Требования к обработке персональных данных

Под персональными данными понимают любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

Таким образом, любое образовательное учреждение осуществляет обработку персональных данных и является оператором персональных данных. Следовательно, необходимо знать и соблюдать требования, предъявляемые действующим законодательством к обработке персональных данных.

Особую остроту вопросы защиты персональных данных в образовательных учреждениях приобретают в связи с имеющимися в действующем законодательстве предписаниями обеспечить всем организациям на территории Российской Федерации требуемый уровень безопасности персональных данных в действующих информационных системах не позднее 01.01.2010.

Нормативно-правовая база защиты персональных данных

В названных нормативных актах даны основные понятия информации, информационных систем и технологий, доступа к информации и ее конфиденциальности и др.

Так, информационные технологии рассматриваются как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов (п. 2 ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации»). Под информационной системой понимается совокупности содержащихся в базах данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальная информация - это документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Конфиденциальная информация не подлежит передаче третьим лицам без согласия ее обладателя. Обладателем информации является лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать к ней доступ на основании закона или договора.

Помимо этого статьями 10 и 11 Федерального закона «О персональны* пан ных» установлены специальные данные, в отношении которых дей< мукя ни вышенные меры защиты от несанкционированной обработки и распро< гран< НН1

Это информация, касающаяся касающихся расовой, национальной прима;

ности, политических взглядов, религиозных или философских убеждении >.• стояния здоровья, интимной жизни.

Если от сбора информации о национальности работников, обучающим | образовательные учреждения вполне могут отказаться, то информация о 00 стоянии здоровья необходима большинству образовательных учреждений 11 тому образовательным учреждениям, как правило, приходится работ;) п. специальными данными.

Отметим также, что специально уполномоченным лицам, например работникам милиции или прокуратуры, доступ к персональным данным разреш Им предоставляются сведения о сотрудниках и учащихся образовательною у реждения в необходимом для работы объеме.

Условия обработки данных

Действующим законодательством не допускаются сбор, передача, уничтожение, хранение, использование и распространение информации о частно! жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайму переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Режим конфиденциальности персональных данных снимается в случаях обезличивания этих данных или по истечении 75-летнего срока их хранения, если иное не определено законом.

Безопасность персональных данных должна достигаться путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Обработка персональных данных но общему правилу производится с согласия субъекта персональных данных. И лишь в определенных законом случаях такое согласие не требуется. Так, согласие не требуется, если обработка данных:

1)обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2)обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3)обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4)обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5)обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи; '

6)обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7)осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Если образовательное учреждение формирует какие-либо базы данных работников (например, педагогических работников для их аттестации, формирования заявок на прохождение повышения квалификации и т.д.), то необходимо получить согласие работника на обработку персональных данных.

Работа с персональными данными должна осуществляться только в целях, по перечням и в сроки, которые необходимы для выполнения задач соответствующего держателя или пользователя персональных данных, и устанавливается действующим законодательством,

лицензией или договором.
Также можно обрабатывать персональные данные студентов, учащихся И их родителей, если с ними подписан соответствующий договор. Однако при этом нельзя передавать персональные данные работников, учащихся и их родителей, если такая передача не связана с исполнением договора. В этой связи, и частности, не могут быть предоставлены органу управления образования данные о доходах работников образовательного учреждения (даже при введении новых систем оплаты труда), нельзя также передать без согласия родителе! учащихся сведения о них и об учащихся органам управления образованием. Об ли не удастся доказать, что это связано с исполнением
В тоже время данные об учащихся, как было отмечено выше, часто содержат сведения об их здоровье. Тем самым они относятся к специальным данным Однако требования по обработке специальных данных действующим законодательством установлены более строгие.
Обработка специальных категорий персональных данных согласно ст. 1(1 Федерального закона «О персональных данных» допускается только в случая* если:
1)субъект персональных данных дал согласие в письменной форме на об работку своих персональных данных;
2)персональные данные являются общедоступными;
3)персональные данные относятся к состоянию здоровья субъекта перс о начальных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизнен но важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
4)обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
5)обработка персональных данных членов (участников) общественною объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими и соответствии с законодательством Российской Федерации, для достижения за конных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных; »
6)обработка персональных данных необходима в связи с осуществлением правосудия;
7)обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.
Таким образом, без специального разрешения, с персональными данными о состоянии здоровья учащихся может работать только медицинский работник образовательного учреждения в медико-профилактических целях.
В результате получается, что для доступа остальных работников к таким данным требуется согласие учащегося, а до его совершеннолетия - его родителей (законных представителей). При этом можно получить согласие на обработку данных, а можно попытаться получить согласие на признание этих данных общедоступными.
Последнее, конечно, облегчит решение ряда формальных вопросов, касающихся обработки персональных данных.

При этом следует иметь в виду, что согласно ст. 18 Федерального закона «О персональных данных» если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
1)наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
2)цель обработки персональных данных и ее правовое основание;
3)предполагаемые пользователи персональных данных:
4)установленные Федеральным законом № 152-ФЗ права субъекта персональных данных.

В соответствии с Постановлением № 781 и Федеральным законом «О персональных данных» образовательное учреждение, получившее доступ к персональным данным, должен обеспечить их сохранность и предотвратить несанкционированный доступ к информации. Для этого оно обязано принять необходимые организационные и технические меры защиты, используя шифровальные (криптографические) средства, исключающие уничтожение, изменение, блокировку, копирование и распространение персональных данных

Права работников, учащихся и их родителей в отношении персональных данных

Субъект персональных данных самостоятельно решает вопрос передачи кому-либо сведений о себе, за исключением случаев, предусмотренных законодательством. В свою очередь, субъект имеет право на доступ к персональным данным, относящимся к его личносги, И на получение сведений о наличия данных и самих данных. При наличии оснований, подтвержденных соответствующими документами, субъект персональных данных вправе требовать от оператора-держателя этих данных внесения в них изменений и дополнений. С другой стороны, субъект обязан сообщить держателю об изменении персональных данных.
Поэтому работник образовательного учреждения вправе в любое время посмотреть свое личное дело и сделать копни нужных ему документов (ст.89 ТК РФ). Кроме того, на основании ст. 14 Федеральною закона « О персональных данных» работники, учащиеся (после совершеннолетия) и их родители (законные представители) вправе:
- получить сведения об операторе (в данном случае работодателе), м его нахождения;
- требовать уточнения своих данных, их блокировки или уничтожения в случае, если они являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите свои» прав;
- получить данные в доступной форме (в них не должны содержаться сведения, относящиеся к другим лицам);
- иметь доступ к своим данным через законного представителя или на с основании письменного запроса. Запрос должен содержать номер основного документа, удостоверяющего личность (паспорт), сведения о дате его выдачи и выдавшем его органе, а также собственноручную подпись работника либо его законного представителя.
Работник, учащийся (совершеннолетний) и их родители при обращении или запросе имеет право на получение информации, касающейся обработки его данных, в том числе содержащей:
- подтверждение факта обработки данных, а также ее цель;

- способы обработки данных, применяемые работодателем в учреждении;
- сведения о лицах, которые имеют доступ к данным работника или которым он может быть предоставлен;
- перечень обрабатываемых данных и источник их получения;
- сроки обработки данных, в том числе сроки их хранения;
- сведения о юридических последствиях обработки персональных данных.

Право субъекта персональных данных на доступ к своим персональным данным ограничивается, если:
- обработка данных, в том числе полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности и охраны правопорядка;
- обработка данных ведется органами МВД, задержавшими данное лицо по подозрению в преступлении либо по обвинению в рамках уголовного дела либо применившими к нему меру пресечения до предъявления обвинения, за исключением случаев, предусмотренных уголовно-процессуальным законодательством РФ;
- предоставление персональных данных нарушает конституционные права и свободы других лиц.
Образовательное учреждение в случае личного обращения работника или родителя учащегося за информацией, касающейся его персональных данных, или его письменного запроса либо через законного представителя обязан предоставить ее в течение 10 рабочих дней с даты получения запроса.. Информацию о персональных данных образовательное учреждение обязано предоставить работнику или родителям учащихся безвозмездно (п. 3 ст. 20 Федерального закона «О персональных данных»). В случае отказа в предоставлении данных должен быть дан мотивированный ответ, исходя из положений Федерального закона «О персональных данных», в срок, не превышающий семи рабочих дней со дня получения запроса
Уведомление об обработке персональных данных
Образовательное учреждение вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:
- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- полученных оператором в связи с заключением договора, стороной кото рого является субъект персональных данных (обучающийся и др.), если персо
нальные 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;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональны\ данных на территорию образовательного учреждения или в иных аналогичных целях;
-включенных в информационные системы персональных данных, имею щие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка (включая базы данных, формируемые и связи с ЕГЭ);

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечении) «Опасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.
Во всех остальных случаях оператор (руководитель образовательного учреждения и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

-уведомление и рекомендации по заполнению

Ответственность за нарушение
порядка обработки персональных данных

Согласно ст. 24 Федерального закона «О персональных данных» на Я виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность. В Трудовом кодексе РФ (ст. 90 ТК РФ) также положения, предусматривающие ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника: лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной, материальной, ОДММ административной и уголовной ответственности.
Гражданский кодекс РФ предусматривает защиту нематериальных благ граждан, включая неприкосновенность частной жизни, личную и семейную тайну, честь, доброе имя и деловую репутацию. За распространение сведений, порочащих честь, достоинство и деловую репутацию работника или учащегося, его родителей, в соответствии со ст. 150-152 ГК РФ может взыскана денежная компенсация морального вреда или имущественного ущерба.
Согласно
положений Федерального закона «О персональных данных» субъект персональных данных имеет право на защиту своих прав и законных интересов, том числе на возмещение убытков и (или) компенсацию морального ущерба в судебном порядке.
Однако не может быть удовлетворено требование о возмещении убытке предъявляемое лицом, которое не приняло обязательных мер по соблюдению конфиденциальности информации или нарушило установленные законодательством РФ требования о ее защите.
К работникам образовательного учреждения, ответственным за хранен персональных данных, могут быть применен дисциплинарные взыскания, предусмотренные ст. 192 ТК РФ, в том числе замечание, выговор или увольнение. Однако к ответственности могут быть привлечены только те работники, которые в соответствии с условиями своих трудовых договоров и должности, инструкций обязаны были соблюдать правила работы с персональными данными, указаны в перечне лиц, имеющим доступ к персональным данным. То же относится, в том числе и к работникам, ответственным за ведение, хранение, учет и выдачу трудовых книжек.
Теоретически нарушение требований к работе с персональными данными может повлечь даже уголовную ответственность. Преступлением является, в частности, незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах

массовой информации. Согласно ст. 137 УК РФ наказание за это преступление устанавливается следующее:

- штраф в размере до 200 000 руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев;
- либо обязательные работы на срок от 120 до 180 часов;
- либо исправительные работы на срок до одного года;
- либо арест на срок до четырех месяцев.

При этом те же деяния, совершенные лицом с использованием своего служебного положения (то есть, например, директором образовательного учреждения), наказываются:

- штрафом в размере от 100 000 до 300 000 руб. или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет;
- либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет;
- либо арестом на срок от 4 до 6 месяцев.

Незаконный отказ должностного лица в предоставлении гражданину информации также является основанием привлечения к уголовной ответственности. В соответствии со ст. 140 УК РФ если должностное лицо неправомерно отказывает в предоставлении собранных в установленном порядке документов и материалов, затрагивающих права и свободы гражданина, либо предоставляет гражданину неполную или заведомо ложную информацию, и такие действия причинили вред правам и законным интересам граждан, то должностное лицо наказывается:

- штрафом в размере до 200 000 руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев;
- либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

На практике более часто встречается привлечение должностных лиц образовательных учреждений к административной ответственности. На настоящий момент административная ответственность для операторов (за исключением лиц, для которых обработка персональных данных является профессиональной деятельностью и подлежит лицензированию) предусмотрена:

- за отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо их несвоевременное предоставление, непредоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 КоАП РФ) - указанные правонарушения влекут наложение административного штрафа на должностных лиц в размере от 500 до 1000 руб.;
- за нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных (ст. 13.11 КоАП РФ) предусматривается ответственность в виде предупреждения или наложения штрафа на граждан в размере от 300 до 500 руб.; на должностных лиц - от 500 до 1000 руб.; на юридических лиц - от 5000 до 10 000 руб.);
- за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет за собой уголовную ответственность) лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ) влечет наложение административного штрафа на граждан в размере от 500 до 1000 руб.; на должностных лиц - от 4000 до 5000 руб. Такое наказание применяется за исключением случаев

уголовной ответственности и кроме случаев, предусмотренных ч. 1 ст. 14.33 КоАП РФ.
Таким образом, если, например, были разглашены персональные данные учителя работником образовательного учреждения, то ему может быть наложен штраф от 500 до 1000 рублей, если это сделало должностное лицо (в частности, директор учреждения), то штраф составит от 4000 до 5000 руб.
При отсутствии положения о персональных данных может быть наложен штраф на образовательное учреждение в размере от 5000 до 10 000 руб.
Уполномоченным органом по контролю за соблюдением законодательства персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Этот орган проводит плановые (целевые, комплексные) проверки, а также про верки по жалобам и обращениям физических и юридических лиц.
Проверки систем защиты персональных данных могут также осуществляется и я ФСТЭК России или ФСБ России при проведении контроля систем защиты конфиденциальных данных или использования криптосредств.
Судебная практика за нарушение режима персональных данных уже имеется. Из нее следует, что требования о защите персональных данных работников, заключающиеся, в том числе в издании локального нормативного акт организации о персональных данных, носят обязательный характер. Реализация их на практике позволит избежать привлечения к ответственности, а также дополни тельных затрат в случае проведения проверок.
Постановление ФАС Московского округа от 27.11.2006 № КА-А40/11424-06 позволяет сделать вывод о том, что в целях обеспечения прав и свобод чело века и гражданина согласно п. 8 ст. 86 ТК РФ работодатель и его представители при обработке персональных данных работника обязаны ознакомить работники под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях м этой области. Отсутствие письменных доказательств ознакомления являете! нарушением упомянутого правила и влечет наступление ответственности по ст. 5.27 КоАП РФ. Причем проверить выполнение порядка ознакомления трудовая инспекция вправе и по бывшим работникам, уволившимся к моменту проведения проверки.
При этом суд указал, что у организации была реальная возможность для соблюдения правил и норм трудового законодательства, но оно свою обязанность не выполнило без наличия уважительных причин. В результате Постановлением Государственной инспекции труда по г. Москве на основании протокола об административном правонарушении Общество было привлечено к административной ответственности за совершение правонарушения, предусмотренного ч. 1 ст. 5.27 КоАП РФ, выразившееся в нарушении п. 8 ст. 86 ТК РФ, поскольку работник Общества Г. не был ознакомлен под подпись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. Суд оставил это наказание без изменений.
В Постановлении ФАС Московского округа от 1 ноября 2006 г. № КА-А40/10787-06: суд указал, что отсутствуют основания для признания аналогичного правонарушения малозначительным.
Постановлением Государственной инспекции труда по г. Москве на основании протокола об административном правонарушении Общество было привлечено к административной ответственности за совершение правонарушения, предусмотренного ч. 1 ст. 5.27 КоАП РФ, выразившееся в нарушении ст. ст. 86 - 88 ТК РФ, а именно в неиздании локального нормативного акта, которым устанавливается порядок обработки персональных данных

работников, а также их права и обязанности в этой области. На Общество был наложен штраф в размере 30 тыс. руб.
Как указано в кассационной жалобе, по мнению Общества, нарушение является малозначительным, а назначенное наказание - чрезмерно суровым, в связи с чем Обществом был поставлен вопрос об отмене судебных актов, состоявшихся по делу. Судом в удовлетворении кассационной жалобы было отказано.
В Решении Арбитражного суда г. Москвы (первая инстанция) от 01.06.2006, 25.05.2006 по делу № А40-32068/06-96-156 суд также не согласился с доводом заявителя о том, что отсутствие предусмотренного ст. ст. 86, 87 ТК РФ локального акта, устанавливающего порядок хранения и использования персональных данных работников работодателем, является малозначительным административным правонарушением, т.к. отсутствие у заявителя указанного акта длительное время является нарушением прав и свобод работников.
В Постановлении Девятого арбитражного апелляционного суда от 07.06.2006, 14.06.2006 № 09АП-4259/2006-АК по делу № А40-8448/06-119-84 судьи отметили, что работодатель должен создать технические условия охраны персональных данных работников от их неправомерного использования, в частности, обеспечить особый режим доступа в помещение, где хранится соответствующая информация, оборудовать места ее хранения, исключающие несанкционированный доступ к информации и т.п.
Приведем также перечень органов, которые могут проводить проверки и предметы проверок:
1. Роскомнадзор:
- по обращению субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки;
- проверка сведений, содержащихся в уведомлении об обработке персональных данных;
- внеплановые проверки по контролю нарушений обязательных требований.
2. ФСТЭК России:
- надзор за деятельностью лицензиата ФСТЭК России;
- по обращению Роскомнадзора;
- внеплановые проверки по контролю нарушений обязательных требований.
3. ФСБ России:
- контроль за соблюдением правил пользования средств криптографической защиты информации;
- надзор за деятельностью лицензиата ФСБ России;
- внеплановые проверки по контролю нарушений обязательных требований;
- по обращению Роскомнадзора.

Персональные данные и информационные системы

Согласно ст. 1 Федерального закона «О персональных данных» настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру

действий (операций), совершаемых с персональными данными с использованием средств автоматизации.
Такое внимание к вопросам автоматизации обработки персональных данных влечет за собой необходимость выполнения специальных норм законодательства, касающихся использования информационных технологий. При этом необходимо внимательное изучение нормативной правовой базы, которая в настоящее время может толковаться весьма неоднозначно, особенно в части предъявления требований к информационным системам.

Понятие «информационная система» в действующем законодательстве

Согласно статье Федерального закона «Об информации, информационных технологиях и защите информации» информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Исходя из этого определения, можно сделать вывод о том, что не может существовать информационных систем без использования компьютерной техники и соответствующего программного обеспечения.
Однако ст. 3 Федерального закона «О персональных данных» информационная система персональных данных содержит более широкое определение информационной системы - совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
Разберем детально составляющие этого определения, определения которых можно обнаружить в Федеральном законе «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006, других законах и в нормативных актах Правительства РФ.
Под базой данных понимается совокупность организованных взаимосвязанных данных на машиночитаемых носителях (Временное положение о государственном учете и регистрации баз и банков данных, утверждено Постановлением Правительства РФ от 28 февраля 1996 г. № 226). В этом же Временном положении дано еще и определение банка данных - под ним понимается совокупность баз данных, а также программные, языковые и другие средства, предназначенные для централизованного накопления данных и их использование с помощью электронных вычислительных машин.
Однако в IV части Гражданского кодекса РФ (абзац второй пункта 2 статьи 1260) дано более развернутое определение базы данных. Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).
Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ п. 27.07.2006).
Под **техническими средствами,** позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и

телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах (Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено Постановлением Правительства РФ от 17.11.2007 № 781).

Таким образом, в состав технических средств входят и копировальные устройства, и программное обеспечение, однако ключевым в определении информационной системы персональных данных является понятие «базы данных», т которого следует, что обработка базы данных осуществляется с помощью компьютера (носители должны быть машиночитаемы). Если же обработка ведется без использования компьютера и базы данных (машиночитаемых носителей), то формально отсутствует информационная система. Кроме того, без технических средств, позволяющих осуществлять обработку персональных данных, баш данных также не может быть признана информационной системой.

Средства автоматизации

Итак, информационная система означает обязательное использование для обработки компьютерной техники с соответствующим программным обеспечением. Однако программное обеспечение может быть различным и, в зависимости от его обеспечиваемых им функций, обработка персональных данных может осуществляться с использованием средств автоматизации или без использования таких средств.

Существует точка зрения, согласно которой под использованием средств автоматизации подразумевается любая компьютерная обработка или обработка с помощью электронных устройств. Если хранится база данных на компьютере (например, в электронной таблице или бухгалтерской программе), или, например, в записной книжке сотового телефона, то это уже является автоматизированной обработкой персональных данных и подлежит уведомлению Роскомнадзора. Такие специалисты полагают, что обработка без использования средств автоматизации может вестись лишь на бумаге (в журналах, заполняемых от руки, в рукописных списках).

Мы полагаем, что данные точка зрения ошибочна и не соответствует действующей в России нормативной правовой базе.

Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера (ЕТ8 № 108, Заключена в г. Страсбурге 28.01.1981) определяет, что «автоматизированная обработка» включает в себя следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение.

Конвенция вступила в силу 01.10.1985. Россия подписала Конвенцию 07.11.2001 (Распоряжение Президента РФ от 10.07.2001 № 366-рп) и ратифицировала ее с рядом заявлений Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

С международными нормами права вполне соотносится и российское законодательство. В соответствии с ч. 3 ст. 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 Российской Федерации с учетом 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. Согласно п. 1. указанного Положения обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной 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 согласно п. 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 нее.

Таким образом, можно констатировать, что с точки зрения определений, данных в действующем законодательстве, подавляющее большинство информационных систем, используемых образовательными учреждениями, формально можно рассматривать как осуществляемые без использования средств автоматизации (включая АРМ «Директор», и значительную часть бухгалтерского программного обеспечения). Ведь все лицевые карточки в этих системах правятся в соответствующих окнах вручную человеком. Для уничтожения лицевых карточек также необходимо их выделение в списке оператором и нажатие специальной клавиши 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 из 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.) является неотъемлемой частью таких программ.

Если же передача данных в другие программы (в т.ч. для целей налогового учета) 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.

В этой связи рекомендации Рособразования, изложенные в письме от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных», имеют довольно ограниченное применение на практике. В целях автоматизации обработки персональных данных в анкетах Рособразованием рекомендуется дополнительно указывать внутренний идентификационный номер (личный код) субъекта персональных данных, присваиваемый на весь период обучения или работы. Это позволит обезличить базы данных, если в них не содержатся иные персональные данные, и существенно сократить затраты на защиту информации.

Однако для автоматизации управленческой деятельности в образовательном учреждении необходимы как минимум фамилии, имена, отчества сотрудников, обучающихся, студентов, а также ряд их других персональных данных. Обращение же к личным кодам,

содержащимся на листочках (анкетах) при остальной обработке данных с помощью компьютерного программного обеспечения будет выглядеть, как минимум странно, снижая эффективность внедрения современных информационных технологий. При этом, в зависимости от формы используемых анкет, их можно даже будет признать частью информационной системы (как являющихся составной частью базы данных), что полностью лишит смысла такую дополнительную кодировку (такая кодировка требуется в случае целесообразности обезличивания данных, например, для проведения статистических исследований).

Порядок обработки персональных данных, осуществляемой без использования средств автоматизации

Итак, как было рассмотрено выше, несмотря на компьютеризированную обработку, в большинстве случаев обработка персональных данных в образовательных учреждениях осуществляется без использования средств автоматизации (неавтоматизированно).

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы считается осуществленной 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.

Обработка персональных данных без использования средств автоматизации регламентируется Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 №687.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными актами образовательного учреждения.

Содержание Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации свидетельствует, что оно ориентировано прежде всего на обработку персональных данных без использования компьютера, хотя из п. 1 и п. 2 явно следует, что возможна и неавтоматизированная обработка персональных данных с использованием программного обеспечения.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Поэтому обработка персональных данных, осуществляемая без использования средств

автоматизации, должна осуществляться таким образом, чтобы для каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер устанавливается образовательным учреждением в соответствии с требованиями, предъявляемыми нормативными правовыми актами по защите персональных данных.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

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

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.

Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства РФ от 17 ноября 2007 г. № 781 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,. Причем, как следует из п. 1 названного положения, в нем по термином «информационные системы» понимаются только информационные системы, позволяющие осуществлять обработку персональных данных с использованием средств автоматизации.

Таким образом, на информационные системы, в которых обработка персональных данных осуществляется без использования средств автоматизации, требования Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных не распространяются.

Если же в образовательном учреждении производится автоматизированная обработка персональных данных, то необходимо выполнять следующие дополнительные требования.

Согласно названному положению безопасность персональных данных достигается:

- путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных;
- путем исключения иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей:

- организационные меры;
- средства защиты информации;
- информационные технологии.

Средства защиты информации включают в себя:

- шифровальные (криптографические) средства,
- средства предотвращения несанкционированного доступа,
- средства предотвращения утечки информации по техническим каналам,
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных.

Для обеспечения безопасности персональных данных при их обработке и информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. При этом содержание электронного журнала обращений должно периодически проверяться соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления и устранения причин нарушений.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. При этом методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю (ФСТЭК) и Федеральной службой безопасности РФ (ФСБ) в пределах их полномочий.

Безопасность персональных данных при их обработке в информационной системе

обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом. Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

При этом информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности РФ и Министерством информационных технологий и связи РФ. Такой порядок был установлен совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Кроме того, установлены также требования помещениям и их охране. Согласно п. 8 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Для этого образовательное учреждение (орган управления образованием, информационно-аналитический центр, централизованная бухгалтерия и т.п.) должны устанавливать дополнительную сигнализацию в указанные помещения, в дверные проемы устанавливаются дополнительные замки либо металлические двери.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с

эксплуатационной и технической документацией;
д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией
и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижении уровня защищенности персональных данных, разработку и принятие мер но предотвращению возможных опасных последствий подобных нарушений;
к) описание системы защиты персональных данных.
Лица, которые имеют доступ к информационным базам с персональными данными, подписывают обязательства о неразглашении конфиденциальных сведений (такое обязательство может быть включено и в трудовой договор. Только после этого образовательное учреждение допускает их к обработке персональных данных.
При обработке персональных данных в информационной системе образовательным учреждением должно быть обеспечено:
а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, имеющим права доступа к такой информации;
б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного ДОС тупа к ним;
д) постоянный контроль за обеспечением уровня защищенности персональных данных.
Для разработки и осуществления мероприятий по обеспечению безопасно ста персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.
Следует также обратить особое внимание на то, что согласно п. 17 Положения об обеспечении безопасности персональных данных при их обработке информационных системах персональных данных реализация требований (и обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.
Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.
Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию. В отношении

действующих информационных систем, обрабатывающих персональные данные, согласно ст. 25 Федерального закона «О персональных данных» операторы обязаны привести в соответствие с требованиями этого закона до 01.01.2010. В том числе необходимо провести их классификацию с оформлением соответствующего акта, реализовать комплекс мер по защите персональных данных, провести оценку соответствия информационной системы персональных данных требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия. В некоторых случаях необходимо также получение учреждением лицензии на организацию технической защиты информации.

В результате необходимо организовать и поддерживать систему защиты конфиденциальной информации от несанкционированного доступа в соответствии с установленным классом информационной системы, с использованием средств защиты, сертифицированных в установленном порядке. При этом система защиты персональных данных должна строиться на основе сертифицированных ФСТЭК России и ФСБ России средствах защиты (технических, программных, программно-аппаратных и криптографических).

Однако подчеркнем еще раз, что все эти требования проведения сертификации (аттестации), декларирования соответствия касаются лишь информационных систем, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации.

Классификация информационных систем персональных данных

Классификация информационных систем персональных данных, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации, осуществляется образовательным учреждением - оператором в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 в зависимости от категории обрабатываемых данных и их количества.

Установлены следующие 4 категории персональных данных:

Категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

Категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

Категория 4 - обезличенные и (или) общедоступные персональные данные.

В любом вузе на общедоступных стендах можно встретить различные списки студентов, включающих в себя сочетание ФИО студента, курс, группа, которые позволяют однозначно определить студента. В результате такая комбинация персональных данных заставляет отнести их к персональным данным третьей категории. В результате на размещение этих данных в общедоступном месте формате требуется согласие студента.

Личная карточка работника (Форма Т-2), личное дело учащегося - относятся к категории 2, так как это персональные данные, не только позволяющие идентифицировать субъекта персональных данных, но и получить I нем дополнительную информацию.

Информационные системы персональных данных подразделяются на типовые и

специальные. К типовым системам относятся системы, в которых требуется обеспечить только конфиденциальность персональных данных. Вес остальные системы относятся к специальным.

К специальным информационным системам также должны быть отнесены:

- **информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;**
- **информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных, решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.**

Таким образом, если в образовательном учреждении осуществляется автоматизированная обработка данных о здоровье, то такие информационные системы относятся к специальным. На основе приведенной классификации можно констатировать, что любые медицинские данные, а также кадровый учет, содержащий графу «национальность» (а таковы почти все действующие анкеты и медицинские листки по учету кадров, используемые в настоящее время), необходимо № носить к первой категории.

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих 4 классов:

- **класс 1 (К1) - информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;**
- **класс 2 (К2) - информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;**
- **класс 3 (КЗ) - информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;**
- **класс 4 (К4) - информационные системы, для которых нарушения приводят к негативным последствиям для субъектов персональных данных.**

Однако в нормативных документах не расшифровывается, что относится к просто негативным последствиям для субъекта персональных данных, а что к значительным негативным или незначительным, поэтому классификация по сути своей является довольно бессмысленной, хотя и приводящей к проблемам вследствие установления требований информационным системам в зависимости от ее класса.

Класс типовой информационной системы определяется в соответствии с таблицей, приведенной в Порядке проведения классификации информационных систем персональных данных (выделен столбец, касающийся образовательных учреждений). *

егории персональ-данных	информационной системе одновременно обрабатываются персональные данные		
	ее чем 1000 ектов персо-ных данных персональные ые субъектов ональных ых в пределах	1000 до 100 000 ектов ональных данных персональные ые субъектов ональных данных, тающих в отрасли	е чем 100 000 ектов персо-ных данных персональные ые субъектов ональных ых в преде-
егория 4 Категория			

егория 2			
егория 1			

Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных по результатам анализа исходных данных в соответствии с методическими документами ФСТЭК России.

Для определения класса специальной информационной системы образовательному учреждению необходимо обратиться в ФСТЭК России для получения следующих документов ДСП:

- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;
- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Таким образом, интегрированные информационные системы, осуществляющие автоматизированную обработку данных, как правило, подпадают классы К1 и К2, либо к специальным системам (при наличии данных о здоровье учащихся, студентов) и требуют больших затрат на защиту персональных данных. При наличии таких систем в образовательных учреждениях (органам управления образованием) целесообразно сегментировать сложную систему ни несколько отдельных, не связанных друг с другом систем, различных по целям и регламентам обработки персональных данных, приводя тем самым к у прошению требований по защите персональных данных.

Для распределенной базы информационной системы обработки персональных данных при необходимости обеспечения конфиденциальности потребуется защита передаваемых и хранимых персональных данных, что соответствует действующим требованиям ФСБ России к автоматизированным информационным системам, предназначенным для защиты конфиденциальной информации, не составляющей государственной тайны. В таких случаях должна осуществляться защита всей конфиденциальной информации, передаваемой по каналам связи; информация, передаваемая по каналам связи, должна быть зашифрована с использованием средств криптографической защиты информации (СКЗИ), или для ее передачи должны использоваться защищенные каналы связи.

Кроме того, должна осуществляться защита информации, записываемой ив отчуждаемые носители последнее требование касается изолированных информационных систем, не имеющих каналов для передачи персональных данных, т.е. для отдельных рабочих мест, обрабатывающих персональные данные.

Таким образом, для обработки персональных данных информационные системы должны быть аттестованы по классу не ниже АК2 в классификации ФСБ России. Например, такому классу соответствует защищенная WINDOWS XP с пакетом обновления Secure Раск Rus. В состав средств защиты должны входить средства криптографической защиты информации (СКЗИ) класса не ниже КС2. Исходя из этого для любой информационной системы, обрабатывающей персональные данные категорий выше 4-й, потребуется выполнение всех требований класса АК2 в классификации ФСБ России.

Из архитектуры информационной системы при достаточно большом количестве обрабатываемых персональных данных (показатель 1 или 2) однозначно будет выделяться серверная компонента, для которой также потребуется защита. В этом случае должна осуществляться защита всей конфиденциальной информации, хранимой на магнитных носителях рабочих станций и серверов, что соответствует требованиям класса АКЗ.

Поэтому разработчикам информационных систем необходимо использовать средства, специально адаптированные для защиты персональных данных и имеющие необходимые разрешительные документы. К таким относятся, в частности, средства криптографической защиты семейства Сгур1оРго.

Руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144 были также утверждены Методические рекомендации но обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Названными Методическими рекомендациями необходимо руководствоваться в случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств (за исключением случая, когда оператором является физическое лицо, использующее персональные данные исключительно для личных и семейных нужд), а также при обеспечении безопасности персональных данных при обработке в информационных системах, отнесенных к компетенции ФСБ России. В частности, Методическими рекомендациями необходимо руководствоваться в следующих случаях:

- при обеспечении с использованием криптосредств безопасности персональных данных при их обработке в государственных информационных системах персональных данных (часть 5 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);
- при использовании криптосредств для обеспечения персональных данных в случаях, предусмотренных п. 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

Настоящие Методические рекомендации не распространяются на информационные системы персональных данных, в которых:

- персональные данные обрабатываются без использования средств автоматизации;
- обрабатываются персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну;
- технические средства частично или целиком находятся за пределами Российской Федерации.

Таким образом, ФСБ России также четко разграничивает информационные системы на осуществляющие обработку с использованием и без использования средств автоматизации.

Согласно методическим рекомендациям различают шесть уровней КС1, КС2, КСЗ, КВ1, КВ2, КА1 криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, и, соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КСЗ, КВ1, КВ2, К А1. При этом:

- встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

- встраивание криптосредств класса КС3, КВ1, КВ2 и КА1 осуществляется только под контролем со стороны ФСБ России.
- встраивание криптосредств класса КС1, КС2 или КС3 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России.
- встраивание криптосредства класса КВ1, КВ2 или КА1 осуществляется организацией, имеющей соответствующую лицензию ФСБ России.

Практически выполнить все многочисленные требования ФСТЭК образовательному учреждению маловероятно, так как методические документы ФСТЭК позволяют весьма разнообразные и широкие толкования угроз и мере приятии по защите персональных данных.

Угрозой безопасности персональных данных называется не только их утечка, но и иные несанкционированные или непреднамеренные воздействия ни информацию. В результате под понятие данное ФСТЭК подпадает достаточно широкий спектр угроз. Среди каналов реализации угроз ФСТЭК упоминает про электромагнитные излучения и наводки, а также акустику.

Среди всех угроз (потенциальных) надо еще выявить актуальные. Актуальной считается угроза, которую можно реализовать и которая опасна для персональных данных.

Согласно Методике угрозы являются актуальными, за исключением угроз I

- с низкой опасностью и низкой и средней возможностью реализации;
- со средней опасностью и низкой возможностью реализации.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности информационной системы персональных данных и частота (вероятность) реализации рассматриваемой угрозы. Иол уровнем исходной защищенности информационной системы персональных данных понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, перечисленных в методике (в том числе, территориальная распределенность информационной системы персональных данных, наличие подключения к Интернет, наличие встроенных механизмом регистрации событий, уровень обезличивания персональных данных и др.)

После определения для каждой угрозы вероятности ее реализации и исходного уровня защищенности вычисляется коэффициент реализуемости угрозы по приведенной в Методике формуле.

Опасность угрозы оценивается экспертным путем специалистами по замш те информации данной информационной системы персональных данных.

Декларирование, сертификация (аттестация) и лицензирование деятельности по защите персональных данных

В перечисленных выше методических документах ФСТЭК устанавливается следующий порядок оценки соответствия степени защищенности информационных систем требованиям безопасности:

- для информационных систем 1 и 2 класса соответствие степени защищенности требованиям безопасности устанавливается путем обязательной сертификации (аттестации);
- для информационных систем 3 класса соответствие требованиям безопасности подтверждается путем сертификации (аттестации) или (по выбору оператора) декларированием соответствия, проводимым оператором персональных данных;
- для информационных систем 4 класса оценка соответствия не регламентируется и осуществляется по решению оператора персональных данных.

Декларирование соответствия - это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством РФ, руководящими и нормативно-методическими документами ФСТЭК и ФСБ.

Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

Специализированным организациям, имеющим соответствующие лицензии, могут быть поручены:

- методическая поддержка и консультирование при проведении сегментирования интегрированных информационных систем, определении состава и классификации информационных систем, обрабатывающих персональные данные;
- консультирование и помощь в формировании перечня организационно-технических мероприятий, необходимых для создания системы защиты информационных систем, обрабатывающих персональные данные;
- консультирование при подготовке декларации соответствия для систем класса К3;
- аудит информационных систем персональных данных, подбор и установка необходимых технических средств защиты информации для систем классов К2 и К1, а также распределенных информационных систем класса К3;
- подготовка, проведение аттестационных испытаний информационных систем классов К2 и К1 с выдачей Аттестата соответствия.

Перечень органов (организаций) по аттестации системы сертификации средств защиты информации по требованиям безопасности информации, в которые могут обращаться образовательные учреждения и органы управления образованием, не имеющие необходимых специалистов и лицензий, а также Государственный реестр сертифицированных средств защиты информации размещены на сайте ФСТЭК России. Однако стоимость проведения таких процедур достаточно велика и измеряется сотнями тысяч рублей.

В случае проведения декларирования на основе собственных доказательств оператор самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3.

Независимо от используемой формы подтверждения соответствия оператор может также предоставить протоколы испытаний, проведенных в исследовательской лаборатории.

Декларация о соответствии оформляется на русском языке и должна содержать:

- наименование и местонахождение заказчика;
- информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект, класс информационной системы персональных данных;
- наименование документов, на соответствие требованиям которых подтверждается информационной системы персональных данных;
- указание на схему декларирования соответствия;
- заявление заказчика о принятии им мер по обеспечению соответствия продукции необходимым требованиям;
- сведения о документах, послуживших основанием для подтверждения соответствия продукции требованиям;
- срок действия декларации о соответствии.

Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны имеют одинаковую юридическую силу. Они имеют действие, аналогичное действию сертификата (аттестата) соответствия.

Аттестационные (сертификационные) испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России. При этом под аттестацией понимают комплекс мер, позволяющих привести информационную систему в соответствие с требованиями по безопасности информации к заявленному классу, изложенными в нормативно-методических документах ФСТЭК России.

Аттестационные (сертификационные) испытания содержат в себе анализ уже имеющихся на объекте информационных систем персональных данных, а также вновь принятых решений по обеспечению безопасности информации и включают проверку:

- организационно-режимных мероприятий по обеспечению защиты информации;
- защищенности информации от утечек по техническим каналам;
- защищенности информации от несанкционированного доступа.

По результатам аттестационных испытаний принимается решение о выдаче Аттестата соответствия информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

В методических документах ФСТЭК установлены также дополнительные требования по наличию лицензий на ведение деятельности по защите персональных данных. Без наличия соответствующих лицензий проведение мероприятий по защите персональных данных возможно только для информационных систем класса К3, а также для информационных систем класса К4.

Для проведения мероприятий по обеспечению безопасности персональных данных для специальных информационных систем, систем 1 и 2 класса и распределенных (в том числе подключенных к Интернет) систем 3 класса операторы обязаны в установленном порядке получить лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

- наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
- наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;
- наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
- использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки

соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

- использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;
- наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю.

Для применения криптографических средств защиты персональных данных (в том числе для изготовления ключей или сертификатов), в зависимости от планируемых действий, также требуются различные лицензии ФСБ России, регламентирующие работы в области криптографической защиты информации.

В тоже время законность требований проведения процедур декларирования, сертификации (аттестации) и лицензирования образовательными учреждениями на основании методических документов ФСТЭК вызывает большие сомнения.

Во-первых, документами ДСП, не опубликованными в установленном порядке не могут быть установлены обязанности для организаций, тем более, влекущие за собой значительные финансовые затраты, держащих сведения, составляющие государственную тайну, или сведения конфиденциального характера.

Акт, признанный Министерством юстиции Российской Федерации не нуждающимся в государственной регистрации, подлежит опубликованию в порядке, определяемом федеральным органом исполнительной власти, утвердившим акт. При этом порядок вступления данного акта в силу также определяется федеральным органом исполнительной власти, издавшим акт.

Поэтому, полагаем, что образовательные учреждения и органы управления образованием, осуществляющие автоматизированную обработку персональных данных, в случае предъявления требований о получении лицензий, проведении декларирования или сертификации (аттестации) могут обжаловать такие требования в судебном порядке (особенно, если используемые средства защиты персональных данных уже были сертифицированы их производителем).

Отметим, что риски в случае несогласия суда с такой позицией весьма невелики, по сравнению с затратами на лицензирование и сертификацию. Статья 13.11 КоАП РФ устанавливает за нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных на должностных лиц - от 500 до 1000 руб.; на юридических лиц - от 5000 до 10 000 руб.

В самом худшем случае, если будет судом признано, что получение лицензии на деятельность по технической защите конфиденциальной информации, является обязательным для образовательного учреждения, имеющего информационную систему персональных данных определенных классов, является обязательным, учреждением может быть привлечено к административной ответственности за осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии) согласно ст. 19.20 КоАП РФ.

Осуществление деятельности, не связанной с извлечением прибыли, без специальной лицензии, если такая лицензия обязательна, влечет наложение административного на должностных лиц в размере от одной тысячи до двух тысяч рублей, а на юридических лиц - от десяти тысяч до двадцати тысяч рублей.