**С. В. Вихорев**

**О защите**

**персональных данных**

**(для школьных работников)**

**Москва, 2014 г.**

ОГЛАВЛЕНИЕ

[От Автора 4](#_Toc378252689)

[Глава I. Общеобразовательная 5](#_Toc378252690)

[О чем пойдет речь 5](#_Toc378252691)

[*Что такое персональные данные?* 5](#_Toc378252692)

[Признаки отнесения информации к персональным данным 5](#_Toc378252693)

[Идентификационные персональные данные 6](#_Toc378252694)

[Биометрические персональные данные 7](#_Toc378252695)

[Специальные категории персональных данных 8](#_Toc378252696)

[Общедоступные персональные данные 8](#_Toc378252697)

[*Что такое защита персональных данных?* 9](#_Toc378252698)

[Три кита защиты информации 9](#_Toc378252699)

[Система защиты персональных данных 10](#_Toc378252700)

[*Что такое «оператор персональных данных»?* 11](#_Toc378252701)

[*О роли согласия* 12](#_Toc378252702)

[Что такое согласие субъекта? 12](#_Toc378252703)

[Конклюдентное действие, как вид согласия 12](#_Toc378252704)

[Некоторые исключения. 13](#_Toc378252705)

[*От общего к частному.* 13](#_Toc378252706)

[Где и какие персональные данные есть в школе? 13](#_Toc378252707)

[Особенности получения согласия от несовершеннолетних 15](#_Toc378252708)

[Кто есть кто 15](#_Toc378252709)

[Защита персональных данных – это важно! 16](#_Toc378252710)

[*Зачем надо защищать персональные данные?* 16](#_Toc378252711)

[*Почему надо защищать персональные данные?* 17](#_Toc378252712)

[*От кого надо защищать персональные данные?* 18](#_Toc378252713)

[Что такое угрозы безопасности персональным данным? 18](#_Toc378252714)

[Что такое модель угроз и зачем она нужна? 19](#_Toc378252715)

[*Кто регулирует отношения?* 19](#_Toc378252716)

[Глава II. Специальная 21](#_Toc378252717)

[С чего начать защиту данных? 21](#_Toc378252718)

[*Ревизия информационных ресурсов* 21](#_Toc378252719)

[Проводим инвентаризацию ресурсов 22](#_Toc378252720)

[Способ обработки: автоматизированный или неавтоматизированный? 23](#_Toc378252721)

[Определяем тип информационных систем 24](#_Toc378252722)

[Формируем перечень обрабатываемых персональных данных 25](#_Toc378252723)

[*Определяем уровень защищенности персональных данных* 25](#_Toc378252724)

[Типы угроз безопасности персональным данным. 26](#_Toc378252725)

[Что такое недекларированные возможности программного обеспечения? 27](#_Toc378252726)

[Как оценить вред субъекту? 28](#_Toc378252727)

[Пример выбора требуемого уровня защищенности персональных данных. 29](#_Toc378252728)

[Меры и средства защиты 31](#_Toc378252729)

[*Выбираем меры по защите персональных данных* 31](#_Toc378252730)

[Классификация мер защиты персональных данных. 31](#_Toc378252731)

[Общий порядок действий по выбору мер защиты информации. 33](#_Toc378252732)

[Определение базового набора мер защиты информации. 34](#_Toc378252733)

[Адаптация базового набора мер. 34](#_Toc378252734)

[Уточнение адаптированного набора мер. 35](#_Toc378252735)

[Дополнение уточненного адаптированного набора мер. 35](#_Toc378252736)

[*Выбираем средства защиты информации.* 36](#_Toc378252737)

[Что должно получиться? 36](#_Toc378252738)

[*Организационная составляющая.* 37](#_Toc378252739)

[Состав основных организационно-распорядительных документов. 37](#_Toc378252740)

[Регламент обеспечения безопасности информации. 38](#_Toc378252741)

[Рекомендации по разработке организационно-распорядительных документов. 38](#_Toc378252742)

[*Техническая составляющая* 39](#_Toc378252743)

[На что надо обратить внимание. 40](#_Toc378252744)

[*Как и зачем оптимизировать обработку персональных данных?* 40](#_Toc378252745)

[Исключение из обработки лишних персональных данных. 40](#_Toc378252746)

[Сегментирование информационной системы. 41](#_Toc378252747)

[Обезличивание персональных данных. 42](#_Toc378252748)

[*О личных компьютерах учителей.* 43](#_Toc378252749)

[*Аутсорсинг обработки персональных данных* 44](#_Toc378252750)

[Приложения. 45](#_Toc378252751)

[*Приложение 1.* Основные нормативные правовые акты, по обеспечению безопасности персональных данных в школе 46](#_Toc378252752)

[Перечень основных нормативных правовых актов 46](#_Toc378252753)

[Краткий анализ Федерального закона № 152-ФЗ «О персональных данных» 47](#_Toc378252754)

[*Приложение 2.* Примерный перечень документов (ресурсов) обрабатываемых в школе, где могут находиться персональные данные 49](#_Toc378252755)

[Документы, в которых могут находится персональные данные постоянного состава школы (персонал): 49](#_Toc378252756)

[Документы, в которых могут находится персональные данные переменного состава школы (учащихся): 50](#_Toc378252757)

[Документы, в которых могут находится персональные данные субъектов, не относящихся к школе: 51](#_Toc378252758)

[*Приложение 3.* Статус организаций по отношению к персональным данным, обрабатываемым в школе 52](#_Toc378252759)

[*Приложение 4.* Примерные алгоритмы действий 53](#_Toc378252760)

[Алгоритм действий по проведению инвентаризации информационных ресурсов школы 53](#_Toc378252761)

[Алгоритм действий по определению уровня защищенности персональных данных и выбору мер их защиты. 54](#_Toc378252762)

[*Приложение 5.* Таблица выбора уровней защищенности персональных данных по Постановлению Правительства РФ № 1119 от 01.11.2012 г. 55](#_Toc378252763)

[*Приложение 6.* Состав общих мероприятий по защите персональных данных, которые должен выполнить оператор 56](#_Toc378252764)

[*Приложение 7.* Соотношение классов средств защиты информации с уровнями защищенности персональных данных 57](#_Toc378252765)

[*Приложение 8.* Состав и содержание базового набора мер, необходимых для обеспечения 3 уровня защищенности персональных данных и типы средств защиты, реализующих технические меры защиты 58](#_Toc378252766)

[*Приложение 9.* Примерный рекомендуемый перечень документов, которые необходимы для обеспечения защиты персональных данных 60](#_Toc378252767)

[Локальные нормативные акты 60](#_Toc378252768)

[Должностные обязанности (в части обеспечения безопасности персональных данных): 60](#_Toc378252769)

[Инструкции (в части обеспечения безопасности персональных данных) о порядке и правилах: 60](#_Toc378252770)

[Документы, необходимые для реализации технической защиты 60](#_Toc378252771)

# От Автора

Уважаемые, дорогие Учителя! Знаю, знаю я, что Вы очень-очень заняты. Но мы живем в век бурного развития информационных технологий и уже активно в нашу жизнь входят разные «гаджеты». С одной стороны это облегчает общение и повышает коммуникативность, а с другой – увеличивают те риски, о которых раньше мы и не подозревали. Я говорю об информации, вернее о тех проблемах, которые возникают при ее обработке и которые могут причинить вред. Информация всегда играла важную роль в жизни человеческого общества, являясь основой его духовного развития, и любая социальная деятельность связана с процессом сбора и обработки информации. Информация, представляя собой накопленные человечеством знания, является гуманитарной ценностью, которая служит формированию культуры и нравственности, образованию и воспитанию подрастающих поколений. Но многие ли задумываются при этом о том, на сколько безопасно использовать эти современные средства для передачи информации и можно ли им доверять свои тайны.

Живя в эпоху откровений Сноудена и бурного обсуждения проблем «электронного» беспардонного влезания в частную жизнь, в полный рост встает проблема защиты информации. Это та сфера, которая затрагивает практически каждого человека на каждом шагу. Но раскрыть все нюансы этой глобальной проблемы в этой книге не получится – слишком мало места и слишком мало времени, да и задача у нас иная. Поэтому остановимся только на одном, но довольно важном аспекте: защите персональных данных. Здесь Вы найдете и некоторые рекомендации как защищать персональные данные в школах, которые могут быть Вам полезны в практической деятельности.

Задача автора не рассказывать об ужасах, связанных с неправильной защитой персональных данных, а показать и убедить Вас в важности этой проблемы и необходимости совершения определенных действий. Я прекрасно понимаю, то что ясно и понятно специалисту, вызывает определенные трудности для тех, кто с этим не связан. Защита информации – сфера хитрая, здесь образовался конгломерат из технических и юридических знаний (и чего больше – трудно сказать) и, подчас, даже специалистам трудно найти общий язык. Все это так, но защищать персональные данные надо. В том числе и Вам, учителям. Поэтому, попробую вести простой разговор, стараясь объяснить трудные моменты.

Я надеюсь, что эта книга будет полезна не только тем, кому будет поручена задача защиты персональных данных в школе, но и просто неравнодушным учителям, которые любят и уважают своих подопечных и заботятся об их благополучии.

# Глава I. Общеобразовательная

*Самая высокая степень человеческой мудрости - это умение приспособиться к обстоятельствам и сохранять спокойствие вопреки внешним грозам.*

*Даниель Дефо*

Проблема защиты персональных данных – это, наверное самая «вопросоемкая» сфера обеспечения безопасности информации на сегодня. С одной стороны это еще очень и очень молодая область деятельности – еще и десяти лет не насчитывает. А требования закона по защите персональных данных – жесткие. Но, для того чтобы говорить на одном языке надо вначале познакомиться с некоторыми категориями, которые используются в этой предметной области.

## О чем пойдет речь

Уже из названия понятно, что речь пойдет о защите персональных данных. В рассматриваемой предметной области можно выделить две важнейшие категории: персональные данные и защита. Казалось бы, что на бытовом уровне здесь все ясно и понятно, однако, на самом деле мы затрагиваем некоторые юридические аспекты процесса обработки и оборота персональных данных, а в этой области должно быть все четко определено. Итак, без длинных предисловий начнем.

### *Что такое персональные данные?*

Подсчитано, что в законах и подзаконных актах упоминается более 40 видов тайн[[1]](#footnote-1). Но есть группа тайн, которая касается всех и каждого. Неприкосновенность частной жизни – конституционное право каждого гражданина.

#### *Признаки отнесения информации к персональным данным*

Конституция декларирует недопустимость сбора, хранения, использования и распространения информации о частной жизни лица[[2]](#footnote-2). В содержание тайны частной жизни входят конфиденциальные сведения, составляющие личную, семейную тайну лица, тайну переписки, почтовых, телефонных переговоров и иных сообщений, тайну голосования, тайну усыновления, персональные данные. Особое место в этой когорте занимают персональные данные. Это не только фамилия, имя и отчество. Закон гласит: персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[[3]](#footnote-3). Словосочетание «любая информация» ясно указывает на широкое определение этого понятия. На сколько это понятие может быть широким, иллюстрирует такой пример[[4]](#footnote-4): в ходе судебного процесса по вопросу об опеке над девочкой был произведен нейро-психиатрический анализ ее состояния, в ходе которого был представлен ее рисунок, характеризующий ее семью. Рисунок содержал информацию о ее состоянии (состояние здоровья с психиатрической точки зрения) и то, что она думала о поведении отца и матери. Суд признал, что рисунок содержит сведения, которые относятся к персональным данным. Не менее важную смысловую нагрузку в определении несет и слово «относящаяся». И этого следует важный вывод: составить исчерпывающий список сведений, которые составляют персональные данные – невозможно.

На первый взгляд сведения тогда относятся «к лицу», когда они «о лице». Но это не совсем так. К примеру, при приеме на работу учитель заполняет кадровую форму Т-2 в которой указываются сведения о родственниках. И эти персональные данные уже будут «относиться» не только учителю, но также и к его родственникам.

Персональные данные могут быть в любой форме – текстовой, цифровой, графической, видео или акустической. Сюда входит все: и информация, зафиксированная на бумаге, и информация, хранимая в памяти компьютера как в двоичной виде, так и в виде, например, звука и изображения.

Итак, определяющими признаками отнесения той или иной информации к персональным данным являются:

* возможность прямо или косвенно определить на основании этой информации конкретное физическое лицо (субъекта), которому принадлежат эти данные;
* возможность прямо или косвенно отнести эту информацию к уже определённому физическому лицу (субъекту).

Персональные данные – не однородны. Есть несколько особых категорий таких данных. В зависимости от категории накладываются разные ограничения на их обработку, а, следовательно, защищаются такие данные по-разному.

#### *Идентификационные персональные данные*

Для того, чтобы информация попала в разряд персональных данных, должно быть, чтобы либо уже кто-то ранее установил конкретное лицо к которому относится информация, либо по этой информации в данный момент можно установить какое-либо конкретное лицо. Но для этого надо иметь определенного рода информацию, которая, позволяет однозначно идентифицировать это лицо. Такую информацию называют идентификационной информацией. Это важная категория персональных данных, крайне необходимая для установления личности.

У каждого человека с момента его рождения появляются определенные права. И среди этих прав весьма достойное место занимает неотчуждаемое неотъемлемое личное право на имя[[5]](#footnote-5). Именно имя по закону является средством индивидуализации личности и гражданин приобретает и осуществляет свои права и обязанности под своим именем, включающим фамилию и собственно имя и отчество[[6]](#footnote-6). Каждый гражданин имеет паспорт – основной документ, удостоверяющий личность. В Положении о паспорте есть пункт, в котором сказано: «В паспорт вносятся следующие сведения о личности гражданина: фамилия, имя, отчество, пол, дата и место рождения[[7]](#footnote-7)». Но, в жизни все проще. В классном журнале указаны только фамилия и имя учащегося, но этого достаточно учителю, чтобы общаться с ним. Таким образом, можно констатировать:

* фамилия, имя, отчество, пол, дата и место рождения в совокупности являются полными идентификационными персональными данными;
* даже по сокращенному (неполному) набору данных можно идентифицировать субъекта, но с вероятностью ошибки.

#### *Биометрические персональные данные*

Биометрические персональные данные – это физиологические особенности конкретного человека[[8]](#footnote-8). Эти особенности являются объективной реальностью и не зависят ни от субъективных факторов, ни от способа их обработки, ни от целей обработки.

Закон накладывает ограничения при обработке биометрических персональных данных для целей его идентификации (требуется письменное согласие субъекта). В остальных случаях ограничений нет. Если, например, где-то хранится фото, но не используется для идентификации субъекта, оно, не переставая быть биометрическими персональными данными, не требует получения письменного согласия субъекта для обработки.

Можно ли по отпечатку пальца идентифицировать субъекта? Если кто-то нашел на улице предмет с отпечатком пальца, единственное, что можно сказать, что этот предмет держал человек, а не примат. Но кто конкретно держал невозможно сказать до тех пор, пока найденный отпечаток не будет сверен с дактилоскопической базой данных, где имеются идентификационные данные субъекта. То есть в данном случае отпечаток пальца послужил дополнительным идентификатором субъекта, но сам по себе не определил субъекта.

Таким образом:

* биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека;
* биометрические персональные данные объективны, уникальны и присущи именно конкретному субъекту;
* сами по себе биометрические персональные данные не являются идентифицирующими данными, а служат только идентификатором, но и на их основе можно установить личность;
* ограничения в виде необходимости получения письменного согласия субъекта на обработку биометрических данных накладываются только в том случае, если они используются для установления личности.

Из этого, например, следует, что при размещении фотографии школьников или учителей на школьном сайте письменное согласие субъекта требуется только в том случае, если помимо фотографии указана дополнительная информация, позволяющая идентифицировать субъекта. Размещение общих фотографий или фотографий отдельных субъектов с недостаточным для идентификации набором персональных данных (например, только имя или класс учащегося) не требует обязательного согласия субъекта.

#### *Специальные категории персональных данных*

Специальные категории персональных данных – это данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни[[9]](#footnote-9). Эта категория охватывает наиболее чувствительную область частной жизни и, как правило, субъекты проявляют особую заботу о них. На их обработку накладываются самые жесткие ограничения. Так, общая норма закона гласит, что обработка специальных категорий персональных данных, не допускается. Хотя, как и всегда, есть и исключения. Например, субъект дал согласие в письменной форме на обработку специальных категорий персональных данных или добровольно сделал их общедоступными, а также когда законодательством предусмотрена (специально оговорена) необходимость обработки таких данных для целей:

* переписи населения,
* социальной помощи,
* защиты жизни и здоровья,
* усыновления,
* пенсионного обеспечения,
* медико-профилактических целей,
* осуществления правосудия.

Действия с этими данными без должных гарантий обеспечения прав субъекта персональных данных могут нанести ему повышенный ущерб.

#### *Общедоступные персональные данные*

Ещё одна, категория – общедоступные персональные данные. Это такие персональные данные, которые стали общедоступными по воле самого субъекта. И на обработку таких персональных данных никаких ограничений не накладывается и никакого согласия не требуется[[10]](#footnote-10). Правда, прежде чем их обрабатывать, необходимо доказать, что эти персональные данные сделаны общедоступными самим субъектом[[11]](#footnote-11). Эту категорию нельзя путать с понятием, «персональные данные, включённые в общедоступные источники». Это разные понятия. Общедоступные источники (источники, создаваемые в целях информационного обеспечения) формируются кем-то для каких-то целей (например, телефонный справочник) и здесь требуется письменное согласие субъекта[[12]](#footnote-12), а перевод персональных данных в категорию общедоступных (например, публикация на школьном сайте) – это либо право самого субъекта, либо требование закона[[13]](#footnote-13) (например, данные о кандидате в ходе избирательной компании). И при этом никакого согласия не требуется, ни письменного, ни устного.

### *Что такое защита персональных данных?*

В современной литературе по проблемам защиты информации, иногда понятие объект защиты ассоциируется с информационной сетью, системой или отдельным компьютером. Это не верно. И сеть, и система, и отдельный компьютер всего лишь средства обработки информации. Злоумышленник проникает в компьютер не для того, чтобы нарушить его работу, а для того, чтобы завладеть информацией или затруднить возможность ее использования. То есть, главной целью злоумышленника является именно информация. Но, всякая сущность ценна не сама по себе, а потому, что она обладает полезными свойствами, которые и требуют защиты. Каковы же эти свойства?

#### *Три кита защиты информации*

Конфиденциальность. Накладывая ограничения на доступ к персональным данным, субъект защищает свои законные права и интересы. Здесь проявляется первое полезное свойство информации: конфиденциальность – неизвестность информации лицам, не имеющим право доступа к ней. Это свойство, очень специфическое: либо оно есть, либо его нет. Третьего не дано. Если конфиденциальность утрачена (информация стала известна), то это уже навсегда. Восстановлению она не подлежит. Именно поэтому всем операторам, обрабатывающим персональные данные законом вменена обязанность безусловного соблюдения их конфиденциальности[[14]](#footnote-14).

Целостность. Конечно же субъекту важна неискаженная информация. Любые изменения в персональных данных могут затронуть его интересы. Здесь проявилось второе полезное свойство информации: целостность – способность информации не подвергаться изменению. Целостность, в отличие от конфиденциальности, достаточно эластична. В одном случае даже малейшее изменение персональных данных (например, даты рождения) может привести к необратимым последствиям, а в другом – даже утрата некоторой части данных (например дневника) не влияет на интересы субъекта. При обработке персональных данных оператор должен оберегать их от неправомерного или случайного уничтожения или изменения[[15]](#footnote-15).

Доступность. Субъекту важно получать информацию именно тогда, когда она ему нужна, когда возникает необходимость. Здесь проявляется третье полезное свойство информации: доступность – свойство персональных данных быть доступными и использоваться по запросу со стороны субъекта. А оператор должен обеспечить доступность персональных данных (защитить от блокирования)[[16]](#footnote-16).

Эти свойства составляют каноническую триаду безопасности информации:

* конфиденциальность,
* целостность,
* доступность.

Защита персональных данных как раз и нацелена на сохранение трех полезных свойств информации, в значительной степени влияющие на ее ценность.

#### *Система защиты персональных данных*

Оператор обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных[[17]](#footnote-17):

* от неправомерного или случайного доступа к ним,
* от уничтожения,
* от изменения,
* от блокирования,
* от копирования,
* от распространения,

Защита персональных данных это не только «техническая» проблема, заключающаяся в установке средств защиты. Это комплексная задача и решается она созданием целостной системы защиты в равной степени объединяющей:

* набор правил (локальные документы, определяющие порядок защиты),
* «человеческий фактор» (персонал, выполняющий эти правила),
* «активную составляющую» (набор технических мер защиты)
* «пассивную составляющую» (комплекс организационных мероприятий для поддержки исполнения установленных правил и реализации мер защиты).

Вся эта совокупность элементов в той или иной степени задействована в процессе обработки персональных данных и должна быть направлена на ликвидацию угроз безопасности персональным данным и достижение требуемого уровня их защищенности. Надежность любой сложной системы определяется надежностью ее самого слабого элемента. Поэтому при ее создании должна быть обеспечена одинаковая надежность всех ее элементов по отдельности. В результате вокруг персональных данных создается целостная и доверенная среда, исключающая возможность несанкционированных действий с ними (модификации, уничтожения, блокирования, копирования). И, если правила обработки разрабатываются непосредственно оператором и рассчитаны на его персонал («человеческий фактор»), то состав и содержание организационных и технических мер определяются уполномоченными федеральными органами власти (ФСТЭК России, ФСБ России), а оператор имеет право выбрать нужные ему меры.

### *Что такое «оператор персональных данных»?*

Ранее уже встречалось понятие «оператор персональных данных» или просто, «оператор». Оператор – это государственный орган или юридическое лицо самостоятельно или совместно с другими лицами осуществляющие обработку персональных данных[[18]](#footnote-18). То есть, школа (образовательное учреждение) как юридическое лицо, является оператором. В определении содержатся основные полномочия оператора. Это лицо, которое:

* организует и (или) осуществляет обработку персональных данных;
* определяет цели обработки персональных данных;
* определяет состав персональных данных, подлежащих обработке;
* определяет действия, совершаемые с персональными данными.

Самое главное полномочие оператора – это право определять цели обработки персональных данных. Из определения следует также, что оператор вправе поручить обработку персональных данных другому лицу. Это очень полезно.

Но, оператор несет и определенную ответственность. Именно он получает согласие субъекта на обработку персональных данных, в том числе письменное. Каждый субъект вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения, если информация является неполной, устаревшей, неточной, незаконно полученной, а оператор обязан принять необходимые меры. Ну, и наконец, оператор несет всю полноту ответственности, предусмотренную законодательством, если нарушены интересы субъекта.

В плане защиты информации, именно оператор обязан принимать меры, необходимые для обеспечения защиты персональных данных в том числе он[[19]](#footnote-19):

* назначает ответственного за организацию обработки персональных данных;
* издает документы, определяющие политику обработки персональных данных;
* выбирает организационные и технические меры по защите персональных данных;
* знакомит сотрудников, с положениями законодательства и требованиями к защите;
* осуществляет внутренний контроль за обработкой персональных данных;
* оценивает вред, который может быть причинен субъектам неправомочными действиями.

Из смысла понятия «оператор» следует еще одно важное наблюдение. Порядок обработки и защиты персональных данных, установленный законом, не распространяется на тех, кто не является юридическим лицом. Если персональные данные обрабатываются самим субъектом исключительно для личных и семейных нужд и если при этом не нарушаются права других субъектов, то каждый волен поступать как хочет. Можно спокойно использовать смартфон или планшетник, в котором есть адресная книга и ни у кого не спрашивать согласия.

###  *О роли согласия*

Одним из важнейших условий обработки персональных данных является наличие явного согласия субъекта персональных данных на их обработку. Без такого согласия любые действия с персональными данными – незаконны. Каждый из нас постоянно сталкивается в повседневной жизни с тем, что надо свои данные кому-то сообщить, что бы взамен что-то получить или сделать. Заходим в банк, сообщаем свою фамилию, номер счета и получаем доступ к своим денежным средствам, заходим в аптеку, показываем социальную карту и получаем скидку. Но есть и другие, более серьезные поводы сообщать свои персональные данные. И всегда мы должны давать свое согласие.

#### *Что такое согласие субъекта?*

Согласие – это свидетельство того, что субъект принял решение о предоставлении своих персональных данных для обработки в соответствии с целями, которые заявляет оператор. Субъект вправе отозвать свое согласие и тогда необходимо прекратить обработку его персональных данных. Закон определил пять случаев, когда требуется получение согласия в письменной форме:

* если персональные данные будут размещаться в общедоступных источниках,
* если будут обрабатываться специальные категории персональных данных,
* если биометрические персональные данные используются для идентификации,
* если персональные данные передаются заграницу в страну, где нет защиты,
* если будет приниматься значимое решение на основе исключительно автоматизированной обработки персональных данных.

В остальных случаях форма, в которой должно быть получено согласие – не оговаривается. Но в любом случае бремя доказательства наличия согласия субъекта лежит на операторе[[20]](#footnote-20).

#### *Конклюдентное действие, как вид согласия*

Надо отметить, что субъект дает согласие на обработку персональных данных своей волей и в своем интересе. С точки зрения гражданского права такие действия односторонними сделками[[21]](#footnote-21). Сделки могут совершаться устно или письменно. При этом, устная сделка считается совершенной и в том случае, когда из поведения лица явствует его воля совершить сделку (конклюдентные действия). То есть, не обязательно выражать свою волю словами, достаточно это сделать каким-то понятным действием, например, ответить на вопрос: «Вы согласны передать ваши персональные данные?» – просто кивнув головой. Согласие на обработку персональных данных может быть выражено конклюдентным действием. Можно, например, «кликнуть» мышкой в определенном месте сайта. И такое согласие не противоречит закону.

#### *Некоторые исключения.*

Существуют случаи, когда согласия субъекта не обработку персональных данных не требуется. Такие случаи обязательно должны быть оговорены законами. Например, согласия не требуется, если персональные данные обрабатываются для осуществления правосудия или исполнения судебного акта, предоставления государственных услуг, осуществления профессиональной деятельности журналиста. Не требует согласия и обработка общедоступных персональных данных и данных, подлежащих опубликованию или обязательному раскрытию по закону.

Но есть случай, который особо важен для школ (образовательных учреждений). Согласия не требуется, если обработка персональных данных необходима для исполнения договора, стороной которого является сам субъект. Это исключение позволяет не требовать согласия при обработке персональных данных сотрудников школы, если эти данные обрабатываются в рамках трудового договора, например, при ведении кадрового и бухгалтерского делопроизводства.

### *От общего к частному.*

Попробуем приложить основные понятия к практической области и посмотреть как это ложится на школьную жизнь.

#### *Где и какие персональные данные есть в школе?*

Деятельность любой школы связана с обработкой персональных данных различных категорий субъектов:

* учащиеся (переменный состав),
* родители и законные представители учащихся,
* учителя и преподаватели (постоянный состав),
* обеспечивающий персонал (бухгалтерия, делопроизводство и др.),
* персонал взаимодействующих организаций (охрана, пищеблок и др.)

Каждая из этих категорий находится в разных правовых отношениях со школой как оператором персональных данных.

Главное в школе – учебный процесс. Он сопровождается целым рядом атрибутов, в которых могут содержаться персональные данные учащихся, их родителей, учителей. Это традиционные «бумажные» документы, такие, как:

* классные журналы, ведомости,
* тетради и дневники учащихся,
* анкеты и характеристики учащихся,
* личные дела учащихся.

Как правило, защита персональных данных в этом случае осуществляется традиционными методами: учетом документов и организацией их хранения. Этим ограничиваются. Однако, на самом деле здесь также необходим полный комплекс организационных мер защиты, но об этом чуть позже.

В учебный процесс все шире внедряются современные информационные технологии и появляются:

* электронные дневники,
* школьные сайты,
* социальные электронные карты и электронные карты учащихся,
* школьные информационные системы и форумы,
* специальные системы (Школьный офис, Карта учащегося, База данных ЕГЭ),
* системы дистанционного обучения и многое другое.

За порядком в школе тоже надо следить. Уже во многих школах активно применяются современные средства охраны и контроля, которые также могут обрабатывать персональные данные, в том числе, возможно, и биометрические:

* системы видеонаблюдения,
* системы контроля и управления доступом в помещения школы.

Зачастую внедряя современные технологии никто не задумывается о необходимости защиты информации в целом и персональных данных при их использовании. А именно обработка персональных данных с использованием этих технологий наиболее подвержена различным угрозам. Чаще всего школьные информационные системы являются собственной разработкой и служат для широкого спектра целей: ведения учебной статистики, составления расписаний, ведение электронного журнала. Основными особенностями данных систем является то, что обработка данных в них производится исключительно для внутренних целей школы в основном для упрощения учебного процесса. В таких системах, как правило, одновременно обрабатываются персональные данные учащихся и преподавателей.

Деятельность школы (образовательного учреждения) не ограничивается только самим учебным процессом. Это, хотя и важная, но не единственная составляющая школьной жизни. Не будем забывать и о тех, кто учит и обеспечивает процесс познания. Учителей и обеспечивающий персонал связывают со школой определенные трудовые отношения. И в ходе этих отношений возникают различные ситуации, когда необходима обработка всего спектра их персональных данных, в том числе и с применением компьютеров и информационных технологий:

* кадровая работа (прием и увольнение, отпуска, аттестация и пр.)
* бухгалтерия (начисление и выплата заработной платы, пособий и пр.),
* отчетность перед государственными органами образования,
* проведение служебных расследований и работа с жалобами.

Кроме того, школа, как самостоятельный хозяйствующий субъект находится в договорных отношениях с различными организациями:

* охранные предприятия,
* интернет провайдеры и провайдеры связи,
* предприятия питания,
* строительные и подрядные организации и пр.

Здесь, с одной стороны появляется возможность ознакомления сотрудников школы с персональными данными сотрудников других организаций, а с другой стороны не исключается возможность ознакомления этих «чужих» сотрудников с персональными данными постоянного и переменного состава школы. И эти вопросы тоже надо урегулировать и обеспечить защиту и тех и других.

Не будем забывать и о медицинских кабинетах и пунктах в которых обрабатываются особые (специальные) категории персональных данных, требующие особого внимания и защиты, например, медицинские карты.

Примерный перечень документов (ресурсов) обрабатываемых в школе (образовательном учреждении), в которых могут находиться персональные данные приведен в приложении к данной книге (Приложение № 9).

#### *Особенности получения согласия от несовершеннолетних*

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает его законный представитель[[22]](#footnote-22). Полной дееспособностью обладают лица, достигшие восемнадцатилетнего возраста и в некоторых случаях, оговоренных Гражданским кодексом[[23]](#footnote-23), приобретшие полную дееспособность несовершеннолетние в возрасте от 14 до 18 лет. Законными представителями своих детей являются их родители[[24]](#footnote-24). Именно они выступают в защиту прав и интересов ребенка в отношениях с любыми физическими и юридическими лицами без специальных полномочий. За несовершеннолетних, не достигших четырнадцатилетнего возраста могут совершаться только их родителями или законными представителями, а сделки в возрасте от четырнадцати до восемнадцати лет совершаются несовершеннолетним только с письменного согласия родителей[[25]](#footnote-25), иначе они признаются оспоримыми[[26]](#footnote-26) и могу быть признаны недействительными.

Таким образом, согласие на обработку персональных данных несовершеннолетних учащихся в возрасте до 14 лет могут дать только родители, а в возрасте старше 14 лет, такое согласие дают сами учащиеся, но с письменного согласия их родителей или законных представителей.

#### *Кто есть кто*

Организуя обработку персональных данных важно определить какой статус имеет школа по отношению к обрабатываемым персональным данным. От этого зависит кто имеет право устанавливать правила их обработки и требования по защите, а кто обязан выполнять эти правила и требования. В предыдущих разделах мы уже отмечали, что школа является оператором. Однако, это только общее заявление.

По отношению к тем или иным персональным данным школа может выступать как оператор или обработчик. И если, как было уже отмечено, оператор определяет цели обработки и выдвигает требования, то обработчик действует в интересах оператора и выполняет его поручение, в том числе и защищает персональные данные в соответствии с требованиями оператора. При этом, именно на операторе остается ответственность перед субъектом за все нарушения, а обработчик несет регрессную ответственность перед оператором. Именно оператор отвечает за получение согласия субъекта на обработку персональных данных и, если это требуется, уведомляет контролирующие органы (Роскомнадзор) об обработке персональных данных.

Статус школы (образовательного учреждения) по отношению к тем или иным персональным данным, которые могут обрабатываться в ее информационных системах, приведен в приложении к данной книге (Приложение № 3).

## Защита персональных данных – это важно!

Практически каждая организация, от детского садика и школы до государственного ведомства, в той или иной степени обрабатывает персональные данные. На самом деле закон «О персональных данных» – самый массовый закон, который затрагивает интересы всех. Здесь все переплетено: сегодня ты выступаешь, как субъект, а завтра, ты уже оператор. Сегодня ты на стороне тех, кто хочет сэкономить на защите персональных данных, а завтра ты уже сам радеешь за то, чтобы твои персональные данные защищали самым тщательным образом.

### *Зачем надо защищать персональные данные?*

Затем, что неправомерное использование персональных данных может навредить субъекту. Главная цель защиты персональных данных – обеспечение защиты прав и свобод человека (субъекта), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Необходимость обеспечения безопасности персональных данных в наше время – объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения. Именно поэтому персональные данные нуждаются в самой серьезной защите. Для граждан, от степени защищенности персональных данных зависит физическая и имущественная безопасность, а для операторов — обеспечение надлежащего функционирования организации.

Несколько примеров, как это может навредить субъекту. Доскональное знание имени, фамилии, места жительства, даты рождения и других подобных сведений поможет злоумышленнику выдавать себя за другое лицо. И чем больше такой информации об увлечениях, хобби и личной жизни есть у мошенника, тем точнее будет сходство. А паспортные данные и вовсе могут помочь злоумышленнику взять на чужое имя кредит или получить доступ к банковским вкладам (как-то, в СМИ проскочила новость, что от лица одного российского гражданина, воспользовавшись его паспортными данными, некто попытался купить особняк в Италии за 4 млн евро). Номер мобильного или городского телефона, впрочем как и адрес электронной почты, привязан к конкретной личности. Злоумышленник, узнав телефонные номера может идентифицировать владельца номера. Точно также, как и для электронного адреса, для телефонов есть опасность SMS- или даже голосового спама. Мы часто заполняем разные анкеты, участвуем в сомнительных лотереях и конкурсах. Самыми легкими последствиями будет «бомбардировка» наших телефонов разным рекламным спамом и сообщениями «радостной новости о крупном выигрыше». Но, зная электронный адрес и основы поиска в Google, можно без труда вытянуть всю остальную информацию – имя фамилию, место жительство, дату рождения. Зная персональные данные ребенка, можно использовать их для неблаговидных целей, вовлекать их в противоправные действия, а то и того хуже: использовать в преступных целях, в том числе и для донорства органов. К сожалению, у нас есть и киднепинг, и педофилия. Разглашение специальных персональных данных может спровоцировать обострение взаимоотношений в коллективе. И еще многое другое.

Не менее ощутимы последствия несоблюдения режима защиты персональных данных и для самой школы. Их разглашение создает проблемы, провоцируя, так называемые имиджевые (репутационные) риски. Утечки персональных данных подчас приводят к действительно непоправимым последствиям в сфере имиджа образовательного учреждения. Маловероятно, что кто-либо продолжит сотрудничество со школой, доброе имя которой подпорчено негативом инцидента в сфере защиты конфиденциальных данных. Не исключается утрата доверия граждан, жалобы субъектов в надзорные органы, публикация негативной информации о нарушениях в СМИ. Кроме того, нарушения порядка обработки и защиты персональных данных для оператора влечет за собой репрессивные риски, обусловленные применением репрессивных мер дисциплинарного, административного или уголовного характера, а также финансовые риски – обусловленные прямыми финансовыми потерями (ущерб и убытки).

### *Почему надо защищать персональные данные?*

Потому, что так предписывает закон. Персональные данные, даже если они обрабатываются в школьных информационных системах, не принадлежат школе. Это то, что передано школе субъектом для использования, но не для нанесения ему ущерба. Неприкосновенность частной жизни – конституционное право каждого гражданина[[27]](#footnote-27). Серьезность намерений государства, как патроната интересов граждан, в этом вопросе очевидна: уже сформирована нормативная база, определена ответственность, регуляторы получили соответствующие полномочия, растет количество проверок. Все мы являемся законопослушными гражданами и обязаны выполнять требования законодательства, которым защита персональных данных возложена на те организации, где они обрабатываются. Защиту персональных данных обязаны осуществлять все без исключения организации. То есть, если организация является оператором, она обязана выполнить требования Закона.

Защита персональных данных является обязанностью организации, а не правом. Закон содержит императивную, обязательную норму. Требования по защите персональных данных установлены правительством, а разработка технических требований по защите и контроль их исполнения возложены на уполномоченные органы власти.

 За нарушение норм законодательства о персональных данных предусматривается как административная, так и уголовная ответственность, возможна также гражданская и дисциплинарная ответственность. И в настоящее время отмечается устойчивая тенденция усиления ответственности за нарушение порядка обработки и защиты персональных данных.

Законом также закреплены права субъекта персональных данных[[28]](#footnote-28) и он вправе принимать законные меры по защите своих прав. В помощь ему, впервые в российской практике введен специальный институт уполномоченных по защите прав субъектов, на который возлагается надзор за соответствием обработки персональных данных требованиям закона[[29]](#footnote-29).

### *От кого надо защищать персональные данные?*

От последствий действий хакеров, злоумышленников, инсайдеров, а иногда и от нашей собственной беспечности. А еще от последствий различных проявлений техногенных факторов: отключения электричества, выходя из строя компьютеров, протечек воды, и много другого, что может уничтожить или исказить информацию. Проще говоря – от всего того, что может причинить вред субъекту, то есть от различных угроз безопасности персональным данным.

#### *Что такое угрозы безопасности персональным данным?*

Любую угрозу можно описать совокупностью источника, фактора и способа (метода) ее реализации:

Угроза = *f*(источник угрозы, уязвимость [фактор], способ [метод] реализации)

Очень удобная формула, позволяющая правильно выбрать методы защиты (устранения угроз). Формула показывает, что если нет источника угрозы, но есть какая-то уязвимость, то и угроза не будет реализована. Точно также, если есть уязвимость, но нет источникам угроз – она также не будет реализована. Следовательно, достаточно направить усилия на устранение либо источника, либо уязвимости. Такой подход позволяет экономить деньги при создании системы защиты персональных данных. Логическая взаимосвязь составных элементов угрозы показана на рисунке.



На самом деле угроз не так уж и много. Все угрозы можно разложить по тем полезным свойствам информации, которые защищаются и сформировать конечный список угроз:

* при обеспечении конфиденциальности информации:
	+ хищение (копирование) информации и средств ее обработки
	+ утрата (неумышленная потеря, утечка) информации
* при обеспечении целостности информации:
	+ модификация (искажение) информации
	+ отрицание подлинности информации
	+ навязывание ложной информации
* при обеспечении доступности информации:
	+ блокирование информации
	+ уничтожение информации и средств ее обработки

#### *Что такое модель угроз и зачем она нужна?*

Один и тот же источник угрозы может использовать разные факторы и уязвимости для достижения своей неблаговидной цели. Поэтому различных реализаций угроз может быть сколь угодно много. Описанный особым образом набор таких возможных реализаций составляет модель угроз. Это обязательный документ, разработка которого предписана требованиями уполномоченных государственных органов. Он позволяет обосновать необходимость применения тех или иных способов и методов защиты персональных данных и, в то же время, дает возможность исключить некоторые реализации угроз, как не актуальные для конкретной школы.

Разработка модели угроз – кропотливая работа, требующая времени, специальных знаний и опыта. Не каждый оператор обладает такими возможностями. Поэтому, законодатель обязал государственные органы в пределах своих полномочий разрабатывать модели актуальных для отрасли с учетом содержания персональных данных, характера и способов их обработки[[30]](#footnote-30). Такие модели согласовываются с уполномоченными государственными органами. Школа, как оператор персональных данных, в данном случае должна использовать отраслевую модель актуальных угроз, а не разрабатывать свою.

### *Кто регулирует отношения?*

Государство взяло патронат над обработкой персональных данных и защитой интересов субъектов. Регулирование в этой обрасти осуществляют:

* Правительство Российской Федерации;
* Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор России);
* Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
* Федеральная служба безопасности (ФСБ России).

Правительство РФ осуществляет меры по обеспечению законности, прав и свобод граждан. В сфере защиты персональных данных Правительство РФ уполномочено:

* определять перечень мер, направленных на обеспечение защиты информации,
* устанавливать уровни защищенности определенных информационных систем,
* определять требования к защите персональных данных,
* определять государственные органы, осуществляющие лицензирование деятельности в этой области и утверждать положения о лицензировании.

Роскомнадзор определен уполномоченным органом по защите прав субъектов персональных данных[[31]](#footnote-31). На Роскомнадзор возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям закона[[32]](#footnote-32). Полномочия в этой области определены серьезные, в том числе проведение проверок как в плановом режиме, так и по заявлениям субъектов. В рамках исполнения своих функций, должностные лица Роскомнадзора имеют право:

* выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области обработки персональных данных;
* составлять протоколы об административном правонарушении или направлять в органы прокуратуры материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных;
* направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии,
* принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства.

ФСТЭК Росси является регулятором в области обеспечения безопасности информации не криптографическими методами, а ее нормативные акты, касающиеся защиты информации, являются обязательными для всех организаций, которые находятся под юрисдикцией России[[33]](#footnote-33). Она имеет свою систему сертификации средств защиты информации[[34]](#footnote-34). В рамках этой системы проводится обязательная сертификация средств, предназначенных для защиты персональных данных. ФСТЭК России наделена полномочиями:

* устанавливать требования по защите информации не криптографическими методами,
* определять состав и содержание организационных и технических мер по обеспечению безопасности информации ограниченного доступа,
* поводить лицензирование видов деятельности, связанных с защитой информации,
* организовывать и проводить сертификацию средств защиты информации, использующих не криптографические методы защиты,
* осуществлять контроль и надзор за выполнением требований по обеспечению безопасности информации.

ФСБ России является регулятором в области использования криптографических средств защиты информации. ФСБ России отвечает за все вопросы применения криптографических методов защиты информации. ФСБ России имеет систему сертификации средств криптографической защиты информации (система сертификации СКЗИ)[[35]](#footnote-35). В рамках этой системы проводится сертификация шифровальных средств.

Все органы действуют строго в рамках своей компетенции. Таким образом:

* Роскомнадзор отвечает за общий контроль и надзор, представление интересов субъектов при обработке их персональных данных,
* ФСТЭК России регламентирует вопросы технической защиты персональных данных не криптографическим методами,
* ФСБ регламентирует вопросы защиты персональных данных криптографическими методами.

Причем при осуществлении своих функций знакомиться с персональными данными, обрабатываемыми в организации, имеют право только сотрудники Роскомнадзора.

# Глава II. Специальная

*Приступая к обработке чужих персональных данных, помните, что в этот момент кто-то обрабатывает Ваши персональные данные.*

Обеспечить защиту персональных данных усилиями только одного-двух специально назначенных сотрудников школы нельзя. Здесь необходимы усилия практически всего персонала школы. Безопасность персональных данных достигается, в частности:

* определением угроз безопасности персональных данных;
* оценкой и выбором уровня защищенности персональных данных;
* применением организационных и технических мер защиты;
* применением сертифицированных средств защиты информации;
* оценкой эффективности принимаемых мер защиты;
* учетом машинных носителей персональных данных;
* обнаружением фактов несанкционированного доступа к персональным;
* восстановлением модифицированных или уничтоженных персональных данных;
* установлением правил доступа к персональным данным;
* обеспечением регистрации действий, совершаемых с персональными данными;
* контролем за принимаемыми мерами защиты персональных данных.

Кроме того, защита предполагает применение технических мер, поэтому могут потребоваться консультации специалистов. А так как защита информации является лицензируемым видом деятельности, то такие специалисты должны быть из организаций, имеющих лицензии на оказание услуг по защите конфиденциальной информации.

## С чего начать защиту данных?

Для защиты персональных данных целесообразно создавать единую целостную систему, которая охватывает все аспекты защиты. Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в школьных информационных системах. Создание любой сложной системы, а именно таковой является система защиты персональных данных, целесообразно проводить по этапам.

### *Ревизия информационных ресурсов*

Существует несколько факторов, влияющих на состав мер защиты:

* способ обработки персональных данных;
* требуемый уровень защищенности персональных данных.

Способ обработки может быть либо автоматизированный, либо без использования средств автоматизации.

Критерии, определяющие требуемый уровень защищенности персональных данных установлены Постановлением Правительства РФ.

Чтобы правильно определить состав мер защиты персональных данных, необходимо представлять кто, где и какие категории персональных данных обрабатывает в школе. Для этого целесообразно провести инвентаризацию всех информационных ресурсов[[36]](#footnote-36), которые могут быть в школе.

#### *Проводим инвентаризацию ресурсов*

Инвентаризация – процесс трудоемкий, но он оправдывает себя. Для проведения инвентаризации информационных ресурсов целесообразно назначить сотрудников, имеющих представление о составе школьных информационных систем и знающих какая информация может обрабатываться. Комиссия должна определить:

* в каких школьных подразделениях могут находиться документы (информационные ресурсы), содержащие персональные данные;
* способ обработки персональных данных (автоматизированный, не автоматизированный);
* состав документов (информационных ресурсов) в которых могут находиться персональные данные и состав находящихся в них персональных данных;
* категории субъектов, чьи персональные данные обрабатываются (учащиеся, родители и законные представители учащихся, учителя, обеспечивающий персонал, персонал взаимодействующих организаций и др.);
* категории обрабатываемых персональных данных (специальные, биометрические, общедоступные, идентификационные, иные).

Особое внимание (но не только!) необходимо обратить на документы, обрабатываемые в таких школьных подразделениях, как:

* медицинский пункт (кабинет);
* канцелярия (делопроизводство);
* кадровое делопроизводство;
* бухгалтерия;
* серверные школьных информационных систем;
* преподавательские (учительские);
* архивы, в том числе электронные;
* библиотека.

В ходе работы комиссии надо проанализировать все возможные документы (информационные ресурсы), которые могут быть в школе на предмет наличия в них персональных данных. За основу, в этой работе можно взять Примерный перечень документов (ресурсов) обрабатываемых в образовательном учреждении, в которых могут находиться персональные данные, приведенный в Приложении № 2. Однако, это не окончательный перечень, в каждой школе могут найтись и свои специфические ресурсы, содержащие персональные данные.

Результатом работы комиссии должен стать перечень документов (ресурсов) обрабатываемых в образовательном учреждении, в которых могут находиться персональные данные. Такой перечень будет являться исходными данными для дальнейших действий по организации защиты персональных данных. Отметим, что при подготовке перечня могут возникнуть некоторые сложности. И одной из них является определения способа обработки персональных данных.

#### *Способ обработки: автоматизированный или неавтоматизированный?*

Определение способа обработки персональных данных оказывает существенное влияние на состав мер их защиты. Если при автоматизированной обработке обязательно применение тех или иных технических мер, то при неавтоматизированной – можно обойтись только некоторыми организационными мерами, что проще и дешевле. Вместе с тем, этот, казалось бы, простой вопрос на практике вызывает много споров. Определения способов обработки, данные в нормативных актах, запутанны и противоречивы. При этом, сам по себе факт использования в процессе обработки персональных данных средств автоматизации не всегда является критерием отнесения этого процесса к тому или ному способу.

С одной стороны нормативными актами определено, что обработка персональных данных, содержащихся в информационной системе 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, а сами персональные данные отделены от другой информации (путем фиксации их на отдельных материальных носителях, в специальных разделах или полях форм). Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе либо были извлечены из нее[[37]](#footnote-37). Исходя из этого, некоторые организации полагают, что всю обработку персональных данных можно отнести к неавтоматизированной, поскольку во всех случаях имеется факт «обработки при непосредственном участии человека». Дело в том, что почти во всех операциях по обработке персональных данных в информационных системах участвует человек, но это не значит, что обработка неавтоматизированная. Достаточно просто сохранить информацию в виде файла на компьютере – и обработка станет автоматизированной (хранение персональных данных это действие, которое относится к их обработке, а хранение в памяти компьютера – это использование средств автоматизации для обработки). Примером неавтоматизированной обработки может стать выдача бумажного одноразового пропуска на территорию школы. Проще говоря, обработка персональных данных будет являться неавтоматизированной при условии, что компьютер используется в качестве «пишущей машинки», а набранные с его помощью тексты, содержащие персональные данные, распечатаны на листе бумаги (материальном носителе), при условии что они не будут сохранены в памяти компьютера. Если же такие документы сохранены в виде файла в памяти компьютера, то в этом случае нужно рассматривать такие действия как автоматизированную обработку персональных данных.

С другой стороны, нормативные акты устанавливают, что если обработка персональных данных без использования средств автоматизации соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях[[38]](#footnote-38), то такая обработка признается равнозначной автоматизированной со всеми вытекающими отсюда последствиями.

Определив способ обработки тех или иных информационных ресурсов в школе, необходимо выделить те, обработка которых осуществляется неавтоматизированными способами. Защита этих ресурсов будет проводиться организационными методам о которых мы поговорим позже.

Для остальных ресурсов, которые обрабатываются с использованием средств автоматизации (автоматизированная обработка) необходимо определить требуемый уровень защищенности. Для этого надо выделить категории персональных данных, подлежащих обработке и на их основе определить тип информационной системы.

#### *Определяем тип информационных систем*

Для определения требуемого уровня защищенности, в зависимости от категории персональных данных выделяются следующие типы информационных систем:

* обрабатывающие специальные персональные данные;
* обрабатывающие биометрические персональные данные;
* обрабатывающие общедоступные персональные данные;
* обрабатывающие иные категории персональных данных;
* обрабатывающие обезличенные данные;
* обрабатывающие персональные данные только сотрудников оператора;
* обрабатывающие персональные данные субъектов, не являющихся сотрудниками оператора.

Информационная система считается информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней для целей идентификации субъекта обрабатываются сведения, которые характеризуют его физиологические и биологические особенности, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов, полученные только из общедоступных источников персональных данных.

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные выше. К этому типу информационных систем относятся и информационные системы, обрабатывающие идентификационные персональные данные.

Информационная система является информационной системой, обрабатывающей обезличенные данные, если перед вводом в информационную систему персональные данные прошли процедуру обезличивания и в самой информационной системе отсутствуют идентификационные персональные данные.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях считается, что информационная система, обрабатывает персональные данные субъектов, не являющихся сотрудниками оператора. Для школ характерно то, что их информационные системы, как правило, относятся к информационным системам, обрабатывающим персональные данные субъектов персональных данных, не являющихся сотрудниками оператора. Это объясняется тем, что учащиеся, чьи персональные данные обрабатываются на ряду с персональными данными учителей, не относятся к персоналу школы.

#### *Формируем перечень обрабатываемых персональных данных*

Результатом, завершающим этап ревизии информационных ресурсов, является формирование Перечня персональных данных, обрабатываемых в образовательном учреждении. Жестких требований к такому перечню – нет, поэтому он оформляется в любой произвольной форме. Вместе с тем, в этом перечне целесообразно отразить:

* подразделение школы, где обрабатываются персональные данные;
* помещения школы в которых хранятся и обрабатываются персональные данные;
* состав ресурсов (документов), содержащих персональные данные;
* цели обработки персональных данных;
* состав обрабатываемых персональных данных;
* категория обрабатываемых персональных данных;
* способ обработки персональных данных;
* тип информационной системы (при автоматизированной обработке);
* состав лиц, допущенных к обработке персональных данных (по должности).

### *Определяем уровень защищенности персональных данных*

В школе могут быть несколько обособленных или взаимосвязанных информационных систем, обрабатывающих персональные данные. Например, информационная система бухгалтерии (на базе программы 1С), информационная система, обеспечивающая работу школьного сайта, специальные информационные системы (Школьный офис, Карта учащегося, База данных ЕГЭ) и пр. Эти информационные системы могут объединять несколько средств обработки (компьютеры, серверы, принтеры) или состоять только из одного рабочего места (компьютера). Но для каждой информационной системы необходимо выбрать требуемый уровень защищенности персональных данных. Выделяются четыре основных критерия[[39]](#footnote-39), определяющие требуемый уровень защищенности персональных данных:

* категория обрабатываемых персональных данных (тип информационной системы);
* объем обрабатываемых персональных данных;
* тип угроз персональным данным;
* принадлежность обрабатываемых данных к сотрудникам оператора.

Алгоритм действий по выбору требуемого уровня защищенности и таблица выбора уровней защищенности персональных данных в соответствии с этими критериями приведена в Приложениях № 4 и № 5.

Как определить категорию обрабатываемых персональных данных (тип информационной системы) и принадлежность обрабатываемых данных к сотрудникам оператора мы рассмотрели выше.

Относительно объема обрабатываемых персональных данных Постановление Правительства РФ устанавливает граничное значение, влияющее на требуемый уровень защищенности, в 100 000 записей о субъектах. В школе вряд ли будут обрабатываться персональные данные более, чем 100 000 субъектов. Поэтому, при выборе этого критерия проблем не возникает.

Таким образом, для определения требуемого уровня защищенности персональных данных, обрабатываемых в школьных информационных системах остается разобраться с типом угроз. Отметим, что определение типа угроз безопасности персональных данных, актуальных для информационной системы, является прерогативной оператора, который проводит эту работу с учетом оценки возможного вреда субъекту персональных данных[[40]](#footnote-40).

#### *Типы угроз безопасности персональным данным.*

Правительством РФ установлены три типа угроз:

* Угрозы 1-го типа – связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.
* Угрозы 2-го типа – связаны с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.
* Угрозы 3-го типа – не связаны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Видно, что тип угроз напрямую зависит от наличия так называемых недокументированных (недекларированных) возможностей в программном обеспечении.

С типом программного обеспечения разобраться просто. Под системным программным обеспечением понимается комплекс программ, которые обеспечивают управление компонентами компьютерной системы, такими как процессор, оперативная память, устройства ввода-вывода, сетевое оборудование. Оно является, своеобразным интерфейсом между компьютером и прикладными программами (приложениями). Как правило, к системному программному обеспечению относятся операционные системы, специальные утилиты (дефрагментаторы, утилиты работы с реестром, утилиты очистки памяти и пр.), системы программирования (ассемблеры, компиляторы, компоновщики, отладчики и пр.), системы управления базами данных. Прикладное программное обеспечение (приложение) – это программа, предназначенная для выполнения определенных пользовательских задач и рассчитанная на непосредственное взаимодействие с пользователем. Прикладные программы не могут обращаться к ресурсам компьютера напрямую, а взаимодействуют с оборудованием посредством операционной системы. К этому типу программного обеспечения относятся компьютерные программы, написанные для пользователей или самими пользователями для решения практических задач (текстовые и графические редакторы, мультимедийные программы, гипертекстовые программы, компьютерные игры и пр.) В отличие от прикладного, системное программного обеспечения не решает конкретные практические задачи, а лишь обеспечивает работу других программ, предоставляя им сервисные функции и управляет аппаратными ресурсами вычислительной системы.

Гораздо сложнее разобраться с наличием недокументированных (недекларированных) возможностей, так как это специальное понятие, используемое в профессиональной среде защитников информации.

#### *Что такое недекларированные возможности программного обеспечения?*

Нормативные документы определяют недекларированные возможности, как функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности информации[[41]](#footnote-41). Например, специальные комбинации клавиш сотовых телефонов, открывающие доступ к инженерным или диагностическим меню (команда ӿ#06#, которая позволяет получить доступ к идентификационным данным телефона или его конфигурации).

К сожалению, очень часто под недокументированными (недекларированными) возможностями понимают уязвимость программного обеспечения. Но понятие уязвимости гораздо шире, чем понятие недекларированные возможности. Уязвимость принадлежит системе в целом, а не программному обеспечению в частности и может возникнуть в результате ошибок программирования и проектирования информационной системы, использования ненадежных паролей, вирусных атак и применения других вредоносных программ. Недекларированные возможности могут служить уязвимостью, но не всякая уязвимость обусловлена ими.

Неправомерные действия с информацией могут совершать либо субъекты (санкционированные пользователи), имеющие легальный доступ к информации, но превышающие свои права, либо субъекты (несанкционированные пользователи), не имеющие легального доступа к информации, но стремящиеся получить такой доступ для достижения своих преступных целей, в том числе и имеющих желание самовыразиться или потешить свое самолюбие. При этом, злоумышленнику надо решить сразу две задачи: найти способ как проникнуть в информационную систему и найти способ как воспользоваться недекларированными возможностями. Он должен иметь высокую квалификацию и иметь доступ к материалам, описывающим недекларированные возможности. Использовать недекларированные возможности «в слепую» вряд ли кто-то будет. Использовать такой механизм добывания информации в силу сложности его реализации будут в случае, если надо получить какие-то конкретные персональные данные о каком-то конкретном субъекте. В противном случае это экономически не оправдано.

При оценке актуальности угроз учтем следующее:

* Для получения общедоступных персональных данных вряд ли будут использоваться недекларированные возможности программного обеспечения. Их можно получить из открытых источников не прибегая ни к каким хитростям.
* Биометрические персональные данные для целей идентификации обрабатываются не во всех организациях и с использованием специального программного обеспечения. Такое программное обеспечение, как правило, написано под заказ и проходит строгий выходной контроль. Наличие недекларированных возможностей в таком программном обеспечении маловероятно.
* Обработка специальных категорий персональных данных – явление редкое.

Таким образом, для оценки актуальности угроз, которые могут быть реализованы с использованием недекларированных возможностей, прежде всего надо оценивать важность самой информации (персональных данных), а так же квалификацию и возможности злоумышленника.

#### *Как оценить вред субъекту?*

Это, пожалуй, самый сложный вопрос. Закон устанавливает[[42]](#footnote-42), что оценка вреда производится в целях определения соотношения вреда субъекту и принимаемых оператором мер защиты. Формально размер потенциального вреда должен влиять на требуемый уровень защищенности персональных данных и чем выше потенциальный вред, тем более строгие меры защиты обязан принимать оператор. Вместе с тем, к сожалению, в настоящее время никакой единой методологии оценки вреда и определения влияния его размера на состав принимаемых оператором мер защиты персональных данных, нет.

Поэтому оценку степени возможного вреда, который может быть причинён субъекту в результате нарушения свойств безопасности персональных данных (конфиденциальности, целостности, доступности) целесообразно проводить экспертным методом комиссионно (внутренней комиссией) на основании качественных экспертных оценок в зависимости от степени возможных негативных последствий для субъектов по следующей качественной (вербальной) шкале:

* значительный вред – при возникновении значительных негативных последствий;
* средний вред – при возникновении умеренных негативных последствий;
* незначительный вред – при возникновении незначительных негативных последствий;
* отсутствие вреда – при отсутствии негативных последствий.

Оценка вреда проводится относительно каждого информационного ресурса, установленного в ходе инвентаризации. При этом, вначале определяется нарушение каких свойств безопасности может причинить вред, а затем определяется степень вреда. Например, имеются информационные ресурсы, содержащие паспортные данные учителей. Несанкционированное разглашение (нарушение конфиденциальности) этих сведений может повлечь за собой их использование для получения злоумышленником кредита в банке или совершения иного противоправного действия, что может причинить значительный ущерб субъекту. Вместе с тем, искажение в записи паспортных данных (нарушение целостности) или задержка в получении необходимых сведений (нарушение доступности) не принесет существенного вреда субъекту. Таким образом, ресурсы, содержащие паспортные данные учителей, критичны к нарушению конфиденциальности, что приводит к значительному вреду для субъекта и мало критичны к нарушению целостности и доступности, что может привести к незначительному вреду или полному его отсутствию для субъекта. С другой стороны, для ресурсов, содержащих текущие оценки деятельности учеников, разглашение содержащихся в них сведений (нарушение конфиденциальности) не принесет существенного вреда субъекту, искажение нескольких оценок (нарушение целостности) может привести к неправильной годовой оценке деятельности ученика и тем самым причинить ему вред средней тяжести. Поэтому такие ресурсы критичны к нарушению целостности, что может привести к среднему вреду субъекту и не критичны к нарушению конфиденциальности, не влекущей никакого ущерба для субъекта.

Результаты работы комиссии по оценке возможного вреда отражаются в Перечне персональных данных, обрабатываемых в образовательном учреждении, добавляя в него следующие графы для каждого ресурса:

* критичные свойства безопасности (конфиденциальность, целостность, доступность);
* оценка возможного вреда от нарушения критичных свойств.

Оценка возможного вреда не может повлиять на выбор типа угроз, но учитывается при определении актуальности угроз и при выборе мер защиты. Так, отсутствие вреда субъекту при реализации той или иной угрозы относительно критичных свойств безопасности, может явиться причиной признания ее не актуальной и, следовательно, сокращению количества мер защиты. А наличие незначительного вреда субъекту при реализации угрозы – основанием для замены рекомендованных мер защиты более простыми компенсирующими мерами.

#### *Пример выбора требуемого уровня защищенности персональных данных.*

Разберем ситуацию на примере обычной среднестатистической школы[[43]](#footnote-43) и таблицы выбора уровней защищенности персональных данных, приведенной в Приложении № 5. Положим в школе имеется информационная система, которая обрабатывает персональные данные постоянного состава (учителей) для целей исполнения трудовых отношений и информационная система обрабатывающая персональные данные переменного состава (школьников) для целей обеспечения учебного процесса.

В первой информационной системе (учителя) обрабатываются: паспортные данные, ИНН, СНИЛС, сведения об образовании, квалификации и наличии специальных знаний, анкетные данные, сведения о малолетних детях, сведения о состоянии здоровья (инвалидность, беременность), трудовой договор, копии приказов о назначении, форма Т-2, заявления, результаты аттестации. Видно, что данная информационная система обрабатывает только персональные данные сотрудников оператора. Перечень показывает, что биометрические персональные данные для идентификации учителей не используются. Есть, конечно специальные персональные данные (о состоянии здоровья учителя и его родственников), но вероятность, что для получения этих сведений будут применяться методы, основанные на использовании недекларированных возможностей системного и прикладного программного обеспечения – весьма мала в силу незначительности степени возможного вреда субъекту. Для данной информационной системы актуальны угрозы только 3-го типа. Таким образом, для данной информационной системы требуется 3 (специальные категории персональных данных и биометрические персональные данные) или 4 (общедоступные и иные категории персональных данных) уровни защищенности персональных данных.

Во второй информационной системе (школьники): обрабатываются сведения, из документов удостоверяющих личность школьника, сведения о составе семьи, паспортные данные родителей, номер полиса медицинского страхования, сведения о состоянии здоровья, сведения о праве на дополнительные гарантии и компенсации, предусмотренные законом. Можно с уверенностью сказать, что число учащихся в среднестатистической школе менее 100 000 человек. Также видно, что биометрические данные для идентификации личности школьника не используются. Получается, что за исключением сведений о состоянии здоровья, приведенные персональные данные можно отнести к «иным» персональным данным. Для таких информационных систем актуальны угрозы 3-го типа и, соответственно, требуется 4 уровень защищенности персональных данных. Со сведениями о состоянии здоровья школьника для среднестатистической школы также проблемы нет. Использовать недекларированные возможности программного обеспечения для получения таких сведений гораздо дороже, чем обыкновенный и тривиальный подкуп школьной медсестры. Поэтому и для этой категории персональных данных актуальны угрозы 3-го типа (и, может быть, в редких случаях, угрозы 2-го типа). Поэтому и в данном случае можно считать, что требуется 3 уровень защищенности персональных данных.

Это, конечно, весьма грубая оценка актуальности угроз. Более точную картину можно будет получить, когда появятся отраслевые модели актуальных угроз. Но и такая оценка показывает, что для персональных данных, обрабатываемых в школьных информационных системах, как правило, требуется 3 уровень защищенности персональных данных при обработке специальных категорий персональных данных и биометрических персональных данных и 4 уровень защищенности при обработке общедоступных и иных категорий персональных данных. И только в некоторых конкретных случаях, в зависимости от реальных условий, требуемый уровень защищенности может быть и повышен.

## Меры и средства защиты

Блокирование (нейтрализация) актуальных угроз обеспечивается выбором мер по обеспечению безопасности персональных данных и их реализацией в системе защиты персональных данных. Состав необходимых для каждого уровня защищенности персональных данных мер защиты устанавливается ФСТЭК России[[44]](#footnote-44). Оператор из предложенного перечня мер должен выбрать те, которые позволяют нейтрализовать актуальные угрозы безопасности при обработке персональных данных.

Если оператор считает, что отдельные меры из перечня регулятора невозможно технически реализовать в школьной информационной системе или их реализация в школьной информационной системе нецелесообразна по экономическим соображениям, он может взамен этих мер применить иные, компенсирующие меры, обеспечивающие нейтрализацию актуальных угроз. В этом случае оператор должен обосновать применение этих компенсирующих мер и доказать, что они способны нейтрализовать актуальные угрозы безопасности.

### *Выбираем меры по защите персональных данных*

Правильный выбор мер и средств защиты информации требует специальных знаний и навыков, которые не характерны для работников школы. Поэтому на этом этапе может потребоваться консультация специалистов из организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации.

#### *Классификация мер защиты персональных данных.*

В систему защиты персональных данных в зависимости от актуальных угроз безопасности и структурно-функциональных характеристик информационной системы[[45]](#footnote-45) включаются следующие классы мер:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищенности персональных данных;
* обеспечение целостности информационной системы и информации;
* обеспечение доступности персональных данных;
* защиту среды виртуализации;
* защиту средств обработки информации;
* защиту информационной системы, ее средств и систем связи и передачи данных;
* выявление инцидентов безопасности персональных данных;
* управление конфигурацией информационной системой и системой защиты.

Меры по идентификации и аутентификации призваны обеспечивать присвоение субъектам доступа и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту предъявленного им идентификатора.

Меры по управлению доступом направлены на управление правами и привилегиями субъектов доступа, разграничение доступа субъектов к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по ограничению программной среды служат для исключения возможности установки (инсталляции) неиспользуемого в обработке персональных данных или запрещенного к использованию программного обеспечения, в том числе средств разработки и отладки программ.

Меры по защите машинных носителей информации позволяют исключить несанкционированный доступ к носителям и персональным данным хранящимся на них, а также несанкционированное использование съемных машинных носителей информации.

Меры по регистрации событий безопасности обеспечивают распознавание, запись, хранение и защиту информации о событиях в информационной системе, относящихся к безопасности персональных данных, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите направлены на обнаружение в информационной системе компьютерных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования персональных данных или нейтрализацию средств защиты.

Меры по обнаружению (предотвращению) вторжений служат для обнаружения действий по несанкционированному доступу к информации с целью ее добывания, уничтожения и блокирования.

Меры по контролю (анализу) защищенности персональных обеспечивают проведение систематического анализа защищенности информационной системы и тестирование работоспособности системы защиты информации.

Меры по обеспечению целостности информационной системы и информации направлены на обнаружение фактов нарушения целостности информационной системы и информации, и позволяют восстановить информационную систему и информацию.

Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих право доступа к персональным данным в штатном режиме эксплуатации информационной системы.

Меры по защите средств обработки информации позволяют ограничить доступ к техническим средствам обработки персональных данных, средствам обеспечения функционирования информационной системы и в помещения в которых они постоянно расположены, а также защиту технических средств от внешних воздействий.

Меры по защите информационной системы, ее средств и систем связи и передачи данных служат для защиты информации при взаимодействии сегментов информационной системы, информационной системы с другими информационными системами и информационно-телекоммуникационными сетями.

Меры по выявлению инцидентов безопасности персональных данных направлены на обнаружение, идентификацию и анализ инцидентов, а также принятие мер по их устранению.

Меры по управлению конфигурацией информационной системой и системой защиты позволяют контролировать изменения конфигурации информационной системы и системы защиты, а также проводить анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных.

Отметим, что для 3 уровня защищенности персональных данных, который характерен для школьных информационных систем, обрабатывающих биометрические и специальные категории персональных данных, меры по обнаружению вторжений, обеспечению целостности информационной системы, ограничению программной среды, обеспечению доступности персональных данных, защите среды виртуализации, выявлению инцидентов и реагированию на них выполнять не требуется, что значительно упрощает систему защиты и сокращает расходы на ее создание. А для 4 уровня защищенности персональных данных, типичного для большинства остальных школьных информационных систем, обрабатывающих общедоступные и иные категории персональных данных, дополнительно исключаются меры, направленные за защиту машинных носителей и управление конфигурацией информационной системы и системы защиты персональных данных.

#### *Общий порядок действий по выбору мер защиты информации.*

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в системе защиты персональных данных, проводится в следующей последовательности:

* выбор базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных, обрабатываемых в информационной системе;
* адаптацию выбранного базового набора мер применительно к структурно-функциональным характеристикам информационной системы и с учетом целей защиты персональных данных (конфиденциальности, целостности, доступности);
* дополнение адаптированного базового набора мер дополнительными мерами приведенными в приказе ФСТЭК России, но не определенными в качестве базовых, но необходимых для блокирования (нейтрализации) актуальных угроз безопасности, а также дополнительными мерами, обеспечивающими выполнение требований по обеспечению безопасности персональных данных, установленными иными нормативными правовыми актами в области защиты информации.

Алгоритм действий по выбору мер защиты информации приведен в Приложении № 4.

#### *Определение базового набора мер защиты информации.*

Определение базового набора мер защиты является первым шагом в выборе мер защиты. Состав базового набора мер защиты информации напрямую зависит от требуемого уровня защищенности персональных данных, который был определен для персональных данных, обрабатываемых в школе. В качестве начального выбирается один из четырех базовых наборов мер защиты информации из приложения к приказу ФСТЭК России.

Требования базового набора мер защиты являются минимальными требованиями, выполнение которых должно быть обеспечено, если эта мера не исключена на последующем этапе (этап адаптации базового набора мер защиты). Содержание каждой базовой меры защиты информации можно найти в приказе ФСТЭК России.

Состав и содержание базового набора мер защиты для 3 уровня защищенности персональных данных, а также способы их реализации и типы необходимых технических средств защиты приведен в Приложении № 8.

#### *Адаптация базового набора мер.*

Вторым шагом после является изменение начально выбранного базового набора мер защиты в части его максимальной адаптации к структуре школьной информационной системы и особенностям ее эксплуатации. При адаптации базового набора мер защиты информации надо учитывать:

* цели и задачи защиты персональных данных в информационной системе;
* мероприятия проводимые по обеспечению безопасности в школе в целом;
* применяемые информационные технологии и структурно-функциональные характеристики информационной системы.

Адаптация базового набора мер защиты предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе. Например, в школьной информационной системе при обработке персональных данных не используются технологии виртуализации или беспроводного подключения компьютеров. В этом случае все меры, направленные на защиту среды виртуализации или каналов беспроводного доступа и приведенные в базовом наборе мер защиты, могут быть исключены. Нам этом этапе набор мер защиты может существенно сократиться по сравнению с базовым.

#### *Уточнение адаптированного набора мер.*

После адаптации базового набора мер, проводится уточнение адаптированного набора мер защиты информации. Это делается для того, чтобы оценить возможности этого набора мер защиты информации адекватно блокировать (нейтрализовать) все актуальные угрозы безопасности, включенные в модель угроз, или, по крайней мере, снизить вероятность их реализации исходя из условий функционирования информационной системы. Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень актуальных угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

При уточнении адаптированного набора мер защиты информации для каждой угрозы безопасности информации, включенной модель угроз, из адаптированного набора мер защиты информации сопоставляется мера защиты информации, обеспечивающая блокирование этой угрозы или снижающая вероятность ее реализации. В случае, если адаптированный набор мер защиты информации не обеспечивает перекрытие всех угроз безопасности информации в него включаются дополнительные меры защиты информации, покрывающие эти угрозы. Такие меры выбираются из состава мер, приведенных в приложении к приказу ФСТЭК России для соответствующего уровня защищенности персональных данных. При этом содержание такой меры защиты информации определяется с учетом потенциала нарушителя. В результате этих действий, вполне вероятно, что набор мер защиты будет расширен.

На этом же этапе проводится выбор компенсирующих мер блокирования (нейтрализации) актуальных угроз безопасности и обоснование необходимости их реализации.

#### *Дополнение уточненного адаптированного набора мер.*

Если в информационной системе кроме персональных данных обрабатывается другая информация, для которой законами установлены особые требования по защите (например, в бухгалтерии наряду с фамилией именем и отчеством работников школы может обрабатываться информация, отнесенная к банковской или налоговой тайне), то в этом случае уточненный адаптированный набор мер надо дополнить специфическими мерами, обеспечивающими выполнение особых требований, если они не перекрываются уже выбранными.

При дополнении уточненного адаптированного набора мер защиты может быть обосновано, что меры защиты информации, включенные в уточненный адаптированный набор мер защиты информации, достаточны для выполнения требования, установленного специальными нормативными актами и в этом случае дополнение уточненного адаптированного базового набора мер защиты не требуется. А может быть потребуется усиление требований к некоторым мерам защиты, ранее включенным в уточненный адаптированный набор мер, и обоснование их достаточности для выполнения установленного нормативным актом требования.

### *Выбираем средства защиты информации.*

Некоторые меры защиты информации требуют технической реализации, то есть использования встроенных в программное обеспечение специальных функций безопасности, либо применения дополнительных средств защиты. Согласно требованиям регуляторов, все средства защиты информации, используемые для защиты персональных данных должны пройти обязательную процедуру оценки соответствия требованиям законодательства РФ по безопасности информации. Такая оценка проводится в форме сертификации средств защиты. Поэтому для выбора средств защиты целесообразно использовать Реестры средств защиты информации, прошедших сертификацию и публикуемых на официальных сайтах ФСТЭК России и ФСБ России.

При оценке (сертификации) средств защиты определяется тот набор функций безопасности, которые они могут реализовать. В зависимости от набора этих функций, средствам защиты присваивается класс защищенности в зависимости от их предназначения. Для каждого уровня защищенности персональных данных требуются средства защиты определенного класса. Для облегчения выбора нужного средства защиты, в Приложении № 6 указаны типы средств защиты, которые можно использовать для реализации мер защиты для 3 уровня защищенности персональных данных, а в Приложении № 7 дано соотношение классов средств защиты с требуемыми уровнями защищенности персональных данных.

## Что должно получиться?

В результате работы по проведению инвентаризации информационных ресурсов, выбору требуемого уровня защищенности персональных данных, определения набора мер защиты, должен появиться следующий набор документов:

* Модель актуальных угроз безопасности персональным данным;
* Перечень персональных данных, обрабатываемых в образовательном учреждении;
* Перечень персональных данных, обрабатываемых без использования средств автоматизации;
* Перечень школьных информационных систем, обрабатывающих персональные данные с указанием требуемого уровня защищенности;
* Состав средств обработки персональных данных, входящих в состав информационных систем;
* Перечень мер защиты, подлежащих реализации при обработке персональных данных в образовательном учреждении;
* Перечень типов средств защиты информации, которые необходимо использовать в школьных информационных системах для реализации мер защиты персональных данных.

Таким образом, в результате реализации первых этапов, собраны необходимые исходные данные, определен требуемый уровень безопасности персональных данных и выбраны необходимые меры защиты. Этого вполне достаточно, чтобы приступить непосредственно к созданию в школе системы защиты персональных данных. Как уже отмечалось, такая система должна объединять организационную и техническую составляющие.

### *Организационная составляющая.*

Организационная составляющая представляет собой систему локальных нормативных актов, определяющих политику обработки и защиты персональных данных в школе и направленных на реализацию выбранных организационных мер защиты. Эти документы формируют политику школы в части обработки и обеспечения безопасности персональных данных. В общем случае, документы, формирующие политику безопасности персональных данных должны разрабатываться на основе принципов:

* максимальной дружественности к персоналу,
* персональной ответственности,
* минимизации привилегий,
* разделения обязанностей,
* разумной достаточности.

Каждая школа имеет устоявшуюся организационную структуру, управление, подчинение подразделений, распределение функциональных обязанностей, сложившиеся традиции делового общения и обмена информацией в ходе обеспечения учебного процесса и жизнедеятельности школы. Формирование организационной составляющей, как правило, сводится к тому, что в рамках существующей организационной структуры школы уточняются роли каждого субъекта в решении задач защиты персональных данных, пересматриваются функциональные обязанности и должностные инструкции, устанавливается персональная ответственность, налаживается взаимодействие.

#### *Состав основных организационно-распорядительных документов.*

Документы, формирующие политику безопасности персональных данных должны охватить множество аспектов, в том числе:

* нормативное урегулирование процесса обмена персональными данными между участниками информационного обмена;
* установление организационно-правового режима использования информационных ресурсов и ответственности субъектов за соблюдение этого режима;
* реализацию комплекса организационных и технических мер обеспечению конфиденциальности целостности и доступности персональных данных;
* предоставление персоналу школы необходимых сведений для сознательного поддержания установленного уровня защищенности персональных данных;
* организацию постоянного контроля эффективности принятых мер защиты и функционирования системы защиты персональных данных;
* создание резервов и возможностей по ликвидации последствий нарушения режима защиты персональных данных и восстановления их безопасности.

Примерный состав документов, необходимых для организации защиты персональных данных в школе приведен в Приложении № 9.

#### *Регламент обеспечения безопасности информации.*

Одним из важнейших документов является Регламент обеспечения безопасности информации. Именно этот документ определяют общие правила разграничения доступа к информационным ресурсам, основные обязанности и ответственность конкретных субъектов за обеспечение безопасности персональных данных с учетом сложившегося делового стиля общения при информационном обмене. Как правило, Регламент устанавливает:

* правила обеспечения режима защиты персональных данных;
* роли и ответственность персонала школы за обеспечение безопасности персональных данных, требования по соблюдению конфиденциальности;
* правила регистрации пользователей школьных информационных систем и назначения им прав доступа;
* процедуры управления информационными ресурсами в соответствии с установленными правилами разграничения доступа;
* правила работы пользователей с защищаемыми информационными ресурсами, меры по поддержанию требуемого порядка допуска к операциям с информацией
* порядок организации физической защиты средств обработки персональных данных;
* порядок проведения регламентных работ и сервисного обслуживания на оборудовании школьных информационных систем;
* порядок контроля режима защиты персональных данных и реагирования на нарушения режима защиты (разбор инцидентов);
* порядок ликвидации последствий при возникновении нештатных ситуаций и нарушении установленного режима защиты.

#### *Рекомендации по разработке организационно-распорядительных документов.*

Чтобы не запутаться и чего-нибудь не пропустить, при подготовке организационно-распорядительных документов:

* уясните какие вопросы обеспечения безопасности персональных данных подлежат регулированию предполагаемым к разработке локальным нормативным актом;
* уясните с учетом правомочий субъектов информационных отношений к чьей компетенции относятся вопросы, подлежащие регулированию;
* выберите, тип организационно-распорядительного документа, подлежащего к разработке;
* ознакомьтесь с «Примерным рекомендуемым перечнем документов, которые необходимы для обеспечения защиты персональных данных» (см. Приложение) и уточните какие из уже разработанных в школе локальных нормативных актов могут содержать нормы, затрагивающие предполагаемую область регулирования;
* сформулируйте необходимые для регулирования отношений нормы, учитывая требуемый состав мер защиты, уже имеющиеся документы, и подготовьте проект локального нормативного акта;
* проверьте, есть ли действующие нормативные документы, регулирующие аналогичные или смежные вопросы, оцените необходимость внесения в них изменений и подготовьте такие изменения;
* определите (при необходимости) состав дополнительных документов более низкого уровня, которые необходимо разработать в развитие положений проекта локального нормативного акта.

### *Техническая составляющая*

Техническая составляющая системы защиты персональных данных направлена на реализацию технических мер защиты информации и формируется на следующих основных принципах:

* системности и комплексности;
* максимальной дружественности к персоналу;
* оптимальности и разумной разнородности;
* простоты применения;
* разумной достаточности.

В состав технической составляющей включаются различные технические программные и программно-аппаратные устройства, в том числе и криптографические, а также средства контроля и управления, реализующие те или иные механизмы защиты информации. Формирование этой составляющей в основном, сводится к техническому проектированию и построению системы защиты информационной системы , соответствующей установленному уровню защищенности персональных данных. Средства защиты позволяют локализовать защищаемые информационные ресурсы, обеспечить к ним санкционированный доступ, защитить персональные данные при передаче по каналам связи. Результатом реализации технических мер защиты персональных данных должно быть:

* снижение вероятности реализации актуальных угроз персональным данным;
* поддержание полноты и неизменности информационных ресурсов, задействованных в обработке персональных данных;
* определение подлинности субъекта доступа и отслеживание действий всех субъектов информационных отношений.

Проектирование системы защиты, реализующей установленные технические меры – процесс сложный. В частности он предполагает:

* разработку решений по применению средств защиты и средств контроля;
* разработку технического проекта системы защиты информации;
* разработку рабочей документации системы защиты информации;
* организацию поставки средств защиты информации;
* тестирование технических средств и программного обеспечения.
* реализацию проектных решений;
* проверку способности персонала обеспечить функционирование системы защиты;
* настройка и наладка технических и программных средств защиты информации;
* Оценка эффективности реализованных технических мер защиты.

Разработка проектной и рабочей конструкторской документации систему защиты персональных данных, реализующую технические меры крайне важна и этим этапом нельзя пренебрегать. Она не только фиксирует состояние системы на момент ее создания, но и все изменения, которые могут произойти в процессе ее эксплуатации. С одной стороны наличие такой документации позволит обосновать перед надзорными органами правильность реализации технических мер защиты в случае возникновения инцидентов, а с другой стороны – позволит найти и устранить любые неисправности в системе защиты персональных данных даже в случае увольнения сотрудников, непосредственно участвовавших в ее создании, настройке и наладке. Кроме того, такая документация позволяет производить периодическую проверку работоспособности и правильности настройки средств защиты, которая определена документами регуляторов[[46]](#footnote-46).

Отметим, что несмотря на то, что в настоящее время многими производителями средств защиты разработаны различные типовые решения по защите информации, в школе не всегда имеются специалисты, способные правильно и грамотно спроектировать систему защиты персональных данных. Поэтому, по всей вероятности, для выполнения данных работ потребуется привлечение специализированных организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

## На что надо обратить внимание.

Нюансов, которые возникают при обработке персональных данных в школьных информационных системах, достаточно много. Остановимся только на нескольких моментах.

### *Как и зачем оптимизировать обработку персональных данных?*

Оптимизация процесса обработки персональных данных позволяет значительно сократить расходы на обеспечение их безопасности и упростить систему защиты. В результате оптимизации может измениться категория персональных данных, что приводит и к изменению состава мер защиты. Оптимизация может быть проведена следующими методами:

* методом исключения из обработки лишних персональных данных;
* методом сегментирования информационной системы;
* методом обезличивания персональных данных.

Оптимизация процесса обработки персональных данных проводится по результатами проведенной ревизии информационных ресурсов.

#### *Исключение из обработки лишних персональных данных.*

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки[[47]](#footnote-47). В результате проведенной ревизии информационных ресурсов, наверняка выявятся факты излишнего количества обрабатываемых персональных данных, которые не требуются для достижения заявленных целей обработки. Например, в школе в дополнение к охраннику используется СКУД – система контроля и управления доступом в помещения (электронный турникет на входе, к которому каждый входящий прикладывает свою персональную электронную карточку-пропуск). Часто на пропуске наносится фотография ученика или сотрудника с указанием его фамилии, имени, отчества, класса и пр. Эти данные содержат в себе биометрические персональные данные (фото) и в совокупности позволяют охраннику идентифицировать входящего, а сама СКУД в этом случае будет относится к информационным системам обработки биометрических персональных данных для идентификации субъекта, что потребует получения письменного согласия субъекта на обработку и принятия дополнительных мер защиты к самой СКУД.

Вместе с тем, собственно права на вход в школу определяются той специальной информацией, которая содержится в электронной карточке и, как правило, не связывается непосредственно с личностью входящего. Охраннику важно определить, что карточка, позволяющая войти в школу, принадлежит именно тому субъекту, который входит и это он может сделать по фотографии на карточке. При этом, ему совсем не обязательно знать как зовут этого субъекта. Следовательно, такие персональные данные, как фамилия, имя, отчество (идентификационные персональные данные) для обработки с целью организации в школе пропускного режима не требуются. Если убрать с электронной карточки-пропуска и из СКУД идентификационные персональные данные, такая информационная система перестает быть системой, обрабатывающей биометрические персональные данные для идентификации субъекта. Следовательно, не требуется наличия письменного согласия субъекта, а меры защиты СКУД будут минимальными. В результате исключения из процесса обработки излишних для достижения поставленной цели (пропуск на территорию школы) персональных данных, изменилась категория персональных данных и тип информационной системы.

Внимательное изучение существующих в школе процессов обработки персональных данных в разных случаях позволяет значительно сократить объем обрабатываемых персональных данных и, тем самым, выполнить установленные законом условия обработки персональных данных и сократить расходы на защиту.

#### *Сегментирование информационной системы.*

Разделение информационной системы на несколько сегментов позволяет с одной стороны выполнить условие закона, запрещающего объединять в единых базах данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой[[48]](#footnote-48). С другой стороны сегментирование позволяет ограничить количество средств обработки информации, требующих применения технических мер защиты, что приводит к упрощению системы защиты. В добавок, сегментирование позволяет ограничить количество пользователей, имеющих возможность доступа к персональным данным, которые не требуются им для исполнения своих функциональных обязанностей.

Под выделенным сегментом, предназначенным для обработки персональных данных понимается ограниченная для доступа неуполномоченных пользователей часть информационной системы, объединяющая защищаемые информационные ресурсы, средства обработки и отображения информации, используемые для их обработки, элементы телекоммуникационной инфраструктуры, предназначенные для обмена данными между элементами сегмента и пограничные коммутирующие устройства. Границей сегмента является внешний порт того самого пограничного коммутирующего устройства, которое соединяет сегмент с остальной информационной системой. Практически получается, что сегмент это маленькая локальная сеть, сопряженная с информационной системой по определенным правилам доступ к которой «чужим» пользователям заказан.

Сегментирование информационной системы может проводиться по разным признакам. К примеру, информационная система в которой одновременно обрабатывается бухгалтерская информация, информация кадрового отдела, данные необходимые для обеспечения процесса обучения, можно разделить на специальные сегменты, объединяющие пользователей бухгалтерии, службы кадров, учителей и так далее. Такое деление называется сегментированием по функциональному признаку.

Сегментирование информационных систем может быть выполнено на физическом уровне, когда обосабливаются непосредственно средства обработки информации, или на логическом уровне, когда разделение на сегменты происходит с использованием технологий создания обособленных виртуальных локальных сетей (VLAN). Применение того или иного способа зависит прежде всего от используемых в школьных системах информационных технологий и удобства для персонала школы.

#### *Обезличивание персональных данных.*

Обезличивание персональных данных позволяет значительно снизить затраты на их защиту за счет разделения всего массива персональных данных на два: небольшой массив идентификационных персональных данных, подлежащий защите и основной массив данных, который не требует защиты от несанкционированного использования. Обезличивание персональных данных должно обеспечивать не только их защиту от несанкционированного использования, но и позволять проводить их обработку. Процесс обезличивания персональных данных определяется нормативными документами[[49]](#footnote-49) и представляет собой процедуру выделения идентификационных персональных данных из общего массива персональных данных и замены их специальными идентификаторами. При этом формируется таблица соответствия идентификаторов идентификационным персональным данным (ключевая база данных). Эта база позволяет, при необходимости, провести обратную процедуру и соотнести данные с конкретным субъектом.

Для обезличенных данных защита не требуется, так как их нельзя соотнести с субъектом и ущерба ему от несанкционированных действий с ними не будет. В то же время, казалось бы, что ущерб от разглашения идентификационных данных для субъекта – минимальный и по этой причине вполне логично было бы установить для такой базы минимальный уровень защищенности. Но это неверно. Ущерб в этом случае надо оценивать не относительно несанкционированных действий со сведениями, хранящихся в ней, а от несанкционированных действий со всем массивом данных о субъекте, который можно получить с использованием сведений из ключевой базы. То есть уровень защищенности ключевой базы должен быть не ниже уровня защищенности всего не обезличенного массива сведений о субъекте. Ключевая база должна храниться отдельно от обезличенного массива данных, полностью должна быть защищена и к ней должен быть ограничен доступ пользователей.

В качестве идентификатора могут быть использованы, например, идентификационные номера свидетельства о присвоении индивидуального номера налогоплательщика (ИНН), страхового свидетельства государственного пенсионного страхования (СНИЛС), свидетельства об обязательном медицинском страховании (ОМС) или порядкового номера карточки-пропуска (при условии, что в информационной системе СКУД не хранятся идентификационные данные). Могут быть использованы и любые другие разработанные самостоятельно идентификаторы.

Особенно актуален процесс обезличивания для специальных категорий персональных данных, требующих особой защиты. Например, все сведения о медицинских манипуляциях с пациентами в школьном медицинском пункте (кабинете) могут храниться не по фамилии, имени, отчеству, а по номеру СНИЛС, свидетельства ОМС или по специально разработанному идентификатору. Предъявляя такой идентификатор, пациент может получить необходимую медицинскую услугу, а медицинский работник может в обезличенном массиве данных отыскать и выделить те, которые относятся к истории болезни конкретного пациента. Либо наоборот, обратившись за медицинской услугой пациент может назвать свою фамилию и имя, а медицинский работник, обратившись к ключевой базе определить его идентификатор и затем, перейдя в массив обезличенных данных выбрать необходимую историю болезней или запись.

### *О личных компьютерах учителей.*

В последнее время отмечается широкое использование личных гаджетов сотрудников для доступа к ресурсам корпоративных информационных систем – так называемый сценарий BYOD (*Bring Your Own Device*). Вполне естественно, что и учителя стремятся использовать новейшие информационные технологии в своей деятельности. И некоторые из них используют свои личные компьютеры, планшетники и смартфоны для подготовки материалов, необходимых в учебном процессе. Нередко подготовка таких материалов сопряжена с обработкой персональных данных учеников. Все это повышает риск нарушения правил обработки персональных данных и причинения ущерба субъектам. Необходимо отметить, что ответственность за нарушения правил обработки персональных данных, доверенных субъектами образовательному учреждению, остается в первую очередь за самим образовательным учреждением[[50]](#footnote-50). Если кто-то из учителей случайно потеряет планшетник на котором хранятся персональные данные учеников, штрафные санкции будут наложены на школу и ее руководителя, как ответственн6ого должностного лица. Поэтому обработка персональных данных учеников на личных компьютерах, планшетниках и других гаджетах учителей – недопустима. При проведении ревизии школьных информационных ресурсов необходимо обратить особое внимание на этот факт и постараться исключить нарушения в правилах обработки персональных данных.

### *Аутсорсинг обработки персональных данных*

В школе часто встречаются случаи, когда обработка персональных данных передается третьему лицу (аутсорсеру). К примеру это может быть в случаях:

* организации бухгалтерского учета;
* обеспечения кадровой работы (управления персоналом);
* обеспечения обязательного и добровольного медицинского страхования;
* обеспечения взаимодействия с пенсионными фондами;
* обеспечения банковского обслуживания персонала школы (зарплатные карты).

Закон предусматривает, что отношения с обработчиком (аутсорсером) строятся на договорной основе и определяет существенные условия такого договора: обязанность обработчика (аутсорсера) соблюдать законные принципы обработки персональных данных и обеспечивать их конфиденциальность и безопасность обработке. Юридической основой взаимоотношений оператора и аутсорсера является договор поручения или договор возмездного оказания услуг (в зависимости от характера действий, совершаемых с персональными данными).

Закон накладывает определенные общие обязанности и на оператора, которые не исчезают с появлением аутсорсера. Ответственность за организацию защиты всегда остается за оператором. Еще до передачи персональных данных для обработки, оператор обязан убедиться, что аутсорсер готов к их обработке и защите. Поэтому договор должен содержать ряд условий, которые должен выполнить аутсорсер и при выполнении которых возможно начало обработки информации. Невыполнение этих условий в установленный оператором срок, должно рассматриваться, как достаточное условие одностороннего расторжения договора со стороны оператора. В договор целесообразно включать требования к аутсорсеру:

* не раскрывать третьим лицам доверенные ему персональные данные;
* принять технические и организационные меры защиты;
* установить правила доступа к персональным данным;
* провести до начала обработки оценку эффективности принятых им мер защиты;
* предоставить оператору право осуществлять проверку порядка обработки персональных данных.

Форма и рамки договора не позволяют включить всю необходимую для защиты персональных данных информацию. Поэтому оператор должен подготовить специальное поручение аутсорсеру (обработчику), которое является необъемлемой частью договора с аутсорсером и включает в себя:

* цель обработки и состав персональных данных, подлежащих обработке;
* перечень действий (операций), которые совершаются в ходе обработки;
* требуемый уровень защищенности персональных данных, который должен быть достигнут;
* состав конкретных требований по защите персональных данных;
* порядок уничтожения или обезличивания персональных по завершении обработки;
* порядок оценки эффективности принятых мер защиты.

# Приложения.

## *Приложение 1.* Основные нормативные правовые акты, по обеспечению безопасности персональных данных в школе

Перечень основных нормативных правовых актов

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. ETS № 108. Страсбург, 1981 г.

Конституция Российской Федерации

Федеральный закон № 223-ФЗ, 1995 г. «Семейный кодекс РФ (СК РФ)» (ст. ст. 15, 139)

Федеральный закон № 197-ФЗ, 2001 г. «Трудовой кодекс РФ (ТК РФ)» (гл. 14)

Федеральный закон № 195-ФЗ, 2001 г. «Кодекс РФ об административных правонарушениях (КоАП)»

Федеральный закон № 152-ФЗ, 2006 г. «О персональных данных» (в ред. № 261-ФЗ, 2011 г.)

Федеральный Закон № 149-ФЗ, 2006 г. «Об информации, информационных технологиях и защите информации»

Федеральный закон № 27-ФЗ, 1996 г. «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования» (ст. ст. 2, 6)

Федеральный закон № 326-ФЗ, 2010 г. «Об обязательном медицинском страховании в РФ» (ст. 47)

Федеральный закон № 323-ФЗ, 2011 г. «Об основах охраны здоровья граждан в РФ» (ст. ст. 13, 92)

Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ Роскомнадзора от 05.09.2013 г. № 996 «Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе функционирующих в рамках федеральных целевых программ»

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008 г.

Краткий анализ Федерального закона № 152-ФЗ «О персональных данных»

Закон «О персональных данных[[51]](#footnote-51)» находится на перепутье между публичными и частными федеральными законами. С одной стороны он регулирует весьма узкую и специфическую область отношений – обработку и защиту персональных данных и поэтому может считаться частным, а с другой стороны, эта узкая область затрагивает интересы каждого гражданина и поэтому его можно отнести к публичным.

Защита конституционных прав и свобод гражданина – одна из важнейших функций государства. Обеспечивая защиту персональных данных, государство тем самым создает благоприятную обстановку для всестороннего развития граждан и общества в целом. Этот закон является базовым, устанавливающим критерии законности действий, связанных с обработкой персональных данных, а также пределы ограничения прав субъектов персональных данных.

Надо сказать, что это уже вторая редакция закона. Новая редакция максимально приближена по своим положениям к нормам международного права[[52]](#footnote-52). В новой редакции закона уточнена сфера его действия используемые в нём основные понятия. Существенно уточнены принципы и условия обработки персональных данных. Переработаны нормы, регламентирующие права и обязанности оператора, взаимоотношения оператора и субъекта, вопросы трансграничной передачи данных, меры по обеспечению безопасности персональных данных. Хотя концепция закона не изменилась, он получил существенно новое наполнение.

Закон основан на конституционных положениях, гарантирующих защиту прав на неприкосновенность частной жизни, личную и семейную тайну[[53]](#footnote-53), запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия[[54]](#footnote-54), возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы человека[[55]](#footnote-55), право свободно искать, получать, передавать, производить и распространять информацию любым законным способом[[56]](#footnote-56).

Закон устанавливает унифицированные правила сбора и обработки персональных данных, а также правовые механизмы защиты прав граждан при сборе и обработке персональных данных. Сферой действия закона являются отношения, связанные с обработкой персональных данных, с использованием средств автоматизации или без использования таковых[[57]](#footnote-57).

В новой редакции закона изменен статус принципов обработки персональных данных, каждый принцип уточнен и выведен в самостоятельную часть статьи[[58]](#footnote-58). Акцент сделан на законность обработки персональных данных и соответствие содержания и объема персональных данных целям обработки. Хотя в Законе в прямую не сказано, но, по смыслу, введено понятие «обработчик»: оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта на основании поручения оператора. Такое лицо обязано соблюдать принципы и правила обработки персональных данных, но не обязано получать согласие субъекта. Ответственность перед субъектом за действия указанного лица несет оператор[[59]](#footnote-59). В законе даны существенные условия договора с «обработчиком».

Главным условием обработки персональных данных является то, что субъект персональных данных самостоятельно принимает решение о предоставлении кому-либо своих персональных данных (наличие согласия субъекта) и, вместе с тем, в новой редакции существенно расширен перечень случаев, когда не требуется согласие субъекта на обработку персональных данных, в частности, согласия не требуется, если обработка осуществляется[[60]](#footnote-60):

* для исполнения судебного акта,
* для предоставления государственной или муниципальной услуги,
* для регистрации субъекта на портале государственных услуг,
* для заключения договора по инициативе субъекта,
* для реализации прав и законных интересов оператора и третьих лиц,
* для достижения общественно значимых целей,
* для законной деятельности средства массовой информации.

Обязанность предоставить доказательство получения согласия субъекта на обработку его персональных данных или доказательство того, что имеется случай, когда согласия субъекта не требуется, возлагается на оператора.

Закон дополнил содержание и самого понятия «согласие субъекта на обработку персональных данных». Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом[[61]](#footnote-61). Эти изменения позволяют применить для выражения согласия конклюдентные действия.

Всем операторам, обрабатывающим персональные данные вменена законом обязанность соблюдения их конфиденциальности. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом[[62]](#footnote-62). При этом, раскрытие персональных данных определенному лицу или определенному кругу лиц в обеспечение конфиденциальности не входит.

Кроме того, рядом положений настоящего Закона установлен особый правовой режим защиты специальных категорий персональных данных, в числе которых называются сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни[[63]](#footnote-63). Действия с этими персональными данными без должных гарантий обеспечения прав субъекта персональных данных могут нанести ему повышенный ущерб.

При обработке биометрических персональных данных акцент перенесен на факте использования данных для установления личности субъекта. Биометрические персональные данные это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта[[64]](#footnote-64). Биометрические персональные данные это объективное понятие, не зависящие ни от субъективных факторов, ни от способа их обработки, ни от целей их обработки. Они могут обрабатываться только при наличии письменного согласия субъекта. Но, если, например, в информационной хранится фото, но не используется для идентификации субъекта, оно не переставая быть биометрическими персональными данными, не требует получения письменного согласия субъекта для обработки.

Законом также закреплены права субъекта персональных данных[[65]](#footnote-65). Субъект вправе требовать от оператора уточнения персональных данных, их блокирования или уничтожения, если информация является неполной, устаревшей, неточной, незаконно полученной или не требуется для заявленной цели обработки. Хотя , в некоторых случаях. Права субъекта могут быть и ограничены. Между тем, субъект вправе принимать законные меры по защите своих прав.

Впервые в российской практике, для обеспечения защиты прав субъектов, закон вводит специальный институт уполномоченных по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям закона[[66]](#footnote-66).

Для нашей предметной области (защиты персональных данных) наиболее интересны положения главы 4 данного закона, которые определяют обязанности оператора, в том числе и по организации защиты персональных данных при их обработке. Закон содержит императивную норму, обязывающую оператора применять правовые, организационные и технические мер по обеспечению безопасности персональных данных[[67]](#footnote-67). При этом, государство, пользуясь своим конституционным правом[[68]](#footnote-68), определяет, что уровни защищенности и требования по защите персональных данных устанавливает Правительство РФ с учетом возможного вреда субъекту, объема и содержания обрабатываемой информации и актуальности угроз, а состав и содержание требований к защите персональных данных устанавливаются уполномоченными федеральными органами исполнительной власти[[69]](#footnote-69). В отличие от предыдущей редакции, в этом законе некоторые положения, касающиеся обеспечения безопасности персональных данных, были подняты с уровня подзаконных актов на уровень закона, в частности, необходимость моделирования угроз безопасности, обязательность применения организационных и технических мер защиты персональных данных, обязательность применения средств защиты, которые прошли процедуру оценки соответствия установленным требованиям.

Надо так же отметить, что впервые на законодательном уровне определено, что такое угроза безопасности персональных данных и уровень защищенности персональных данных[[70]](#footnote-70).

Определив, что моральный вред, причиненный субъекту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных законом, а также требований к защите персональных данных, установленных в соответствии с законом, подлежит возмещению в соответствии с законодательством Российской Федерации, закон позволяет применить для возмещения вреда положения Гражданского кодекса РФ[[71]](#footnote-71). При этом, возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

*Приложение 2.* Примерный перечень документов (ресурсов) обрабатываемых в школе, где могут находиться персональные данные

Документы, в которых могут находится персональные данные постоянного состава школы (персонал):

Копия паспортных данных работника

Копия свидетельства о присвоении индивидуального номера налогоплательщика (ИНН)

Копия страхового свидетельства государственного пенсионного страхования (СНИЛС)

Копия свидетельства об обязательном медицинском страховании (ОМС)

Копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву)

Копия документа об образовании

Копия документа о квалификации

Копия документа о наличии специальных знаний

Копия свидетельства о присвоении ученой степени

Документы, заполненные и представленные работником при поступлении на работу или в процессе работы:

 Анкеты

Автобиография

Личная карточка (форма Т-2)

 Документы о семейном положении работника

 Документы о перемене фамилии

 Документы о наличии детей и иждивенцев

 Справки с прежнего места работы

 Заявления о приеме на работу, об отпуске, о получении льгот

Справки о судимости или ее отсутствии, копии приговоров суда

Документы о возрасте малолетних детей и мете их обучения,

Документы о состоянии здоровья детей и родственников:

 Справки об инвалидности

 Справки о наличии хронических заболеваний и др.

Документы о состоянии здоровья работника:

 Листки временной нетрудоспособности

 Документы об инвалидности

 Документы о беременности и др.

Медицинские заключения о результатах обязательных и периодических медосмотрах

Документы добровольного медицинского страхования (ДМС)

Трудовой договор

Трудовая книжка

Документы бухгалтерского делопроизводства:

 Ведомости начисления и выплаты заработной платы

Табели учета рабочего времени

Распоряжения и договоры о перечислении заработной платы на счета и карты

Исполнительные листы

Командировочные предписания

Заключение по данным психологического исследования

Приказы о приеме, переводах, увольнении, повышении заработной платы,

Приказы о премировании, поощрении и взыскании

Объяснительные записки, служебные записки работника

Документы о прохождении аттестации

Документы по повышении квалификации

Служебные записки и документы о результатах служебных расследований

Общие списки сотрудников

Расписания занятий

Учетные карточки школьных библиотек

Видеозаписи программ школьного телевидения

Фотографии

Документы, в которых могут находится персональные данные переменного состава школы (учащихся):

Копии документов, удостоверяющих личность учащегося:

 Копии свидетельства о рождении

 Копии паспортных данных

Копии документов о семье обучающегося:

Копии документов о месте проживания

Копии документов о составе семьи

Копии паспортных данных родителей (законных представителей)

Документы о месте работы членов семьи

Документы о способах связи с родителями (законными представителями) в критических ситуациях

Документы, подтверждающие права на дополнительные гарантии и компенсации

 Документы о наличии родителей-инвалидов

 Документы о наличии неполной семьи

 Документы подтверждающие сиротство

Документы о получении образования, необходимого для поступления в соответствующий класс:

 Личное дело учащегося с предыдущего места обучения

 Справки с предыдущего места обучения

Характеристики

 Оценочные ведомости

 Заключения по результатам собеседования и тестирования

Копия страхового свидетельства государственного пенсионного страхования (СНИЛС)

Копия свидетельства об обязательном медицинском страховании (ОМС)

Документы о состоянии здоровья учащегося:

 Документы об инвалидности

 Документы о наличии хронических заболеваний

 Журналы обращений за медицинской помощью

Документы о сделанных прививках и профилактических мероприятиях

Медицинские заключения по результатам обследований и медицинских осмотрах

 Медицинские заключения об отсутствии противопоказаний для обучения

Документы добровольного медицинского страхования (ДМС)

Приказы о зачислении и исключении из образовательного учреждения

Общие списки учащихся

Учетные карточки школьных библиотек

Видеозаписи программ школьного телевидения

Фотографии

Документы, формируемые в ходе учебного процесса

 Классные журналы, в том числе электронные

 Дневники учащегося, в том числе электронные

 Зачетные ведомости, табели

 Унифицированные списки сдавших или сдающих единый государственный экзамен

 Документы, содержащие результаты единого государственного экзамена

 Сочинения на личные и семейные темы

Документы, в которых могут находится персональные данные субъектов, не относящихся к школе:

Списки попечительского совета

Списки ветеранов

Архивные документы школьных музеев

Договоры с подрядными организациями

….

## *Приложение 3.* Статус организаций по отношению к персональным данным, обрабатываемым в школе

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Информационные ресурсы,****содержащие ПДн** | **Цель обработки** | **Школа** | **Вышестоящая организация** | **Учащиеся,** **родители** | **Учителя,** **преподаватели** | **Внешние** **организации** |
| Классные журналы, ведомости, тетради и дневники учащихся, анкеты, характеристики и личные дела учащихся, электронные дневники, школьные сайты, школьные информационные системы и системы дистанционного обучения, | Обработка персональных данных учащихся, их законных представителей и учителей для целей обеспечения учебного процесса | Оператор | Обработчик | Субъект | Субъект | Не используют |
| Специальные системы вышестоящих организаций (Школьный офис, Карта учащегося, База данных ЕГЭ и др.) | Обработка персональных данных для статистических целей и целей, определяемых вышестоящей организацией | Обработчик | Оператор | Субъект | Субъект | Не используют |
| Системы видеонаблюдения и системы контроля и управления доступом в помещения школы | Общее наблюдение за обстановкой на объекте, обнаружение фактов нарушения установленного режима безопасности и фиксации таких фактов, контроль пребывания учащихся в школе | Обработчик | Не используют | Субъект | Субъект | Оператор (охранные организации) |
| Бухгалтерские системы и системы кадровой службы и школьного делопроизводства | Обработка персональных данных персонала школы в целях исполнения трудового договора | Обработчик | Обработчик | Не используют | Субъект | Оператор (централизованная бухгалтерия, органы ОМС и ДМС) |
| Медицинские карты, электронные истории болезней | Обработка специальных персональных данных учащихся для защиты их жизни и здоровья | Оператор | Не используют | Субъект | Не используют | Обработчики (медучреждения) |
| Школьное делопроизводство | Обработка персональных данных персонала внешних организаций в целях исполнения гражданско-правового договора, стороной которого является субъект | Оператор | Не используют | Не используют | Не используют | Субъект |

*Приложение 4.* Примерные алгоритмы действий

Алгоритм действий по проведению инвентаризации информационных ресурсов школы



Алгоритм действий по определению уровня защищенности персональных данных и выбору мер их защиты.



## *Приложение 5.* Таблица выбора уровней защищенности персональных данных по Постановлению Правительства РФ № 1119 от 01.11.2012 г.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Уровень защищенности**  **Критерии выбора уровня защищенности** | **1-й** **уровень**  | **2-й** **уровень**  | **3-й** **уровень**  | **4-й** **уровень**  |
|
| **По принадлежности к оператору** | **По кол-ву субъектов** | **По содержанию** **обрабатываемых ПДн** | **По типу угроз** |
| Обрабатываются ПДн**не сотрудников** **оператора**  | мене 100 000 | Специальные ПДн | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| Биометрические ПДн | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| Общедоступные ПДн |   | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |
| Остальные ПДн | Угрозы 1-го типа (НДВ СПО) |   | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |
| более 100 000 | Специальные ПДн | Угрозы 1-го типа  | Угрозы 3-го типа (нет НДВ) |   |   |
| Угрозы 2-го типа |
| Биометрические ПДн | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| Общедоступные ПДн |   | Угрозы 1-го типа  |   | Угрозы 3-го типа (нет НДВ) |
| Угрозы 2-го типа |
| Остальные ПДн | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| Обрабатываются ПДн **только сотрудников** оператора  | **Специальные ПДн** | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| **Биометрические ПДн** | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |   |
| **Общедоступные ПДн** |   | Угрозы 1-го типа (НДВ СПО) | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |
| **Остальные ПДн** | Угрозы 1-го типа (НДВ СПО) |   | Угрозы 2-го типа (НДВ ППО) | Угрозы 3-го типа (нет НДВ) |

## *Приложение 6.* Состав общих мероприятий по защите персональных данных, которые должен выполнить оператор

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Уровень защищенности** **Содержание требования** | **1-й уровень**  | **2-й уровень**  | **3-й уровень**  | **4-й уровень**  |
|
| **Мероприятия по Закону «О персональных данных»** |
| **Издание политики оператора в отношении обработки персональных данных [ст. 181.1.(2)]** | **+** | **+** | **+** | **+** |
| **Применение организационных и технических мер защиты персональных данных [ст.181.1.(3)]** | **+** | **+** | **+** | **+** |
| **Осуществление внутреннего контроля (аудита ) обработки персональных данных [ст.181.1.(4)]** | **+** | **+** | **+** | **+** |
| **Оценка вреда субъектам ПДн при нарушении режима обработки персональных данных [ст. 181.1.(5)]** | **+** | **+** | **+** | **+** |
| **Ознакомление работников с положениями законодательства по персональных данных [181.1.(6)]** | **+** | **+** | **+** | **+** |
| **Оценка эффективности мер безопасности персональных данных до ввода в эксплуатацию [ст. 19.2.(4)]** | **+** | **+** | **+** | **+** |
| **Восстановление персональных данных, модифицированных или уничтоженных вследствие НСД к ним [ст. 19.2.(7)]** | **+** | **+** | **+** | **+** |
| **Установление правил доступа к персональным данным обрабатываемым в информационной системе [19.2.(8)]** | **+** | **+** | **+** | **+** |
| **Регистрация и учет всех действий, совершаемых с персональными данными в информационной системе [19.2.(8)]** | **+** | **+** | **+** | **+** |
| **Контроль мер по обеспечению уровня защищенности персональных данных [19.2.(9)]** | **+** | **+** | **+** | **+** |
| **Мероприятия по Постановлению Правительства РФ № 1119** |
| **Обеспечение режима безопасности помещений информационных систем** | **+** | **+** | **+** | **+** |
| **Обеспечение сохранности носителей с персональными данными** | **+** | **+** | **+** | **+** |
| **Издание Перечня лиц, допущенных к обработке персональных данных** | **+** | **+** | **+** | **+** |
| **Проведение оценки соответствия средств защиты информации, используемых в информационной системе**  | **+** | **+** | **+** | **+** |
| **Назначение должностного лица, ответственного за безопасность персональных данных** | **+** | **+** | **+** |   |
| **Ограничение доступа к содержанию электронного журнала сообщений**  | **+** | **+** | **+** |   |
| **Организация автоматизированной регистрации изменения полномочий**  | **+** |   |   |   |
| **Создание структурного подразделения обеспечения безопасности персональных данных** | **+** |   |   |   |

Цветом в таблице выделены те мероприятия, которые требуют применения специальных средств защиты, то есть наиболее затратные. Остальные мероприятия - организационные.

*Приложение 7.* Соотношение классов средств защиты информации с уровнями защищенности персональных данных

|  |  |  |
| --- | --- | --- |
| **Уровень** **защищённости ПДн** | **Класс защиты СЗИ** | **Уровень контроля ПО СЗИ** **на** **отсутствие** **НДВ** |
| **СВТ** | **САВЗ** | **СОВ** | **МЭ** |
| Угрозы 2 типаили взаимодействие с сетями МИО | Угрозы 3 типаи отсутствие взаимодействия с сетями МИО | Угрозы 2 типаили взаимодействие с сетями МИО | Угрозы 3 типаи отсутствие взаимодействия с сетями МИО | Угрозы 1 и 2 типа иливзаимодействие с сетями МИО | Угрозы 3 типаи отсутствие взаимодействия с сетями МИО |
| **УЗ-1** | Не ниже5 класса | Не ниже 4 класса | Не ниже 4 класса | Не ниже3 класса | Не ниже4 класса | 4 уровень |
| **УЗ-2** |
| **УЗ-3** |   |   |   |   | 4 уровень(в случае актуальности угроз 2 типа) |
| **УЗ-4** | Не ниже6 класса | Не ниже 5 класса | Не ниже 5 класса | 5 класс | **-** |

Сети МИО – сети международного информационного обмена

СЗИ – средства защиты информации

СВТ – средства вычислительной техники

САВЗ – системы антивирусной защиты

СОВ – системы обнаружения вторжений

МЭ- межсетевые экраны

НДВ – недекларированные возможности

*Приложение 8.* Состав и содержание базового набора мер, необходимых для обеспечения 3 уровня защищенности персональных данных и типы средств защиты, реализующих технические меры защиты

| **Условное** **обозначение** **и номер меры** **по Приказу ФСТЭК № 21** | **Содержание мер по обеспечению безопасности  персональных данных** | **Способ реализации мер защиты** | **Тип СЗИ, реализующих технические меры** |
| --- | --- | --- | --- |
| **Организационный** | **Технический** |
|  | **I. Идентификация и аутентификация субъектов и объектов**  |  |  |  |
| **ИАФ.1**  | Идентификация и аутентификация пользователей, являющихся работниками оператора  |  | **+** | Средства ОС (парольная защита) |
| **ИАФ.3**  | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов  | **+** | **+** | Средства ОС |
| **ИАФ.4**  | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации  | **+** |  |  |
| **ИАФ.5**  | Защита обратной связи при вводе аутентификационной информации  |  | **+** | Средства ОС |
| **ИАФ.6**  | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)  |  | **+** | Средства ОС (парольная защита) |
|  | **II. Управление доступом субъектов к объектам доступа**  |  |  |  |
| **УПД.1**  | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей  | **+** | **+** | Средства ОС (управление учетными записями) |
| **УПД.2**  | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа  |  | **+** | СЗИ от НСД |
| **УПД.3**  | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами  |  | **+** | МЭ |
| **УПД.4**  | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы  | **+** | **+** | СЗИ от НСД, средства ОС |
| **УПД.5**  | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы  | **+** |  |  |
| **УПД.6**  | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)  |  | **+** | Средства ОС СЗИ от НСД, |
| **УПД.10**  | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу  |  | **+** | Средства ОС СЗИ от НСД, |
| **УПД.11**  | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации  |  | **+** | Средства ОС СЗИ от НСД, |
| **УПД.13**  | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети  | **+** | **+** | МЭ с функцией VPN, протоколы SSL, HTTPS |
| **УПД.14**  | Регламентация и контроль использования в информационной системе технологий беспроводного доступа  | **+** |  |  |
| **УПД.15**  | Регламентация и контроль использования в информационной системе мобильных технических средств | **+** |  |  |
| **УПД.16**  | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)  | **+** | **+** | МЭ |
|  | **IV. Защита машинных носителей персональных данных**  |  |  |  |
| **ЗНИ.8**  | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания  | **+** | **+** | Средства ОС, утилиты стирания |
|  | **V. Регистрация событий безопасности**  |  |  |  |
| **РСБ.1**  | Определение событий безопасности, подлежащих регистрации, и сроков их хранения  | **+** |  |  |
| **РСБ.2**  | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации  | **+** |  |  |
| **РСБ.3**  | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения  |  | **+** | Средства логирования СЗИ и ОС |
| **РСБ.7**  | Защита информации о событиях безопасности  |  | **+** | Средства логирования СЗИ и ОС |
|  | **VI. Антивирусная защита**  |  |  |  |
| **АВЗ.1**  | Реализация антивирусной защиты  |  | **+** | САВЗ |
| **АВЗ.2**  | Обновление базы данных признаков вредоносных компьютерных программ (вирусов)  | **+** | **+** | САВЗ |
|  | **VIII. Контроль (анализ) защищенности персональных данных**  |  |  |  |
| **АНЗ.1**  | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей  | **+** |  |  |
| **АНЗ.2**  | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации  | **+** |  |  |
| **АНЗ.3**  | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации  | **+** |  |  |
| **АНЗ.4**  | Контроль состава технических средств, программного обеспечения и средств защиты информации  | **+** |  |  |
|  | **XII. Защита технических средств**  |  |  |  |
| **ЗТС.3**  | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ  | **+** |  |  |
| **ЗТС.4**  | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр  | **+** |  |  |
|  | **XIII. Защита информационной системы, ее средств, систем связи и передачи данных**  |  |  |  |
| **ЗИС.3**  | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |  | **+** | СКЗИ, протоколы SSL, HTTPS |
| **ЗИС.20**  | Защита беспроводных соединений в информационной системе  | **+** | **+** | ПО роутера (защищенная сеть),СКЗИ |
|  | **XV. Управление конфигурацией информационной системы и системы защиты персональных данных**  |  |  |  |
| **УКФ.1**  | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных  | **+** |  |  |
| **УКФ.2**  | Управление изменениями конфигурации информационной системы и системы защиты персональных данных  | **+** |  |  |
| **УКФ.3**  | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных  | **+** |  |  |
| **УКФ.4**  | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты  | **+** |  |  |

*Приложение 8.* Примерный рекомендуемый перечень документов, которые необходимы для обеспечения защиты персональных данных

Локальные нормативные акты

* Положение об обработке персональных данных в информационной системе
* Положение о порядке неавтоматизированной обработки персональных данных в школе
* Регламент обеспечения безопасности персональных данных в школе
* Перечень информационных ресурсов, содержащих персональные данные

Должностные обязанности (в части обеспечения безопасности персональных данных):

* системного администратора информационной системы
* администратора баз данных информационной системы
* сотрудников службы безопасности
* сотрудников кадровой службы
* пользователей информационной системы

Инструкции (в части обеспечения безопасности персональных данных) о порядке и правилах:

* взаимодействия с другими организациями при обмене информацией
* использования паролей пользователей информационной системы
* регистрации пользователей информационной системы и назначения им прав доступа
* подключения к информационной системе сторонних (взаимодействующих) организаций
* установки, модификации и техническом обслуживании программного обеспечения и технических средств обработки информации информационной системы
* защиты от вредоносных программ и вирусов
* резервного копирования и восстановления данных в информационной системе
* приема и увольнения сотрудников организации

Документы, необходимые для реализации технической защиты

* Технический проект системы защиты информации
* Матрица доступа субъектов к информационным ресурсам и операциям с информацией
* Список средств защиты информации, используемых в школьных информационных системах
1. *Лопатин В.Н.* Защита права на тайну в России: Учебное пособие. СПб., 2000. [↑](#footnote-ref-1)
2. Конституция Российской Федерации, ст. ст. 23, 24 [↑](#footnote-ref-2)
3. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., пункт 1, ст. 3 [↑](#footnote-ref-3)
4. WP 136 Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data (Международная рабочая группа № 136. Мнение 4/2007 о понятии «персональные данные») [↑](#footnote-ref-4)
5. Международный пакт о гражданских и политических правах, Нью-Йорк, 19.12.66 г. [↑](#footnote-ref-5)
6. Гражданский кодекс РФ, ст. 19 [↑](#footnote-ref-6)
7. Постановление Правительства РФ от 08.07.1997 г. № 828, «Положение о паспорте гражданина Российской федерации», п. 4 [↑](#footnote-ref-7)
8. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 11 [↑](#footnote-ref-8)
9. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 10. [↑](#footnote-ref-9)
10. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., пункт 10, часть 1, ст. 6. [↑](#footnote-ref-10)
11. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 3, ст. 9. [↑](#footnote-ref-11)
12. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 1, ст. 8. [↑](#footnote-ref-12)
13. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., пункт 11, часть 1, ст. 6. [↑](#footnote-ref-13)
14. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 7. [↑](#footnote-ref-14)
15. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 19. [↑](#footnote-ref-15)
16. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 19. [↑](#footnote-ref-16)
17. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 19. [↑](#footnote-ref-17)
18. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 3. [↑](#footnote-ref-18)
19. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 181. [↑](#footnote-ref-19)
20. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 3, ст. 9. [↑](#footnote-ref-20)
21. Гражданский кодекс РФ, ст. ст. 154, 155. [↑](#footnote-ref-21)
22. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 6, ст.9. [↑](#footnote-ref-22)
23. Гражданский кодекс РФ, ст. ст. 21, 27. [↑](#footnote-ref-23)
24. Семейный кодекс РФ, ст. 64 [↑](#footnote-ref-24)
25. Гражданский кодекс РФ, ст. 28 [↑](#footnote-ref-25)
26. Гражданский кодекс, ст. 175 [↑](#footnote-ref-26)
27. Конституция Российской Федерации, ст. ст. 23, 24 [↑](#footnote-ref-27)
28. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., глава 3 [↑](#footnote-ref-28)
29. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 23 [↑](#footnote-ref-29)
30. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 5, ст. 19. [↑](#footnote-ref-30)
31. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 23. [↑](#footnote-ref-31)
32. Постановление Правительства РФ от 16.03.2009 года № 228, «Об утверждении Положения о Федеральной службе по надзору в сфере связи и массовых коммуникаций». [↑](#footnote-ref-32)
33. Указ Президента РФ от 16.08.2004 г. № 1085 «Вопросы федеральной службы по техническому и экспортному контролю», п. 5 Положения о Федеральной службе по техническому и экспортному контролю. [↑](#footnote-ref-33)
34. Регистрационный номер Госстандарта России РОСС RU.0001.01БИ00. «Положение о сертификации средств защиты информации по требованиям безопасности информации» Утв. Приказом Гостехкомиссии при Президенте РФ от 27.10.1995 г. № 199 [↑](#footnote-ref-34)
35. Регистрационный номер Госстандарта России РОСС RU.0001.030001, Положение утв. Генеральным директором ФАПСИ 28.10.93 г. [↑](#footnote-ref-35)
36. Информационный ресурс – отдельные документы и отдельные массивы документов, документы и массивы документов содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов). ГОСТ Р 51275-2006, п. 2.1 [↑](#footnote-ref-36)
37. Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [↑](#footnote-ref-37)
38. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 1. [↑](#footnote-ref-38)
39. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [↑](#footnote-ref-39)
40. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п. 7 [↑](#footnote-ref-40)
41. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». [↑](#footnote-ref-41)
42. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., п. 5 ч. 1 ст. 18.1 [↑](#footnote-ref-42)
43. А. Б. Вифлеемский, И. Г. Лозицкий «Персональные данные и информационные технологии в образовании», М: 2010 г. [↑](#footnote-ref-43)
44. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [↑](#footnote-ref-44)
45. К структурно-функциональным характеристикам информационной системы относятся: (a) структура и состав информационной системы; (b) физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, а также с иными информационными системами и информационно-телекоммуникационными сетями; (c) режимы обработки информации в информационной системе и в ее отдельных сегментах; (d) иные характеристики информационной системы. [↑](#footnote-ref-45)
46. Приказ ФСТЭК России от 18.022013 г. № 21 «Об утверждении состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», п. 6 [↑](#footnote-ref-46)
47. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ч. 5 ст. 5 [↑](#footnote-ref-47)
48. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ч. 3 ст. 5 [↑](#footnote-ref-48)
49. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе функционирующих в рамках федеральных целевых программ» [↑](#footnote-ref-49)
50. Гражданский кодекс РФ, ст. 1068 [↑](#footnote-ref-50)
51. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., (в ред. Федеральных законов № 266-ФЗ, 2009; № 363-ФЗ, 2009; № 123-ФЗ, 2010; № 204-ФЗ, 2010; № 227-ФЗ, 2010; № 313-ФЗ, 2010; № 359-ФЗ, 2010; №123-ФЗ, 2011; № 261-ФЗ, 2011) [↑](#footnote-ref-51)
52. «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». ETS № 108. Страсбург, 1981 г. Ратифицирована Федеральным законом № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», 2005 г. <http://www.pd.rsoc.ru/law/document170.htm?print=1> [↑](#footnote-ref-52)
53. Конституция Российской федерации, часть 1 ст. 23. [↑](#footnote-ref-53)
54. Конституция Российской Федерации, часть 1 ст. 24. [↑](#footnote-ref-54)
55. Конституция Российской Федерации, часть 2 ст. 24 [↑](#footnote-ref-55)
56. Конституция Российской федерации, часть 4 ст. 29 [↑](#footnote-ref-56)
57. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 1, ст. 1. [↑](#footnote-ref-57)
58. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 5. [↑](#footnote-ref-58)
59. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 6. [↑](#footnote-ref-59)
60. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 1 п.1 ст. 6, ст. ст. 9, 11 [↑](#footnote-ref-60)
61. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 9. [↑](#footnote-ref-61)
62. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 7. [↑](#footnote-ref-62)
63. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. ст. 7, 10. [↑](#footnote-ref-63)
64. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 11. [↑](#footnote-ref-64)
65. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., глава 3 [↑](#footnote-ref-65)
66. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., ст. 23 [↑](#footnote-ref-66)
67. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 1 ст. 181 [↑](#footnote-ref-67)
68. Конституция Российской федерации, ст. ст. 2, 11 [↑](#footnote-ref-68)
69. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 2, часть 4. ст. 19 [↑](#footnote-ref-69)
70. Федеральный закон № 152-ФЗ «О персональных данных», 2006 г., часть 11 ст. 19. [↑](#footnote-ref-70)
71. Гражданский кодекс РФ, ст. 151 [↑](#footnote-ref-71)