МИНИСТЕРСТВО
ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное агентство
по образованию
(Рособразование)**

РУКОВОДИТЕЛЬ

ул. Люсиновская, д.51, Москва, М-93, ГСП-8, 115998
Телефон: (495) 237-67-24 Факс: (495) 236-01-71
Telex: 485152 RUFAO RU
E-mail: bicab@ed.gov.ru
ОКПО 00083411 ОГРН 1047796317832
ИНН/КПП 7725509655/772501001

22.10.2009 № 17-187

На № _____

Руководителям
учреждений,
подведомственных
Федеральному агентству
по образованию

Об обеспечении защиты
персональных данных

Федеральное агентство по образованию напоминает, что все действующие информационные системы, обрабатывающие персональные данные, должны быть до 1 января 2010 года приведены в соответствие с требованиями Федерального закона Российской Федерации от 26.07.2006 г. № 152-ФЗ «О персональных данных».

В дополнение к письму Федерального агентства по образованию от 29.07.2009 г. № 17–110 «Об обеспечении защиты персональных данных» (www.ed.gov.ru/files/materials/10432/pi17-110.pdf) направляем Вам рекомендации по проведению работ в подведомственных Рособразованию учреждениях по обеспечению защиты информационных систем персональных данных (приложение 1), в том числе по обследованию и классификации информационных систем, а также уменьшению затрат на защиту информации. Основные нормативные и инструктивные документы размещены на специализированном портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) pd.rsoc.ru и официальном сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru.

В первоочередном порядке следует привести в соответствие с требованиями законодательства, Роскомнадзора и ФСТЭК России внутренние регламенты и ознакомить с ними сотрудников учреждения, работающих с персональными данными. Рекомендации по подготовке документов, регламентирующих обработку персональных данных в подведомственных Рособразованию учреждениях, приведены в приложении 2.

Данные рекомендации являются примерными и должны быть адаптированы учреждением с учетом конкретных условий обработки персональных данных.

В целях актуализации базы данных, сформированной в соответствии с письмом Рособразования от 28.04.2008 г. № ФАО-6748/52/17-02-09/72, просим Вас в срок до 15 ноября 2009 г. направить в Административно-правовое управление Рособразования по уточненной форме (приложение 3) сведения о характеристиках информационных систем, обрабатывающих персональные данные в подведомственных Рособразованию учреждениях, на бумажном и электронном носителях (e-mail: ispd@ministry.ru).

В соответствии с Федеральным законом Российской Федерации от 26.07.2006 г. № 152-ФЗ «О персональных данных» об изменениях в составе и классификации информационных систем персональных данных необходимо в установленном порядке уведомить территориальный орган Роскомнадзора в течение десяти рабочих дней с даты возникновения изменений.

Приложения на 40 л.

Н.И. Булаев

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

Приложение 2

РЕКОМЕНДАЦИИ
по подготовке документов, регламентирующих обработку персональных данных в подведомственных Рособразованию учреждениях.

1. ***Приказ о создании комиссии по защите персональных данных с наделением ее полномочиями по проведению мероприятий, касающихся организации защиты персональных данных.***

В комиссию рекомендуется включать руководителей или полномочных представителей всех структурных подразделений учреждения, обрабатывающих персональные данные. Председателем комиссии целесообразно назначить заместителя руководителя учреждения. При необходимости вместо создания отдельной комиссии по защите персональных данных могут быть расширены состав и полномочия комиссии по защите сведений, составляющих государственную тайну.

2. ***Приказ об утверждении Положения об обработке и защите персональных данных.***

В Положении рекомендуется отразить следующее.

Общие положения, в том числе:

- предмет Положения (например, *порядок получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора)*;

- цель и задачи учреждения в области защиты персональных данных (например, *обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных работников, учащихся и выпускников, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных)*;

- понятие и состав персональных данных *(персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами* «наименование учреждения»*)*;

- кто является Оператором персональных данных (например, «наименование учреждения». *Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений)*;

Порядок получения и обработки персональных данных, в том числе:

- как происходит получение персональных данных *(получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами учреждения на основе согласия субъектов на обработку их персональных данных. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации)*;

- как они обрабатываются и используются *(обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Не допускается 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. В случае увольнения, отчисления субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями Оператора*);

- в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные *(Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным Положением об обработке и защите персональных данных, распорядительными документами и иными письменными указаниями Оператора.* Также целесообразно привести в приложении к приказу об утверждении Положения укрупненный перечень персональных данных и перечень структурных подразделений и (или) отдельных должностей, имеющих право на их обработку*)*;

- на каком основании персональные данные защищаются от несанкционированного доступа *(персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Оператора)*;

<u>Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных,</u> в том числе:

- права субъекта персональных данных в целях обеспечения защиты своих персональных данных *(в целях обеспечения защиты своих персональных данных субъект*

персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право

на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

на обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке).

- Обязанности Оператора при сборе персональных данных *(Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.*

В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных).

- права Оператора на передачу персональных данных третьим лицам *(Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации)*;

- ответственность Оператора за разглашение персональных данных *(Оператор, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные).*

3. ***Письменное согласие субъектов персональных данных на их обработку.***

Требования к оформлению согласия субъектов персональных данных на их обработку 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*.

4. ***Приказ/ы о возложении на персональной ответственности за защиту персональных данных.***

В приказе рекомендуется привести список конкретных лиц, ответственных за защиту информационных систем и групп обрабатываемых в учреждении персональных данных.

5. ***Разрешительные документы о допуске конкретных сотрудников к обработке персональных данных.***

Приказы или иные утвержденные руководством учреждения разрешительные документы должны включать списки сотрудников Оператора и временно привлекаемых лиц, допущенных к обработке укрупненных групп персональных данных. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

6. ***Уведомление об обработке персональных данных.***

В соответствии со статьей 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ. «О персональных данных», приказами Роскомнадзора и утвержденной формой уведомления, размещенными на его официальном сайте *www.rsoc.ru*, уведомление об обработке персональных данных, должно быть направлено в соответствующее территориальное подразделение Роскомнадзора.

В соответствии с приведенными законодательными и нормативными актами уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес Оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;

7) описание мер, которые Оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных.

Если обработка персональных данных смешанная, то в уведомлении описание мер и средств обеспечения безопасности персональных данных рекомендуется осуществлять для автоматизированного и неавтоматизированного способов обработки с указанием соответствующих категорий персональных данных.

В случае изменений Оператор обязан уведомить соответствующее территориальное подразделение Роскомнадзора в течение десяти рабочих дней с даты возникновения изменений.

Без уведомления Оператор вправе осуществлять обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с Оператором трудовые отношения;

2) полученных Оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

7. Должностные инструкции сотрудников, имеющих отношение к обработке персональных данных

Должностные инструкции сотрудников учреждения, дополненные положениями о необходимости соблюдения утвержденного Положения об обработке и защите персональных данных и Инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

8. Журнал обращений по ознакомлению с персональными данными.

Журнал рекомендуется вести в каждом структурном подразделении в произвольной форме. В журнале необходимо фиксировать все обращения субъектов персональных данных (дата, ФИО, адрес) по ознакомлению с их персональными данными, дату направления запрашиваемых данных почтовой связью или предоставления лично

заявителю. В случае отзыва данных субъектом персональных данных или выявления их несоответствия, в журнале должны быть сделаны соответствующие записи. По каждому обращению необходимо указывать, когда и каким образом на него было отреагировано. Хранение журналов должно исключать несанкционированный доступ к ним.

9. ***Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.***

   В Инструкции рекомендуется отразить следующее.

   Общие положения, в том числе:

- предмет Инструкции (например, *обязательные для всех структурных подразделений «учреждения» требования по обеспечению конфиденциальности документов, содержащих персональные данные)*;

- определение персональных данных *(персональные данные - 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.*

- когда обеспечение конфиденциальности персональных данных не требуется (*в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных);*

- необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку (например, *конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку. Согласие субъекта персональных данных не требуется на обработку данных:*
  - *в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;*
  - *адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;*
  - *данных, включающих в себя только фамилии, имена и отчества;*
  - *в целях однократного пропуска на территорию, или в иных аналогичных целях;*
  - *персональных данных, обрабатываемых без использования средств автоматизации.*
- порядок ведения перечней персональных данных (например, *в структурных подразделениях «учреждения» формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных* ***по прилагаемой форме****. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается*);

- нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации (*Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями 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" и от 15 сентября 2008 г.*

№ 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее);

- общие правила хранения и передачи персональных данных (например, *запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.*

Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках);

- ответственность за защиту обрабатываемых персональных данных (*например, сотрудники подразделений «учреждения», сотрудники организаций-Операторов или лица, осуществляющие такую обработку по договору с Оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в «учреждении», несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами);*

- порядок ознакомления с Инструкцией (например, *сотрудники подразделений «учреждения» и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией)*.

Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации, в том числе:

- условия хранения персональных данных (например, *обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.*

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию).

- использование типовых форм документов и журналов учета (*при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:*

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке

пропуска субъекта персональных данных на территорию, на которой находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

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

- порядок уничтожения или обезличивания персональных данных (*уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными*).

Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации**,** в том числе:

- правила доступа, хранения и пересылки персональных данных (например, *безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.*

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается).

- общие требования по защите персональных данных в автоматизированных системах (например, *технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.*

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных).

- специфические требования по защите персональных данных в отдельных автоматизированных системах (например, *специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации).*

Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации, в том числе:

- организация учета носителей персональных данных (например*, все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.*

Учет и выдачу съемных носителей персональных данных ***по прилагаемой форме*** *осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники «учреждения» получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.*

- правила использования съемных носителей персональных данных (например, *запрещается:*

- *хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;*
- *выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.*

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для

документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения).

- порядок действий при утрате или уничтожении съемных носителей персональных данных (например, *о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.*

Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт ***по прилагаемой форме****)*.

Пример формы учета
персональных данных

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в структурных подразделениях

_____
наименование учреждения

_____
наименование структурного подразделения

№ п/п	**Наименование (вид, типовая форма) документов с персональными данными**	**Регламентирующие документы (Наименование, дата, номер)**	**Наименование информационной системы/ без использования средств автоматизации**	**Отдел**	**Место хранения (комната)**	**ФИО ответственных за обработку и хранение**
1						
2						
3						

_____ _____
Должность и ФИО начальника структурного подразделения Подпись

_____ _____
Должность и ФИО ответственного за защиту Подпись
персональных данных в структурном подразделении

Пример формы журнала
учета съемных носителей

ЖУРНАЛ

учета съемных носителей персональных данных

_____

наименование структурного подразделения

Начат «__» _____На _____листах
Окончен «__» _____ 200_ г.

_____ _____
Должность и ФИО ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Пример акта.

«УТВЕРЖДАЮ»

_____ _____
« »_____ 200 г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от № в составе:

_____
(должности, ФИО)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
	2	**3**	**4**

Всего съемных носителей_____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены
_____
путем (разрезания, демонтажа и т.п.) ,
_____
измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья

_____ _____
(наименование предприятия) (Дата)

Председатель комиссии Подпись Дата

Члены комиссии

(ФИО) Подпись Дата

При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для системы высоких классов – также администратор системы безопасности. Инструкции для этого должностного лица составляются отдельно. Для технического обслуживания оборудования должен быть предусмотрен соответствующий обслуживающий персонал.

В зависимости от класса системы и ее характеристик инструкции обслуживающего персонала (включая администраторов систем) и пользователей будут существенно различаться. Применительно к нераспределенным информационным системам класса К3 в Инструкции пользователя и Инструкции администратора по обеспечению мониторинга защиты информации и антивирусного контроля рекомендуется отразить следующее.

10. Инструкция пользователя при обработке персональных данных на объектах вычислительной техники

В Инструкции рекомендуется отразить следующее.

Общие положения, в том числе:

- предмет Инструкции (например, *основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) «учреждения»).*

- общие требования к пользователю (например, *пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.*

Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

Обязанности пользователя, например:

- *выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;*
- *при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;*
- *соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;*
- *после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;*
- *оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;*
- *не допускать "загрязнение" ПЭВМ посторонними программными средствами;*
- *знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий,*
- *знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;*

- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

- *знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;*
- *при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.*

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- *приостановить работу;*
- *немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;*
- *оценить необходимость дальнейшего использования файлов, зараженных вирусом;*
- *провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).*

Запрещаемые действия, например**:**

- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в подключении и размещении технических средств;

- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

Права пользователя ПЭВМ, например:

Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным

программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

Ответственность пользователей ПЭВМ, например, за:

- *надлежащее выполнение требований настоящей инструкции;*
- *соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;*
- *сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;*
- *сохранность персональных данных.*

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

11. Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

В Инструкции рекомендуется отразить следующее.

Общие положения, определяющие предмет Инструкции (например, *порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации «учреждения»).*

Мониторинг аппаратного обеспечения, например:

Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

Мониторинг парольной защиты, например:

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- *установление сроков действия паролей (не более 3 месяцев);*
- *периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).*

Мониторинг целостности, например:

Мониторинг целостности программного обеспечения включает следующие действия:

- *проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;*
- *обнаружение дубликатов идентификаторов пользователей;*
- *восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.*

Мониторинг попыток несанкционированного доступа, например:

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- *фиксацию неудачных попыток входа в систему в системном журнале;*
- *протоколирование работы сетевых сервисов;*
- *выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.*

Мониторинг производительности, например:

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

Системный аудит, например:

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности должны включать:

- *отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;*
- *проверку содержимого файлов конфигурации на соответствие списку для проверки;*
- *обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);*
- *проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);*
- *проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;*
- *проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).*

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости),

либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Антивирусный контроль, например:

Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- *резидентные антивирусные мониторы, контролирующие подозрительные действия программ;*
- *утилиты для обнаружения и анализа новых вирусов.*

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие невыявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- *осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;*
- *проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.*

На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- *отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;*
- *немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.*

Анализ инцидентов, например:

Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- *факт попытки несанкционированного доступа (НСД);*
- *продолжается ли НСД в настоящий момент;*
- *кто является источником НСД;*
- *что является объектом НСД;*
- *когда происходила попытка НСД;*
- *как и при каких обстоятельствах была предпринята попытка НСД;*
- *точка входа нарушителя в систему;*
- *была ли попытка НСД успешной;*
- *определить системные ресурсы, безопасность которых была нарушена;*
- *какова мотивация попытки НСД.*

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

При анализе системных журналов администратору необходимо произвести следующие действия:

- *проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;*
- *проверить не уничтожен ли системный журнал и нет ли в нем пробелов;*
- *просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;*
- *проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам;*
- *проверить наличие мест в журналах, которые выглядят необычно;*
- *выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;*
- *выявить наличие неудачных попыток входа в систему.*

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- *проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;*
- *проверить не уничтожен ли системный журнал и нет ли в нем пробелов;*
- *проверить наличие мест в журналах, которые выглядят необычно;*
- *выявить попытки изменения таблиц маршрутизации и адресных таблиц;*
- *проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.*

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- *составить базовую схему того, как обычно выглядит система;*
- *провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;*
- *проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;*
- *проверить целостность системных программ;*
- *проверить систему аутентификации и авторизации.*

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

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