152 ФЗ – Что? Как? Когда?

Методическое пособие для руководителей ИТ службы

К читателю

Уважаемый руководитель ИТ службы!

Вы держите в руках документ, который должен ответить Вам на вопросы:

- Что такое ФЗ 152?
- Коснется ли меня этот закон?
- Что мне нужно делать и нужно ли что-то делать?
- Как будет контролироваться исполнение закона?
- Что уже сделали мои коллеги, ИТ руководители других компаний?
- Что предлагают делать ИТ компании? Какие советы дают эксперты по информационной безопасности?

Документ подготовлен Клубом 4CIO при участии ИТ компаний и представителей ИТ сообщества. Все материалы, собранные нами в данном документе, получены официальным путем и публикуются с разрешения авторов.

Оглавление

Введение

7 ноября 2001 года Российская Федерация подписала конвенцию Европы о защите физических лиц при автоматизированной обработке персональных данных. Согласно этой конвенции, государством был принят Федеральный закон №152 «О персональных данных». По этому закону организации и компании, если они обрабатывают персональные данные людей такие, как:

- имя,
- фамилия,
- год рождения,
- адрес,
- группа крови,
- другие данные,

должны эти данные защищать, с целью обеспечения защиты свободы и прав человека и гражданина.

Основная статья 152 ФЗ – ст.19 «Меры по обеспечению безопасности персональных данных при их обработке». Согласно этой статье, компании и организации должны привести свои информационные системы, в которых обрабатываются персональные данные, в соответствие с предъявленными требованиями до 1 января 2010 года.

Данный закон коснется государственных органов, муниципальных органов, юридических лиц и физических лиц, которые осуществляют обработку персональных данных. Таким образом, 90% организаций и компаний, осуществляющих деятельность на территории Российской Федерации, попадают под действие данного закона.

1. Основные понятия

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. То есть, согласно данной формулировке, к операторам можно отнести 90% организаций, занимающихся различной деятельностью.

Обязанности оператора:

- Операторами должна обеспечиваться конфиденциальность ПДн.
- Информационные системы персональных данных (ИСПДн), созданные до дня вступления в силу Федерального закона (до 26.01.2007), должны быть приведены в соответствие с требованиями не позднее 1 января 2010 года.
- Операторы, которые осуществляют обработку ПДн, обязаны направить уведомление в уполномоченный орган (Роскомнадзор).
- Операторы должны провести классификацию ИСПДн в зависимости от объемов обрабатываемых ими ПДн и угроз безопасности жизненно важным интересам личностей, общества и государства.
- Порядок проведения классификации информационных систем установлен совместно ФСТЭК России, ФСБ России и Минкомсвязи.
- Средства защиты информации, применяемые в ИСПДн, проходят процедуру оценки соответствия. Результаты оценки соответствия оцениваются в ходе экспертизы, осуществляемой ФСТЭК России и ФСБ России в пределах их полномочий.

Перечень объектов автоматизации:

Аттестации в системе средств защиты информации по требованиям, предъявляемым к безопасности информации, подлежат:

- Автоматизированные системы различного уровня и назначения.
- Системы связи, приема, обработки и передачи данных.
- Системы отображения и размножения.
- Помещения, предназначенные для ведения конфиденциальных переговоров.

2. Федеральные законы, постановления, документы

2.1 Федеральные законы и постановления

- ✓ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» - http://pd.rsoc.ru/low/document7.htm
- ✓ Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» - http://www.zki.infosec.ru/law/personal/doc/155/
- ✓ Постановление Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» - http://pd.rsoc.ru/low/document21.htm
- ✓ Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» - http://pd.rsoc.ru/low/document38.htm
- ✓ Постановление правительства РФ «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 года № 687» - http://pd.rsoc.ru/low/document45.htm
- ✓ Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 марта 2008 г. N 154 "Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных" - http://base.garant.ru/193180.htm
- ✓ Приказ Россвязькомнадзора №08 от 17.07.2008 «Об утверждении образца формы уведомления об обработке персональных данных» - http://www.zki.infosec.ru/law/personal/doc/145/

2.2 Методические документы ФСТЭК России и ФСБ России

- ✓ - Порядок проведения классификации информационных систем ПД.
- ✓ - Базовая модель угроз безопасности ПД при их обработке в ИС ПД (РД ФСТЭК от 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»). *Документ ДСП. Высылается ФСТЭК по прямому запросу компании*
- ✓ - Методика определения угроз безопасности ПД при их обработке в ИСПД (РД ФСТЭК от 14.02.2008 «Методика определения актуальных угроз»). *Документ ДСП. Высылается ФСТЭК по прямому запросу компании*
- ✓ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных»; *Документ ДСП. Высылается ФСТЭК по прямому запросу компании*
- ✓ «Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России). *Документ ДСП. Высылается ФСТЭК по прямому запросу компании*

- ✓ - Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" от 21 февраля 2008 года. http://www.zki.infosec.ru/law/personal/doc/139/
- ✓ - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации" от 21 февраля 2008 года. http://www.zki.infosec.ru/law/personal/doc/140/

3. Регуляторы

3.1. Роскомнадзор

Роскомнадзор – федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. http://www.rsoc.ru/

Роскомнадзор ведет:

- реестр операторов, занимающих существенное положение в сети связи общего пользования;
- единые общероссийские реестры средств массовой информации;
- реестры лицензий.

Деятельность, связанную с ведением реестра операторов персональных данных, Роскомнадзор осуществляет в соответствии с прямой нормой Федерального закона №152.

Роскомнадзор имеет право:

- запрашивать и получать сведения, необходимые для принятия решений в сфере своей компетенции;
- применять в сфере своей компетенции меры профилактического и пресекательного характера, направленные на недопущение нарушений юридическими лицами и гражданами обязательных требований в этой сфере и (или) ликвидацию последствий таких нарушений.

На Роскомнадзор, как на уполномоченный орган по защите прав субъектов персональных данных, возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона. В то же время, не имея технической, методологической и кадровой базы для обеспечения организации и контроля эффективности специальных и технических требований по защите информации, Роскомнадзор в соответствии с Федеральным законом играет важнейшую связующую и организующую роль, и прежде всего в области защиты законных прав субъектов персональных данных от рисков и потерь, связанных с незаконным использованием их персональных данных.

3.2. ФСТЭК России

ФСТЭК (Федеральная служба по техническому и экспортному контролю) России является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию и по противодействию техническим средствам разведки на территории Российской Федерации (далее именуется - техническая защита информации). http://www.fstec.ru/

ФСТЭК России имеет право:

- ✓ - осуществлять контроль деятельности по технической защите информации, определять порядок, формы и методы контроля;
- ✓ - выдавать предписания на приостановление работ на объектах в случае выявления в ходе осуществления контроля нарушений норм и требований, касающихся технической защиты информации;

- ✓ - запрашивать и получать от организаций и должностных лиц необходимые для осуществления деятельности ФСТЭК России информацию, документы и материалы;
- ✓ - приостанавливать или отменять действие выданных сертификатов;
- ✓ - вносить в установленном порядке представления о применении мер ответственности за нарушения законодательства Российской Федерации по вопросам ее деятельности;
- ✓ - рассматривать в пределах своей компетенции дела об административных правонарушениях;
- ✓ - издавать в пределах своей компетенции нормативные правовые акты, методические документы и индивидуальные правовые акты;
- ✓ - осуществлять контроль за соблюдением лицензионных требований и условий организациями, имеющими лицензии ФСТЭК России, при осуществлении ими лицензируемых видов деятельности, приостанавливать в установленном порядке действие выданных лицензий.

Согласно Положению № 781, **ФСТЭК России в пределах своих полномочий:**

- ✓ - устанавливает методы и способы защиты информации в информационных системах, предназначенных для хранения и обработки персональных данных;
- ✓ - определяет возможные каналы утечки информации при обработке персональных данных в информационных системах;
- ✓ - осуществляет экспертизы для оценки соответствия и (или) тематические исследования средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах;
- ✓ - согласовывает правила пользования средствами защиты информации, предназначенными для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаемые к указанным средствам, а также изменение условий применения этих средств;
- ✓ - определяет перечни индексов, условных наименований и регистрационных номеров средств обеспечения безопасности персональных данных при их обработке в информационных системах, используемых для учета этих средств.

3.2. ФСБ России

ФСБ (Федеральная Служба Безопасности). Одной из основных задач ФСБ России является организация обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Для решения указанной задачи **ФСБ России в пределах своих полномочий** осуществляет следующие функции:

- ✓ - координирует деятельность Федеральных органов исполнительной власти и организаций по обеспечению криптографической безопасности информационно-телекоммуникационных систем;
- ✓ - определяет порядок осуществления контроля за организацией и функционированием криптографической безопасности информационно-телекоммуникационных систем;

- ✓ - разрабатывает и утверждает нормативные и методические документы по вопросам обеспечения информационной безопасности информационно-телекоммуникационных систем и сетей критически важных объектов, а также организует и осуществляет контроль за обеспечением информационной безопасности указанных систем и сетей.

Согласно статье 19 Федерального закона № 152, ФСБ России, как Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, осуществляет контроль и надзор за выполнением установленных Правительством РФ требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных в пределах своих полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Согласно Положению № 781, **ФСБ России в пределах своих полномочий**:

- ✓ - устанавливает методы и способы защиты информации в информационных системах, предназначенных для хранения и обработки персональных данных;
- ✓ - определяет возможные каналы утечки информации при обработке персональных данных в информационных системах;
- ✓ - осуществляет экспертизы для оценки соответствия и (или) тематические исследования средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах;
- ✓ - определяет сроки проведения контрольных тематических исследований в отношении шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах;
- ✓ - согласовывает правила пользования средствами защиты информации, предназначенными для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаемые к указанным средствам, а также изменение условий применения этих средств;
- ✓ - определяет перечни индексов, условных наименований и регистрационных номеров средств обеспечения безопасности персональных данных при их обработке в информационных системах, используемых для учета этих средств;
- ✓ - устанавливает особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах.

4. Ответственность операторов

4.1. Кодекс об Административных правонарушениях РФ:

- ✓ - Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет за собой наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда (МРОТ), на должностных лиц – от пяти до десяти МРОТ, а на юридических лиц – от пятидесяти до ста МРОТ.
- ✓ - Статья 13.12. Нарушение правил защиты информации. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, влечет наложение административного штрафа на граждан в размере от пяти до десяти МРОТ с конфискацией этих средств, на должностных лиц – от десяти до двадцати МРОТ, а на юридических лиц – от ста до двухсот МРОТ труда с конфискацией несертифицированных средств .
- ✓ - Разглашение информации, доступ к которой ограничен федеральным законом, и в частности, персональных данных, (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, которое имело к ней доступ по служебным или профессиональным обязанностям карается административным штрафом от пяти до пятидесяти МРОТ.
- ✓ Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль). (в ред. Федерального закона от 20.08.2004 N 114-ФЗ). 2. Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа - (в ред. Федеральных законов от 20.08.2004 N 114-ФЗ, от 08.05.2006 N 65-ФЗ, от 09.04.2007 N 45-ФЗ) влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до десяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от двухсот тысяч до пятисот тысяч рублей. (в ред. Федеральных законов от 09.05.2005 N 45-ФЗ, от 22.06.2007 N 116-ФЗ)

4.2. Уголовный Кодекс РФ:

- ✓ Статья 137. Нарушение неприкосновенности частной жизни. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации - наказываются штрафом, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев...»
- ✓ Статья 140. Отказ в предоставлении гражданину информации. Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, - наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет...»
- ✓ Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном

носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет…»

4.3. Трудовой Кодекс РФ:

Глава 14. Защита персональных данных работника

- ✓ Статья 85. Понятие персональных данных работника. Обработка персональных данных работника. Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.
- ✓ Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:
  - обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
  - при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;
  - все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;
  - работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
  - работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами; при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения; защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;

работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
работники не должны отказываться от своих прав на сохранение и защиту тайны;
работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

- ✓ Статья 87. Хранение и использование персональных данных работников. Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований настоящего Кодекса и иных федеральных законов.
- ✓ Статья 88. Передача персональных данных работника. При передаче персональных данных работника работодатель должен соблюдать следующие требования:
  - не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;
  - не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
  - предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;
  - осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
  - разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
  - не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
  - передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
- ✓ Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:
  - полную информацию об их персональных данных и обработке этих данных;
  - свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
  - определение своих представителей для защиты своих персональных данных;
  - доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

✓ Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. (в ред. Федерального закона от 30.06.2006 N 90-ФЗ).

5. Мероприятия по обеспечению безопасности ПДн

- Определение угроз безопасности ПДн, формирование модели угроз.
- Разработка на основе модели угроз системы защиты персональных данных (СЗПДн) с использованием методов и способов защиты, предусмотренных для соответствующего класса ИС
- Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
- описание СЗПДн

6. Классификация ИСПДн

$X_{пд}$ \ $X_{нпд}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Рис.1. таблица классификации ИС.

Расшифровка таблицы классификации ИС

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

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

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

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

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.

$X_{нпд}$ может принимать следующие значения:

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом.

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, 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 персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

7. Порядок построения систем защиты персональных данных.

Типовой порядок при их обработке в информационных системах.

От чего отталкиваемся?

Не углубляясь в рассмотрение всего правового поля, охватывающего вопросы создания систем защиты персональных данных (СЗПДн), отметим лишь, во-первых, необходимость обязательного обращения к методическим документам регуляторов – ФСТЭК России и ФСБ России. И прежде всего – ФСТЭК России, поскольку ориентироваться на документы ФСБ России необходимо лишь в случае использования в СЗПДн средств криптографической защиты информации (СКЗИ).

Среди документов ФСТЭК России в свою очередь выделим «Основные мероприятия…»[11]. Следует также руководствоваться РД «Рекомендации…»[2], а также четко представлять себе методологии защиты, разработанные в ФСТЭК России для защиты конфиденциальной информации вообще и изложенные в руководящем документе от 2002 года – «СТР-К».

Кроме того, порядок создания СЗПДн должен соответствовать рекомендациям ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения».

Стадии создания СЗПДн

Согласно «Основным мероприятиям…» и ГОСТ, создание СЗПДн должно включать следующие стадии и этапы:

предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

стадия проектирования и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания, а также оценку соответствия ИСПДн требованиям безопасности информации.

Предпроектная стадия

В ходе предпроектного обследования ИСПДн:

определяется перечень ПДн, обрабатываемых в ИСПДн, и в них выделяется совокупность ПДн, подлежащих защите;

определяются условия размещения технических средств ИСПДн и доступа к ним;

определяются конфигурация и топология ИСПДн, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами;

определяются технические средства и системы, составляющие ИСПДн, используемые общесистемные и прикладные программные средства;

определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;

определяется класс ИСПДн;

[1] Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных

[2] Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

уточняется степень участия должностных лиц в обработке ПДн, характер их взаимодействия между собой;

определяются (уточняются) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн, разрабатывается модель угроз.

По результатам предпроектного обследования разрабатывается техническое (частное техническое) задание на разработку СЗПДн, в которое включаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн.

Стадия проектирования и реализации ИСПДн

На стадии проектирования и создания ИСПДн в соответствии с требованиями ТЗ (ЧТЗ) на разработку СЗПДн:

разрабатывается задание на проведение работ и выполняются работы в соответствии с проектной документацией;

разрабатываются мероприятия по защите информации в соответствии с предъявляемыми требованиями;

проводится обоснование состава и закупка технических средств ИСПДн и сертифицированных средств защиты информации и их установка;

осуществляется разработка эксплуатационной и организационно-распорядительной документации на ИСПДн по обеспечению режима информационной безопасности при обработке ПДн и разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;

выполняются другие мероприятия, характерные для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

Стадия ввода в действие СЗПДн

На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

приемо-сдаточные испытания СЗПДн по результатам опытной эксплуатации;

оценка соответствия ИСПДн требованиям по безопасности ПДн.

Виды и особенности работ

Вне зависимости от того, привлекает ли организация для проведения работ по проектированию и созданию СЗПДн специализированную стороннюю организацию или строит систему защиты самостоятельно, она должна решить следующие основные задачи.

1) **Категорирование ПДн.** Иметь четкое представление об использовании персональных данных в своей производственной деятельности. Перечень обрабатываемых ПДн утвердить приказом руководителя. Включить в него сведения о подразделениях и сотрудниках, допущенных к соответствующим категориям ПДн.

2) **Изучение бизнес-процессов.** Идентифицировать и описать бизнес-процессы, связанные с обработкой ПДн. Определить, посредством каких программных и технических средств реализуется каждый из этих процессов.

3) **Составление схемы сети.** Вычертить функциональную схему корпоративной сети организации, на которой отметить технические средства, задействованные в обработке ПДн, и казать линии связи, по которым осуществляется передача ПДн.

4) Составление карты сети. Вычертить карту сети, на которой указать помещения, серверы, АРМ, прочие технические средства, используемые для обработки ПДн, места прокладки линий, по которым передаётся защищаемая информация.

5) Сегментация сети. Используя представление о бизнес-процессах, схему и карту сети, выделить в инфраструктуре сети отдельные совокупности технических средств – сегменты сети, в каждом из которых:

- обрабатываются исключительно свойственные для данной совокупности технических средств категории ПДн;

- ставятся цели обработки ПДн, отличные от целей обработки ПДн в других сегментах сети.

Каждый выделенный таким образом сегмент сети может представлять собой отдельную ИСПДн. В случае отделения от остальной сети межсетевым экраном соответствующего класса, данная ИСПДн может быть классифицирована отдельно от других.

Данный принцип – принцип сегментирования – является одним из способов достижения реализуемости требований по защите при одновременном снижении трудозатрат.

6) Идентификация ИСПДн. Идентифицировать все ИСПДн, существующие в IT инфраструктуре организации, на основе принципов, описанных в п.5. Для этого необходимо принципиальное решение о закупке и установке сертифицированных межсетевых экранов. Решение должно быть обосновано путем сравнения затрат на создание и эксплуатацию СЗПДн сети в целом с затратами на создание и эксплуатацию нескольких обособленных сегментов защиты.

С идентификации ИСПДн должны начинаться и от неё должны отталкиваться все процессы по приведению информационных систем организации в соответствие требованиям федерального закона.

Идентификация ИСПДн позволяет очертить области внедрения СЗПДн, назначить подразделения и персонал, ответственные за выполнение требований по защите, распределить роли и ответственность.

Для каждой идентифицированной ИСПДн проводится отдельный комплекс работ и разрабатываются отдельные комплекты организационно-распорядительной и эксплуатационной документации, проводится оценка соответствие и выдаётся аттестат (декларация) соответствия требованиям по безопасности информации.

Отдельные ИСПДн могут иметь более высокий класс, другие – более низкий. Вывод ИСПДн высоких классов в отдельную область защиты позволяет сузить сферу внедрения дорогостоящих средств защиты и получить за счет этого не только экономию денег, но и в минимальной степени затронуть бизнес-процессы в остальных сегментах сети.

7) Классификация ИСПДн. Для каждой идентифицированной ИСПДн должен быть определен её класс и разработан обязательный документ – Акт классификации. Классы ИСПДн определяются порядком, установленным приказом ФСТЭК, ФСБ и Мининформсвязи от 13.02.2008 г. № 55/86/20. Классы типовых ИСПДн определяются с учетом категорий и объёма обрабатываемых ПДн. Класс специальной информационной системы определяется на основе модели угроз в соответствии с методическими документами ФСТЭК России.

В различных разделах Приказа № 55/86/20, а также в документах ФСТЭК России «Основные мероприятия…» и «Рекомендации…» содержатся рекомендации по классификации ИСПДн, сущность

которых необходимо понимать достаточно глубоко для того ,чтобы избежать ошибок при определении класса.

С одной стороны, устанавливается принцип, согласно которому сначала строится модель угроз, а затем на основе экспертной оценки выводится класс ИСПДн, требования по соответствию которому должны быть выполнены.

Однако согласно «Основным мероприятиям…» устанавливается, что вначале определяется класс ИСПДн, а затем разрабатывается модель угроз и задаются конкретные требования по безопасности.

Тут же, немного ниже, содержится указание определять класс ИСПДн безотносительно к её типу (типовая или специальная) исходя из того, насколько значительными для субъектов персональных данных могут быть негативные последствия в случае нарушения заданной характеристики безопасности. При этом устанавливаются следующие классы:

- класс 1 (К1) – негативные последствия могут быть значительными;
- класс 2 (К2) – последствия могут быть негативными;
- класс 3 (К3) – могут быть незначительные негативные последствия;
- класс 4 (К4) – негативные последствия отсутствуют.

И далее – снова встречный отсыл на приказ № 55/86/20 – классификация проводится согласно порядку, установленному данным приказом, т.е. в зависимости от характеристик ИСПДн.

Таким образом, рассматриваемые нормативно-правовые акты содержат неоднозначные сведения о порядке классификации ИСПДн.

Определение класса ИСПДн становится непростой аналитической задачей, требующей знания руководящих документов, методов оценки угроз и тщательного изучения информационной системы.

8) Разработка модели угроз

Разработка модели угроз входит в состав мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах, предусмотрена методическими документами ФСТЭК России и ФСБ России.

В случаях, указанных в документе ФСБ России «Методические рекомендации», модель угроз разрабатывается в соответствии с документами ФСТЭК России «Базовая модель…»[1] и «Методика…»[2] либо в соответствии с указанным документом ФСБ России.

Модель угроз является обязательным для разработки документом.

9) Обоснование требований по обеспечению защиты ПДн

Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в системе, проводится в соответствии с нормативными и методическими документами ФСТЭК России и ФСБ России, государственными стандартами РФ и на основании РД «Основные мероприятия…». При этом выявление и оценка актуальности угроз безопасности персональных данных при их обработке в ИСПДн осуществляется с использованием РД ФСТЭК России «Базовая модель…» и «Методика…».

10) Разработка замысла защиты

В ходе разработки замысла защиты осуществляется выбор основных способов защиты ПДн.

[1] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

[2] – Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Рекомендуется следующий порядок формирования замысла защиты:

- определение основных направлений деятельности по защите ПДн – по подразделениям, по уязвимым звеньям (направлениям), по категориям ПДн;

- выбор способов защиты ПДн – по направлениям защиты, по актуальным угрозам, по возможности реализации с учетом затрат;

- решение основных вопросов управления защитой ПДн: организация охраны, служебной связи, сигнализации, взаимодействия, управления администрированием, резервирования программного и аппаратного обеспечения;

- решение основных вопросов обеспечения защиты ПДн: финансового, технического, программного, информационного, кадрового.

11) Выбор мер и средств защиты

При выборе способов обеспечения безопасности ПДн, обрабатываемых в системе, необходимо определить организационные меры и технические (аппаратные, программные и аппаратно-программные) средства защиты. Следует использовать только сертифицированные средства защиты информации.

В соответствии с руководящими документами, в ИСПДн обязательны к применению:

- системы защиты информации от несанкционированного доступа;

- системы антивирусной защиты;

Дополнительно: в ИСПДн, имеющих подключения к внешним сетям (другим ЛВС, Интернет), обязательны к применению:

- системы маршрутизации, коммутации и межсетевого экранирования;

- системы обнаружения атак.

Дополнительно: в распределенных ИСПДн, реализующих технологии передачи ПДн по незащищенным каналам связи (Интернет и др.), а также в ИСПДн, реализующих технологии совместного использования различными субъектами доступа (разделяемых) носителей данных, а также съёмных носителей данных (дискет, микрокассет и т.п.) долговременной внешней памяти, обязательны к применению:

- системы криптографической защиты информации.

Дополнительно: в ИСПДн, для которых согласно разработанных для них моделям угроз требуется защита от утечки информации по техническим каналам, обязательны к применению:

- системы защиты информации от утечки за счет побочных электромагнитных излучений и наводок;

- системы защиты информации от утечки по цепям электропитания и заземления.

Дополнительно: в ИСПДн, для которых согласно разработанных для них моделям угроз требуется защита от утечки информации при её озвучивании в ходе переговоров, совещаний и т.п. мероприятий, обязательны к применению:

- системы защиты информации от утечки по акустическому (виброакустическому) каналу;

- системы защиты информации от утечки за счет акустоэлектрических преобразований и высокочастотного навязывания.

Требования и рекомендации по выбору средств защиты представлены ниже.

12) Организация управления обеспечением безопасности ПДн

Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты включает в себя:

- распределение функций управления доступом к данным и управления их обработкой между должностными лицами;
- определение порядка изменения правил доступа к защищаемой информации, а также к информационным и аппаратным ресурсам;
- определение порядка действий должностных лиц в случае возникновения нештатных ситуаций (инцидентов);
- определение порядка проведения контрольных мероприятий и действий по их результатам.

13) Разработка регламентирующих документов

При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в системе с применением комплекса мер защиты ИСПДн **в обязательном порядке** разрабатываются:

- положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- требования по обеспечению безопасности ПДн при их обработке в ИСПДн;
- должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Разработка документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации системы защиты ИСПДн, является важнейшим элементом построения комплексной системы управления информационной безопасности (СУИБ) организации.

14) Получение лицензии на деятельность по технической защите конфиденциальной информации

В соответствии с документом ФСТЭК России «Основные мероприятия…», на основании Федерального закона от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» и постановлением 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 персональных данных (конфиденциальной информации) при их обработке в информационных системах 1, 2 классов и распределенных информационных системах 3 класса должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации.

- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Николай Конопкин, *заместитель директора Департамента внедрения и консалтинга компании Leta IT-Company*

8. Перечень внутренних документов компании

1. Приказ о создании комиссии по защите ПД с наделением ее полномочиями по проведению всех мероприятий, касающихся организации защиты.
2. Положение о персональных данных и их защите.
3. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.
4. Приказы о возложении персональной ответственности за защиту ПД.
5. Договор с субъектом персональных данных, который может содержать отдельное письменное согласие субъекта ПД на их обработку.
6. Нормативный документ (перечень), аккумулирующий информацию о персональных данных, обрабатываемых оператором (в том числе их категория, объем и сроки хранения).
7. Перечень информационных систем, обрабатывающих персональные данные.
8. Регламент допуска сотрудников к обработке персональных данных.
9. Перечень сотрудников, допущенных к обработке персональных данных.
10. Должностные инструкции сотрудников, имеющих отношение к обработке ПД.

9. Рекомендации ИТ директоров

9.1 Виктория Сапрыкина, ПрофМедиа Менеджмент

Начальник Отдела Информационных Технологий

Дано: Холдинговая структура, n бизнес единиц. Каждая бизнес единица – самостоятельное юридическое лицо.

Управляющая Компания оценивает риски и берет руководство проектом на себя. Преследуется несколько целей, а именно - минимизация затрат, контроль исполнения закона в целях минимизации рисков потери активов, контроль над исполнением закона (над всем проектом).

В рамках УК создается рабочая группа, куда входят специалисты ИТ, ИБ, HR, legal, а также менеджер-координатор.

По экспертной оценке ИСПДн в back office системах одинаковы по классу или мы придем к двум классам (2 и 3). Это позволит минимизировать расходы на этапе подготовки типовых документов, форм, регламентов и прочей типовой документации, которая будет незначительно доработана под специфику каждой Компании. Однако, это может не сработать на этапе установки/замены технических средств защиты, но и на этом этапе ожидаем получить эффект синергии.

Консультантов и/или интеграторов планируем привлекать после самостоятельного обследования систем.

Резюмируя вышесказанное можно заметить, что УК хочет получить case и растиражировать решение на Компании Холдинга.

В свою очередь, УК проводит совещания на уровне директоров Компаний с разъяснением сути и пути реализации проекта. Руководители Компаний выделяют ответственных за проект внутри Компании. В таком взаимодействии планируем реализовывать проект.

9.2. Владимир Катречко, ГК Цезарь Сателлит

ИТ директор

Обсуждение проекта по ПД в нашей компании началось по инициативе Директора департамента ИТ (а кого еще!) в прошлом году. Но к сожалению, важность и необходимость проведения мероприятий в соответствии с 152ФЗ донести тогда не удалось. Причин несколько, но основная - на мой взгляд - практически никто тогда особо и не задумывался об этом. Материалов и разъяснений в прессе было мало, компаний которые приступили к выполнению положений закона еще меньше. Реализованных в полном объеме проектов не было (или мы о них не слышали). Да и что конкретно надо делать, а что не надо тогда мало кто представлял. Казалось что год до вступления закона в силу – это очень много. Но во второй половине 2009 года стало очевидно, что все-таки выполнять закон придется. Мы у себя провели ряд встреч с компаниями, занимающимися этим вопросом и получили ряд предложений. Стало понятно, что к 1 января в полном объеме выполнить все мероприятия мы не успеем, но провести аудит и подготовить документы к сертификации вполне сможем. Несколько успокоил взвешенный подход регуляторов – обещали не карать строго (я слышал это на ряде конференций), если компания покажет, что имеет план выполнения мероприятий и действительно их выполняет. Поэтому задача компаниям, участвующим в тендере на этот проект, ставилась следующая: выполнить максимальное количество действий в соответствии с законом, естественно за минимальные деньги. Впечатлил разброс цен от 1200 000 до 3500 000 рублей (это стоимость обследования и проектирования системы защиты персональных данных, сертификация и аттестация не включены)! По крайней мере, сейчас уже в целом понятно что надо делать, сколько это займет времени и сколько стоит. Но! Остается еще один вопрос (вполне естественный для бизнеса!) – а надо ли тратить деньги, да и еще в кризис? Может пока посудиться? Дешевле выйдет? Разъяснений по этому поводу я пока не нашел. Хотя в законе прописана ответственность, некоторые юристы считают, что можно успешно отстоять свою позицию в суде. Было бы хорошо получить четкие разъяснения от регуляторов по этому поводу.

9.3. Борис Славин, НПФ «Благосостояние».

Директор департамента по ИТ, Председатель Правления Союза ИТ-директоров России (СоДИТ)

«Нестандартный» проект по защите персональных данных.

В тему «152-го ФЗ» я по-настоящему окунулся лишь в конце 2008 года, причем одновременно и как директор ИТ службы, и как руководитель межрегиональной общественной организации «Союз ИТ-директоров» России. Как руководитель службы в конце прошлого года я должен был заложить в ИТ бюджет 2009 года расходы на деятельность, связанную с доработками и приведением информационной системы в соответствие с новыми требованиями закона о защите персональных данных, которые должны были вступить с 2010 года. И здесь сразу же возникло интересное обстоятельство, которое выделило этот проект в разряд нестандартных (он таким и остался до сих пор). Выяснилось, что регулирующие органы только-только разработали необходимые документы, конкретизирующие требования, но никому их не показывают. По очень большому секрету мне эти «недоступные» документы дали посмотреть «из чужих рук», что, конечно же, не сильно помогло в оценке бюджета. Счастливчиков, знакомых с новыми требованиями было единицы, а сколько могут стоить работы для нашей организации оценить в разумные сроки вообще никто не мог.

Поскольку закон разрабатывался сразу тремя ведомствами, и даже получил название «трехглавый», я также решил поделиться ответственностью с представителем «соседнего» ведомства – руководителем нашей организации в области безопасности. Отставных генералов, как известно, не бывает, поэтому мы совместно с «рыцарем плаща и кинжала» полностью сошлись во мнении относительно нестандартности проекта, и оценили не столько необходимые работы, сколько некий предел, больше которого мы на эту задачу денег не дадим. Кстати, как показало будущее – не сильно ошиблись (хотя и пришлось подрядчиков под наш предел слегка подмять). Выработанный нами подход был прост: в первую очередь удовлетворить требования законодательства настолько, насколько это необходимо, чтобы быть вполне законопослушными, хотя и не «полностью пушистыми». И второе – по возможности получить пользу (или минимизировать вред) от тех преобразований, которые необходимы по закону.

О том, что проект будет непростым, я понял еще и как руководитель Союза ИТ-директоров, когда участвовал в организованном нашим комитетом по ИБ в начале 2009 года семинаре на тему 152-го ФЗ. Это сейчас закон о ЗПДн – хитовая тема, а тогда никто не знал, что это такое и что с этим делать. Эксперты Государственной Думы, представители Роскомнадзора, ФСТЭК и ФСБ на нашем семинаре в один голос подтвердили существенные изъяны законодательства, которые вряд ли удастся устранить, но придется учитывать. Особенно бессмысленно пытаться понять назначение некоторых требований, их лучше принимать как есть, и в рамках них пытаться работать. Единственно, что успокаивало: масштаб проблемы, умноженный на низкое качество проработки материалов, внушал ужас не только ИТ-директорам, но и самим регуляторам. Все регуляторы клялись регулировать крайне «аккуратно». Мои коллеги подготовили рекомендации ИТ-директорам, которые мало что объясняли, но давали понять, что делать. Рекомендации пользовались успехом, не хуже бестселлера.

К концу года организация, в которой я сейчас руковожу ИТ службой, пройдет предаттестационный аудит. Аудит покажет, что у нас уже хорошо (это будет касаться регламентов,

работы с персональными данными), а что не очень хорошо (это будет касаться части не сертифицированного ПО). Результат мы знаем заранее, поскольку сознательно на него идем. И в этом также нестандартность этого проекта. Можно было пройти аттестацию и до конца года, но тогда пришлось бы установить оборудование или программные продукты, функциональность которых очень низка – просто сертификацию они прошли раньше. Мы лучше подождем, когда сертифицируют более функциональные продукты, и доведем аттестацию до конца красиво. Уверен, что такой прагматичный подход найдет отклик у регулирующих органов, и будет не во вред информационной системе организации. Двигаться вперед, не спеша, но и не отставая – самый лучший лозунг в реализации требований 152-го ФЗ.

9.4. Сергей Климаш, METRO

CIO

Для нашей компании это вопрос, который относится к сфере compliance.

В рамках данного проекта, был создан steering committee из руководителей Юридического, IT и Security департаментов, а также организована рабочая группа из сотрудников вышеперечисленных отделов. Было принято решение о проведении предварительного обследования деятельности компании в рамках выработки оптимальной программы действий в сфере исполнения Федерального закона о защите персональных данных.

Был составлен следующий план проведения предварительного обследования, в рамках которого необходимо:

1. Проанализировать все эксплуатируемые ИС и хранилища данных для выявления тех, где присутствуют и обрабатываются ПДн. В рамках этой задачи необходимо установить какие ИС используются Компанией для ведения своей деятельности, и в каких из ИС осуществляется обработка ПДн (сбор, уточнение, передача, хранение, использование и т.п.); также необходимо классифицировать количество серверов, АРМ и установленное на них системное и прикладное ПО. Кроме этого необходимо определить средства обеспечения информационной безопасности используемых в рамках ИС обрабатывающих ПДн.
2. Определить основания для обработки ПДн, с учетом случаев, когда необходимо согласие субъекта. Необходимо проанализировать типовые договоры с работниками, клиентами, партнерами и контрагентами в части обработки ПДн.
3. - Определить механизмы взаимодействия Компании с субъектами ПДн в части предоставления первыми информации, кроме этого, выявить правила обработки и хранения ПДн. Необходим анализ всей имеющейся документации (Положения, Инструкции, Процедуры и прочая документация), определяющей порядок по обращению и предоставлению доступа к ПДн. Обязательно необходимо проанализировать процедуры обработки и хранения ПДн после окончания договорных отношений с субъектами ПДн.
4. Необходимо определить режимы обработки и категории обрабатываемых ПДн. Имеется ввиду использование автоматизированной и неавтоматизированной обработка данных на разных этапах работы с ПДн. Обрабатываются ли персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни. Производится ли обработка персональных данных, позволяющих идентифицировать субъекта и получить о нем дополнительную информацию (например: при на основании паспортных данных субъекта и информации о сделанных им на протяжении некоторого времени покупках, можно получить дополнительную информацию о пристрастиях, личной жизни, состояния здоровья субъекта и т.п.).

5. Определение объема обрабатываемых персональных данных - количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе.

Планируем завершить этот этап работы на следующей неделе, по результатам будет составлен план дальнейших мероприятий. Этап предварительного обследования выполнялся с привлечением внешних консультантов.

9.5. Леонид Леин, АвтоСпецЦентр

Директор Департамента по ИТ

Странная вещь, оказывается, эти «персональные данные». Сами по себе они субъекту не нужны. Они нужны ему как элемент общения с внешним миром, посредством которого он сообщает этому миру – это я, а не кто-то другой. При этом в большинстве случаев, добровольно сообщает, без всякого насилия извне.

Если говорить о коммерческой организации, то она принимает эти данные для того, чтобы:

- ✓ оформить свои отношения с клиентом в соответствии с требованиями госорганов (заполнение реквизитов документов коммерческой сделки)
- ✓ в будущем предложить клиенту воспользоваться снова ее услугами или просто напомнить о себе.
- ✓ Первое – хочешь не хочешь, второе – здесь вроде бы обоюдная выгода и клиенту и бизнесу.
- ✓ Так нет, давайте так «защитим» эти самые персональные данные, которые нам клиент сам и доверил, так чтобы брать их у этого клиента стало себе дороже.

Т.е. коммерческая организация должна для себя решить, что для нее будет эффективней (выгодней, дешевле) хранить эти самые данные в защищенном в соответствии с законом виде в надежде отбить вложенные средства на адресном предоставлении услуг или не хранить эти данные, а обслуживать только «здесь и сейчас». Не уверен, что второй вариант проиграет в этом сравнении.

Тем не менее сейчас практически все бросились готовиться к 010110.

Оценка вложения в защиту в персональных данных, которую сделали для нас специализированные фирмы, даже в минимальном объеме оказались колоссальны. Если принять во внимание «очень удачный момент нашей экономической истории» и, особенно ситуацию в авто бизнесе, было принято решение готовиться к вступлению закона своими силами, максимально попытавшись удовлетворить его требованиям.

Первое и самое очевидное, что предпринимают все организации и авто дилеры в том числе, - запастись согласием клиентов на обработку и хранения их персональных данных. Соответствующие фразы, подготовленные юристами, вставляются во все печатные формы, в которых хоть как-то фигурирует клиент. (Кстати, на днях, оформляя депозитный договор в банке видел в теле договора такую фразу мелким курсивом на полстраницы. Правда сам договор, подписанный мной, мне так и не дали; сказали, что для моего же удобства.). Так как по условиям дилерских контрактов авто дилер обязан предоставлять информацию о клиентах представителям импортера (производителя), то все официальные дилеры получили соответствующие циркуляры, обязывающие дилера согласовать с клиентом передачу данных импортеру, т.е. третьему лицу. Так что в печатные формы документов были включены и эти фразы, под которыми клиент подписывается.

Второе, и это безусловная польза от введения закона, - аудит информационных ресурсов на предмет выявления лишних клиентских данных. Т.е. пришлось, насколько это оказалось возможным, выявлять наличие электронных источников (копии БД, файлы, почтовые сообщения), в которых могли быть данные клиентов, и безжалостно уничтожать. Здесь важна организационно-разъяснительная работа с пользователями на предмет введения строгих регламентов по работе с выборками по клиентам. Особенно это относилось к сотрудникам клиентских отделов, обеспечивающих оповещение и опросы клиентов. Кроме того, подверглись аудиту и программные

решения на предмет необходимости той или иной клиентской информации и организации доступа к карточкам клиентов.

Третье – это, на основании проведенного аудита, запланирован ряд мероприятий по модернизации OLTP-софта (благо, он у нас самописный ☺). Цель – максимально затруднить проведение соответствия идентификационных данных клиента и всего остального массива этих данных, тем самым, по возможности, понизив класс защиты. Так же предполагается значительно усилить систему разграничения прав доступа пользователей к клиентским данным, использовать шифрование этих данных как при хранении так и при их передаче.

Как следствие осознания рисков, с введением закона принято решение приостановить создание ЕКБ всех клиентов группы компаний, так как при этом мы бы столкнулись с необходимостью защищать каналы передачи данных, арендуемые у провайдера.

Т.е., возвращаясь к началу, так как хранение персональных данных оказывается слишком дорого, то бизнес будет пытаться зарабатывать, отказываясь от ряда услуг связанных с обработкой КБ, а максимально выкладываясь в момент сделки.

9.6. Федор Потапов, ИНТЕР РАО ЕЭС

Если описать кратко, то наш подход к реализации требований основывается на выполнении методический указаний ФСТЭК, ФСБ и Мининформсвязи и состоит из следующих этапов:

- Комплексное обследование информационных систем, обрабатывающих ПД (ИСПД), с разработкой модели угроз согласно требованиям руководящих документов (РД) ФСТЭК;
- Классификация ИСПД, по результатам проведения комплексного обследования, и разработка модели угроз.
- Разработка Технического задания на Систему Защиты Персональных Данных, по результатам классификации ИСПД, согласно требованиям РД ФСТЭК. В ТЗ на СЗПД определить требования по защите ПД при их обработке в ИСПД на основе присвоенного класса и результатов моделирования угроз безопасности ПД;
- Проектирование Системы Защиты Персональных Данных.
- Реализация проекта на создание СЗПД.
- Оценка соответствия ИСПД, с требованиями безопасности согласно присвоенному классу.

Реализация данных этапов планируется как с помощью использования собственных кадровых ресурсов, так и с привлечением сторонних организаций.

9.7. частное мнение эксперта в области ИТ

Для решения данной задачи (с целью минимизации затрат) принято решение свести ее к защите данных в фискальном учете, который ведут ограниченное число юр.лиц по договору аутосорсинга.

Т.е. в результате число сотрудников попадающих под фз не более 20, а юр. лиц -2

В рамках фискального учета группы компаний можно выделить и рассмотреть типовую информационную систему по хранению и обработке персональных данных (ИСПДн) сотрудников организаций (кадровые данные) и ПДн физлиц, клиентов организаций (ФИО+номер договора).

Данная ИСПДн состоит из программного обеспечения (ПО), которое непосредственно используется для ввода ПДн:

- ✓ 1с:Зарплата и управление персоналом
- ✓ 1с:Бухгалтерия предприятия

И иного ПО:

- ✓ Microsoft Windows XP
- ✓ Microsoft SQL server 2005
- ✓ Microsoft server 2003

Особенности данной системы применительно к 152-ФЗ:

В едином информационном пространстве ведется учет нескольких юрлиц. Сам учет ведут одно или два юрлица по договору аутсорсинга.

Оператором ПДн является каждое юрлицо , а аутсорсер выступает как уполномоченное лицо (152-ФЗ ст. 2, ст. 6, ч. 4)

В договорах аутсорсинга (указания услуг по ведению учета) должно быть упоминание о передаче ПДн и конфиденциальности их использования (152-ФЗ ст. 6, ч. 4)

Сотрудник как Субъект ПДн должен письменно подтверждать согласие на обработку своих ПДн (152-ФЗ ст. 6)

Физлицо с которым заключен договор не должно письменно подтверждать согласие на обработку своих ПД (152-ФЗ ст. 6)

Оператор ПДн при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. (152-ФЗ ст. 19 ч. 1)

При обработке ПДн сотрудников и физлиц с которыми заключен договор, оператор не обязан уведомлять Роскомнадзор (152-ФЗ ст. 22)

Классификация ИСПДн

Проводится на основании принадлежности информационной системы к категории по составу данных (Хпд) и категории по количеству субъектов ПД (Хнпд)(Приказ ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. N 55/86/20)

Однозначного ответа по принадлежности кадровых данных к той или иной категории нет, т.к. неясно что такое «персональные данные, позволяющие идентифицировать субъекта персональных данных» и дополнительная информация о субъекте ПД (ссылка <http://pd.rsoc.ru/faq/faq22.htm>)

Т.е. Хпд будет 2 или 3 категория

Критерии классификации по количеству субъектов ПД тоже нечеткие, но с большей долей вероятности Хнпд = 2

В результате класс типовой ИС получается либо 2 (худший вариант, требующий сертификации), либо 3.

Оценка проекта

По всей видимости, самостоятельное толкование нормативов не даст однозначного результата. Тем более остаётся много вопросов по реализации самого проекта. Возникает необходимость использования услуг сторонних подрядчиков. Ориентировочная стоимость проекта составляет 2 млн. рублей (без ПО). При этом однозначно потребуется лицензирование всего ПО, используемого на рабочих местах на которых ведётся обработка персональных данных. В некоторых случаях (пример Локальная вычислительная сеть для обработки персональных данных, сопряженная с Интернет <http://www.altx-soft.ru/personal2.htm>) и применение сертифицированного ПО, что помимо увеличения прямых затрат на его закупку вызывает необходимость изменения в программной и сетевой инфраструктуре и в её поддержке.

10. Сертифицированное ПО. Что дает? Насколько необходимо? Можно ли без него?

В соответствии с 152-ФЗ «О персональных данных» информационные системы, в которых обрабатываются персональные данные, подлежат обязательной проверке и аттестации.

Аттестация информационных систем предполагает проверку не отдельных компонентов, а законченной информационной системы, что является сложной комплексной задачей. Защищенность информационной системы зависит от многих факторов — аппаратное обеспечение, программное обеспечение, сборка из отдельных компонентов, регламенты функционирования. Для успешной аттестации законченной информационной системы необходимо доверие ко всем компонентам, из которых она состоит.

Возможно два принципиальных пути аттестации системы:

- Если организация использует не сертифицированные средства, проводятся непосредственные испытания на месте всех компонентов информационной системы. Это является длительным и дорогостоящим процессом. Кроме того, состояние всей системы после аттестации жестко фиксируется. Это означает, что при внесении в систему любых изменений — от перенастройки до установки обновлений ПО — потребуется ее повторная аттестация.

- Если информационная система сформирована из сертифицированных компонентов, задача значительно упрощается. Фактически достаточно проверить корректность сборки системы из отдельных компонентов и использование разумных регламентов ее функционирования. Если поставщик ПО обеспечивает сертификационную поддержку, в частности, оперативную сертификацию обновлений, также автоматически решается и вопрос обновления однажды аттестованной системы.

Таким образом, сертифицированное ПО значительно упрощает приведение системы в соответствие с требованиям законодательства. Если есть выбор из нескольких альтернативных решений, рекомендуется использовать то из них, которое прошло сертификацию.

Компания VDEL

Заключение

Мы надеемся, что данное методическое пособие, стало для Вас полезным. Если Вы не нашли какую-то интересующую Вас информацию, то свяжитесь с нами, и мы обязательно найдем её для Вас, и вставим в следующую редакцию данного пособия.

В ближайшее время, после конференции «152 ФЗ – основные ловушки и способы разминирования», выйдет новая редакция методического пособия, в которой появится крайне важный раздел – «Вопросы - Ответы», данный раздел будет содержать ответы регуляторов на вопросы ИТ сообщества.

Приложения

1. Выдержка из парламентских слушаний

20 октября в Государственной Думе Российской Федерации состоялось парламентские слушания, темой которого стал Федеральный закон №152 «О персональных данных». Представитель клуба 4CIO присутствовал на данном мероприятии.

Одной из самых главных и часто озвучиваемых поправок стал перенос сроков по исполнению требований по статье 19 152 ФЗ. Напомню, что согласно данной статье операторы должны привести свои ИС в соответствие с требованиями, предъявленными данным законом до 1 января 2010 года, а после 1 января 2010 года ФСТЭК и ФСБ начнут проводить проверки на соответствие. Собственно вступление в силу закона предлагают перенести на разные сроки, кто на год, кто на два. Отдельно хочется отметить, что одним из инициаторов переноса является Роскомнадзор. Вот цитата Шередина Романа, заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и коммуникаций: «Мы будем требовать переноса сроков…».

Так как на парламентском слушании были представители комитетов Государственной Думы, министерств, банков, страхования, федеральных структур, то и рекомендаций к закону поступило много, и все они были различные.

Вот основные рекомендации, которые поступили от докладчиков:

- в законе указать или предусмотреть передачу данных третьим лицам,
- уточнить случаи, при которых не требуется согласие субъекта на обработку его ПДн,
- убрать стандарты защиты на уровне от интернациональных разведок,
- точнее определить понятие ПДн,
- определить сроки между проверок регуляторами.

Государственная Дума РФ до конца 2009 года должна рассмотреть все эти поправки и принять решение, вносить их или нет.

2. Порядок проведения классификации информационных систем

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ N 55

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ N 86

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ N 20

ПРИКАЗ от 13 февраля 2008 года

ОБ УТВЕРЖДЕНИИ ПОРЯДКА ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с пунктом 6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах

персональных данных" (Собрание законодательства Российской Федерации, 2007, N 48, часть II, ст. 6001), приказываем:

Утвердить прилагаемый Порядок проведения классификации информационных систем персональных данных.

Директор Федеральной службы по техническому и экспортному контролю

С.И.ГРИГОРОВ

Директор Федеральной службы безопасности Российской Федерации

Н.П.ПАТРУШЕВ

Министр информационных технологий и связи Российской Федерации

Л.Д.РЕЙМАН

Утвержден Приказом

ФСТЭК России,

ФСБ России,

Мининформсвязи России

от 13 февраля 2008 г. N 55/86/20

ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий Порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы)[1].

2. Классификация информационных систем проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор)[2] .

[1] Абзац первый пункта 1 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 (Собрание законодательства Российской Федерации, 2007, N 48, часть II, ст. 6001) (далее - Положение).

[2] Абзац первый пункта 6 Положения

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

4. Проведение классификации информационных систем включает в себя следующие этапы:

сбор и анализ исходных данных по информационной системе;

присвоение информационной системе соответствующего класса и его документальное оформление.

5. При проведении классификации информационной системы учитываются следующие исходные данные:

категория обрабатываемых в информационной системе персональных данных - X ; пд

объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) - X ; нпд

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.

6. Определяются следующие категории обрабатываемых в информационной системе персональных данных (X): пд

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

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

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

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

7. X может принимать следующие значения: нпд

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, 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 персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

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 безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

9. По структуре информационные системы подразделяются:

на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (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 (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

10. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

11. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

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

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

14. 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.

15. Класс типовой информационной системы определяется в соответствии с таблицей.

X X	3	2	1
ПД НПД			

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

16. По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"[1] <*>.

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

18. Результаты классификации информационных систем оформляются соответствующим актом оператора.

19. Класс информационной системы может быть пересмотрен:

по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

[1] Собрание законодательства Российской Федерации, 2007, N 48, часть II, ст. 6001

3. Типовые документы

3.1 Образец уведомления об обработке (намерении осуществлять обработку) персональных данных

Руководителю Управления Федеральной службы по надзору в сфере связи и массовых коммуникаций по

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

_____

(наименование (фамилия, имя, отчество), адрес оператора)

руководствуясь _____

(правовое основание обработки персональных данных)

с целью _____

(цель обработки персональных данных)

осуществляет обработку: _____

(категории персональных данных)

принадлежащих: _____

_____

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

_____

(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)

_____

(Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:

_____

(должность) (подпись) расшифровка подписи «___»_____200_ г.

Адрес страницы: http://pd.rsoc.ru/operators-registry/operators-registry-documents/

3.2. Официальные рекомендации по заполнению образца формы уведомления об обработке (намерении осуществлять обработку) персональных данных

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее – Уведомление).

2. Уведомление оформляется на бланке оператора, осуществляющего обработку персональных данных, и направляется в территориальный орган Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее – территориальный орган Россвязькомнадзора).

3. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. В поле «наименование (фамилия, имя, отчество), адрес оператора» указывается:

4.1. Для юридических лиц (операторов):

полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;

наименование филиала(ов) (представительства(в) юридического лица (оператора), осуществляющего обработку персональных данных (1);

место нахождения (2);

Примечание 1. Если для каких-либо операторов (с учетом филиалов (представительств) значения пунктов 5-12 отличаются, то для них формируется отдельное уведомление.

Примечание 2. Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом, необходимо уточнить – обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).

Индивидуальный номер налогоплательщика (ИНН),

4.2. Для физических лиц:

фамилия, имя, отчество физического лица (оператора); место жительства (3);

данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ, удостоверяющий личность.

Для индивидуальных предпринимателей:

фамилия, имя, отчество индивидуального предпринимателя (оператора);

место жительства (4);

индивидуальный номер налогоплательщика (ИНН).

4.3. Для государственных, муниципальных органов (операторов):

полное и сокращенное наименование государственного, муниципального органа;

наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;

место нахождения (5);

индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

5. В поле «цель обработки персональных данных» указываются цели обработки персональных данных (а также их соответствие полномочиям оператора) (Примечание № 1).

Примечание № 1: Под «целью обработки персональных данных» понимаются, как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по обработке персональных данных.

6. В поле «категории персональных данных» указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные (любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата рождения, место рождение, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая необходимая информация).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность).

7. В поле «категории субъектов, персональные данные которых обрабатываются» указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются. Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

8. В поле «правовое основание обработки персональных данных» указываются:

Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Примечание № 1);

Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных. (Примечание № 2).

Примечание № 1: Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных. (Например: ст.ст. 85-90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона «Об актах гражданского состояния» и др.).

Примечание № 2: Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.

9. В поле «перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных», указываются действия, совершаемые оператором с персональными данными, а также описание используемых оператором способов обработки персональных данных:

- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных. (Примечание № 1).

Примечание № 1: При автоматизированной обработке персональных данных либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации.

10. В поле «описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке», указываются организационные и технические меры, в том числе использование шифровальных (криптографических) средств, используемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий при их обработке.

11. В поле «дата начала обработки персональных данных» указывается конкретная дата начала совершения действий с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе

передачу), обезличивание, блокирование, уничтожение персональных данных (фактическая дата начала обработки персональных данных).

12. В поле «срок или условие прекращения обработки персональных данных» указывается конкретная дата или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

(1) Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта – согласно справочнику «Коды регионов», утвержденному приказом ФНС России от 13.10.2006 года № САЭ-3-04/706@ «Об утверждении формы сведений о доходах физических лиц» зарегистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Россвязькомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств) (Примечание № 1).

(2) Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, а также место нахождения филиала(ов) (представительств) юридического лица, контактная информация (Примечание № 2).

(3) Указывается место жительства физического лица в соответствии с данными документа, удостоверяющего личность, а в случае расхождения, также фактическое место жительство, контактная информация.

(4) Указывается место жительства индивидуального предпринимателя (оператора) в соответствии с данными документа, удостоверяющего личность, и свидетельством о постановке индивидуального предпринимателя на учет в налоговом органе, контактная информация.

(5) Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, контактная информация.

Адрес страницы: http://pd.rsoc.ru/operators-registry/operators-registry-documents/

3.3 Вариант запроса согласия на обработку ПДн

ВНИМАНИЕ! Ознакомьтесь с информацией перед заполнением анкеты (резюме) кандидата

Согласие на обработку персональных данных

В соответствии с законом «О персональной информации» (от 27 июля 2006 г. №152 – ФЗ), вступившего в силу с 1 января 2007 года, даю согласие на обработку персональных данных Обществу с ограниченной ответственностью «ЕТ Консалтинг», его подразделениям и его группе лиц (опред. ст. 9 ФЗ «О защите конкуренции№135-ФЗ от 26.07.2006г.). Данное соглашение выдается без ограничения его сроков действия.

Под обработкой персональных данных я понимаю любую персональную информацию, переданную, уточненную мною ООО «ЕТ Консалтинг», подразумевая мое согласие о предоставлении персональных данных.

Я гарантирую достоверность персональных данных, предоставленных компании.

ООО «ЕТ Консалтинг» гарантирует конфиденциальность в использовании предоставленных персональных данных, информация будет использована только для выполнения обязательств по

предоставлению услуг компании и обязуется не разглашать информацию третьим лицам, не являющимся официальными клиентами компании.

Личные сведения:

Фамилия* –

Имя* –

Отчество* –

Пол* –

День рождения* –

Семейное положение* –

Дети: количество, возраст –

4. Консультанты по 152 ФЗ

4.1 LETA IT-company

Услуги LETA IT-company по защите персональных данных:

- Обследование информационных систем персональных данных – определение плана работ по приведению процессов обработки персональных данных в соответствие требованиям закона. В ходе работ собирается достоверная информация о структуре и порядке обработки ПДн. Формируются рекомендации по снижению рисков карательных санкций со стороны регуляторов.
- Проектирование систем защиты персональных данных – выполнение требований регуляторов к порядку построения информационных систем ПДн. В ходе работ разрабатывается комплект необходимой документации для внедрения и эксплуатации системы защиты ПДн.
- Внедрение систем защиты персональных данных – выполнение требований регуляторов, предъявляемых к механизмам защиты ПДн. В ходе работ внедряются ранее разработанные технические решения защиты ПДн.
- Оценка состояния защиты персональных данных требованиям законодательства – независимое экспертное заключение о выполнении требований законодательства по защите ПДн.
- Контроль защищенности информационных систем персональных данных – подтверждение неизменности (целостности) состояния защиты информационных систем ПДн, прошедших процедуру аттестации (оценки соответствия). Выявляются изменения информационной системы ПДн, которые могут привести к потере требуемого уровня защиты ПДн. Разрабатываются предложения по корректировке системы защиты.
- Подготовка к получению лицензии ФСТЭК России – оказание помощи Заказчику по приведению его объектов информатизации и документации в соответствие с лицензионными требованиями ФСТЭК России.
- Аттестация информационных систем персональных данных – подтверждение того, что информационные системы ПДн 1 и 2 класса соответствуют требованиям государственных стандартов, руководящих и нормативно-методических документов ФСТЭК России.
- Обучение специалистов – повышение осведомленности сотрудников Заказчика в вопросах защиты ПДн.
- Сопровождение системы защиты персональных данных, разработанной компанией LETA – поддержание системы защиты персональных данных в актуальном состоянии.

Кроме этого, компания предлагает весть спектр услуг в области обеспечения информационной безопасности.

LETA IT-company занимает ведущие позиции на рынке ИБ: 3 место в рейтинге «CNews Security 2007: крупнейшие ИТ-компании России в сфере защиты информации»; 1 место в рейтинге CNews «Защита информации и бизнеса от инсайдеров» и др.

LETA обладает всеми необходимыми лицензиями ФСТЭК и ФСБ, необходимыми для деятельности в области защиты информации; входит в сообщество ABISS, объединяющее пользователей стандартов Центрального Банка Российской Федерации по обеспечению информационной безопасности организаций банковской системы РФ; а так же является Авторизованным партнером BSI (British Standards Institution) по проведению аудита Системы Управления Информационной Безопасностью (СУИБ) первой и второй стороны.

Контакты:

109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2

Тел./факс: +7 (495) 921 1410,

e-mail: info@leta.ru

www.leta.ru

4.2. Oberon IT

Услуги:

- Оценка соответствия компании требованиям законодательства в области защиты персональных данных и разработка плана работ:
- Классификация информационных систем персональных данных;
- Оценка эффективности и достаточности имеющихся мер обеспечения ИБ;
- Подготовка и согласование отчета.
- Разработка моделей угроз и нарушителей для ИСПДн.
- Создание нормативно-методической базы по защите персональных данных при их обработке в ИСПДн.
- Техническое задание на разработку системы защиты персональных данных;
- Закупка и ввод в опытную эксплуатацию системы защиты персональных данных;
- Сертификация (аттестация) ИСПДн.

Контактные данные:

Москва, ул. Мытная, д.1, стр.1.

(495) 980 0770

info@oberon-it.ru

www.oberon-it.ru

4.3 ReignVox

Услуги:

Специалисты компании Рэйнвокс разработали оптимальную методику исследования информационных систем заказчика и проектирования системы защиты персональных данных, которая позволяет минимизировать затраты при выполнении требований Законодательства о персональных данных.

Данные об отзывах Клиентов компании могут предоставляться по запросу.

Контактные данные:

Москва, Старопетровский проезд, д.7а

(495) 981 6182

info@reignvox.ru

www.reignvox.ru

4.4 Accenture

Услуги:

- в области управленческого консалтинга,
- в области информационных технологий,
- в области аутсорсинга.

Контактные данные:

www.accenture.com

Пестун Вадим Анатольевич, старший менеджер, Руководитель подразделения Технологического консалтинга.
vadim.pestun@accenture.com
7 495 755 9770

4.5 Terralink

Услуги:

- комплексное обследование информационных систем компании,
- выявление угроз, связанных с несоответствием закону,
- составление рекомендаций по устранению недостатков систем,
- реализация рекомендованных мероприятий, внедрение недостающих элементов защиты.

Контактные данные:

Москва, Кутузовский проспект, 12/2
(495) 721 1721
info@terralink.ru
www.terralink.ru

4.6 ИЦ Телеком-сервис

Услуги:

- Обследование предприятия и выявление ИСПД, требующих защиты и регламентации
- Составление плана работ, консультации заказчика и помощь в переработке(разработке) нормативного и правового обеспечения,
- Управление проектом по приведению в соответствие с ФЗ ИСПД и инфраструктуры,
- Комплексные меры по защите информации,
- Последующее юридическое сопровождение компании при проверках.

Контактные данные:

Москва, ул. Бакунинская, дом 84.
int@teleserv.ru
www.teleserv.ru
Алмазов Андрей Александрович,
Зам. генерального директора
тел. офис: +7 (495) 737 4747
факс: +7 (495) 730 0342
моб.: +7 (495) 920 8229

4.7 Информзащита

Услуги:

- Обследование текущего состояния, целей и способов обработки персональных данных, организации их защиты;
- Анализ достаточности предусмотренных законодательством оснований для обработки персональных данных, выработка предложений по совершенствованию договорной работы с персоналом и контрагентами, правового обеспечения деятельности, связанной с персональными данными;
- Инвентаризация, описание и классификация информационных систем персональных данных в соответствии с установленным государственными органами порядком;

- Анализ возможных путей минимизации затрат на реализацию требований Законодательства РФ в части защиты персональных данных, разработка рекомендаций по выбору и реализации оптимальных организационных и технических мер защиты персональных данных с учетом специфики деятельности Заказчика;

- Разработка и внедрение организационных мер по обеспечению защиты персональных данных, создание полного пакета внутренних нормативных документов, регламентирующих обработку персональных данных;

- Формирование (в случае необходимости) актуализированной модели угроз персональным данным и определение на ее основании требований по обеспечению безопасности хранения, обработки и передачи персональных данных по техническим каналам связи;

- Проектирование технического решения по защите персональных данных;

- Выбор конкретных средств защиты, их поставка и ввод в эксплуатацию;

- Аттестация (сертификация) информационных систем персональных данных;

- Определение необходимости получения лицензий на определенные виды деятельности (техническая защита конфиденциальной информации, использование криптографических средств), подготовка организации к необходимому лицензированию;

- Обучение всех категорий работников организации, связанных с обработкой персональных данных – лиц, ответственных за организацию обработки и обеспечение безопасности, а также технических специалистов, обслуживающих средства защиты;

- Повышение осведомленности конечных пользователей информационных систем персональных данных в вопросах безопасности обрабатываемых данных (обучение персонала, обрабатывающего ПДн).

Контактные данные:

Москва, ул. Образцова, 38

Александра Васюнина, специалист по направлению «Персональные данные» департамента маркетинга,

тел.: (495) 980-2345,

Email: a.vasyunin@infosec.ru,

www.infosec.ru

4.8 КРОК

Услуги:

КРОК реализует проекты по приведению информационных систем в соответствие требованиям Федерального закона №152-ФЗ «О персональных данных».

Стоимость технических решений, позволяющих реализовать требования законодательства, зависит от имеющихся в распоряжении заказчика средств и систем защиты, выявленных угроз персональным данным, а также класса информационной системы, обрабатывающей персональные данные. Класс информационной системы определяется согласно Приказу ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Перечень подсистем защиты персональных данных и их стоимость корректируется по результатам обследования.

КРОК обеспечивает соответствие всех средств и систем, которые используются для защиты персональных данных, требованиям по защите информации, регламентируемыми ФСТЭК России в документе «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных». При этом применяются сертифицированные по требованиям безопасности информации средства защиты информации.

Контактные данные:

Москва, ул. Волочаевская, д. 5, корп.1
(495) 9742274
croc@croc.ru
www.croc.ru

5. Справочник сертифицированного ПО

5.1. ИБМ Восточная Европа/Азия

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
IBM WebSphere MQ 6.0	19.04.2007	19.04.2010	Сертификат ФСТЭК России № 1372 (на производство) на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД2 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки безопасности ИТ" и может использоваться при создании автоматизированных систем класса защищенности до 1Г включительно в соответствие с руководящим документом "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации".
IBM WebSphere Portal 5.1.0.1	19.04.2007	19.04.2010	Сертификат ФСТЭК России № 1373 (на производство) на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД2 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки безопасности ИТ" и может использоваться при создании автоматизированных систем класса защищенности до 1Г включительно в соответствие с руководящим документом "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации".

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
IBM Tivoli Access Manager 6.0 (fixpack 3)	11.04.2007	11.04.2007	Сертификат ФСТЭК России № 1370 на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД3 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ" и может использоваться при создании автоматизированных систем класса защищенности до 1Г включительно в соответствие с руководящим документом "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации".
IBM DB2 UDB ESE v.9.1	14.12.2007	14.12.2010	Сертификат ФСТЭК России №1531 на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД4 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ"
IBM Tivoli Identity Manager v.4.6	18.12.2007	18.12.2010	Сертификат ФСТЭК России № 1533 (на производство) на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД3 (усиленный) в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ" и может использоваться при создании автоматизированных систем класса защищенности до 1Г включительно в соответствие с руководящим документом "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации".
IBM Lotus Domino Enterprise Server and Notes for Multiplatforms v.7.0.2 -(включает Lotus Domino Enterprise Server 7.0.2, Lotus Notes with Collaboration 7.0.2, Admin & Designer Client 7.0.2**)**	7.07.2008	7.07.2011	Сертификат соответствия ФСТЭК России №1637 на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД1 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ"

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
IBM WebSphere Message Broker v.6.0	4.03.2009	4.03.2012	сертификат соответствия ФСТЭК России №1793 на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД4 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ"
IBM WebSphere Application Server v.6.1 FixPack2 - (включает IBM WebSphere Application Server Base v.6.1 FixPack2и IBM WebSphere Application Server Network Deployment v.6.1 FixPack2)	4.03.2009	4.03.2012	сертификат соответствия ФСТЭК России №1794 на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1.Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей " - по 4 уровню контроля, имеет оценочный уровень доверия ОУД1 в соответствие с требованиями РД "Безопасность информационных технологий. Критерии оценки ИТ".
Программные комплексы: **IBM Lotus Notes and Domino v.8.5** и **IBM WebSphere Portal v.6.1**	до 31.01.2010	–	Будут сертифицированы на соответствие требованиям Руководящего документа ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - по 5 классу защищенности; Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля; Руководящего документа ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» по классу 1Г ; на соответствие требованиям, предъявляемым к средствам защиты информации, входящих в состав информационных систем персональных данных (ИСПДН), относящихся к классу К2

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Программно-аппаратные комплексы: **IBM Proventia Network Intrusion Prevention System GX3002, GX4002, GX4004, GX5008, GX5108, GX5208, firmware 1.7**	до 31.01.2010	–	Будут сертифицированы на соответствие требованиям, предъявляемым к средствам защиты информации, входящих в состав информационных систем персональных данных (ИСПДН), относящихся к классу К2
Программный комплекс: **IBM Proventia Management SiteProtector 2.0 SP 7.0**	до 31.01.2010	–	Будет сертифицирован на соответствие требованиям Руководящего документа ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - по 5 классу защищенности; Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля; Руководящего документа ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» по классу 1Г ; на соответствие требованиям, предъявляемым к средствам защиты информации, входящих в состав информационных систем персональных данных (ИСПДН), относящихся к классу К2
Программные комплексы: **IBM Tivoli Access Manager Enterprise Single Sing-On 8.0, IBM Tivoli Identity Manager 5.0, IBM Informix Dynamic Server 11.5, IBM DB2 9.7, IBM Filenet P8 Platform 4.6, IBM Infosphere MDM Server 8.5, IBM Infosphere MDM Server for PIM 6.0**	в 2010	–	Будут сертифицированы на соответствие требованиям Руководящего документа ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - по 5 классу защищенности; Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля; Руководящего документа ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» по классу 1Г ; на соответствие требованиям, предъявляемым к средствам защиты информации, входящих в состав (ИСПДН), относящихся к классу К2.

Контакт: Мартынова Анна, специалист по сертификации ПО.

e-mail: Anna_Martynova@ru.ibm.com

телефон: 8 (916) 596-98-56

5.2. 1С

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Программно-аппаратный комплекс "**1С:Предприятие версия 8.1**"	декабрь 2009		В составе: технологическая платформа (с фиксацией контрольных сумм) и конфигурации согласно ТУ (отсутствие исполняемых модулей и наличие достаточного сценария разграничения доступа, что не мешает делать частые обновления). В настоящее время в соответствии с решением ФСТЭК России номер 2847 от 05.10.09г. ОАО ГИСЦПСВТ проводит работы по сертификации, на соответствие требованиям -по НСД по 5 классу защищенности -по отсутствию НДВ по 4 уровню контроля -использование в АС до класса 1Г включительно - защиты информации в ИСПДн до 2 класса включительно. Заявитель ООО "Научно-производственный центр "1С", имеющий соответствующие лицензии ФСТЭК Сертифицируется партия в 10 000 образцов. Кроме того, сертифицируется производство с тем, чтобы НПЦ "1С" в дальнейшем мог выпускать необходимое количество сертифицированных коробок

5.3 Cisco

Компания Cisco сертифицировала ряд своих продуктов. С сертифицированными продуктами компании Вы сможете ознакомиться на официальном сайте: http://www.cisco.com/web/RU/downloads/Cisco_Security_Certificates.pdf.

5.4 Check Point

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NG AI, R55"**	19.01.2009	19.01.2012	Сертификат №1020/1. Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ третий. ИСПДн класса 2 (К2) включительно. Единичный экземпляр. Испытательная лаборатория ЗАО "Королёвская лаборатория информационных объектов".
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NGX"**	13.11.2006	13.11.2009	Сертификат №1241/1. Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ третий. партия 50 экземпляров ИСПДн класса 2 (К2) включительно. партия 50 экземпляров. Испытательная лаборатория ЗАО "НПП БИТ".
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NGX, R62"**	09.07.2008	09.07.2011	Сертификат №1641. Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ четвертый. ИСПДн класса 2 (К2) включительно. Единичный экземпляр. Испытательная лаборатория ЗАО "ППШ".
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NGX, R62"**	04.12.2007	04.12.2010	Сертификат №1519. Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ третий. ИСПДн класса 2 (К2) включительно. Единичный экземпляр. Испытательная лаборатория ЗАО "Королёвская лаборатория информационных объектов".

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NGX, R65"**	28.11.2007	28.11.2010	Сертификат №1515. Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ третий. ИСПДн класса 2 (К2) включительно. Партия 20 экземпляров. Испытательная лаборатория ЗАО "Королёвская лаборатория информационных объектов".
Межсетевой экран **"Check Point Firewall-1/VPN-1, версия NGX, R65 HFA50"**	Декабрь 2009	Декабрь 2012	Межсетевой экран Check Point FireWall-1/VPN-1 является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей посредством контроля межсетевых взаимодействий. Сертифицирован на соответствие РД МЭ, класс МЭ третий. Возможность работы с СКЗИ "КриптоПро CSP". ИСПДн класса 2 (К2) включительно. Партия 60 экземпляров, далее сертификация производства. Испытательная лаборатория ООО "Газинформсервис".
Вэб-шлюз удаленного доступа **"Check Point Connectra, версия NGX, R66.1"**	Февраль 2010	Февраль 2013	Вэб-шлюз Check Point Connectra является программным средством защиты информации, обрабатываемой в вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа при подключении мобильных и удаленных пользователей к корпоративным ресурсам в рамках установленного SSL туннеля. Сертифицируется на соответствие РД МЭ, класс МЭ третий при выполнении ограничений ТУ. Возможность работы с СКЗИ "КриптоПро CSP/TLS". ИСПДн класса 2 (К2) включительно. Партия, далее сертификация производства.
Система защиты рабочих станций **"Check Point Endpoint Security, версия R72"**	Февраль 2010	Февраль 2013	Система защиты рабочих станций Check Point Endpoint Security является программным средством защиты информации от несанкционированного доступа к конечным точкам сети посредством контроля внешнего и внутреннего трафика. Сертифицируется на соответствие РД МЭ, класс МЭ четвертый. Возможность работы с СКЗИ "КриптоПро CSP/TLS". ИСПДн класса 2 (К2) включительно. партия, далее сертификация производства

Контактные данные:

Телефон: +7 495 967 7 444

www.rus.checkpoint.com

5.5 SUN

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Система управления учетными записями **Sun Java Identity Manager 8.0**	4.08.2009	4.08.2012	Средство защиты от несанкционированного доступа к информации, автоматизированного управления учетными записями, ролями, запросами на предоставление и прекращения прав доступа. Предоставляет широкие возможности по аудиту эффективных прав доступа, подготовки отчетов и синхронизации и интеграции с внешними системами. Благодаря масштабируемой и гибкой архитектуре Sun Java Identity Manager позволяет централизованно управлять миллионами учетных записей. Может быть использован при создании защищенных автоматизированных систем до класса защищенности 1Г включительно. Сертификат № 1881. Сертифицирована партия из 20 маркированных носителей. Сертификационные испытания проведены ООО “Газинформсервис”.
Доверенная операционная система «**Циркон 10**» на базе **ОС Sun Solaris 10 Update 4** с установленным **Solaris Trusted Extensions**	29.12.2008	29.12.2011	Программное средство защиты от несанкционированного доступа к информации. Соответствует 4 уровню контроля отсутствия недекларированных возможностей и 4 классу защищенности. Сертификат № 1752. Схема сертификации предусматривает маркировку носителей специальными знаками по факту прохождения инспекционного контроля. Сертификационные испытания проведены ОАО “Синклит”.
Программное обеспечение терминального доступа «**Циркон-Т**» на базе ПО **SunRay Server/Client Firmware v4 update 2**	29.12.2008	29.12.2011	Программное обеспечение для осуществления терминального доступа. Соответствует 4 уровню контроля отсутствия недекларированных возможностей. Сертификат № 1753. Схема сертификации предусматривает маркировку носителей специальными знаками по факту прохождения инспекционного контроля. Сертификационные испытания проведены ОАО “Синклит”.

Контактные данные:

117198, Москва, Ленинский проспект, 113/1, офис В200

Виктор Буряков, Руководитель подразделения GSE

e-mail: Victor.Bouryakov@sun.com

www.ru.sun.com

5.6 Symantec

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Symantec Data Loss Prevention (DLP)		до 2013	Система защиты от утечек данных (защита от утечек персональных данных, конфиденциальной информации, интеллектуальной собственности и т.д. по всем основным каналам утечки). / Предназначен для использования в ИСПДн класса К4-К1.
Symantec Endpoint Protection (SEP)		до 2013	Антивирус, система защиты конечный устройств (защита рабочих станций и серверов от угроз ИБ). / Предназначен для использования в ИСПДн класса К4-К1.
Symantec Critical System Protection (CSP)		до 2012	Система комплексной защиты серверов (защита критически важных серверов Unix/Linux/ Windows). Может быть использован в ИСПДн.
Symantec Brightmail Gateway (SBG)		до 2012	Шлюзовое решение по защите электронной почты предприятий (защита электронной почты от вирусов, угроз, спама, а также контроль содержимого исходящих сообщений для защиты от утечек). Может быть использован в ИСПДн.
Symantec Mail Security for MS Exchange (SMSME)		до 2012	Решение по защите электронной почты предприятий (защита электронной почты на серверах MS Exchange от вирусов, угроз, спама). Может быть использован в ИСПДн.
Symantec Mail Security for Lotus Domino (SMSDOM)		до 2012	Решение по защите электронной почты предприятий (защита электронной почты на серверах Lotus Domino от вирусов, угроз, спама). Может быть использован в ИСПДн.

Контакт: Кирилл Керценбаум, руководитель группы технических специалистов по ИТ безопасности, Symantec в России и странах СНГ.
Тел.: (495) 662-83-00
e-mail: Kirill_Kertsenbaum@symantec.com
Skype: kkirill2000

5.7 VDEL

Наименование ПО	Дата сертификации	Срок действия сертификата	Информация о сертифицированном ПО
Red Hat Enterprise Linux AS Version 4 Update 4	4 мая 2008	4 мая 2011	Сертификата №1294/3. ОУД4 (усиленный), НДВ4. Серверная операционная система, сертификация в составе комплекса с оборудованием IBM — System x, System p, System i, System z.
Red Hat Enterprise Linux WS Version 4 Update 4	4 мая 2008	4 мая 2011	Сертификата №1294/3. ОУД4 (усилен-ный), НДВ4. Операционная система для вычислительных кластеров, сертификация в составе комплекса с оборудованием IBM — System x, System p, System i, System z.
Комплексное серверное решение OpenReferent on ServerUnited 1.0.10 в составе: Red Hat Enterprise Linux 5.2 Server; Lotus Domino 8.0.1; OpenReferent 3.1.4	5 марта 2009	5 марта 2012	Сертификата №1798. ОУД2, НДВ4. Комплексное решение: высокопроизводительная серверная операционная система RHEL5.2 Server, система совместной работы IBM Lotus Domino 8.0.1, система контроля дисциплины и управления заданиями Open Referent 3.1.4. Для продукта выстроена система сертифика-ционной поддержки.
Комплексное клиентское решение OpenReferent on DesktopUnited 1.0.6 в составе: Red Hat Enterprise Linux 5.2 Desktop; Lotus Notes 8.0.1	5 марта 2009	5 марта 2012	Сертификата №1797. ОУД2, НДВ4. Комплексное решение: клиентская операционная система RHEL5.2 Desktop с набором пользовательских приложений, клиент системы совместной работы IBM Lotus Notes 8.0.1. Для продукта выстроена система сертификационной поддержки.
МСВСфера 5.2 Сервер	-	-	Решение 2786 от 3 августа. ОУД2, НДВ4 (завершается). Серверная операционная система со встроенными серверными службами. Для продукта выстроена система сертификационной поддержки.
МСВСфера 5.2 Десктоп	-	-	Решение 2789 от 3 августа. ОУД2, НДВ4 (завер-шается). Клиентская операционная система с набором пользовательских приложений. Для продукта выстроена система сертифика-ционной поддержки.

Контакт: Алексей Васюков, старший консультант ГК VDEL.
E-mail: alexey.vasyukov@vdel.com

Тел.: +7 (495) 956 68 95
Моб: +7 (926) 550 89 60

6. Контакты регуляторов

6.1. Роскомнадзор

Телефоны:
Справочно-информационный центр:
(495) 987–68-00 (тел)
(495) 987–68-01 (факс)
пн-чт 9:00-18:00, пт 9.00-16:45

Приемная Руководителя Федеральной службы — телефон (495) 987–67–50
Пресс-служба – Воробьев Михаил Николаевич - (495) 987 67-63, 8 (926) 779 40-29.
Общий адрес электронной почты – rsoc_in@rsoc.ru

6.2. ФСТЭК

Номера контактных телефонов:
дежурный по ФСТЭК России: (495) 696-94-20, 696-49-04
по вопросам лицензирования и сертификации: (499) 263-30-57
по вопросам подготовки и повышения квалификации кадров: (495) 696-73-41

7. О клубе 4CIO

Клуб 4CIO это

- - Сообщество ТОП менеджеров, управленцев в области ИТ
- - Более 7 лет на рынке, более 100 действительных Членов Клуба, общая аудитория более 400 CIO
- - Партнеры - более 100 ИТ - компаний
- - Обмен опытом, общение, интересные и полезные деловые и дружеские контакты
- - Совместный отдых

Клуб 4CIO организует

- - Деловые поездки и референс визиты
- - Конференции и конгрессы
- - Специализированные заказные отраслевые конференции
- - Тематические Деловые завтраки
- - Тематические Заседания Членов Клуба
- - ИТ семинары
- - Совместный отдых: Яхт клуб, Кулинарные и Автомобильные секции

Присоединяйтесь!

www.4cio.ru