными данными, на совершение которых даётся согласие, общее описание используемых оператором способов обработки персональных данных;
8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
9) подпись субъекта персональных данных.

Обратим внимание на то, что работник имеет право не давать такого согласия. В таком случае школа не имеет права передавать его данные на обработку сторонней организации для ведения кадрового и бухгалтерского учёта.

В Москве Департамент образования настоятельно рекомендует заключать договора аутсорсинга с различными организациями вместо ведения бухгалтерского учёта силами собственной бухгалтерии. Одновременно Департамент требует передачи данных в некие информационные системы (сначала это было требование передачи данных в некую УАСОФД, затем в АУИС Бюджетный учёт). При этом Департамент образования города Москвы игнорирует требования законодательства о защите персональных данных, из которых следует, что без согласия работника его персональные данные не могут быть переданы на обработку третьим лицам.

Между тем, исходя из требований законодательства о защите персональных данных, необходимо иметь согласия работников как на обработку аутсорсинговой организацией, так и организацией — оператором «облаков», как бы они ни назывались (УАСОФД, АУИС Бюджетный учёт или иначе). При отсутствии таких согласий персональные данные нельзя передать ни аутсорсинговой организации, ни в «облака». Ответственность за незаконную передачу персональных данных на обработку несёт директор образовательного учреждения.

Кроме того, следует учитывать напоминание Минобрнауки России о том, что *«если обработка персональных данных субъекта диктуется интересами организации, а не интересами субъекта, то согласие может быть признано ничтожным и аннулировано, а обработка данных — нарушающей требования законодательства»*.

Региональные и муниципальные органы управления образованием, создавая «облака», должны обосновать цель их создания, соответствующую требованиям законодательства о персональных данных. При этом сделать это будет очень не просто, так как к трудовым отношениям в подведомственных учреждениях эти органы не могут иметь никакого отношения.

Статьёй 3 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» одним из основных принципов государственной политики и правового регулирования отношений в сфере образования является автономия образовательных организаций. Статья 28 Закона об образовании в РФ в развитие данного принципа устанавливает, что образовательная организация обладает автономией, под которой понимается самостоятельность в осуществлении образовательной, научной, административной, финансово-экономической деятельности, разработке и принятии локальных нормативных актов в соответствии с настоящим Федеральным законом, иными нормативными правовыми актами Российской Федерации и уставом образовательной организации.

Согласно статье 89 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» управление системой образования осуществляется

на принципах законности, демократии, автономии образовательных организаций, информационной открытости системы образования и учёта общественного мнения и носит государственно-общественный характер. Составляющие управление системой образования указаны в части 2 статьи 89. Таким образом, создание не предусмотренных федеральным законодательством об образовании государственных или муниципальных систем ведения кадрового учёта и расчёта заработной платы работников образовательных учреждений, может быть расценено в качестве нарушения федерального законодательства об образовании.

Требования к государственным и муниципальным «облакам»

В случае создания государственной или муниципальной информационной системы, использующей «облачные» технологии, должен быть реализован полный перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, утверждённый Постановлением Правительства РФ от 21 марта 2012 г. № 211.

Операторы, являющиеся государственными или муниципальными органами, обязаны принять следующие меры:

1) назначить ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих данного органа;

2) утвердить актом руководителя государственного или муниципального органа следующие документы:

- правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;
- правила работы с обезличенными данными;
- перечень информационных систем персональных данных;
- перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;
- перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;
- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения

с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

• типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

• порядок доступа служащих государственного или муниципального органа в помещения, в которых ведётся обработка персональных данных;

3) при эксплуатации информационных систем персональных данных в случае, если государственный или муниципальный орган является оператором таких информационных систем, принять правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищённости персональных данных;

4) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведённой проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии;

5) осуществить ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих;

6) уведомить уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным законом «О персональных данных»;

7) согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных, осуществить обезличивание персональных данных, обрабатываемых в информационных системах персональных данных.

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Обратим особое внимание на то, что весь этот обширный перечень мер и документов не распространяется на государственные и муниципальные учреждения (в том

числе на образовательные учреждения), не являющиеся государственными или муниципальными органами. Технические меры по обеспечению безопасности в государственных информационных системах, которые должны предпринять государственные и муниципальные органы, также весьма обширны и разнообразны. Их перечень можно найти в Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждённые приказом ФСТЭК России от 11.02.2013 № 17.

Требования обязательны при обработке информации в государственных информационных системах, функционирующих на территории РФ, а также в муниципальных информационных системах, если иное не установлено законодательством РФ о местном самоуправлении. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» детализирует организационные и технические меры защиты информации.

Выбор мер защиты информации осуществляется исходя из класса защищённости информационной системы, определяющего требуемый уровень защищённости содержащейся в ней информации, и угроз безопасности информации, включённых в модель угроз безопасности информационной системы, а также с учётом структурно-функциональных характеристик информационной системы, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в её отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности её функционирования.

Ответственность за нарушение требований по обработке персональных данных

За нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) статьёй 13.11 Кодекса РФ об административных правонарушениях предусмотрены следующие санкции:

- предупреждение или наложение административного штрафа на граждан в размере от трёхсот до пятисот рублей;
- на должностных лиц — от пятисот до одной тысячи рублей;
- на юридических лиц — от пяти до десяти тысяч рублей.

Как видим, санкции за нарушения невелики. Однако ситуация уже к моменту выхода в свет журнала может измениться. Государственной думой ФС РФ в первом чтении 24.02.2015 был принят проект Федерального закона № 683952–6 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», которым увеличиваются как количество санкций за различные нарушения порядка обработки персональных данных, так и размеры штрафов. Если образовательное учреждение или орган управления образованием, являющийся оператором персональных данных, *нарушит требования к содержанию письменного согласия субъекта персональных данных,* ему будет грозить штраф в размере от 3 до 8 тысяч руб. (для должностных лиц) либо в размере от 15 до 50 тысяч руб. (для юридических лиц).

Обработка персональных данных без согласия субъекта и в отсутствие иных условий обработки, предусмотренных законодательством, повлечёт штрафы в размере от 5 до 15 тысяч руб. (для должностных лиц) и от 30 до 50 тысяч руб. (для юридических лиц).

Незаконная обработка специальных категорий персональных данных может повлечь ещё более значительные санкции, чем первые два нарушения. За это должностных лиц предлагается штрафовать на сумму от 10 до 25 тысяч руб., а юридических лиц — на сумму от 150 до 300 тысяч руб.

Напомним, что к специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни гражданина, а также персональные данные о судимости. Случаи использования специальных категорий персональных данных, не оговорённые в статье 10 Федерального закона о персональных данных, являются нарушением законодательства о персональных данных. В результате, если в электронном журнале в «облаках» будут обрабатываться и сведения о состоянии здоровья учащихся (включая пометку «болен» в ЭКЖ) без письменного согласия на это родителей несовершеннолетних учащихся, скоро размеры штрафов могут неприятно поразить руководителей образовательных учреждений.

Невыполнение обязанности по обезличиванию персональных данных и несоблюдение установленных требований и методов по такому обезличиванию влечёт наказание *должностных лиц* государственных и муниципальных *органов управления образованием,* которым будет грозить предупреждение либо штраф от 3 до 6 тысяч руб.

За неопубликование политики в области ПД операторов предполагается установить штраф в размере от 3 до 6 тысяч руб. (для должностных лиц) и от 15 до 30 тысяч руб. (для юридических лиц).

Непредоставление гражданину информации об обработке его персональных данных станет основанием для привлечения оператора к административной ответственности в виде штрафа 4–6 тысяч руб. для должностных лиц и 20–40 тысяч руб. для юридических лиц.

Несвоевременное выполнение требований гражданина об уточнении, блокировании или уничтожении его персональных данных в случае, если личные данные неполные, устаревшие, неточные, незаконно полученные или не являются необходимыми для заявленной цели обработки, повлечёт штрафы в размере от 4 до 10 тысяч руб. для должностных лиц и от 25 до 45 тысяч руб. для юридических лиц.

И, наконец, *ненадлежащая защита персональных данных, повлёкшая несанкционированный доступ к ним,* грозит штрафом в размере от 4 тысяч до 10 тысяч руб. для должностных лиц и от 25 тысяч до 50 тысяч руб. для юридических лиц. Такие штрафы пока что планируется ввести в отношении тех юридических лиц, которые обрабатывают персональные данные без использования средств автоматизации и хранят их на материальных носителях.

Наказания за утечки персональных данных при их обработке автоматизированным способом пока не предусмотрены. Так что непосредственно ООО «Дневник.ру» или оператор «облаков» (УАСОФД, УАИС Бюджетный учёт) в случае утечки из них персональных данных учащихся и работников школ вполне могут остаться безнаказанными. А это означает, что субъектам персональных данных (учащимся, их родителям (законным представителям) и работникам школ) следует самим озаботиться вопросами защиты своих персональных данных.

Анатолий Борисович Вифлеемский,
действительный член Академии педагогических и социальных наук, доктор экономических наук