1. Сфера действия ФЗ № 152.

Требования Закона «О персональных данных» распространяются на все государственные и коммерческие организации, обрабатывающие персональные данные физических лиц (сотрудников, клиентов, партнеров и т.п.), независимо от размера и формы собственности.

Наиболее остро вопрос защиты персональных данных стоит в сферах здравоохранения, образования, финансов, и в государственных органах.

Эти обстоятельства предъявляют повышенные требования к системе защиты персональных данных и являются приоритетными для проведения проверок контролирующими органами.

Статья 1 Закона № 152-ФЗ «О персональных данных» устанавливает сферу действия Закона: «Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее государственные органы), органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами (далее муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации».

2. Обязанность выполнения требований законодательства

Обеспечение безопасности персональных данных является ***не правом организации, а ее прямой обязанностью***. Несоблюдение организацией требований по обеспечению безопасности персональных данных может повлечь не только ущерб для самой организации, но, в первую очередь, привести к нарушению конституционных прав граждан, повлечь за собой череду гражданско-правовых исков со стороны физических лиц, чьи права могут оказаться нарушенными, и, даже привлечение к административной или уголовной ответственности.

Статья 19 Закона № 152-ФЗ:

«Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

3. Регуляторы в сфере защиты персональных данных

Уполномоченными федеральными органами, регулирующими деятельность в сфере обработки персональных данных, являются:

Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) – ведет реестр операторов персональных данных, контролирует обработку персональных данных операторами и рассматривает обращения субъектов персональных данных.

ФСТЭК России (Федеральная служба по техническому и экспортному контролю) – регулирует сферу обработки и передачи персональных данных между операторами.

ФСБ РФ (Федеральная служба безопасности РФ) - регулирует сферу использования криптографических средств защиты информации при обработке персональных данных.

4. Сроки выполнения требований законодательства

Закон «О персональных данных» был принят 27.07.2006г., вступает в силу с 1 января 2011 года. Информационные системы персональных данных, созданные до 1 января 2010 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2011 года.

Вновь создаваемые и вводимые в эксплуатацию информационные системы персональных данных должны соответствовать требованиями Закона «О персональных данных».

5. Алгоритм построения системы защиты персональных данных

Организационные меры защиты персональных данных включают в себя комплекс мероприятий по разработке организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Шаг 1. Создать специальную комиссию по защите персональных данных или назначить ответственного за обеспечение информационной безопасности.

В зависимости от величины организации целесообразно назначить либо одного человека, ответственного за обеспечение информационной безопасности, либо создать специальную комиссию по защите персональных данных. В качестве председателя комиссии целесообразно назначить кого – либо из первых заместителей руководителя организации, начальника службы безопасности организации или руководителя кадровой службы организации. В состав комиссии рекомендуется включить главного бухгалтера, руководителей подразделений организации обрабатывающих персональные данные, так как они знают структуру обрабатываемых персональных данных, задачи проводимой обработки, а также сотрудников организации, ведущих обработку персональных данных. В качестве лиц, обладающих специальным образованием в области защиты информации и необходимыми познаниями, в состав комиссии следует включить сотрудников организации, имеющей лицензию на техническую защиту конфиденциальной информации, если таковые имеются в штате организации.

Шаг 2. Произвести инвентаризацию информационной системы, обрабатывающей персональные данные.

Часто проведение этого этапа предпроектного обследования считают неразумным или нерациональным, но для построения сбалансированной системы защиты информации он необходим. На этом этапе составляется перечень всех информационных и аппаратных ресурсов организации. Данный перечень будет использоваться в дальнейшем для проведения категорирования, переконфигурирования локальной сети, выработки рекомендаций по построению системы защиты.

Выявляется топология локальной сети, ее архитектура и технологические связи внутренней сети, а также основные информационные потоки.

Также на данном этапе осуществляется определение физической и логической структуры будущей системы защиты информационной системы персональных данных. Устанавливается наличие средств защиты и существующей системы разграничения доступа к информационным ресурсам. Также изучаются имеющиеся сертификаты на средства защиты информации и выясняется необходимость сертификации уже установленных программных и программно-аппаратных комплексов защиты информации.

По итогам данного этапа составляется акт инвентаризации информационных ресурсов.

Шаг 3. Пересмотреть договоры с субъектами и контрагентами

Пересмотреть договоры с работниками и клиентами. Необходимо выяснить, содержаться ли в них пункты, касающиеся обработки и защиты персональных данных. В случае отсутствия подготовить дополнительные соглашения, ознакомить сотрудников и контрагентов. Подписать их.

Шаг 4. Сформировать перечень персональных данных.

В первую очередь, необходимо установить перечень персональных данных (далее ПДн) физических лиц, которые обрабатываются в учреждении. Если кадровый учет и бухгалтерия есть в любом учреждении, то другие направления деятельности, где используются персональные данные, требуется установить: это могут быть данные посетителей, партнеров, контрагентов и т.п.

Также нужно определить цели обработки персональных данных: трудовые отношения с работниками; договор оказания услуг и т.п.

Сроки обработки и хранения. Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых ПДн подлежат уничтожению. Установить перечень ПДн, по которым цели обработки достигнуты.

Шаг 5. Составить и направить в Управление Роскомнадзора "Уведомление об обработке персональных данных".

Начав деятельность, организация обязана подать уведомление о начале обработки персональных данных в Управление Роскомнадзора. На основании уведомления организация регистрируется в реестре операторов, осуществляющих обработку персональных данных.

Уведомление должно быть направлено в письменной форме и подписано руководителем или направлено в электронной форме и подписано электронной цифровой подписью.

Одной из самых распространенных ошибок операторов, не желающих выполнять требования Закона, является ссылка на начало п. 2 ст. 22 Закона:

Операторы ссылаются на оформление договорных отношений с субъектами и размышляют так: «Уведомление подавать не обязательно, значит, работы по созданию системы защиты персональных данных проводить излишне».

«Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных…»

Ссылаясь на этот пункт статьи, забывают о том, что персональные данные сами отправляют в Управление Федеральной налоговой службы, Управление Пенсионного фонда России, в страховые компании, в аутсорсинговые компании и т.д., то есть третьим лицам.

Завершается п. 2 ст. 22 Закона словами:

«… если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных»

Таким образом, все юридические лица обязаны подавать уведомление в Управление Роскомнадзора субъекта Федерации и создавать систему защиты персональных данных.

Шаг 6. Получить согласие субъектов на обработку их персональных данных.

Необходимо разработать "Согласие субъекта на обработку персональных данных", в котором обязательными полями будут перечень персональных данных, цель их обработки, а также методы и способы обработки персональных данных и получить подписи каждого субъекта, персональные данные которого обрабатывает Ваша организация.

Шаг 7. Документально регламентировать работу с персональными данными.

Разработать документы, регламентирующие работу с персональными данными.

Шаг 8. Ограничить доступ своих сотрудников и пользователей информационных систем к персональным данным.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании «Перечня лиц, допущенных персональным данным».

Шаг 9. Сформировать модель угроз персональным данным.

Частная модель угроз организации – оператора составляется в соответствии с руководящим документом ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Поскольку данный документ имеет гриф «для служебного пользования», то получить его можно, отправив запрос в территориальное Управление ФСТЭК с просьбой о предоставлении комплекта документов по защите персональных данных.

Квалифицированное составление частной модели угроз имеет важное значение для организации - оператора. Именно от этого зависит выбор необходимых и достаточных способов защиты информационной системы, подбор оборудования, а, следовательно, конечная стоимость всех работ по обеспечению безопасности персональных данных.

Шаг 10. Классифицировать ИСПДн согласно приказа ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации ИСПДн».

На основании закона «О персональных данных» любая информационная система персональных данных должна быть классифицирована. Процесс классификации - это процесс отнесения информационной системы персональных данных к одному из четырех классов, определенных Приказом Мининформсвязи/ФСТЭК/ФСБ от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Класс присваивается в зависимости от количества субъектов, персональные данные которых обрабатываются в ИСПДн, а также с учетом категории обрабатываемых данных. Категории персональных данных установлены приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва "Об утверждении Порядка проведения классификации информационных систем персональных данных".

Шаг 11. Получить лицензию ФСТЭК на техническую защиту конфиденциальной информации (в случае самостоятельной установки программно-аппаратных средств защиты информации) или воспользоваться услугами сторонней организации, имеющей данную лицензию.

После изучения вопроса и понимания того, что выполнять работы необходимо, каждый руководитель задает себе следующий вопрос: можно ли самостоятельно выполнить требования законодательства или лучше воспользоваться услугами специализированной организации?

С учетом временных ограничений (срок завершения работ – 01.01.2011 года) проведение работ собственными силами может растянуться на длительный период, превышающий установленные законом сроки. Соответственно, возникают риски предъявления претензий со стороны регуляторов за неисполнение требований законодательства.

Шаг 12. Организовать эксплуатацию ИСПДн и контролировать безопасность обработки персональных данных путем проведения ежегодного аудита информационной безопасности.

Необходимо контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Проводить разбирательство и составлять заключения по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн.

Шаг 13. Обучить лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

Для того, чтобы организация могла выполнять требования законодательства по защите персональных данных, мало разработать организационно-распорядительные и эксплуатационные документы и купить технические средства защиты информации. Очень важно на постоянной основе проводить обучение сотрудников новым средствам защиты информации, которые они используют в силу выполнения своих должностных обязанностей, а также правилам работы с этими средствами.

6. Примерный перечень организационно-распорядительных и эксплуатационных документов по ЗПД

1. Согласие на обработку ПД и обязательство о неразглашении ПД.
2. Приказ о введении режима обработки ПДн
3. Приказ о создании комиссии для классификации ИСПДн
4. Приказ о назначении ответственных за безопасность ПДн
5. Описание технологических процессов
6. Перечень информационных систем персональных данных
7. Перечень ПДн
8. Приказ и Перечень общедоступных сведений
9. Приказ о назначении ответственных лиц за ПДн и список ответственных лиц
10. Частная модель угроз
11. Акт Классификации ИСПДн
12. Уведомление об обработке персональных данных
13. Требования по обеспечению безопасности персональных данных
14. Перечень подразделений и сотрудников, допущенных к работе с ПДн
15. Положение о разграничении прав доступа к обрабатываемым персональным данным
16. Инструкция Администратора безопасности
17. Инструкция пользователя ИСПДн
18. Инструкция парольной защиты
19. Инструкция по антивирусному контролю
20. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации
21. Положение по обработке и защите персональных данных
22. Журнал учета носителей ПДн
23. Журнал учёта обращений субъектов ПДн о выполнении их законных прав
24. Протокол оценки соответствия ИСПДн требованиям
25. Акт декларирования соответствия ИСПДн требованиям безопасности информации.

7. Нормативная база по ЗПД

1.Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями от 25 ноября, 27 декабря 2009 г.)

2.Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

3. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении положения и содержания организазионых и технических мер по обеспечению безопасности в информационных системах персональных данных»

5. Методические документы ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

6. Методические документы ФСТЭК России. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

7. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.)

8. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с последними изменениями от 25 ноября 2009 г.)

9.Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

10. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63–ФЗ

11. Федеральный закон о 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

12. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

13. Приказ ФСТЭК от 11 февраля 20013 г.№17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

14. Приказ Министерства образования и науки Российской Федерации от 15 апреля 2009 г. № 133 «Об утверждении порядка формирования и ведения федеральных баз данных и баз данных субъектов Российской Федерации об участниках единого

государственного экзамена и о результатах единого государственного экзамена, обеспечения их взаимодействия и доступа к содержащейся в них информации»

15. Письмо Федерального агентства по образованию от 29.07.2009 № 17–110– «Об обеспечении защиты персональных данных»

8. Нормативные правовые акты по ЗПД МО и молодежной политики Ставропольского края

Приказ министерства образования и молодежной политики Ставропольского края от «06» мая 2014 г. № 406-пр «О внесении изменений в приказ министерства образования Ставропольского края от 26 апреля 2013 г. № 335-пр»
Приказ министерства образования Ставропольского края от «26» апреля 2013 г. №335-пр «О проведении мероприятий по выполнению требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов»
Правила обработки персональных данных в министерстве образования Ставропольского края (приложение 1)
Правила рассмотрения запросов субъектов персональных данных или их представителей министерством образования Ставропольского края (приложение 2)
Правила работы с обезличенными данными в министерстве образования Ставропольского края (приложение 3)
Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами министерства образования ставропольского края (приложение 4)
Порядок доступа служащих министерства образования Ставропольского края в помещения, в которых ведется обработка персональных данных (приложение 5)
Инструкция по организации парольной защиты в министерстве образования Ставропольского края (приложение 6)
Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 7)

Типовую форму согласия на обработку персональных данных в министерстве образования Ставропольского края иных субъектов персональных данных (приложение 8)
Типовое обязательство работника министерства образования Ставропольского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение 9)
Перечень информационных систем персональных данных (приложение 10)
Перечень должностей государственных гражданских служащих и работников министерства образования Ставропольского края, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (приложение 11)
Перечень должностей государственных гражданских служащих и работников министерства образования Ставропольского края, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 12)

Перечень программного обеспечения, разрешенного к использованию в министерстве образования Ставропольского края (приложение 13)
Перечни персональных данных, обрабатываемых в министерстве образования и молодежной политики Ставропольского края в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций (приложение 14)
Должностная инструкция ответственного за организацию обработки персональных данных в министерстве образования и молодежной политики Ставропольского края (приложение 15)

9. Ответственность за неисполнение законодательства по защите персональных данных

Статья	Нарушение	Ответственность
КоАП		
Статья 5.39. Отказ в предоставлении гражданину информации.	Неправомерный отказ в предоставлении гражданину информации об обработке его персональных данных.	Штраф: на должностных лиц - 500 до 1.000руб.
Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	Штраф: на должностных лиц - 500 до 1.000 руб.; на юридических лиц - 5.000 до 10.000 руб.
Статья 13.12. Нарушение правил защиты информации	Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации.	Штраф: на должностных лиц - от 1.000 до 2.000 руб.; на юридических лиц - от 10.000 до 20.000 руб.
Статья 13.14. Разглашение информации с ограниченным доступом	Разглашение персональных данных.	Штраф: на граждан - от 500 до 1.000 руб.; на должностных лиц - от 4.000 до 5.000 руб.
Статья 19.5. Невыполнение в срок законного предписания	1. Невыполнение в установленный срок законного предписания Роскомнадзора.	Штраф: на должностных лиц - от 1.000 до 2.000 руб.; на юридических лиц - от 10.000 до 20.000 руб.
	2. Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа.	Штраф: на должностных лиц - от 5.000 до 10.000 руб.; на юридических лиц - от 200.000 до 500.000 руб.
Статья 19.7. Непредставление сведений	Непредставление Уведомления в Управление Роскомнадзора по	Штраф:

(информации)	Челябинской области.	на должностных лиц - от 300 до 500 руб.; на юридических лиц - от 3.000 до 5.000 руб.
Уголовный Кодекс		
Статья 137. Нарушение неприкосновенности частной жизни	Незаконное собирание или распространение персональных данных либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.	Штраф до **300.000** руб. или в размере заработной платы или иного дохода осужденного за период до 2 лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок **до 5** лет.
Статья 272. Неправомерный доступ к компьютерной информации	Неправомерный доступ к охраняемой законом компьютерной информации (в т.ч. персональных данных).	Штраф до 200.000 руб., либо лишение свободы до 2-х лет.
Трудовой Кодекс		
Статья 81. Расторжение трудового договора по инициативе работодателя.	Разглашение персональных данных другого работника.	Расторжение трудового договора по инициативе работодателя.
Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.	Нарушение норм, регулирующих получение, обработку и защиту персональных данных.	Дисциплинарная, материальная, административная, уголовная ответственность в соответствии с федеральным законодательством.

Базовая модель угроз

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Образцы приказов по БИ для школы

Шаблон акта классификации ИСПДн

Сборник методических материалов

ФСТЭК план проверок

Аттестат соответствия государственной информационной системы «Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования»