Приложение 1

РЕКОМЕНДАЦИИ
по проведению работ в подведомственных Рособразованию учреждениях
по обеспечению защиты информационных систем персональных данных.

В соответствии с рекомендациями ФСТЭК России обеспечение защиты информационных систем персональных данных (ПДн) включает следующие стадии:

1 Предпроектная стадия

- •Обследование информационных систем ПДн
- •Разработка Плана мероприятий по обеспечению защиты ПДн
- •Разработка Технического задания

2 Стадия проектирования и реализации

- •Разработка Технического проекта
- •Внедрение технических средств защиты ПДн
- •Разработка нормативной и регламентирующей документации

3 Стадия ввода в действие

- •Опытная эксплуатация системы защиты ПДн
- •Приемо-сдаточные испытания
- • Оценка соответствия требованиям по безопасности информации
- •Обучение персонала
- •Подача уведомления о начале обработки персональных данных

Для типовых систем обработки персональных данных реализация перечисленных работ, особенно в части проектирования систем защиты, существенно упрощается.

1. Проведение обследования

На этапе обследования информационных систем ПДн выполняются следующие работы:

- формируется перечень ПДн, информационных систем и технических средств, используемых для их обработки;
- определяются подразделения и сотрудники, обрабатывающие ПДн;
- определяются категории ПДн;
- разрабатывается описание объекта защиты, включая состав и характеристики средств обработки данных
- проводится предварительная классификация информационных систем ПДн;
- в соответствии с рекомендациями ФСТЭК России и (или) ФСБ России определяются и уточняются типовые модели угроз и соответствующие им типовые требования к системам защиты ПДн;
- осуществляется оценка необходимых мероприятий и затрат по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Результатами работ на этапе обследования являются:

- перечень и категории ПДн,
- перечни информационных систем и технических средств используемых для обработки ПДн и анализ их состояния,
- состав имеющихся в наличии мер и средств защиты ПДн;
- подразделения и сотрудники, обрабатывающие ПДн;
- предварительная классификация информационных систем, обрабатывающих ПДн на типовые (1 - 4 классов) и специальные;
- описание объектов защиты
- уточненные типовые модели угроз и требования к системам защиты ПДн;

- оценка необходимых мероприятий и затрат по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Если затраты времени и средств на приведение информационных систем персональных данных (ИСПДн) в соответствие с предъявляемыми требованиями окажутся слишком высокими, то следует оценить возможность обезличивания или понижения классов информационных систем и провести необходимые работы повторно.

Наиболее эффективным способом приведению ИСПДн в соответствие с предъявляемыми требованиями является их обезличивание. Оно позволяет классифицировать ИСПДн по низшему классу К4 и самостоятельно определить необходимость и способы их защиты.

Если обезличивание невозможно, то понизить требования по защите персональных данных можно путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ.

После определения способов понижения требований по защите персональных данных и необходимого повторного обследования оформляются акты классификации ИСПДн, осуществляются определение и анализ типовых моделей угроз и требований, определение необходимых мер и средств защиты ПДн, а также внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн.

Завершается предпроектная стадия формированием Плана выполнения работ по обеспечению защиты персональных данных.

Предпроектная стадия является важнейшим этапом работ по обеспечению защиты персональных данных, во многом определяющим состав и эффективность реализации мероприятий и необходимые затраты. Поэтому на данном этапе целесообразно привлекать для анализа результатов обследования и консультаций специалистов в области защиты персональных данных.

2. Классификация информационных систем персональных данных и определение актуальных угроз их безопасности

Для проведения классификации ИСПДн, определения категорий персональных данных и экспертной оценки угроз их безопасности целесообразно сформировать комиссию с привлечением специалистов в области информационной безопасности, в том числе по защите государственной тайны.

Перечень типовых ИСПДн определен приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных» http://www.pd.rsoc.ru/low**.** Классификация ИСПДн осуществляется в зависимости от ***категории персональных данных (ПДн***), не содержащих сведения, относящиеся к государственной тайне:

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

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

категория 3 - ПДн, позволяющие идентифицировать субъекта персональных данных;

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

Целесообразно отдельно определять категории ПДн, обрабатываемых в ИСПДн в электронном и в бумажном виде. В последнем случае следует руководствоваться постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687.

Типовые ИСПДн, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных, относятся к классу 1 (***К1***), - к негативным последствиям – к классу 2 (***К2***), ***к незначительным*** негативным ***последствиям*** – к классу 3 (***К3***), для субъектов персональных данных, ***не приводит к*** негативным ***последствиям*** для субъектов персональных данных – к классу 4 (***К4***).

Кроме того, при классификации учитываются объем и территория охвата субъектов персональных данных в порядке, приведенном в приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

Количество субъектов ПДн в системе **Категория ПДн, обрабатываемых в электронном виде**	Более 100 тыс. ПДн	В объеме		От 1000 до 100000 ПДн	В объеме				До 1000 ПДн
		РФ	субъекта РФ		отрасли	органа власти	муниципального образования	организации	
1. Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь	**1 класс (К1)**			**1 класс (К1)**				**1 класс (К1)**	
2. Позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории **1**	**1 класс (К1)**			***2 класс (К2)***				3 класс (К3)	
3. Позволяющие идентифицировать субъекта персональных данных	***2 класс (К2)***			3 класс (К3)				3 класс (К3)	
4. Обезличенные и (или) общедоступные персональные данные	*4 класс (К4)*			*4 класс (К4)*				*4 класс (К4)*	

ИСПДн, обрабатывающие обезличенные или общедоступные персональные данные класса (категории 4) относятся к классу К4. В этом случае обязательные требования по защите ПДн не устанавливаются.

Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" определены необходимые мероприятия по защите персональных данных. В их число входят определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз; разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем, и другие мероприятия.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации *(прежде всего, регламентирование доступа сотрудников к обработке персональных данных, парольная и антивирусная защита);*

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным *(прежде всего, регламентирование использования и регулярное обновление антивирусных средств);*

в) ***недопущение*** воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование *(охрана и регламентирование использования технических средств);*

г) ***возможность*** незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним *(прежде всего, путем хранения резервных копий на съемных маркированных носителях);*

д) постоянный контроль за обеспечением уровня защищенности персональных данных *(осуществляемый, в основном, администраторами ИСПДн и иным персоналом).*

При этом следует иметь ввиду, что ***в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» основным обязательным требованием к ИСПДн является обеспечение конфиденциальности****. Если право доступа субъекта к своим персональным данным, их изменения, блокирования или отзыва реализуются не самим субъектом непосредственно, а персоналом ИСПДн при обращении или по запросу субъекта или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, если в ИСПДн не обрабатываются персональные данные 1 категории и не предусмотрено принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки персональных данных, то другие требования (кроме конфиденциальности) менее критичны. Так, в случае выявления неправомерных действий с персональными данными для их устранения законом предусмотрено три рабочих дня с даты такого выявления.*

Следует учитывать, что требования к обработке персональных данных и к обработке иной конфиденциальной информации (например, коммерческой тайны) могут различаться. ***Применение к обработке персональных данных положений документов (например, СТР-К), действующих до вступления в силу Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», если эти положения в этом законе или последующих подзаконных актах изложены иначе, юридически некорректно****.*

Если система не может быть отнесена к типовой, модель угроз специальной информационной системы разрабатывается на основе ГОСТ Р 51275-2006 специалистами в области информационной безопасности. Типовые модели угроз приводятся в «Базовой модели угроз безопасности персональных данных».

Определение угроз безопасности персональных данных осуществляется на основе утвержденной ФСТЭК России «Базовой модели угроз безопасности персональных данных». Полный перечень угроз определен ГОСТ Р 51275-2006.

Выбор типовой модели угроз осуществляется в зависимости от того, имеют ли ИСПДн подключение к сетям общего пользования и (или) сетям международного информационного обмена, а также от их структуры (автономные автоматизированные рабочие места, локальные сети, распределенные ИСПДн с удаленным доступом).

Наименьшее количество угроз имеют автоматизированные рабочие места и локальные ИСПДн, не подключенные к сетям общего пользования. ***Если ИСПДн нераспределенные и соответствуют классу К3, то необходимые мероприятия по защите персональных данных могут быть осуществлены без привлечения специалистов в области информационной безопасности****.*

Для каждой угрозы, приведенной в типовой модели, следует оценить возможную степень ее реализации. Если она окажется высокой, то это может потребовать применения соответствующих дополнительных технических средств защиты информации.

Возможность реализации угрозы зависит от исходной защищенности ИСПДн и вероятности реализации угрозы.

Вероятность реализации угрозы - определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности ПДн для каждой ИСПДн:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (например, отсутствует физическое подключение к сети);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, действия персонала оговорены в утвержденном регламенте или имеются средства защиты и инструкции по их применению);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (например, средства защиты имеются, но инструкции по их применению отсутствуют):

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Исходная защищенность ИСПДн определяется в соответствии с утвержденной ФСТЭК России «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Расчет исходной защищенности ИСПДн осуществляется по таблице, приведенной в «Методике...», в зависимости от ряда показателей, по которым подразделяются ИСПДн.

В соответствии с «Методикой...» осуществляется расчет возможности реализации угроз и оценка их опасности.

Определяемый на основе опроса экспертов показатель опасности имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, что соответствует классу К3;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных, что ***соответствует классу К2***;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, что ***соответствует классу К1***.

Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных соответствуют классу К4.

При использовании типовых моделей угроз и соответствующих им требований, приведенных в утвержденных ФСТЭК России «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» следует учитывать, что ***в ряде случаев возможности реализации отдельных угроз могут быть более высокими и потребовать дополнительных мер защиты персональных данных.*** Например, возможность реализации угроз увеличивается, если:

- помещения не запираются;
- при обработке персональных данных используются микрофон и динамики;

- монитор не отвернут от окна и посетителей;
- используются беспроводные устройства, в т.ч. клавиатура и мышь;
- отсутствует парольная защита BIOS;
- используются средства сетевого взаимодействия по электропроводке или беспроводные;
- запуск неразрешенных приложений не контролируется.

Актуальные угрозы определяются по приведенной в «Методике...» таблице в зависимости от их опасности и возможности реализации.

При отсутствии дополнительных опасных факторов (например, перечисленных) для нераспределенных ИСПДн 3 класса анализ угроз можно провести при окончательном уточнении требований на этапе выбора и реализации системы защиты персональных данных.

Исходя из составленного перечня актуальных угроз и класса ИСПДн на основе утвержденных ФСТЭК России «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные требования по защите ИСПДн и осуществляется выбор программных и технических средств защиты информации.

Выписки из документов размещены на официальном сайте ФСТЭК России *www.fstec.ru/_razd/_ispo.htm*.

Анализ актуальности угроз и защита персональных данных могут также осуществляться на основании *Методических рекомендаций ФСБ России по обеспечению* ***с помощью криптосредств*** *безопасности персональных данных* при их обработке в информационных системах персональных данных с использованием средств автоматизации. Однако для типовых ИСПДн 3 класса в большинстве случаев это потребует дополнительных затрат.

Если аномально опасные угрозы не выявлены, то ***для ИСПДн 3 класса, как правило, можно ограничиться типовыми требованиями к средствам защиты, приведенными в выписке из «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных»*** *www.fstec.ru/_spravs/meropriaytiay.doc*.

В документе приводятся три варианта требований к ИСПДн 3 класса:
- при ***однопользовательском*** режиме обработки;
- при многопользовательском режиме обработки и ***равных правах доступа***;
- при многопользовательском режиме обработки и ***разных правах доступа***.

В последнем случае при подключении к Интернет нераспределенных ИСПДн класса К3 сертифицированные межсетевые экраны не указаны, как обязательные. Это существенно уменьшает затраты на реализацию системы защиты персональных данных, но требует настройки ИСПДн с учетом прав доступа конкретных пользователей.

3. Определение способов понижения требований по защите персональных данных

По результатам первичной классификации ИСПДн во многих случаях относятся к 1 или 2 классам, требующим существенных затрат и обязательной аттестации. ***Существенно уменьшить обязательные требования и необходимые затраты на защиту персональных данных можно путем обезличивания и сегментирования***

ИСПДн, отключения сегментов ИСПДн от сетей общего пользования, организации выделенных АРМ и др.

Основная экономия затрат достигается при этом за счет отключения от Интернет, изменения классификации сегментов ИСПДн на К4 или К3 и замены аттестации на декларирование соответствия, а также за счет уменьшения количества защищаемых АРМ в аттестуемых ИСПДн высоких классов К2 и К1.

Наилучшим результатом является обезличивание и обоснование соответствия ИСПДн классу К4, для которого все персональные данные относятся к категории 4 и являются обезличенными или общедоступными.

При этом необходимо иметь ввиду, что ***объявить персональные данные общедоступными только внутри организации даже с согласия субъектов ПДн нельзя***. В соответствии с Федеральным законом Российской Федерации от 27 июля 2007 г. №152-ФЗ «О персональных данных», общедоступными являются персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Поэтому ***в информационных системах бухгалтерского и кадрового учета, учета контингента и успеваемости учащихся обязательно будут иметься персональные данные, которые необходимо защищать***.

В этой связи наиболее эффективным является обезличивание ИСПДн путем замены ФИО субъектов ПДн на их личные коды (табельные номера), используемые для автоматизированного учета в данной организации. Существенным преимуществом этого способа является возможность непосредственной замены всех ФИО кодами вручную или с помощью встроенных средств в недоступных для самостоятельной модернизации ИСПДн (1С бухгалтерия, Парус и др.).

Вторым по эффективности является полное исключение из ИСПДн сведений 1 категории, ***касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни***. Даже, если в действующих ИСПДн сохранились такие показатели, то их целесообразно исключить или стереть соответствующие им данные, или заменить на условные коды. ***При необходимости учет персональных данных 1 категории следует осуществлять в форме анкет, справок, личных дел и иных документов только на бумажных носителях***. Для формирования и ведения списков лиц с ограниченными возможностями здоровья конкретные данные о состоянии здоровья, как правило, не требуются.

Также следует полностью исключить из ИСПДн и выделить в специальное делопроизводство сведения, относящиеся к государственной тайне.

Персональные данные 2 категории, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (за исключением ПДн, относящихся к категории 1) ***целесообразно вывести из интегрированных ИСПДн в отдельные локальные системы и отключить от Интернет.***

Персональные данные 3 категории, позволяющие только идентифицировать субъекта персональных данных, в зависимости от объема данных и класса ИСПДн можно обезличивать или обрабатывать в неизменном виде.

4. Изменение класса информационных систем персональных данных путем обезличивания.

Обезличивание ИСПДн позволяет сохранить действующий порядок доступа пользователей, включая удаленный. Единственным отличием является размещение и использование в обезличенных ИСПДн личных кодов вместо ФИО субъектов

персональных данных. При этом ***нельзя ограничиться обезличиванием вновь вводимых персональных данных, а ранее накопленные оставить в той же базе данных без изменения***. Неиспользуемые персональные данные за предшествующие годы целесообразно скопировать на съемные оптические носители и удалить из действующих ИСПДн.

Обезличивание является наиболее приемлемым способом приведения в соответствие требованиям законодательства интегрированных многофункциональных ИСПДн и распределенных ИСПДн, использующих для обмена данными сети общего пользования.

Обезличивание небольших по объему баз данных может осуществляться вручную. Для обезличивания больших объемов персональных данных целесообразно формировать специальные SQL-запросы.

Наиболее просто обезличить ИСПДн, в которых ФИО использовались только в качестве логинов или паролей для доступа учащихся к информационным системам обеспечения учебного процесса. В этом случае достаточно изменить способ формирования идентификационных данных. Функциональность и порядок использования таких обезличенных информационных систем полностью сохраняются.

Возможен также универсальный способ обезличивания и последующей эксплуатации недоступных для самостоятельной модернизации ИСПДн, которые позволяют выводить предназначенные для распечатки бухгалтерские и иные документы в файл в формате MS Excel или MS Word для последующего редактирования. ***Он заключается в разработке несложной программы или макроса для автоматической обратной замены личных кодов на ФИО в выгруженных из ИСПДн для распечатки документах.*** Файлы кодификатора (таблицы соответствия) ФИО и личных кодов могут быть легко сформированы путем выгрузки нужной формы из действующей ИСПДн и последующей ручной ее обработки, например в Excel, с конвертированием в файлы требуемого формата.

Важными достоинствами указанного способа обезличивания ИСПДн, кроме универсальности, являются:

- сохранение функциональности и сервисного сопровождения обезличиваемых действующих ИСПДн без их программной модернизации;
- использование единого кодификатора ФИО, содержащего персональные данные 3 категории, для распечатки документов, выгружаемых из различных обезличиваемых ИСПДн;
- возможность децентрализованного использования кодификатора ФИО на отдельных АРМ;
- обеспечение надлежащего хранения и использования кодификатора ФИО на защищенном встроенном или отдельном внешнем носителе;
- возможность редактирования и дополнения кодификатора ФИО средствами MS Office.

Если численность учащихся превышает 1000 человек и класс ИСПДн соответствует К2, то кодификатор ФИО также может быть разбит на отдельно хранимые части (файлы), не превышающие 1000 человек (по годам зачисления, курсам, факультетам и др.). При этом база обезличенных данных может оставаться общей.

5. Понижение требований по защите персональных данных путем сегментирования информационных систем персональных данных.

Сегментирование заключается в разделении сетевой ИСПДн на несколько сегментов для уменьшения требований и упрощения защиты персональных данных. Оно ***позволяет:***

- ***децентрализовать обработку персональных данных 2-й категории и понизить класс сегментов ИСПДн до К3, если количество субъектов персональных данных превышает 1000 человек***, ***или если они не принадлежат организации-оператору.***

- уменьшить количество защищаемых АРМ в распределенных ИСПДн.

Данный способ на практике является одним из основных.

При сегментировании ИСПДн на взаимодействующие по сети подсистемы следует иметь ввиду, что класс системы в целом равен наиболее высокому классу ее подсистем (сегментов). Поэтому ***простое разделение на ИСПДн подсистемы без ограничения их взаимодействия не снижает требования по защите персональных данных.***

Простейшим способом ограничения взаимодействия сегментов является их физическое (гальваническое) изолирование друг от друга. Альтернативным способом сегментирования является использование сертифицированных ФСТЭК России межсетевых экранов. Однако на практике оба эти способа сопряжены с приобретением дополнительного серверного оборудования и программного обеспечения и повышенными затратами на администрирование и технологическое сопровождение сегментированной ИСПДн. Поэтому ***наиболее целесообразно сегментировать слабо взаимодействующие подсистемы ИСПДн,*** например, кадрового и бухгалтерского учета персонала и подсистемы обеспечения учебного процесса ***с обменом данными между ними с помощью съемных носителей.***

Более эффективно осуществлять сегментирование до отдельных рабочих мест в сочетании с обезличиванием действующей ИСПДн. При этом затраты на эксплуатацию единой обезличенной ИСПДн не увеличиваются, а хранить кодификаторы ФИО (или их части) можно непосредственно на тех рабочих станциях, на которых персональные данные визуализируются. ***Если ИСПДн не является распределенной и не подключена к Интернет, то мероприятия по защите отдельных рабочих мест не потребуют больших затрат.***

Наиболее сложной является защита персональных данных в распределенных ИСПДн. Поэтому ***пересылку персональных данных по сетям общего пользования целесообразно осуществлять только в обезличенном виде***, ***а обмен кодификаторами ФИО - курьерским способом. Это позволит избежать классификации и защиты распределенных ИСПДн.***

6. Уменьшение требований к защите информации путем отключения ИСПДн от сетей общего пользования.

Подключение ИСПДн к сетям общего пользования, в том числе Интернет, требует дополнительных средств защиты даже в том случае, если передача персональных данных по ним не предусмотрена. Для уменьшения требований и затрат на защиту информации целесообразно изолировать от Интернет все локальные сетевые ИСПДн.

Если персоналу необходим доступ в Интернет, то наиболее просто предусмотреть для этого дополнительные компьютеры (например, устаревшие), не подключая их к ИСПДн.

При невозможности размещения дополнительных рабочих станций требуются дополнительные сертифицированные ФСТЭК России средства защиты подключенных к Интернет персональных компьютеров, если они обрабатывают персональные данные.

Средства защиты информации (сертифицированная операционная система или специализированные средства) не должны разрешать одному и тому же зарегистрированному пользователю обрабатывать персональные данные и выходить в

Интернет. Должны быть также разграничены разделы дисковой памяти и сменные носители информации. Выбор и настройка сертифицированных средств защиты информации могут осуществляться системными администраторами образовательных учреждений при консультировании со специалистами в области информационной безопасности. ***При этом один виртуальный пользователь (со своим логином и паролем) получает возможность выхода в Интернет, а другой – работать с персональными данными. Этими пользователями может быть одно и тоже физическое лицо. По сравнению с выделенными АРМ, изолированными от Интернет, затраты на защиту персональных данных в нераспределенных ИСПДн 3 класса для многопользовательских АРМ с разными правами пользователей увеличиваются незначительно***.

Для уменьшения требований к защите информации типовые ИСПДн (системы бухгалтерского и кадрового учета 1С, Парус и др.) рекомендуется изолировать от сети Интернет. При обработке персональных данных в пределах организации такие системы, как правило, будут соответствовать нераспределенным ИСПДн класса К3. При этом лицензий ФСТЭК России от оператора персональных данных не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Загрузку обновленных антивирусных баз данных, а также программ и форм персонифицированного учета и отчетности целесообразно осуществлять на других компьютерах, подключенных к сети Интернет. Безопасный перенос загруженных файлов в изолированные от Интернет локальные ИСПДн может осуществляться с использованием маркированных съемных носителей, в обязательном порядке проверяемых антивирусными средствами перед загрузкой в ИСПДн.

Официально распространяемые территориальными органами ФНС России и Пенсионного фонда России программы при соблюдении требований информационной безопасности в изолированных ИСПДн класса К3 могут использоваться при подготовке данных персонифицированного учета. При этом сформированные данные персонализированного учета должны выгружаться из ИСПДн на съемные маркированные носители. Незащищенная пересылка по сети Интернет данных, содержащих ФИО физических лиц, недопустима! Исключение могут составлять сведения, идентифицирующие работников только по ИНН, личному коду пенсионного страхования и другим кодам, без передачи ФИО физических лиц.

7. Обеспечение обмена персональными данными.

Обмен персональными данными с помощью маркированных съемных носителей не очень удобный, но менее затратный способ защищенного информационного взаимодействия.

Для обеспечения необходимого информационного взаимодействия по сети Интернет (в том числе пересылки электронных платежных документов, данных персонализированного налогового учета и др.) ***рекомендуется использовать выделенные автоматизированные рабочие места, которые не подключены к локальным сетевым ИСПДн.*** При этом повышенные требования и необходимость использования дополнительных сертифицированных средств защиты пересылаемых данных распространяются только на соответствующие АРМ.

Перенос персональных данных между взаимодействующими по сети Интернет ***выделенными АРМ и локальными ИСПДн целесообразно осуществлять с помощью маркированных съемных носителей.*** В противном случае необходимо дополнительно использовать дорогостоящие сертифицированные межсетевые экраны.

С целью защиты персональных данных при передаче по каналам связи участниками информационного обмена применяются средства криптографической защиты информации (СКЗИ), сертифицированные в установленном порядке.

Так, допускается представление сведений по форме № 2-НДФЛ с привлечением специализированных средств и операторов связи, осуществляющих передачу данных по телекоммуникационным каналам связи от налоговых агентов в налоговые органы. При этом налоговый агент и налоговый орган обеспечивают хранение данных в электронном виде в установленном порядке.

Аналогичные возможности предоставляют территориальные органы Пенсионного фонда РФ. При этом необходимо соблюдать «Регламент обеспечения безопасности информации при обмене электронными документами в СЭД ПФР по телекоммуникационным каналам связи».

При этом также могут использоваться средства специализированных провайдеров (Контур-Экстерн, Такском и др.), которые позволяют отправлять юридически значимые электронные документы по установленным формам в налоговые органы и ПФР, а также в органы государственной статистики.

8. Оформление актов классификации информационных систем персональных данных.

После определения способов понижения класса ИСПДн уполномоченная руководителем учреждения комиссия оформляет акты классификации информационных систем персональных данных по приведенной форме.

Примерная форма акта классификации
информационных систем, обрабатывающих
персональные данные

Утверждаю

_____

"____"_____"____"г.

А К Т

классификации информационной системы, обрабатывающей персональные данные

наименование информационной системы

Комиссия, в соответствии с приказом от № в составе:

председатель:

члены комиссии:

провела классификацию информационной системы *наименование информационной системы*, обрабатывающей персональные данные, и установила:

Выявленные определяющие признаки классификации типовой информационной системы:

- *наивысшая категория обрабатываемых персональных данных (1, 2, 3);*
- *наличие сведений, составляющих государственную или служебную тайну;*
- *количество обрабатываемых субъектов персональных данных (диапазон);*
- *структура системы (автономная, локальная, распределенная);*
- *наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;*
- *режим обработки персональных данных (однопользовательский или многопользовательский);*
- *режим разграничения прав доступа пользователей информационной системы (без разграничения прав доступа или с разграничением прав);*
- *местонахождение технических средств информационной системы (в пределах Российской Федерации, частично или целиком за пределами Российской Федерации.*),

Комиссия, на основании определяющих признаков классификации и в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных", а также с рекомендациями ФСТЭК России,

РЕШИЛА:

присвоить информационной системе *наименование информационной системы,* обрабатывающей персональные данные, класс *К1 или К2 или К3 или специальный.*

Председатель

Члены комиссии

9. Проектирование и реализация средств защиты информационных систем персональных данных 3 и 4 классов.

Проектирование и реализация систем защиты типовых ИСПДн, существенно проще, чем специализированных. При этом разработка технического проекта обычно сводится к выбору наименее затратного подходящего типового технического решения.

Стадия реализации типовых ИСПДн 3 класса сводится к приобретению и внедрению типовых технических средств защиты ПДн и адаптации типового комплекта нормативной и регламентирующей документации.

Стадия ввода в действие включает опытную эксплуатацию системы защиты ПДн, приемо-сдаточные испытания, аттестацию или декларирование соответствия требованиям по безопасности информации, обучение персонала.

На заключительном этапе работ осуществляется подготовка уведомления (или соответствующих изменений) в территориальное подразделение Роскомнадзора.

При реализации средств защиты необходимо иметь ввиду, что обязательные требования по защите ПДн для ИСПДн класса К4, обрабатывающих обезличенные или общедоступные персональные данные, случае не устанавливаются.

Обязательные мероприятия по защите персональных данных в типовых нераспределенных ИСПДн класса К3 могут быть осуществлены без привлечения специалистов в области информационной безопасности. Если в таких системах АРМ пользователей, работающих персональными данными, не подключены к сети (локальной или Интернет), а обмен данными осуществляется с помощью маркированных съемных носителей, то достаточно использовать средства защиты информации (СЗИ), встроенные в сертифицированные ФСТЭК России ОС Windows XP/Vista.

Продукты Майкрософт, сертифицированные во ФСТЭК России, с точки зрения программного кода ничем не отличаются от обычных лицензионных легальных продуктов Майкрософт. Однако ***в соответствии с законодательством России каждый экземпляр сертифицированного ФСТЭК России продукта имеет пакет документов государственного образца о том, что данный продукт является сертифицированным, включая специальный знак соответствия с уникальным номером.*** В комплекте с сертифицированным программным продуктом поставляется специальная эксплуатационная документация, в соответствии с которой осуществляется настройка и контроль сертифицированных параметров этого программного обеспечения.

Кроме того, обладатель сертифицированной версии продукта, имеет защищенный доступ к специализированному сайту для получения сертифицированных обновлений. Сертифицированные продукты Майкрософт имеют оценочный уровень доверия ОУД1 (усиленный) и могут использоваться в составе информационных систем персональных данных.

Настройка и конфигурирование сертифицированной ФСТЭК России ОС Windows XP может осуществляться самостоятельно или приобретаемыми у официальных поставщиков средствами. Более подробная информация о конфигурировании ОС Windows XP в соответствии с требованиями безопасности представлена на сайтах (www.microsoft.com/Rus/Security/Certificate/Default.mspx, www.altx-soft.ru).

Дополнительная защита информации АРМ, в которых один виртуальный пользователь (со своим логином и паролем) получает возможность выхода в Интернет, а другой – работать с персональными данными, может быть осуществлена с помощью утилиты DevCon. Это свободно распространяемая Майкрософт программа с интерфейсом командной строки, которая позволяет включать, выключать, перезапускать, обновлять, удалять и опрашивать отдельные устройства или группы устройств.

Для отключения сетевой карты АРМ пользователя персональных данных при его входе в систему может быть предусмотрено выполнение команды «devcon disable.... Таким образом, данный виртуальный пользователь не может работать в сети, но может работать с персональными данными. Для включения сетевой карты у другого виртуального пользователя сети, при его входе в систему в автозагрузке может быть предусмотрено выполнение команды «devcon enable.... Это дает доступ к сетевым сервисам и услугам корпоративной сети и Интернет, но не позволяет работать с персональными данными. Доступ пользователей к директориям (папкам) с персональными данными при этом должен быть разграничен средствами ОС Windows XP.

Совпадение программных кодов сертифицированных ФСТЭК России и обычных лицензионных ОС Windows XP, имеющихся практически в каждом учреждении, дает возможность осуществить самостоятельную апробацию и опытную эксплуатацию системы защиты ИСПДн до приобретения сертифицированных продуктов. Если в результате опытной эксплуатации возможностей СЗИ ОС Windows XP окажется недостаточно, то от приобретения

сертифицированной версии продукта можно отказаться и приобрести специализированные СЗИ, устанавливаемые поверх обычной лицензионной ОС Windows XP. Государственный реестр СЗИ, сертифицированных ФСТЭК России, можно загрузить с официального сайта www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls.

В более сложных случаях, чем нераспределенные ИСПДн класса К3, для выполнения работ необходимо привлекать специалистов специализированных организаций:www.fstec.ru/_doc/reestr_tzki/_reestr_tzki.xls, www.fstec.ru/_doc/per_org_at/_orgat.xls.

10. Подготовка к проверкам законности обработки персональных данных.

Роскомнадзор, ФСТЭК России и ФСБ России в рамках своей компетенции осуществляют плановые и внеплановые проверки законности обработки персональных данных. Это предусмотрено регламентом проведения проверок при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных (www.rsoc.ru/.cmsc/upload/documents/20090828191123gJ.doc)

Проверка осуществляется в отношении Операторов - государственных органов**,** муниципальных органов, юридических или физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных.

Проверка соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных завершается:

- составлением и вручением Оператору акта проверки;
- выдачей Оператору предписания об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных;
- составлением протокола об административном правонарушении в отношении Оператора;
- подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

О проведении ***плановой проверки*** Оператор уведомляется не позднее, чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Роскомнадзора или ее территориального органа с уведомлением о вручении или иным доступным способом.

Внеплановые проверки проводятся по следующим основаниям:

- истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных;
- поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:
- возникновение угрозы причинения вреда жизни, здоровью граждан;
- причинение вреда жизни, здоровью граждан;
- нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных;

- нарушение Операторами требований настоящего Федерального закона и иных нормативных правовых актов в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

О проведении внеплановой выездной проверки Оператор уведомляется Роскомнадзором или ее территориальным органом не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Должностные лица Роскомнадзора или его территориального органа, в качестве приглашенных специалистов, могут принимать участие в проверках ФСБ России, ФСТЭК России, правоохранительных органов и органов прокуратуры.

В ходе проведения проверки Роскомнадзор или его территориальный орган осуществляют следующие мероприятия по контролю:

а) рассмотрение документов Оператора, включающих сведения:

- содержащиеся в уведомлении об обработке персональных данных, поступивших от Оператора и фактической деятельности Оператора;

- о фактах, содержащих признаки нарушения законодательства Российской Федерации в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Роскомнадзор или его территориальный орган;

- *о* ***выполнении Оператором предписаний об устранении ранее выявленных нарушений*** законодательства Российской Федерации в области персональных данных. ***Данная проверка проводится в виде внеплановой проверки****;*

- о наличии у Оператора письменного согласия субъекта персональных данных на обработку его персональных данных;

- о соблюдении требований законодательства Российской Федерации при обработке ***специальных*** категорий и ***биометрических*** персональных данных;

- о порядке и условиях ***трансграничной*** передачи персональных данных;

- о порядке обработки персональных данных, ***осуществляемой без использования средств автоматизации***;

- ***о соблюдении требований конфиденциальности*** при обработке персональных данных;

- ***о фактах уничтожения Оператором персональных данных*** субъектов персональных данных ***по достижении цели обработки***;

- ***локальные акты Оператора, регламентирующие порядок и условия обработки персональных данных***;

- об иной деятельности, связанной с обработкой персональных данных;

б) исследование (обследование) информационной системы персональных данных, в части касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

Должностные лица Роскомнадзора или его территориального органа при проведении проверок вправе в пределах своей компетенции:

- ***выдавать обязательные для выполнения предписания об устранении выявленных нарушений*** **в** области персональных данных;

- ***составлять протоколы об административном правонарушении*** или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о

возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подследственностью;

- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

- ***использовать необходимую технику и оборудование***, принадлежащие Роскомнадзору или его территориальному органу;

- ***запрашивать и получать необходимые документы (сведения)*** для достижения целей проведения мероприятия по контролю (надзору);

- ***получать доступ к информационным системам персональных данных***;

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

- ***принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства*** Российской Федерации в области персональных данных;

- ***требовать от Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных***.

Примерный перечень запрашиваемых документов:

учредительные документы Оператора;

копия уведомления об обработке персональных данных;

положение о порядке обработки персональных данных;

положение о подразделении, осуществляющем функции по организации защиты персональных данных;

должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных;

план мероприятий по защите персональных данных;

план внутренних проверок состояния защиты персональных данных;

приказ о назначении ответственных лиц по работе с персональными данными;

типовые формы документов, предполагающие или допускающие содержание персональных данных;

журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;

договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;

выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения проверки;

приказы об утверждении мест хранения материальных носителей персональных данных;

письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма);

распечатки электронных шаблонов полей, содержащие персональные данные;

справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных;

заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов);

приказ о создании комиссии и акты проведения классификации информационных систем персональных данных (проверяется только наличие данных документов);

журналы (книги) учета обращений граждан (субъектов персональных данных);

акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);

иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных.

Акт по результатам проверки может содержать одно из следующих заключений:

- ***об отсутствии нарушений*** требований законодательства Российской Федерации в области персональных данных;

- ***о выявленных нарушениях*** требований законодательства Российской Федерации в области персональных данных, с указанием конкретных статей и (или) пунктов нормативных правовых актов.

Наличие и соблюдение персоналом требуемых распорядительных документов и инструкций является необходимым условием обеспечения информационной безопасности персональных данных.

11. Другие вопросы обработки персональных данных.

Другие наиболее важные вопросы обработки персональных данных изложены в письме Федерального агентства по образованию от 29.07.2009 № 17–110 «Об обеспечении защиты персональных данных *www.ed.gov.ru/files/materials/10432/pi17-110.pdf, www.pd.rsoc.ru/low*. Это:

- оформление согласия на обработку персональных данных,
- законодательство о защите персональных данных,
- порядок обработки персональных данных, осуществляемой без использования средств автоматизации,
- основные обязанности операторов информационных систем, обрабатывающих персональные данные,
- основные мероприятия по обеспечению безопасности персональных данных в учреждениях образования,
- порядок проведения аттестационных (сертификационных) испытаний,
- декларирование соответствия.

Исп. Королевский Дмитрий Алексеевич,
ФГУ ГНИИ ИТТ «Информика»
(495) 237-66-84, ispd@ministry.ru