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