

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 5 (192)/2009

Защита персональных данных

Personal Notes

Name

Home address

Home telephone

Mobile

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Защита персональных данных

Олег Слепов,
руководитель направления защиты персональных данных,
Центр информационной безопасности,
компания «Инфосистемы Джет»

СОДЕРЖАНИЕ

Введение	3
Законодательство	4
Персональные данные	4
Состав и содержание персональных данных	4
Категории персональных данных	6
Оператор персональных данных	7
Обязанности оператора ПДн	7
Обработка персональных данных	9
Жизненный цикл персональных данных	10
Неавтоматизированная обработка ПДн	10
Автоматизированная обработка ПДн	11
Обеспечение безопасности персональных данных	11
Обеспечение безопасности ПДн, обрабатываемых в информационных системах персональных данных	12
Защита ПДн при неавтоматизированной обработке	27
Защита биометрических ПДн	28
Защита ПДн при трансграничной передаче	29
Специфика защиты ПДн для различных вертикальных рынков	29
Контроль и надзор за выполнением требований законодательства	32
Роскомнадзор	32
Выводы	34

Введение

Почему необходимо защищать персональные данные?

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, в руках инсайдера — товар для продажи конкуренту... Именно поэтому персональные данные нуждаются в самой серьезной защите.

Необходимость принятия мер по защите персональных данных (далее ПДн) вызвана также возросшими техническими возможностями по копированию и распространению информации. Уровень информационных технологий достиг того предела, когда самозащита информационных прав уже не является эффективным средством против посягательств на частную жизнь. Современный человек уже физически не способен скрыться от всего многообразия явно или неявно применяемых в отношении него технических устройств сбора и технологий обработки данных о людях.

С развитием средств электронной коммерции и доступных средств массовых коммуникаций возросли также и возможности злоупотреблений, связанных с использованием собранной и накопленной информации о человеке. Появились и эффективно используются злоумышленниками средства интеграции и быстрой обработки персональных данных, создающие угрозу правам и законным интересам человека.

Защита персональных данных – это требование бизнеса

Сегодня вряд ли можно представить деятельность организации без обработки информации о человеке. В любом случае организация хранит и обрабатывает данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных приводит к невозможному ущербу, а порой и к полной остановке деятельности организации. Представьте себе работу кредитно-финансовой или телекоммуникационной компании, которая потеряла хотя бы часть информации о своих клиентах. Долго ли просуществует такая компания на рынке?..

Защита персональных данных – это требование законодательства

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту персональных данных. Законодательство Российской Федерации в области ПДн основывается на Конституции РФ и международных договорах Российской Федерации и состоит из Федерального закона РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных», других федеральных законов, определяющих случаи и особенности обработки персональных данных, отраслевых нормативных актов, инструкций и требований регуляторов.

Законодательство

В 1981 году Совет Европы принял Конвенцию «О защите личности в связи с автоматической обработкой персональных данных». 25 ноября 2005 г. Государственная Дума ратифицировала данную Конвенцию (ФЗ от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»), возложив на Российскую Федерацию обязательства по приведению в соответствие с нормами европейского законодательства деятельность в области защиты прав субъектов ПДн. Первым шагом в реализации взятых обязательств стало принятие Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных». Закон вступил в силу в январе 2007 года.

Закон № 152-ФЗ определил высокоуровневые требования, которые затем были конкретизированы в подзаконных актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России) и Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор).

Каждый из этих актов и документов посвящен отдельным областям и тематикам законодательства и будет раскрываться в дальнейшем по ходу изложения материала.

Целью российского законодательства в области ЗПД является обеспечение защиты прав и

свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Законодательством регулируются отношения, связанные с обработкой ПДн, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Персональные данные

В соответствии с Законом № 152-ФЗ персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПДн). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн.

Состав и содержание персональных данных

Состав и содержание персональных данных определяют операторы ПДн¹ в зависимости от целей

Отличие российского и международного законодательства

США, Великобритания и Канада, так же как и Россия, разработали технические регламенты, которые транслируют положения законодательства верхнего уровня в конкретные советы и рекомендации по защите персональных данных. В Великобритании в 1998 году был принят «Закон о защите персональных данных» — «Data Protection Act 1998». Его техническая реализация — проект стандарта «Specification for the management of personal information in compliance with the Data Protection Act 1998» (BS 10012) должен получить статус официального документа в июне 2009. Параллельно с англичанами свою версию стандарта по безопасности ПДн выпустили в США. Проект документа по защите персональных данных для американских государственных структур —

«Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» (SP 800-122) регламентирует выполнение Законов «The Privacy Act of 1974» и «Privacy Protection Act of 1980». Канада выпустила «Privacy Code» — набор документов для реализации законодательства по защите сведений о частных лицах (The Privacy Act и PIPEDA).

Канадский, английский и американский стандарты, в отличие от документов российских регуляторов, дают более общие рекомендации по обеспечению безопасности ПДн и не предписывают, как конкретно должны защищаться персональные данные. Более того, тот же американский стандарт рекомендует по возможности обезличивать персональные данные, чтобы уйти от различных защитных мер, снижающих удобство пользования информацией.

¹ Кто является операторами ПДн, смотрите в разделе III «Оператор персональных данных».

их обработки. Например, перечень персональных данных для популярных в последнее время систем лояльности клиентов компании, как правило, включают контактные данные, необходимые для связи с клиентами, и сведения о предоставленных услугах. Состав этих сведений не должен быть избыточен при этом оставаясь достаточным, чтобы «понимать» предпочтения клиента, его финансовые возможности, «отслеживать» его покупательскую историю и т.п.

Существуют случаи, когда цели, состав и содержание ПДн четко определяются законодательными и нормативно-правовыми актами. Это касается областей, где взаимоотношения между субъектами ПДн и операторами нуждаются в строгой регламентации. При этом в некоторых случаях² субъект персональных данных обязан предоставлять оператору сведения о себе.

Например, функционирование определенных отраслей экономики связано с необходимостью обеспечения безопасности. Так, ФЗ-16 «О транспортной безопасности» определяет необходимость создания единой государственной информационной системы обеспечения транспортной безопасности. Такая система должна состоять из централизованных баз персональных данных о пассажирах, включающих следующие данные:

- фамилия, имя, отчество;
- дата и место рождения;
- вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);
- пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный);
- дата поездки.

Регламентация состава и содержания ПДн касается отношений, связанных с трудовой деятельностью человека. Если речь идет о кадровой системе, к составу персональных данных относятся сведения, предусмотренные унифицированной формой учета кадров Т-2, утвержденной Постановлением № 1 Госкомстата России от 05.01.2004. К таким сведениям относятся:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- знание иностранных языков;

- данные об образовании (номер, серия дипломов, год окончания);
- данные о приобретенных специальностях
- семейное положение;
- данные о членах семьи (степень родства, ФИО, год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;
- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т.п.).

К другим нормативным актам, регулирующим отношения в сфере деятельности человека и определяющим цели обработки, состав и содержание ПДн, относятся ФЗ-179 «Трудовой кодекс РФ», ФЗ-27 «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», ФЗ-129 «О государственной регистрации юридических лиц и индивидуальных предпринимателей» и т.п.

Какие сведения о сотрудниках государственных организаций собирать и как их обрабатывать, определяет Указ Президента РФ от 30 мая 2005 г. N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Своя специфика существует и в различных отраслях экономики. Определенные рамки обработки персональных данных для кредитно-финансовых учреждений устанавливает ФЗ-218 «О кредитных историях», для авиационного транспорта – Воздушный кодекс, для торговых организаций (Интернет-магазинов и т.п.) – Постановление Правительства Российской Федерации от 27 сентября 2007 г. N 612 «Об утверждении Правил продажи товаров дистанционным способом», для туристического бизнеса – Постановление Правительства Российской Федерации от 18 июля 2007 г. N 452 «Об утверждении Правил оказания услуг по реализации туристского продукта» и т.п.

Невозможно не упомянуть и ФЗ-143 «Об актах гражданского состояния», в котором государство четко определяет, какие сведения о личности должны собираться, храниться и обрабатываться на протяжении всей его жизни.

² Российским законодательством определены случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Категории персональных данных

Законодательство определяет различные категории персональных данных. К ним могут относиться общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах персональных данных (далее ИСПДн), биометрические ПДн и другие.

Общедоступные ПДн

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории ПДн

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности,

об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Категории персональных данных, обрабатываемых в ИСПДн

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет следующие категории персональных данных, которые обрабатываются в ИСПДн:

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

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

Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПДн.

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

Категорирование персональных данных при обработке в ИСПДн может также проводиться по параметру «объем обрабатываемых персональных данных». Под этим подразумевается количество субъектов, данные которых обрабатываются в информационной системе. Этот параметр может принимать следующие значения:

1. В информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта РФ или Российской Федерации в целом.
2. В информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.
3. В информационной системе одновременно обрабатываются данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации.

Такое категорирование персональных данных необходимо для определения класса ИСПДн, от которого зависят меры по обеспечению безопасности ПДн при обработке в информационных системах.

Биометрические персональные данные

Биометрические персональные данные — это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Исходя из определения биометрических ПДн, к ним относятся фотографии и видеозображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения — в системах видеонаблюдения и т.п.

Оператор персональных данных

Согласно Закону №152-ФЗ операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Под обработкой ПДн понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использова-

ние, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Исходя из определения, можно сделать вывод о том, что все без исключения организации или компании независимо от форм собственности являются операторами персональных данных, поскольку они как минимум осуществляют сбор, систематизацию, хранение и уточнение сведений о своих сотрудниках в соответствии с российским законодательством (Трудовой Кодекс РФ). Помимо этого многие компании по роду своей деятельности обрабатывают сведения о своих клиентах, партнерах, поставщиках и субподрядчиках, которые им необходимы для выполнения функций в соответствии с их назначением.

При этом бытует ошибочное мнение о том, что в случае, если нет необходимости регистрироваться как оператор ПДн в Роскомнадзоре (а законом такие случаи предусмотрены), то компания не является оператором ПДн и на нее не распространяются обязанности, предусмотренные законодательством. Более того, таким образом компании пытаются оправдать свое бездействие в области обеспечения безопасности ПДн. Если компания не предпринимает никаких усилий по защите персональных данных, это однозначно расценивается как «невыполнение требований российского законодательства».

Обязанности оператора ПДн

Российское законодательство возлагает на операторов ПДн определенные обязанности, основными из которых являются:

1. Обеспечение безопасности обработки персональных данных, что означает обязанность «принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».
2. Уведомительный характер обработки персональных данных. В соответствии со статьей 22 Закона оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Роскомнадзор вносит сведения об операторе в реестр операторов. Информация, содержа-

В каких случаях оператор ПДн имеет право не уведомлять Роскомнадзор

Оператор вправе осуществлять обработку следующих персональных данных без уведомления уполномоченного органа по защите прав субъектов ПДн (Роскомнадзор):

- относящихся к субъектам ПДн, которых с оператором связывают трудовые отношения;
- полученных оператором в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные

данные не будут распространяться без согласия в письменной форме субъектов ПДн;

- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем (далее ИС), а также в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов ПДн.

сящая в реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, является общедоступной.

3. При получении персональных данных (в том числе от третьих лиц) оператор ПДн до начала обработки обязан получить у субъекта этих ПДн письменное разрешение на их обработку (за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если они являются общедоступными).

4. Оператор обязан предоставить субъекту ПДн по требованию все имеющиеся сведения о нем, целях и условиях обработки, способах защиты его персональных данных. Оператор также должен уничтожить или заблокировать соответствующие персональные данные, внести в них необходимые изменения по предоставлению субъектом ПДн или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществ-

Невыполнение требований законодательства?.. Какие последствия?..

Законом предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение его требований. Так, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановку деятельности организации на срок до 90 суток при

осуществлении деятельности по защите персональных данных без лицензии (ст. 19.20 КоАП). В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1-го года, аресте до 6-ти месяцев и лишении права занимать должность на срок до 5-ти лет в случае осуществления защиты персональных данных без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК). При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности.

ляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Более того, оператор ПДн обязан предоставить доказательство получения согласия субъекта ПДн на обработку его персональных данных, а в случае обработки общедоступных персональных данных на него возлагается обязанность доказать, что обрабатываемые ПДн являются общедоступными.

5. Подконтрольность и поднадзорность деятельности операторов персональных данных государственным органам. Это означает обязанность оператора сообщать в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа. Функциями контроля и надзора государство наделило Роскомнадзор, ФСТЭК и ФСБ³.

Обработка персональных данных

В российском законодательстве определяются основные **принципы обработки персональных данных**⁴. К ним, в частности, относятся:

- Оператор персональных данных определяет цели их обработки в соответствии со своими полномочиями.
- Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки.
- Недопустимо объединять созданные для разных целей персональные данные (например, в одну базу данных).
- Персональные данные подлежат уничтожению по достижении целей (утраты необходимости в) их обработки.

Большое значение в Законе уделено **условиям обработки персональных данных**⁵. Так, об-

В каких случаях не требуется согласие субъекта ПДн на обработку сведений о нем?

Согласие субъекта ПДн не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании других федеральных законов, например, некоторыми Федеральными законами предусматриваются случаи обязательного предоставления субъектом ПДн своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- оператор и субъект ПДн связаны договором на выполнение действий, которые требуют обработки персональных данных этого субъекта, например, договор, по которому туристическая фирма (оператор) имеет право использовать персональные данные субъекта для бронирования гостиницы;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн,

если получение его согласия невозможно, например, госпитализация человека при несчастном случае;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

³ Подробнее о контрольных и надзорных функциях и регуляторах смотрите в разделе V «Контроль и надзор за выполнением требований законодательства».

⁴ Вопросу о том, что понимать под обработкой персональных данных, было уделено внимание в III главе данной статьи (см. «Оператор персональных данных»).

⁵ Согласие на обработку персональных данных может быть отозвано субъектом ПДн.

работка персональных данных может осуществляться оператором только с письменного согласия субъектов ПДн.

Существует два вида обработки персональных данных: автоматизированный и неавтоматизированный. Об этих видах обработки ПДн речь пойдет в следующих разделах статьи.

Жизненный цикл персональных данных

Обработка персональных данных требует создание специального режима, в котором четко определены технология их обработки, порядок и условия существования ПДн на каждом этапе их жизненного цикла. Это предусматривает разработку и внедрение процедур их сбора, приема, учета, регистрации, хранения, использования, уничтожения и т.п. Большое значение при этом имеет срок хранения ПДн, а также наличие системы контроля обработки ПДн на всех этапах их жизненного цикла.

Срок обработки ПДн

Определение сроков обработки ПДн крайне важно потому, что Федеральный закон определяет, что «в случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки».

Анализ технологических процессов обработки ПДн

В своих проектах по защите ПДн специалисты компании «Инфосистемы Джет» большое внимание уделяют учету технологических процессов обработки персональных данных (жизненный цикл ПДн) и получению информации о существующих процедурах обработки ПДн. С этой целью ими проводятся следующие работы:

- анализ документов, определяющих технологические процессы обработки ПДн;

Сроки обработки также определяются на основании других нормативно-правовых актов. Так, требованиями трудового, гражданского, пенсионного законодательства, отраслевых нормативных актов устанавливаются определенные сроки обработки персональных данных. Например, для карточек Т-2 — это 75 лет⁶ (Постановление Госкомстата № 1), а для сведений о предоставленных абоненту услугах связи — 3 года (Постановление Правительства № 538).

Неавтоматизированная обработка ПДн

Неавтоматизированная обработка персональных данных осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Согласно данному Постановлению, обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия осуществляются при непосредственном участии человека.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях, в специальных раз-

- проведение интервью с сотрудниками заказчика, реализующими процедуры обработки ПДн;
- определение владельца технологического процесса обработки ПДн (соотнесение технологического процесса со структурным подразделением заказчика и используемой ИСПДн);
- определение процедур сбора, приема, учета и регистрации ПДн в информационных системах персональных данных, хранения, обработки, выпуска, копирования и передачи ПДн, их уничтожения и контроля за этими процедурами.

⁶ 75 лет — это срок, в течение которого должны храниться данные о сотрудниках организации. Это требование обязательно для государственных организаций, для коммерческих — оно носит рекомендательный характер. При этом хранение должно быть обеспечено в соответствии с законодательством об архивном делопроизводстве. В случае невозможности обеспечения такого требования ПДн должны передаваться в специализированные организации (государственные архивы и т.п.).

Что считать неавтоматизированной обработкой ПДн?

Вопрос разделения неавтоматизированной и автоматизированной обработки у многих организаций вызывает затруднения. Рассмотрим п.п. 1 и 2 Постановления РФ:

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только

на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Исходя из этого, некоторые организации полагают, что всю обработку ПДн можно отнести к неавтоматизированной, поскольку во всех случаях имеется факт «обработки ПДн при непосредственном участии человека».

И это является ошибкой. В данном случае неправильно рассматривать эту обработку только как неавтоматизированную. К примеру, если пользователь внес данные в персональный компьютер только для того, чтобы их распечатать, и не сохранял данные на компьютере, то эту обработку можно считать неавтоматизированной. Если пользователь сохранил эти данные в виде файла и хранит их на компьютере, то нужно рассматривать эту обработку ПДн в том числе и как автоматизированную.

делах или на полях форм (бланков). При этом не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн для каждой из них должен использоваться отдельный материальный носитель.

Постановление определяет, какая информация должна быть включена в типовые формы документов, включающих персональные данные, условия ведения журналов (реестров, книг), содержащих ПДн (например, необходимых для однократного пропуска субъекта ПДн на территорию оператора), описывает важнейшие этапы жизненного цикла персональных данных, зафиксированных на материальном носителе.

персональных данных», СЕД №108, от 28 января 1981 г.).

«Автоматизированная обработка ПДн» подразумевает действия с «автоматизированными файлами ПДн», которая включает следующие операции, осуществляемые полностью или частично с помощью средств автоматизации: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение.

Автоматизированная обработка персональных данных

Для того, чтобы определить, что является «автоматизированной обработкой ПДн», необходимо ввести понятие «автоматизированного файла ПДн», которое означает любой комплекс данных о субъектах ПДн, подвергающийся автоматизированной обработке («Конвенция о защите физических лиц при автоматизированной обработке

Обеспечение безопасности персональных данных

В соответствии со статьей 19 Федерального Закона «О персональных данных» оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

В каких случаях обеспечение безопасности ПДн не требуется?..

Обеспечение безопасности (в данном случае конфиденциальности) в соответствии с российским законодательством не требуется лишь для обезличенных и общедоступных персональных данных.

Персональные данные могут быть обезличенными, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПДн.

Персональные данные могут быть общедоступными только с письменного согласия субъекта ПДн. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПДн.

Обеспечение безопасности ПДн, обрабатываемых в информационных системах персональных данных

В данном разделе рассказывается о требованиях к обеспечению безопасности ПДн при их обработке в информационных системах персональных данных (ИСПДн), которые содержатся в Постановлении Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», а также конкретизируются в нормативно-методических документах ФСТЭК и ФСБ.

Кто должен обеспечивать безопасность ПДн?..

Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (уполномоченное лицо). При этом оператор должен заключать договор с уполномоченным лицом. Существенным условием этого договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность ПДн при их обработке в ИСПДн.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом ко-

торого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности ПДн при их обработке в ИСПДн полностью возлагается на оператора персональных данных. В связи с этим оператор обязан:

- проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременно обнаруживать факты НСД к персональным данным;
- не допускать воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- незамедлительно восстанавливать ПДн, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- осуществлять постоянный контроль за обеспечением уровня защищенности ПДн.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах оператором может назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности персональных данных.

Что такое ИСПДн?

Информационные системы персональных данных представляют собой совокупность информационных и программно-аппаратных элементов, основными из которых являются:

- ПДн, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в информационных системах;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства, осуществляющие обработку ПДн, под которыми понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);

Сроки и условия приведения ИСПДн в соответствие с законодательством

Российским законодательством определены сроки и условия приведения ИСПДн в соответствие требованиям по обеспечению безопасности ПДн.

Для информационных систем персональных данных, находящихся в эксплуатации до введения в действие Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», должна быть обеспечена их доработка, обеспечивающая безопасность ПДн в соответствии с требованиями Законодательства, в срок до 1 января 2010 г.

Для функционирующих ИСПДн доработка (модернизация) систем защиты персональных данных (далее СЗПДн) должна проводиться в случае, если:

- изменился состав или структура самой информационной системы или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

- программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы, к которым относятся средства и системы коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, проводной радиотрансляционной сети и приема программ радиовещания и телевидения, электрочасофикации⁷, средства электронной оргтехники).

Какие ИСПДн существуют?

Персональные данные обрабатываются в массе приложений. Как показал опыт компании «Инфосистемы Джет» по выполнению проектов по ЗПД, их количество может варьироваться от 3 до 5 в малых и средних компаниях, от 30 до 50 — в круп-

- изменился состав угроз безопасности ПДн в информационной системе;
- изменился класс ИСПДн.

Для вновь создаваемых или модернизируемых информационных систем деятельность по обеспечению безопасности ПДн является неотъемлемой частью работ по их созданию или модернизации. Производителей приложений, в которых предусмотрена обработка сведений о физических лицах, обязаны реализовывать в своих разработках требования по безопасности ПДн, предусмотренные российским законодательством.

Компания «Инфосистемы Джет», являясь системным интегратором, осуществляет в своих проектах разработку и внедрение различных вычислительных комплексов и бизнес-приложений. Подобные работы проводятся с учетом требований российского законодательства по обеспечению информационной безопасности, в том числе по защите персональных данных.

ных компаниях. К информационным системам персональных данных могут быть отнесены:

- CRM-системы (данные о клиентах — физических лицах и представителях клиентов — юридических лиц);
- биллинговые системы (данные о клиентах, осуществляющих оплату услуг);
- автоматизированные банковские системы (данные о сотрудниках банка, о клиентах, партнерах и т.п.);
- автоматизированные медицинские системы (данные о пациентах и т.п.);
- Call-центры (данные о клиентах и сотрудниках в зависимости от предназначения call-центра);
- кадровые системы (данные о сотрудниках организации);
- бухгалтерские системы (данные о сотрудниках и клиентах организации);
- системы документооборота (данные о сотрудниках организации, клиентах, партнерах);
- почтовые системы (данные о сотрудниках организации, клиентах, партнерах, заполненные карточки в адресных книгах почтовых систем и т.п.);
- автоматизированные системы бюро пропусков (данные о посетителях).

⁷ Системой электрочасофикации называется комплекс технических средств, обеспечивающий показание единого времени на вторичных электрочасах, установленных в разных точках предприятия (учреждения) и управляемых электрическими импульсами от первичных электрочасов.

С точки зрения принадлежности информационные системы могут быть следующих видов: ИСПДн государственных и муниципальных органов, юридических и физических лиц, организующих или осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных (за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд).

Классификация ИСПДн

Классификация ИСПДн проводится оператором в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, а также на основании нормативно-методических документов регуляторов ФСТЭК и ФСБ.

Классификация информационных систем проводится на этапе создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение ей соответствующего класса;
- его документальное оформление (составление и утверждение руководством организации Актов классификации на конкретные ИСПДн).

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных (категория 1, категория 2, категория 3, категория 4)⁸;
- объем обрабатываемых персональных данных (количество субъектов ПДн, персональные данные которых обрабатываются в информационной системе — 1, 2, 3)⁹;
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;

- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, ИСПДн подразделяются на типовые и специальные:

- типовые информационные системы — информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных;
- специальные информационные системы — информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик их безопасности, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

По структуре информационные системы подразделяются:

- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств (автоматизированные рабочие места);
- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- на комплексы автоматизированных рабочих мест и локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и сетям международного информационного обмена информационные системы подразделяются на имеющие и не имеющие подключений к таким сетям.

⁸ Об определении категории ПДн говорилось в разделе «Категории персональных данных, обрабатываемых в ИСПДн»

⁹ Об определении объема обрабатываемых ПДн говорилось в разделе «Категории персональных данных, обрабатываемых в ИСПДн»

По режиму обработки персональных данных в информационной системе ИСПДн подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах РФ, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

Классификация типовых ИСПДн

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

- класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс типовой информационной системы определяется в соответствии с таблицей №1.

Классификация специальных ИСПДн

Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с нормативно-методическими документами регуляторов ФСТЭК и ФСБ.

К специальным ИСПДн автоматически относятся:

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

Составление моделей угроз для специальных ИСПДн

Применительно к основным типам информационных систем разработаны типовые модели угроз безопасности ПДн, характеризующие наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации угрозы в отношении персональных данных. Всего таких моделей шесть и описаны они в документе ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 15 февраля 2008 года:

- типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, имеющих подключения к сетям

Таб. 1. Определение класса типовой информационной системы

	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

- общего пользования и (или) сетям международного информационного обмена;
- типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
 - типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
 - типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
 - типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

На основе базовой модели угроз и в соответствии с нормативным документом ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным 14 февраля 2008 г., разрабатываются частные модели угроз в отношении конкретных ИСПДн. В ходе такой разработки

Классификация ИСПДн

Практика показала, что существуют определенные сложности в проведении классификации ИСПДн силами операторов, поскольку для выполнения данной задачи не всегда хватает компетенции собственных специалистов.

Обладая опытом проведения проектов по защите персональных данных, компания «Инфосистемы Джет» сформировала свой подход к проведению данного вида работ.

При этом отличительной особенностью является «правильная» классификация ИСПДн, при которой удается в значительной степени минимизировать расходы наших заказчиков на создание системы защиты персональных данных. В частности, это становится возможным за счет минимизации мест хранения и обработки ПДн, разделения/сегментирования ИС, снижения требований к части сегментов, сокращения числа сотрудников, имеющих доступ к персональным

составляется перечень актуальных угроз в отношении конкретных информационных систем.

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности ПДн при их обработке в ИСПДн» и «Основных мероприятий по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн», утвержденных ФСТЭК, формулируются конкретные организационно-технические требования по защите информационных систем от утечки данных по техническим каналам, от несанкционированного доступа. Также осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Что подлежит защите в ИСПДн?

Для обеспечения безопасности персональных данных при их обработке в ИСПДн осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также сведений, представленных в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

данным, обезличивания части персональных данных, выведения части данных из ИСПДн.

В ходе анализа технологических процессов обработки ПДн специалистами компании «Инфосистемы Джет» вырабатываются **рекомендации по снижению предполагаемых классов ИСПДн**, которые могут содержать следующее:

- Абстрагирование ПДн — сделать их менее точными, например, путем группирования общих характеристик;
- Скрытие ПДн — удалить всю или часть записи ПДн;
- Замена ПДн — переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи;
- Замена данных средним значением — заменить выбранные данные средним значением для группы ПДн;
- Разделение ПДн на части — использование таблиц перекрестных ссылок;
- Маскирование ПДн — замена одних символов в ПДн другими.

Для обеспечения защиты от угроз в отношении данных применяется понятие «носитель (источник) ПДн. Данное понятие означает физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении голосового ввода данных в информационную систему, либо воспроизведении акустическими средствами ИСПДн, а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;
- видовая информация, представленная в виде текста или изображений, и воспроизводимая при помощи различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- информация в виде электрических, электромагнитных, оптических сигналов, возникающих при обработке ПДн в ИСПДн;
- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.

Мероприятия по защите ПДн при обработке в ИСПДн

В соответствии с Постановлением Правительства РФ от 17 ноября 2007 г. № 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», а также документом ФСТЭК «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утвержденным 15 февраля 2008 г., мероприятия по обеспечению безопасности ПДн при обработке в ИСПДн формулируются в зависимости от класса информационных систем с учетом возможного возникновения угроз безопасности в отношении персональных данных. Такие мероприятия включают в себя:

- определение угроз безопасности в отношении ПДн при их обработке в ИСПДн, формирование на их основе моделей угроз;
- разработку на основе таких моделей угроз системы защиты ПДн (СЗПДн), которая обеспечивает нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проверку готовности средств защиты информации (далее СЗИ) к применению и составление заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию СЗИ в соответствии с эксплуатационной и технической документацией;
- обучение лиц, которые будут эксплуатировать СЗИ, правилам работы с ними;
- контроль за применением СЗИ, учет эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;
- проведение расследований и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн; а также принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн включают:

- мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;
- мероприятия по закрытию утечки ПДн по техническим каналам при их обработке в информационных системах;
- мероприятия по защите ПДн от несанкционированного доступа (далее НСД) и определению порядка выбора средств защиты персональных данных при их обработке в ИСПДн.

Система защиты ПДн при их обработке в ИСПДн

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных.

Что включает СЗПДн?

Структура, состав и основные функции систем защиты персональных данных определяются исходя из класса ИСПДн. СЗПДн включает в себя организационные меры, средства защиты информации, а также используемые в информационной системе информационные технологии.

Организационные меры

Обеспечение безопасности персональных данных при их обработке в ИСПДн должно предусматривать:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач их защиты;
- разработку замысла обеспечения безопасности ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;
- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных в рамках разработки (модернизации) ИСПДн, разработка и развертывание СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации информационных систем;
- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;
- развертывание и ввод в опытную эксплуатацию СЗПДн в информационных системах персональных данных;
- доработку СЗПДн по результатам опытной эксплуатации.

Средства защиты ПДн

В соответствии с классификацией ИСПДн, а также с учетом актуальных угроз, приведенных в адаптивных моделях для «специальных» ИСПДн,

и в соответствии с требованиями нормативно-методических документов регуляторов ФСТЭК РФ и ФСБ РФ, СЗПДн должна включать ряд подсистем, описание которых представлено в следующих разделах.

Средства защиты ПДн от утечки по техническим каналам

С целью предотвращения утечек акустической (речевой), видовой информации, а также утечек информации за счет побочных электромагнитных излучений и наводок применяются специальные технические средства. При этом выделяются пассивные и активные средства защиты.

Пассивные средства защиты, как правило, реализуются на этапе разработки проектных решений при строительстве или реконструкции зданий. Преимущества применения пассивных средств заключаются в том, что они позволяют заранее учесть типы строительных конструкций, способы прокладки коммуникаций, оптимальные места размещения защищаемых помещений.

Защита ПДн при осуществлении пользователями информационных систем голосового ввода данных в ИСПДн или их воспроизведении акустическими средствами ИСПДн обеспечивается путем звукоизоляции помещений, в которых устанавливаются аппаратные средства ИСПДн, систем инженерного обеспечения (вентиляции, отопления и кондиционирования), а также ограждающих конструкций помещений (стены, пол, потолок, окна, двери).

Звукоизоляция обеспечивается с помощью архитектурных и инженерных решений, применением специальных звукопоглощающих строительных и отделочных материалов, виброизолирующих опор, которыми разделяют друг от друга различные ограждающие конструкции. Для обеспечения требований по защите ПДн достаточным является повышение звукоизоляции на 10-15 дБ. Для снижения вероятности перехвата информации такого рода необходимо исключить возможность установки посторонних предметов на внешней стороне ограждающих конструкций помещений и выходящих из них инженерных коммуникаций.

В случае технической невозможности использования пассивных средств защиты помещений, применяют **активные меры защиты**, заключающиеся в создании маскирующих акустических и вибрационных помех.

Средства акустической маскировки используются для защиты речевой информации от утечки по прямому акустическому каналу путем создания акустических шумов в местах воз-

возможного размещения средств подслушивания или нахождения посторонних лиц.

Средства виброакустической маскировки применяются для защиты информации от перехвата с помощью электронных стетоскопов, радиостетоскопов, а также лазерных акустических систем подслушивания.

С целью предотвращения утечки информации по телефонным каналам связи необходимо оконечные устройства телефонной связи, которые имеют прямой выход на городскую автоматическую телефонную станцию, оборудовать специальными средствами защиты информации, которые используют электроакустическое преобразование.

Средства защиты ПДн от несанкционированного доступа

Для осуществления мероприятий по защите ПДн при их обработке в информационных системах от несанкционированного доступа (НСД) и неправомерных действий пользователей и нарушителей СЗПДн могут включать в себя следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- антивирусной защиты;
- обеспечения безопасности межсетевых взаимодействий ИСПДн;
- анализа защищенности;
- обнаружения вторжений.

Подсистема управления доступом, регистрации и учета, как правило, реализуется с помощью программных средств блокирования НСД, сигнализации и регистрации. Это специальные, не входящие в ядро операционной системы программные и программно-аппаратные средства защиты самих операционных систем, СУБД и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения несанкционированных действий пользователей или нарушителей. К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики (тестирование файловой системы), регистрации (журналирование действий и операций), сигнализации (предупреждение об обнаружении фактов несанкционированных действий или нарушения штатного режима функционирования ИСПДн).

Подсистема обеспечения целостности также реализуется преимущественно средства-

ми самих операционных систем и СУБД. Работа данных средств основана на расчете контрольных сумм, уведомлении о сбое в передаче пакетов сообщений, повторе передачи непринятых пакетов.

Частота применения в российских компаниях в качестве операционной системы продуктов компании Microsoft вызвала необходимость использовать в качестве базовой платформы для построения решения подсистемы разграничения и контроля доступа к ресурсам информационной системы функционал Microsoft Windows Server 2003.

Эта сетевая операционная система наряду с необходимым для обеспечения безопасности ПДн набором технологических параметров обладает всеми необходимыми сертификатами на соответствие требованиям регулирующих органов. ФСТЭК России в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 сертифицировал:

- русскую версию Windows Server 2003 (Standard Edition и Enterprise Edition);
- русскую версию Windows Server 2003 R2 (Standard Edition и Enterprise Edition).

Компанией Microsoft также производится сертификация ежемесячно выходящих новых патчей к данным продуктам.

ФСБ России сертифицировала русскую версию серверной операционной системы Windows Server 2003 Enterprise Edition. Сертификат ФСБ удостоверяет, что продукт соответствует требованиям ФСБ России к защите информации, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа в автоматизированных информационных системах класса АК2. Таким образом, данная система может быть использована в качестве средства для защиты ПДн в ИСПДн.

Последней версией Windows Server является версия Windows Server 2008. Ожидается, что к дате выхода данной статьи сертификация данной ОС будет получена и в технических решениях для подсистемы управления доступом, регистрации и учета будет возможно применение Microsoft Windows Server 2008.

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, обеспечивающей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты (подсистема антивирусной защиты). Такие средства способны обеспечивать:

- обнаружение и блокирование деструктивных вирусных воздействий на общесистем-

Что использовать: встроенные или наложенные средства защиты?

Опираясь на накопленный опыт в области защиты информации, специалисты компании «Инфосистемы Джет» в проектировании решений по защите ПДн при их обработке в ИСПДн стараются комбинировать как наложенные средства защиты информации, так и встроенные механизмы защиты в общесистемное и прикладное программное обеспечение (ПО), используемое в ИСПДн. Каждый вариант имеет свои достоинства и недостатки. Наложённые средства далеко не всегда могут в полной мере реализовать требования регуляторов, а также могут оказаться несовместимыми с уже используемыми в ИСПДн программными решениями. Применение встроенных механизмов приводит к возникновению проблем, связан-

ное и прикладное ПО, реализующее обработку ПДн, а также на сами ПДн;

- обнаружение и удаление «неизвестных» вирусов (т.е. вирусов, сигнатуры которых еще не внесены в антивирусные базы данных);
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

Подсистема антивирусной защиты должна строиться с учетом следующих факторов:

- наличия средств централизованного управления функционированием средств антивирусной защиты с рабочего места администратора безопасности информации в ИСПДн;
- возможности оперативного оповещения администратора безопасности информации в ИСПДн обо всех событиях и фактах проявления программно-математических воздействий (ПВМ).

Для реализации подсистемы антивирусной защиты ПДн при их обработке в ИСПДн возможно использование антивирусных средств компании «Лаборатория Касперского».

Продукты компании «Лаборатория Касперского» сертифицированы Федеральной службой безопасности России. Данные сертификаты удостоверяют, что Антивирус Касперского 6.0 для Windows Servers соответствует требованиям к антивирусным средствам класса А1с, Антивирус Касперского 5.5 для Linux и FreeBSD Workstations и File Server соответствует требованиям к антивирусным средствам класса А2с и Kaspersky Administration Kit 6.0 соответствует требованиям

к антивирусным средствам класса А3с. Указанные продукты могут использоваться в органах государственной власти Российской Федерации для защиты информации, содержащей сведения, составляющие государственную тайну.

Специалисты компании «Инфосистемы Джет» отдают предпочтение встроенным механизмам реализации управления доступом к ПДн. Данный подход обусловлен тем, что позволяет минимизировать изменения в структуре как самих ИСПДн, так и механизмов безопасности.

Большое внимание при проектировании СЗПДн специалисты нашей компании также уделяют обеспечению целостности настроек самих средств защиты информации. При выборе данных средств компанией «Инфосистемы Джет» тщательно анализируются собственные механизмы контроля целостности. Только неизменность настроек средств защиты информации может гарантировать оператору ПДн надежную защиту обрабатываемой в ИСПДн информации.

к антивирусным средствам класса А3с. Указанные продукты могут использоваться в органах государственной власти Российской Федерации для защиты информации, содержащей сведения, составляющие государственную тайну.

Кроме того, продукты Антивирус Касперского 6.0 для Windows Servers, Антивирус Касперского 6.0 для Windows Workstation и Kaspersky Administration Kit 6.0 соответствуют требованиям руководящего документа ФСТЭК — по 3 уровню контроля и требованиям технических условий.

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии (**подсистема обеспечения безопасности межсетевого взаимодействия ИСПДн**) применя-

Для получения оптимального уровня антивирусной защиты ИСПДн компания «Инфосистемы Джет» реализует двух-эшелонную систему защиты информации. Первый эшелон организуется на периметре информационной системы оператора ПДн, второй эшелон защищает внутренние ресурсы системы от возможного попадания вирусов путем использования непроверенных носителей информации сотрудниками оператора. Не секрет, что не все антивирусы «одинаково полезны». Опыт нашей компании показывает, что не существует универсального средства безопасности от вирусов, поэтому для наиболее эффективной защиты в проектируемых решениях наши специалисты применяют одновременно антивирусные средства разных производителей.

ется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран устанавливается между защищаемой внутренней и внешней сетями. МЭ входит в состав защищаемой сети. За счет соответствующих настроек задаются правила, которые позволяют ограничивать доступ пользователей из внутренней сети во внешнюю и наоборот.

Для обеспечения безопасного меж сетевого взаимодействия в ИСПДн 3 и 4 классов рекомендуется использовать МЭ не ниже пятого уровня защищенности, в ИСПДн 2 класса – МЭ не ниже четвертого уровня защищенности, в ИСПДн 1 класса – МЭ не ниже третьего уровня защищенности.

Основываясь на требованиях регуляторов РФ и проанализировав реализацию меж сетевого взаимодействия систем своих заказчиков, специалисты компании «Инфосистемы Джет» стараются использовать для защиты персональных данных уже используемые операторами ПДн межсетевые экраны (при наличии сертификата соответствия требованиям должного уровня). Поскольку в состав ИСПДн входит не только серверный сегмент, который обрабатывает ПДн, но и рабочие станции пользователей, реализация меж сетевого взаимодействия должна охватывать весь периметр информационной системы оператора ПДн. В связи с этим, для реализации требований регуляторов в части безопасного меж сетевого взаимодействия ИСПДн компания «Инфосистемы Джет» рекомендует применять как периметровые средства защиты (производительные МЭ), так и персональные МЭ, устанавливаемые на рабочие места пользователей. Такой подход наиболее эффективно предотвращает несанкционированный доступ к защищаемой информации, а также в полной мере закрывает требования регуляторов РФ.

Подсистема анализа защищенности предназначена для осуществления контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяет оценить возможность проведения нарушителями атак на сетевое оборудование, контролирует безопасность программного обеспечения. С помощью таких средств (средства обнаружения уязвимостей) производится сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек меж сетевых экранов и т.п. Данный анализ производится на основании де-

тальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, меж сетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средств анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

Средства обнаружения уязвимостей могут функционировать на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения (application-based). Применяя сканирующее ПО, можно составить карту доступных узлов ИСПДн, выявить используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности реализации НСД. По результатам сканирования системы вырабатываются рекомендации и меры, позволяющие устранить выявленные недостатки.

В качестве средства, применяемого в подсистеме анализа защищенности, специалисты компании «Инфосистемы Джет» часто используют Xspider компании Positive Technologies. Сетевой сканер Xspider сертифицирован ФСТЭК России (сертификат соответствия № 1323от 23 января 2007 г., действителен до 23 января 2010 г.) и Министерством Обороны (сертификат соответствия № 354). Xspider – сетевой сканер безопасности, построенный на базе интеллектуального сканирующего ядра, которое обеспечивает максимально полное и надежное определение уязвимостей на системном и прикладном уровне. XSpider работает под управлением Microsoft Windows, он проверяет все возможные уязвимости независимо от программной и аппаратной платформы узлов, работает с уязвимостями на разном уровне – от системного до прикладного. В частности, XSpider включает мощный и глубокий анализатор защищенности WEB-серверов и WEB-приложений. Xspider поддерживает различные способы сканирования, в том числе и удаленное, при гарантии доступности сетевого сегмента.

В настоящее время компания Positive Technologies проводит работы по сертификации на отсутствие НДВ и соответствие ТУ системы оценки защищенности и контроля соответствия техническим политикам MaxPatrol.

В отличие от сканера безопасности, который оценивает только внешние уязвимости, MaxPatrol проводит внутренний аудит информационных ресурсов.

Применение системы MaxPatrol позволяет:

- Оценивать защищенность информационных систем. MaxPatrol выявляет бреши в защите

автоматизированных систем (АС), формирует задание на их устранение, отслеживает эффективность и своевременность устранения найденных уязвимостей.

- Отслеживать текущее состояние информационных ресурсов. MaxPatrol проводит инвентаризацию защищаемых ресурсов и позволяет своевременно обнаруживать изменения в АС, в частности, в настройках сетевого оборудования, правах пользователей на рабочих станциях, таблицах БД, мандантах ERP-систем.
- Контролировать соответствие АС техническим политикам. MaxPatrol формирует технические стандарты с использованием имеющейся в системе Базы Знаний, включающей комплексные стандарты для сетевого оборудования Cisco/Nortel/Huawei, платформ Windows/Linux/Solaris/, СУБД Microsoft SQL/Oracle, сетевых приложений, Web-служб, почтовых систем, ERP-приложений. MaxPatrol автоматически проводит инспекции на предмет соответствия АС сформированным техническим политикам безопасности.
- Измерять эффективность процессов ИБ в организации. На основе постоянно собираемой информации система формирует метрики безопасности (KPI), по которым оценивается эффективность процессов обеспечения ИБ. Существуют десятки различных метрик: от технических (например, процент рабочих станций, не удовлетворяющих антивирусной политике) до высокоуровневых (процент выполнения филиалом требований по безопасности в сравнении с другими филиалами на протяжении определенного времени). Метрики рассчитываются на основе реальных количественных данных, собранных модулями оценки защищенности, инвентаризации, контроля соответствия. В данный момент ведется сертификация системы MaxPatrol.

Выявление угроз НСД при межсетевом взаимодействии производится с помощью систем обнаружения вторжений (**подсистема обнаружения вторжений**). Такие системы строятся с учетом особенностей реализации атак и этапов их развития. Они основаны на следующих методах обнаружения атак: сигнатурные методы, методы выявления аномалий, комбинированные методы с использованием обоих названных методов.

Для обнаружения вторжений в ИСПДн 3 и 4 классов рекомендуется использовать системы

обнаружения сетевых атак, применяющие методы сигнатурного анализа, 1 и 2 класса — системы, применяющие сигнатурный метод и метод выявления аномалий.

В качестве средства для реализации подсистемы обнаружения и предотвращения вторжений специалисты компании «Инфосистемы Джет» часто используют продукты компании Cisco. Данные средства сертифицированы ФСТЭК и соответствуют требованиям технических условий и стандарту ГОСТ Р ИСО/МЭК 15408-2002.

К таким продуктам, в частности, относится Cisco Intrusion Detection System/Intrusion Preventing System (IPS/IDS), который является основным компонентом решений Cisco Systems по обнаружению и отражению атак. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки. Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating и Meta Event Generator не только помогают существенно уменьшить число ложных срабатываний, но и позволяют администраторам реагировать лишь на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам корпоративной сети.

Средства защиты каналов при передаче ПДн

Для обеспечения безопасности ПДн при передаче по открытым каналам или в несегментированной сети служит подсистема криптографической защиты каналов связи. Помимо вышеназванной задачи данная подсистема позволяет обеспечивать безопасное взаимодействие с технологическими сетями и доступ для осуществления удаленного администрирования. Данная подсистема может быть реализована на основе программно-аппаратного комплекса Cisco Adaptive Security Appliance. Этот комплекс сертифицирован ФСТЭК (соответствие руководящим документам по межсетевым экранам (3 и 4 Класс) и требованиям технических условий).

Cisco ASA 5500 предназначен для решения сразу нескольких задач — разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спама и атак типа «фишинг». Это достигается за счет объединения в одном устройстве лучших защитных средств — межсетевого экрана Cisco Pix, системы предот-

вращения атак Cisco IPS и Cisco VPN 3000 Concentrator.

Помимо описанных выше программно-технических средств защиты компания «Инфосистемы Джет» широко использует продукты других ведущих производителей на рынке информационной безопасности. К ним, в частности, относятся Oracle, Aladdin, Check Point, «С-Терра СиЭс-Пи», «КриптоПро». Данные компании проводят активную позицию по соответствию требований регуляторов и сертификации своих продуктов с целью их применения в решениях по защите персональных данных.

Требования к средствам защиты ПДн

Для реализации перечисленных подсистем, общая структура СЗПДн может включать в себя как существующие, так и дополнительные программно-аппаратные средства защиты информации.

В соответствии с Постановлением Правительства РФ от 17 ноября 2007 г. № 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» технические и программные средства, используемые для обработки данных в ИСПДн, должны в установленном порядке проходить процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации¹⁰.

Результаты оценки соответствия (сертификации) и тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности РФ.

К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Феде-

ральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации (происходящие, например, в ходе модернизации ИСПДн), предусмотренных указанными правилами, согласовывается с ФСТЭК и ФСБ.

Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации.

Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

Все сертифицированные ФСТЭК средства защиты представлены на сайте ФСТЭК (<http://www.fstec.ru/>) в разделе «Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации» (http://www.fstec.ru/_razd/_serto.htm) в подразделе «Государственный реестр сертифицированных средств защиты информации».

Этапы создания СЗПДн

Рекомендуются следующие этапы создания систем защиты персональных данных:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

¹⁰Под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями — периодически проводимые тематические исследования.

Предпроектное обследование

На этапе предпроектного обследования рекомендуются следующие мероприятия:

- устанавливается необходимость обработки данных в ИСПДн;
- определяется перечень ПДн, подлежащих защите от несанкционированного доступа;
- определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ);
- определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;
- определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- определяется класс ИСПДн;
- уточняется степень участия персонала в обработке данных, характер их взаимодействия между собой;
- определяются (уточняются) угрозы безопасности ПДн в конкретных условиях функционирования (разработка частной модели угроз).

Разработка технического задания

По результатам предпроектного обследования с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности данных, включаемые в техническое (частное техническое) задание на разработку системы защиты.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах; класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию информационная система; конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;

- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

Проектирование СЗПДн

На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;
- разработка раздела технического проекта на ИСПДн в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией;
- использование серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка;
- сертификация программных средств защиты информации по требованиям безопасности данных в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;
- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности ПДн;
- разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);
- выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности персональных данных.

Проектирование СЗПДн является одним из самых трудоемких и ответственных этапов по созданию системы защиты. Понимая это и имея значительный опыт в этой области, специалисты компании «Инфосистемы Джет» проводят работы с учетом следующих факторов:

- совместимости средств защиты со штатным программным обеспечением ИСПДн;
- степени снижения производительности функционирования ИСПДн по основному назначению;
- наличия подробной документации по эксплуатации средств защиты;
- возможность осуществления периодического тестирования или самотестирования средств защиты ПДн;
- возможность наращивания состава средств защиты новыми дополнительными средствами без осуществления ограничений работоспособности ИСПДн и «конфликта» с другими типами средств защиты;
- гармонизации средств защиты информации с уже существующими в информационной системе;
- масштабирование (распространение) применяемых решений по защите ПДн на остальные информационные системы.

Только учет данных факторов позволяет добиться того, что созданная в результате проектирования СЗПДн будет отвечать всем требованиям по защите и при этом не оказывать негативного влияния на работу модернизируемой (создаваемой) ИСПДн, а значит и на все бизнес-процессы организации.

Оценка соответствия ИСПДн требованиям безопасности персональных данных

Оценка соответствия ИСПДн по требованиям безопасности ПДн проводится:

- для ИСПДн 1 и 2 классов — обязательная сертификация (аттестация) по требованиям безопасности информации;
- для ИСПДн 3 класса — декларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению оператора);
- для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

Аттестация ИСПДн заказчика по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса ис-

пользуемых в ИСПДн мер и средств защиты данных.

Под аттестацией объекта информатизации понимается комплекс организационно-технических мероприятий, в результате которых специальным документом — «Аттестатом соответствия» подтверждается, что ИСПДн заказчика соответствуют требованиям стандартов и нормативно-технических документов по безопасности ПДн, утвержденных ФСТЭК России.

Оценка соответствия ИСПДн по требованиям безопасности информации включает в себя следующие работы:

1. Разработка пакета аттестационных документов. Формируется пакет организационно-распорядительной и технической документации на аттестуемую ИСПДн, содержащий:
 - программу и методику аттестационных испытаний;
 - проект документа «Перечень персональных данных, обрабатываемых в ИСПДн»;
 - проект документа «Перечень лиц, допущенных к обработке ПДн»;
 - проект документа «Перечень лиц, допущенных в помещения, в которых располагаются технические средства ИСПДн»;
 - проект документа «Акт классификации ИСПДн»;
 - проект документа «Акт внедрения СЗИ»;
 - технический паспорт на ИСПДн;
 - проекты приказов о назначении ответственных за обеспечение режима безопасности персональных данных;
 - инструкция по обеспечению безопасности персональных данных;
 - описание технологии обработки информации в ИСПДн.
2. Проведение аттестационных испытаний. Уровень безопасности информации, оцениваемый в процессе аттестационных испытаний, определяется классом ИСПДн (по классификации в соответствии с нормативно-методическими документами ФСТЭК России). При этом выполняются следующие работы:
 - проведение аттестационных испытаний ИСПДн;
 - разработка отчетных документов.

Аттестационные испытания ИСПДн осуществляются аттестационной комиссией, формируемой органом по аттестации, аккредитованным ФСТЭК России. Аттестационные испытания проводятся по программе и методике испытаний и в соответствии с Положением по аттестации объектов автоматизации.

Аттестационные испытания ИСПДн предполагают проведение следующих проверок:

- проверка состояния технологического процесса автоматизированной обработки персональных данных в ИСПДн;
- проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации;
- испытания ИСПДн на соответствие требованиям по защите информации от несанкционированного доступа.

Результатом работ на данном подэтапе является:

- Протокол аттестационных испытаний;
- Заключение по результатам аттестационных испытаний;
- Аттестат соответствия на ИСПДн (выдается в случае положительного Заключения);
- Акт о переводе СЗПДн в промышленную эксплуатацию (в случае наличия положительного заключения по результатам аттестационных испытаний ИСПДн).

Лицензирование деятельности по защите персональных данных

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и распределенных информационных системах 3 класса должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке.

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

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю. Срок действия лицензии составляет 5 лет и по его окончании может быть продлен по заявлению лицензиата.

Условия получения лицензии

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

- наличие в штате специалистов, имеющих квалификацию по вопросам технической защиты информации (прошедших специализированные курсы ФСТЭК);
- наличие помещений для осуществления обработки ПДн, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации;
- наличие испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
- использование ИСПДн, а также средств защиты ПДн, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
- использование предназначенных для обработки ПДн программ для электронно-вычислительных машин и баз данных;
- наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным ФСТЭК.

Порядок получения лицензии

Для получения лицензии на деятельность по технической защите ПДн необходимо выполнить следующие работы:

1. Подготовить комплект документов для предоставления в ФСТЭК РФ. К ним относятся:
 - Заявление;
 - Копии учредительных документов (заверенные нотариусом);
 - Копии свидетельства о государственной регистрации соискателя лицензии в качестве юридического лица (нотариально заверенные);
 - Копия свидетельства о поставке соискателя лицензии на учет в налоговом органе (нотариально заверенная);
 - Пояснительная записка;
 - Копии документов, подтверждающих право собственности, право хозяйственного ведения на помещения;
 - Копия аттестата соответствия на защищаемое помещение;

- Копии документов на ИСПДн (Технический паспорт, Акт классификации ИСПДн, план размещения ОТСС и ВТСС, аттестат соответствия на ИСПДн, перечень защищаемых ресурсов ИСПДн), описание технологического процесса обработки информации в ИСПДн;
 - Копии документов, подтверждающих право на используемые программы для ЭВМ и базы данных (лицензии);
 - Сведения о наличии производственного и контрольно-измерительного оборудования, средствах защиты информации, средствах контроля защищенности с приложением копий документов о проверке контрольно-измерительного оборудования;
 - Сведения об имеющихся нормативно-правовых актах, нормативно-методических документах по вопросам технической защиты информации.
2. Подготовить не менее двух специалистов, которые будут осуществлять деятельность по защите ПДн (оказывать услуги по защите ПДн) на специализированных курсах ФСТЭК.
 3. Подготовить и провести аттестацию испытаний защищаемого помещения, которая включает: обследование, разработку пакета организационно-распорядительных документов, подготовку и проведение аттестационных мероприятий.
 4. Получить нормативно-методические документы: «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» и «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам».
 5. Предоставить документы во ФСТЭК РФ.

Защита ПДн при неавтоматизированной обработке

Защита ПДн при неавтоматизированной обработке осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Персональные данные при их обработке, осуществляемой без использования средств авто-

матизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

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

Лица, осуществляющие обработку персональных данных, как сотрудники организации-оператора, так и уполномоченного лица (осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

При разработке и использовании типовых форм документов, в которые предполагается включение ПДн, должны соблюдаться определенные условия по их содержанию. Например, они должны содержать сведения о цели обработки, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения ПДн, сроки их обработки, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн, поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку персональных данных и т.п.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться условия:

- наличие акта о необходимости ведения такого журнала, содержащего цели, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к ним и ответственных за их ведение и сохранность, сроки обработки персональных данных, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится оператор;
- недопустимость копирования содержащейся в таких журналах (реестрах, книгах) информации;

- персональные данные каждого субъекта могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта на территорию.

Должна обеспечиваться раздельная фиксация на материальный носитель ПДн, имеющих различную цель обработки. Если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению их раздельной обработки.

В отношении каждой категории ПДн должны быть определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. При этом перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Защита биометрических ПДн

С точки зрения формирования требований к защите персональных данных существует два типа биометрических данных. Первый тип — биометрические данные, которые обрабатываются в ИСПДн. Требования к их защите определены в постановлении Правительства РФ от 17 ноября 2007 г. № 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и ничем не отличаются от требований к защите обычных ПДн, которые обрабатываются в информационных системах.

Второй тип — это биометрические данные, обрабатываемые вне информационных систем персональных данных. Требования по защите таких ПДн сформулированы в Постановлении 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».

При этом под материальным носителем информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека, и на основе которых можно установить его личность.

Материальный носитель таких ПДн должен обеспечивать:

- защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;
- возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими ПДн;
- возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических ПДн, а также оператора, осуществившего такую запись;
- невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

Оператор биометрических данных, используемых вне ИСПДн, обязан:

- осуществлять учет количества экземпляров материальных носителей;
- осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Технологии хранения биометрических персональных данных вне ИСПДн должны обеспечивать доступ к информации, содержащейся на материальном носителе, применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических ПДн, записанных на материальный носитель, а также проверку наличия письменного согласия субъекта ПДн на обработку его биометрических персональных данных.

При хранении биометрических персональных данных вне ИСПДн должна обеспечиваться

регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

Защита ПДн при трансграничной передаче

В законодательстве особое внимание уделено безопасности ПДн при их передаче за пределы Российской Федерации. Такая передача называется трансграничной.

До начала осуществления трансграничной передачи персональных данных оператор ПДн обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов ПДн. Министерство связи и массовых коммуникаций РФ (Минкомсвязи) в своем письме № ДС-П11-2502 от 13.05.2009 определило «адекватную защиту» как защиту, при которой «обеспечивается уровень защищенности прав субъектов персональных данных не ниже, чем в Российской Федерации».

Одним из критериев оценки государства в данном аспекте может выступать факт ратификации им «Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г., ETS № 108. На сегодняшний день в число стран, подписавших и ратифицировавших указанную Конвенцию, входят: Австрия, Андорра, Бельгия, Болгария, Да-

ния, Великобритания, Венгрия, Германия, Греция, Израиль, Ирландия, Исландия, Испания, Италия, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словакия, Словения, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония.

Специфика защиты ПДн для различных вертикальных рынков

Компания «Инфосистемы Джет» учитывает специфику исполнения Закона организациями из разных отраслей. К сожалению, многие поставщики решений по защите персональных данных применяют типовой подход как с точки зрения этапности и состава работ, так и подбора средств защиты. Наши специалисты стараются избежать такой «уравниловки». К примеру, при разработке решений по защите персональных данных в телекоммуникационных организациях специалисты компании «Инфосистемы Джет» учитывают специфику работы с абонентскими базами и биллинговыми системами операторов связи. В случае с кредитно-финансовыми организациями многие компании большое внимание уделяют стандарту СТО БР, поэтому важно при проведении работ по защите персональных данных подбирать такие решения, которые могли бы одновременно закрывать требования и законодательства, и стандарта.

В каких случаях не надо обеспечивать «адекватную защиту» ПДн при трансграничной передаче?..

Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных. То есть субъект ПДн как минимум должен письменно заверить оператора, что «он разрешает организации, которая обрабатывает его персональные данные, не защищать их при передаче за границу». Автор данной статьи скептически относится к такой возможности;
- предусмотренных международными договорами Российской Федерации по вопросам

выдачи виз, а также международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;

- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Таб. 2. Нормативно-правовые акты, устанавливающие требования по защите ПДн для различных вертикальных рынков

Отрасль	Законодательный или нормативный акт, регулирующий защиту ПДн	Описание
Государственные организации	Указ Президента Российской Федерации от 30 мая 2005 г. N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»	4. Руководителям государственных органов: - обеспечить защиту персональных данных государственных гражданских служащих Российской Федерации, содержащихся в их личных делах, от неправомерного их использования или утраты за счет средств государственных органов в порядке, установленном федеральными законами; - определить лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных государственных гражданских служащих Российской Федерации в государственном органе и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.
Торговля	Постановление Правительства Российской Федерации от 27 сентября 2007 г. N 612 «Об утверждении Правил продажи товаров дистанционным способом»	Статья 16: Продавец должен обеспечивать конфиденциальность персональных данных о покупателе в соответствии с законодательством Российской Федерации в области персональных данных.
Транспорт	Федеральный закон Российской Федерации от 9 февраля 2007 г. N 16-ФЗ «О транспортной безопасности»	Статья 7: Субъект транспортной инфраструктуры ... обеспечивает передачу данных, содержащихся в проездных документах (билетах), в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ «О персональных данных»
Воздушный транспорт	Федеральный закон Российской Федерации от 4 декабря 2007 г. N 326-ФЗ «О внесении изменения в статью 85 (1) Воздушного кодекса Российской Федерации»	Статья 85.1. Персональные данные пассажиров воздушных судов 1. В целях обеспечения авиационной безопасности перевозчики обеспечивают передачу персональных данных пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с законодательством Российской Федерации о транспортной безопасности и законодательством Российской Федерации в области персональных данных.
Туристический бизнес	Постановление Правительства Российской Федерации от 18 июля 2007 г. N 452 «Об утверждении Правил оказания услуг по реализации туристского продукта»	Исполнитель (Туроператор) в соответствии с положениями Федерального закона «О персональных данных» принимает необходимые меры по обеспечению безопасности информации о полученных исполнителем в процессе оказания услуг персональных данных потребителя, в том числе при их обработке и использовании.
Медицина	Приказ Федерального фонда обязательного медицинского страхования от 19 августа 2008 г. N 180 «Об утверждении Положения о защите персональных данных работников Федерального фонда обязательного медицинского страхования»	Статья 3.2. В процессе хранения персональных данных работников ФОМС должны обеспечиваться: - требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений; - сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением; - контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

В своей деятельности компания «Инфосистемы Джет» также ориентируется на российское законодательство. В таблице №2 представлены нормативные акты, которые устанавливают требования в данной области для организации различных отраслей.

Компания «Инфосистемы Джет» имеет большой опыт проведения проектов в кредитно-финансовых организациях. В частности, в следующем разделе статьи приводится пример одного из решений, которое было реализовано в одном из крупных российских банков.

Обеспечение безопасности ПДн в кредитно-финансовых организациях

К персональным данным для сегмента автоматизированной банковской системы, связанного с ведением кредитной истории клиента, перечень обрабатываемых ПДн можно определить на основании Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях». В соответствии с данным Законом необходимо иметь следующие сведения о заемщике:

- фамилия, имя, отчество;
- дата и место рождения;
- данные паспорта или иного документа, удостоверяющего личность (номер, дата и место выдачи, наименование выдавшего его органа);
- ИНН;
- страховой номер индивидуального лицевого счета;
- место регистрации и фактическое место жительства;
- сведения о государственной регистрации физического лица в качестве индивидуального предпринимателя.

Если учесть, что количество клиентов, кредитование которых осуществляет среднестатистический Банк, составляет не менее 80 000 человек, то такая совокупность параметров позволяет сделать вывод о том, что АБС относится к ИСПДн 2-го класса. А так как эти данные требуют обеспечения не только конфиденциальности, но и доступности и целостности, то мы относим АБС к специальной ИСПДн 2-го класса. По режиму обработки персональных данных рассматриваемая ИСПДн относится к многопользовательской, а по разграничению прав доступа — к системе с разными правами доступа к ПДн. Это требует проведения определенных мероприятий по обеспечению безопасности.

В подсистеме управления доступом должны осуществляться следующие мероприятия:

- идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- межсетевое экранирование — не ниже третьего уровня защищенности (при наличии подключения к сетям общего пользования в распределенной ИСПДн МЭ должен выполнять функции, как и с ИСПДн 1 класса с многопользовательским режимом и равными правами доступа пользователей);
- идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних

устройств компьютеров по логическим именам;

- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

В подсистеме регистрации и учета должны осуществляться следующие мероприятия:

- регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее корректного выключения;
- учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема);
- регистрация выдачи печатных (графических) документов на «твердую» копию;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрация попыток доступа программных средств к следующим объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей;
- учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей.

В подсистеме обеспечения целостности должны проводиться следующие мероприятия:

- резервное копирование ПДн на отчуждаемые носители информации;
- обеспечение целостности средств защиты от программно-математических воздействий.

В подсистеме антивирусной защиты должны проводиться следующие мероприятия:

- на всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений программно-математических воздействий.

В подсистеме защиты от утечки данных в ИСПДн по техническим каналам для ИСПДн 2-го класса использовались СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Контроль и надзор за выполнением требований законодательства

В соответствии со статьей 23 Федерального Закона «О персональных данных» для обеспечения контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона назначается Уполномоченный орган по защите прав субъектов персональных данных (далее, регулятор). Такие функции возложены на три организации:

- на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных;
- на Федеральную службу безопасности РФ в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн;
- на Федеральную службу по техническому и экспортному контролю в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПДн (не криптографическими методами) при их обработке в ИСПДн.

В рамках своих полномочий регуляторы имеют право проводить плановые и внеплановые проверки.

Роскомнадзор проводит плановые проверки с целью контроля сведений, указанных в уве-

домлении уполномоченного органа по защите ПДн, а также внеплановые — на основании заявления физических лиц с целью проверки информации, указанной в данном заявлении.

ФСБ России имеет право проводить плановые проверки:

- представление по запросу отчета по лицензируемым видам деятельности;
- представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы, в составе которых эксплуатируются системы криптографической защиты информации (СКЗИ);
- явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

ФСТЭК РФ уполномочен осуществлять плановые проверки:

- представление по запросу отчета по лицензируемым видам деятельности;
- представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы;
- представление копий аттестатов соответствия на защищаемые помещения по требованиям безопасности;
- явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

В рамках межведомственного сотрудничества между Роскомнадзором, ФСТЭК России и ФСБ РФ достигнута договоренность о проведении совместных мероприятий по контролю и надзору в области персональных данных.

Роскомнадзор

Роскомнадзор рассматривает обращения субъекта ПДн о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение. Он имеет право:

- запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осу-

- осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных дан-

ных и представлять интересы субъектов персональных данных в суде;

- направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

Итоги Роскомнадзора за 2008 год

В рамках выполнения функций по государственному контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных Роскомнадзором в 2008 году проведено 76 мероприятий по контролю и надзору, в том числе 36 плановых и 40 внеплановых мероприятий.

По результатам проверок выписано 19 предписаний об устранении выявленных нарушений Федерального закона «О персональных данных», 5 материалов направлено в органы прокуратуры, 11 — в судебные органы.

Выявленные нарушения классифицированы по следующим статьям Кодекса Российской Федерации об административных правонарушениях:

- ст. 13.11. — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- ст. 19.7. — непредставление или несвоевременное представление в государственный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а равно представление в государственный орган таких сведений в неполном объеме или искаженном виде.

С начала возложения на Роскомнадзор полномочий по защите прав субъектов персональных данных поступило 146 обращений: из них даны ответы заявителям — 60, направлены в правоохранительные органы — 5, органы прокуратуры — 24, в судебные органы — 22, на момент выхода данной статьи находилось на рассмотрении — 35.

В результате взаимодействия с правоохранительными органами приостановлена деятель-

ность интернет-ресурсов www.nomer.org.ru и www.vslomaj.com, предоставляющих услуги доступа к персональным данным граждан Российской Федерации.

В 2008 году прошли первые судебные процессы по искам в области защиты прав субъектов персональных данных. Судебными инстанциями из 22 административных дел семь рассмотрены в пользу субъектов персональных данных, в шести случаях вынесены решения об отказе в исковых требованиях, девять административных дел на конец года находились в судебном производстве.

Чаще всего субъекты персональных данных обращаются по фактам нарушений Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

- главы 2 статьи 5 «Принципы обработки персональных данных»;
- статьи 6 «Условия обработки персональных данных»;
- статьи 9 «Согласие субъекта персональных данных на обработку своих персональных данных».

Изложенные в обращениях факты нарушения федерального законодательства в ходе рассмотрения подтвердились в большинстве случаев.

Анализ категорий операторов, осуществляющих обработку персональных данных, на действия которых чаще всего поступают обращения от субъектов персональных данных, позволяет утверждать, что «лидерами» являются:

- кредитные учреждения — 34;
- жилищно-коммунальные организации — 21;
- операторы связи — 10;
- страховые компании — 9.

- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
- вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;
- привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

Для решения поставленных задач Уполномоченным органом по защите прав субъектов персональных данных 28 декабря 2007 года был создан координационный центр на федеральном уровне — Управление по защите прав субъектов персональных данных и территориальные органы в субъектах Российской Федерации — соответствующие структурные подразделения в 78 территориальных органах.

Выводы

Государство создало необходимые условия для выполнения требований по безопасности персональных данных. Оно определило понятия ПДн и операторов, которые эти данные обрабатывают. Согласно Законодательству операторами ПДн являются практически все организации, которые ведут свою деятельность на территории РФ, поскольку они как минимум осуществляют сбор, систематизацию и хранение сведений о своих сотрудниках, клиентах и партнерах.

Государство возложило на операторов ПДн определенные обязанности. Важнейшим из них является обеспечение безопасности персональных данных. Это означает, что оператор ПДн обязан принять все необходимые меры для обеспечения конфиденциальности (а в некоторых случаях доступности и целостности) сведений о субъектах ПДн. Уполномоченные государством органы разработали требования по созданию системы защиты персональных данных и конкретизировали их в нормативно-методических документах.

Практика показала, что реализовать данные требования самостоятельно организациям достаточно сложно. На помощь им приходят

специализированные компании, работающие на рынке информационной безопасности. Имея в своем распоряжении достаточные и квалифицированные ресурсы, компании-интеграторы способны реализовать требования законодательства в конкретных решениях.

Защита персональных данных является сегодня приоритетным направлением деятельности Центра информационной безопасности компании «Инфосистемы Джет». Специалисты нашей компании рассматривают эту задачу не только как выполнение требований российского и международного законодательства, но и как возможность создать полноценную систему обеспечения безопасности.

Накопив значительный опыт в проведении проектов по обеспечению информационной безопасности, специалисты компании «Инфосистемы Джет» разработали свой подход к реализации задачи защиты персональных данных. Он базируется на государственных стандартах (ГОСТ 34.201-89, ГОСТ 34.601-90), нормативных актах и документах регулирующих органов, а также на экспертном опыте наших специалистов.

При этом главными принципами при проведении проектов по реализации требований российского законодательства в области защиты персональных данных наша компания считает:

- **Минимизацию затрат на создание СЗПДн.** Компания «Инфосистемы Джет» одной из основных задач в проектах по приведению ИСПДн в соответствие с нормативной базой видит минимизацию расходов заказчиков. Это становится возможным, в первую очередь, за счет оптимизации процессов обработки и хранения персональных данных, из которых исключаются избыточные звенья и ненужные процедуры, сокращения неоправданно большого объема ПДн, рассмотрения возможности их обезличивания, замены персональных данных на условные обозначения или коды, исключения избыточных ИСПДн и сужения круга лиц, вовлеченных в процесс обработки ПДн, а также внедрения альтернативных механизмов защиты.
- **Защиту персональных данных как важнейшего элемента общей системы информационной безопасности организации.** Компания «Инфосистемы Джет» делает акцент не только на удовлетворении нормативных требований, но и на повышении фактической защищенности персональных данных, защите не только средств обработки ПДн, но и самих персональных данных. Здесь речь

идет об информации, которая выходит за рамки ИСПДн и попадает в руки сотрудников, имеющих легальный доступ к персональным данным. По статистике более 80% утечек происходит по вине этих сотрудников (как умышленно, так и по неосторожности). Специалисты компании «Инфосистемы Джет» видят решение этой задачи в построении правильного процесса обработки персональных данных всеми вовлеченными в него сотрудниками, использовании дополнительных механизмов защиты, что в свою очередь повышает общий уровень информационной безопасности компании.

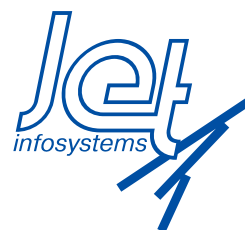
Необходимость учета отраслевой специфики при проведении проектов. Компания «Инфосистемы Джет» учитывает специфику исполнения Закона организациями из разных отраслей. При этом наши специалисты стараются избежать типового подхода как к этапности проведения работ, так и к подбору средств защиты. Это позволяет находить такие решения, которые могли бы одновременно закрывать требования и Закона, и отраслевых стандартов, учитывать при разработке решений по защите персональных данных специфику деятельности организации и ведения ее бизнес-процессов.

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Главный редактор: Дмитриев В.Ю. (vlad@jet.msk.su)
Редактор: Слободчикова Т.А. (slobodchikova@jet.msk.su)
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
[email: JetInfo@jet.msk.su](mailto:JetInfo@jet.msk.su) <http://www.jetinfo.ru>



Издатель: компания «Инфосистемы Джет»

Подписной индекс по каталогу Роспечати

32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем