Ролик https://smotrim.ru/video/771597

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО

от 28 апреля 2020 года N ДГ-375/07

О направлении методических рекомендаций

В соответствии с пунктом 13 Межведомственного плана комплексных мероприятий по реализации Концепции развития сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная ответственность в Российской Федерации, до 2025 года, утвержденного Правительственной комиссией по делам несовершеннолетних и защите их прав 25 сентября 2019 г. (далее - поручение), Минпросвещения России подготовлены и согласованы с Минюстом России методические рекомендации по развитию сети служб медиации (примирения) в образовательных организациях и в организациях для детей-сирот и детей, оставшихся без попечения родителей.

Минпросвещения России направляет данные методические рекомендации для использования в работе.

Одновременно информируем, что в соответствии с поручением, а также с учетом дальнейшего развития сети служб медиации (примирения), указанные методические рекомендации будут актуализированы в 2022 году.

Д.Е.Грибов

Приложение

Методические рекомендации по развитию сети служб медиации (примирения) в образовательных организациях и в организациях для детей-сирот и детей, оставшихся без попечения родителей

1. Общие положения

Методические рекомендации по развитию сети служб медиации (примирения) в образовательных организациях и в организациях для детей-сирот и детей, оставшихся без попечения родителей, рекомендуется использовать для формирования медиативных и восстановительных практик в дошкольных, общеобразовательных и профессиональных образовательных организациях, а также организациях для детей-сирот и детей, оставшихся без попечения родителей.

Данные методические рекомендации разработаны для использования в деятельности органов системы профилактики безнадзорности и правонарушений несовершеннолетних, а также организациями, заинтересованными во внедрении медиативной и восстановительной практик в работу с несовершеннолетними и их семьями.

В настоящих методических рекомендациях используется терминология, содержащаяся в Концепции развития сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная ответственность в Российской Федерации, до 2020 года, утвержденной распоряжением Правительства Российской Федерации от 30 июля 2014 г. N 1430-р:

_____

Распоряжение Правительства Российской Федерации от 30 июля 2014 г. N 1430-р "Об утверждении Концепции развития до 2020 года сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная ответственность" (Собрание законодательства Российской Федерации, 2014, N 32, ст.4557; 2018, N 37, ст.5780).

восстановительное правосудие - новый подход к отправлению правосудия, направленный прежде всего не на наказание виновного путем изоляции его от общества, а на восстановление материального, эмоционально-психологического (морального) и иного ущерба, нанесенного жертве, сообществу и обществу, на осознание и заглаживание вины, восстановление отношений, содействие реабилитации и ресоциализации правонарушителя;

восстановительный подход - использование в практической деятельности, в частности в профилактической и коррекционной работе с детьми и подростками, в том числе при разрешении споров и конфликтов и после совершения правонарушений, умений и навыков, направленных на всестороннее восстановление отношений, доверия, материального и морального ущерба;

медиация - способ разрешения споров мирным путем на основе выработки сторонами спора взаимоприемлемого решения при содействии нейтрального и независимого лица - медиатора;

медиативный подход - подход, основанный на принципах медиации, предполагающий владение навыками позитивного осознанного общения, создающими основу для предотвращения и (или) эффективного разрешения споров и конфликтов в повседневных условиях без проведения медиации как полноценной процедуры.

Медиативные и восстановительные практики в образовании способствуют формированию культуры диалога, способности людей понимать друг друга и договариваться при решении сложных ситуаций. Часто встречающиеся такие реакции в конфликте как: коммуникативное давление (оскорбление, угрозы, манипуляция, обесценивание и иные), отвержение (травля, изгнание из класса, отчисление из образовательной организации) и наказание или угроза наказанием - деструктивно влияют на атмосферу в образовательной организации и

социализацию детей и подростков.

Для решения указанных проблемных ситуаций рекомендуется использовать медиативные и восстановительные практики, которые не являются психологическими, педагогическими, юридическими или правозащитными.

Медиативные и восстановительные практики могут использоваться для профилактики и снижения рисков возникновения конфликтных ситуаций и противоправных действий в образовательной среде. В медиативных и восстановительных практиках могут участвовать все участники образовательных отношений.

В настоящих методических рекомендациях предлагаются две модели реализации процедур для урегулирования конфликтных и проблемных ситуаций: медиативная и восстановительная, которые направлены на мирное урегулирование сложных ситуаций, ответственное принятие решений по урегулированию ситуаций, сотрудничество, взаимопонимание. Процедуры реализации медиативной и восстановительной моделей предполагают участие независимого третьего лица, задача которого состоит в организации конструктивного диалога.

Указанным моделям в настоящих методических рекомендациях соответствуют два типа служб, которые могут быть созданы в образовательных организациях:

1) медиативной модели - службы школьной медиации;

2) восстановительной модели - школьные службы примирения;

3) ситуации, в которых рекомендуется использовать медиативные и восстановительные практики;

4) конфликтная ситуация, возникшая между участниками образовательных отношений;

5) совместная деятельность участников образовательных отношений, требующая согласования действий и решений;

6) сложная/проблемная коммуникация в классе/группе;

7) ситуации с причинением вреда, квалифицируемые как общественно опасные деяния несовершеннолетних;

8) конфликты между родителями и детьми, влияющие на образовательный процесс.

2. Функционирование и развитие служб медиации в образовательных организациях

В целях реализации медиативного подхода рекомендуется создавать **Службы школьной медиации** (далее - СШМ), объединяющие различных участников образовательных отношений (сотрудников

образовательной организации или организаций для детей-сирот и детей, оставшихся без попечения родителей, обучающихся, их родителей (законных представителей) и иных), направленные на оказание содействия в предотвращении и разрешении конфликтных ситуаций, в профилактической работе и мероприятиях, направленных на работу с последствиями конфликтов, асоциальных проявлений, правонарушений.

СШМ рекомендуется создавать приказом образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей. В целях организации работы СШМ утверждается:

1) положение о СШМ, которое согласовывается с советом образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей (совет обучающихся, совет родителей - если таковые имеются);

2) план работы СШМ;

3) журнал учета обращений в СШМ.

Для функционирования СШМ рекомендуется включить в работу координатора СШМ, одного или нескольких специалистов СШМ, а также обучающихся из "групп равных". "Группы равных" - это группа обучающихся, которая объединена для обучения медиативному подходу с целью приобретения навыков поведения в ситуациях стресса и конфликта, предупреждения конфликтов среди сверстников. Участие в "группе равных" - это способ, позволяющий приобретать опыт участия в принятии решений, проявления активной жизненной позиции, уважительного и чуткого отношения к потребностям окружающих. Организация такого обучения возможна в рамках внеурочной деятельности, на классных часах или любыми другими удобными способами, предусмотренными или отвечающими целям и содержанию основной обучающей программы образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей, либо отдельным ее пунктам и программам (например: "Программа воспитания и социализации обучающихся").

Специалистом СШМ может стать сотрудник образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей и родитель (законный представитель) обучающегося. Для них рекомендуется повышение квалификации по программе "Школьный медиатор" 72 академических часа. Рекомендуются следующие базовые темы программы:

_____
http://fedim.ru/wp-content/uploads/2020/02/Tipovaya-Programma-podgotovki-shkolnogo-mediatora-72-ch.pdf.

- понятие конфликта;

- способы разрешения конфликтов и споров;

- стратегии поведения в конфликте;

- восприятие и коммуникация;

- принципы и понятийный аппарат медиативного подхода;

- ценности и понятийный аппарат восстановительного подхода;

- техники и инструменты, используемые в работе СШМ (техники и инструменты, используемые в медиации, медиативная беседа, восстановительная беседа, круги сообществ, семейная конференция).

Специалист СШМ образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей, помогает в разрешении возникающих споров, разногласий, конфликтов при помощи техник и инструментов, используемых в работе СШМ. Одновременно специалист СШМ проводит обучение в "группах равных" и занимается информационно-просветительской деятельностью со всеми участниками образовательных отношений (в рамках внеурочной деятельности, на классных часах, родительских собраниях, коллегиальных совещаниях).

Координатором СШМ может стать сотрудник образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей, который прошел обучение и является специалистом СШМ. Рекомендуется проводить ежегодную ротацию роли координатора СШМ между специалистами СШМ. Координатор СШМ осуществляет координацию действий по плану работы СШМ в образовательной организации и организации для детей-сирот и детей, оставшихся без попечения родителей.

Цели СШМ:

1) принятие участниками образовательных отношений позиции активного участия и соизмеримости с собственными возможностями вклада по отношению к развитию благоприятной среды для духовно-нравственного развития, воспитания и социализации обучающихся;

2) создание условий для участников образовательных отношений, при которых становится возможным самостоятельно восстановить нарушенные отношения, доверие, загладить причиненный ущерб (психологический (моральный), материальный);

3) развитие участниками образовательных отношений знаний, умений и навыков конструктивного поведения в конфликте, которые базируются на таких общечеловеческих ценностях как признание уникальности личности, взаимное принятие, уважение права каждого на удовлетворение собственных потребностей и защиту своих интересов не в ущерб чужим.

Задачи СШМ:

1) формирование группы, состоящей из участников образовательных отношений, готовых использовать техники и инструменты, применяемые в работе СШМ при разрешении конфликтных ситуаций, возникающих между участниками образовательных отношений;

2) информационно-просветительская деятельность с участниками образовательных отношений;

3) снижение деструктивного влияния возникающих конфликтов между участниками образовательных отношений;

4) содействие профилактике агрессивных, насильственных и асоциальных проявлений среди обучающихся, профилактика преступности среди несовершеннолетних;

5) координация усилий родителей (законных представителей, близких родственников и иных лиц) и образовательной организации, организации для детей-сирот и детей, оставшихся без попечения родителей, с целью предотвращения неблагополучных сценариев развития жизни обучающегося;

6) повышение уровня социальной и конфликтной компетентности всех участников образовательных отношений;

7) интеграция медиативных принципов в систему образовательных отношений.

Деятельность СШМ осуществляется с учетом:

- *добровольного* согласия сторон, вовлеченных в конфликт, на участие в его разрешении при содействии специалиста(-ов) СШМ и/или обучающегося(-ихся) из "группы равных". Допускается направление сторон(-ы) конфликта и их законных(-ого) представителей(-я) на предварительную встречу со специалистом СШМ, после которой стороны(-а) могут принять самостоятельное решение о дальнейшем участии или неучастии в последующих встречах. Участники(-к) конфликта могут прекратить свое участие, если посчитают(-ет), что продолжение участия в этих встречах нецелесообразно;

- *конфиденциальности* сведений, полученных на встречах со специалистом(-ми) СШМ и/или обучающимся(-имися) из "группы равных". Договоренности и решения, достигнутые сторонами конфликта на этих встречах, могут быть раскрыты третьим лицам только по согласованию со сторонами конфликта;

- *нейтрального* отношения СШМ ко всем участникам конфликта (в том числе руководящего состава организации). В случае понимания специалистом(-ми) и/или обучающимся(-имися) невозможности сохранения нейтральности из-за личностных взаимоотношений с кем-либо из участников, он(-и) должен(-ы) отказаться от продолжения встречи или передать ее другому специалисту(-ам) СШМ и/или обучающемуся(-имся) из "группы равных";

- *равноправного* участия сторон конфликта в его разрешении, предоставление равных возможностей высказываться и быть выслушанным, предлагать темы для обсуждения и вносить предложения по решению конфликта. Участники в равной степени ответственны за исполнение принятых ими совместно на взаимоприемлемых условиях решений по конфликту;

- *взаимного* уважения и сотрудничества, которые предполагают уважительный стиль общения, недопустимость взаимных оценок и оскорблений на встречах всех участников встречи, включая специалиста(-ов) СШМ и/или обучающегося(-ихся) из "группы равных";

- *ответственного* отношения к принятию решения по урегулированию конфликта, пониманию последствий принятого решения и его исполнению.

(Рекомендуемые техники и инструменты, используемые в работе СШМ, приведены в приложении к методическим рекомендациям по развитию сети служб медиации/примирения в образовательных организациях, организациях для детей-сирот и детей, оставшихся без попечения родителей (стр.19).

_____

Приложение к методическим рекомендациям в таблице "Рекомендуемые техники и инструменты, используемые в работе СШМ".

Особенности организации СШМ

СШМ может формироваться в соответствии с теми потребностями и возможностями, какие присутствуют в той или иной образовательной организации, организации для детей-сирот и детей, оставшихся без попечения родителей. СШМ не является ни юридическим лицом, ни структурным подразделением образовательной организации (если не созреют предпосылки для иного).

При функционировании СШМ рекомендуется учитывать следующие особенности участия обучающихся:

- мнение родителей (законных представителей) об участии своих детей в "группе равных", в индивидуальных и совместных встречах со специалистом(-ми) СШМ;

- возможные трудности обучающегося в проявлении открытости в своих высказываниях в присутствии взрослых (в том числе родителей (законных представителей)), как по объективным, так и по субъективным причинам, что будет влиять на результативность самой встречи как для самого обучающегося, так и в целом на разрешение ситуации;

- быстрота возникновения конфликтных ситуаций между участниками образовательных отношений и необходимость оперативно оказать содействие в их разрешении.

Специалисту СШМ рекомендуется проявлять внимание к потребностям обучающегося, его отношению к участию родителей (законных представителей) при индивидуальных и совместных встречах с участием специалиста(-ов) СШМ и/или обучающегося(-ихся) из "группы равных", а также готовность к различным реакциям как со стороны родителей (законных представителей) так и со стороны самих обучающихся.

Для эффективного функционирования СШМ рекомендуется осознанное понимание представителями администрации образовательной организации, организации для детей-сирот и детей, оставшихся без попечения родителей, контролирующих организаций, органов системы профилактики безнадзорности и правонарушений несовершеннолетних (комиссии по делам несовершеннолетних и защите их прав, органы опеки и попечительства, подразделения по делам несовершеннолетних органов внутренних дел и другие) важности независимой позиции СШМ.

С целью оказания поддержки СШМ в ее функционировании или ее развитии рекомендуется осуществлять взаимодействие между службами медиации из других образовательных организаций и/или организаций для детей-сирот и детей, оставшихся без попечения родителей, а также с региональными службами медиации (если таковые созданы).

3. Функционирование и развитие служб примирения в образовательных организациях

В целях реализации восстановительного подхода рекомендуется создавать **Школьные службы примирения** (далее - ШСП) - это оформленное объединение ведущих восстановительных программ (взрослых и школьников-волонтеров), которое проводит восстановительные программы в образовательной организации, а также осуществляет иную деятельность в рамках восстановительного подхода в целях профилактики эскалации конфликтов, сложных ситуаций, деструктивного поведения и правонарушений несовершеннолетних в образовательной организации. ШСП помогают участникам образовательных отношений в конфликтной/проблемной ситуации укрепить сотрудничество и ответственную позицию, вместе найти решение и согласованно его реализовать.

ШСП рекомендуется создавать приказом образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей.

В целях организации работы ШСП утверждается положение о ШСП, которое важно согласовать с советом образовательной организации или организации для детей-сирот и детей, оставшихся без попечения родителей (совет обучающихся, совет родителей - если таковые имеются).

В ШСП могут входить:

1) один или несколько обученных взрослых - ведущих восстановительных программ, один из которых назначается куратором (руководителем) ШСП;

2) как правило, команда школьников-волонтеров ШСП, проводящих восстановительные программы между сверстниками.

В деятельности службы могут принимать участие представители родительского сообщества.

Школьников-волонтеров ШСП обучают на тренингах. Для создания ШСП предлагается:

1) выбрать одного или нескольких человек, заинтересованных в работе ШСП;

2) провести их обучение у практикующих ведущих восстановительных программ в сфере образовательных отношений;

3) разработать механизмы передачи информации о конфликтах и правонарушениях в службу примирения;

4) разработать формы учета результатов проведения восстановительной программы (журнал поступления заявок и форму фиксации результата восстановительной программы).

При проведении восстановительной программы по случаю совершенного несовершеннолетним общественно опасного деяния, ведущему восстановительных программ важно понимать юридические последствия проведенной программы и информировать участников о способах учета результатов данной работы в комиссии по делам несовершеннолетних и защите их прав, правоохранительных органах или суде.

Куратору (руководителю) ШСП и ведущим восстановительных программ рекомендуется:

1) повышение квалификации по программе "Школьные службы примирения" 72 академических часа у специалистов по восстановительному правосудию, имеющих собственную практику проведения восстановительных программ в образовательных организациях;

_____

www.8-926-145-87-01.ru/wp-content/uploads/2020/02/Программа-школьные-службы-примирения-на-72-часа.doc.

2) участвовать в семинарах, курсах повышения квалификации, конференциях по восстановительным практикам.

Цели ШСП:

1) содействие возмещению ущерба при совершении общественно опасных деяний несовершеннолетними;

2) разрешение конфликтных ситуаций;

3) профилактика правонарушений и безнадзорности несовершеннолетних;

4) нормализация взаимоотношений участников образовательных отношений на основе восстановительного подхода.

ШСП опираются на восстановительный подход, включающий теоретическую основу и набор способов реагирования на конфликты и общественно опасные деяния. В рамках восстановительного подхода могут разрешаться и сложные коммуникативные ситуации, направленные на восстановление способности людей самим сообща и ответственно разрешать свои ситуации без наказания, отвержения, коммуникативного давления, преимущественно силами сообщества, близких и уважаемых людей. Базовой единицей реализации восстановительного подхода является личная встреча всех заинтересованных сторон для конструктивного решения проблемной ситуации.

Задачи ШСП:

1) организация деятельности на основе принципов проведения восстановительных программ;

2) снижение административных и ориентированных на наказание реакций на конфликты, нарушения дисциплины и правонарушения несовершеннолетних;

3) обеспечение доступности деятельности ШСП для всех участников образовательных отношений и приоритетное использование восстановительного способа разрешения конфликтов и криминальных ситуаций;

4) содействие формированию ценностей примирения у педагогов, представителей администрации образовательной организации, обучающихся, законных представителей и ближайшего социального окружения несовершеннолетнего;

5) поддержка деятельности существующих в образовательной организации форм управления и воспитания (родительские собрания, педагогические советы, методические объединения, классные часы и иные) на основе ценностей примирения.

Восстановительный подход реализуется в *восстановительных программах* (восстановительная медиация, семейная конференция, круг сообщества). Ведущий *восстановительных программ* - специалист и/или школьник-волонтер, обученный проведению восстановительных программ. Позиция ведущего восстановительных программ является нейтральной по отношению к участникам ситуации. Он в равной степени поддерживает усилия сторон, направленные на урегулирование конфликтной ситуации и/или восстановительное реагирование на общественно опасное деяние несовершеннолетнего. Ведущий восстановительных программ в коммуникации занимает понимающую (а не экспертную) позицию, не консультирует, не советует, и не оценивает. Он готовит стороны конфликта к совместной встрече и создает наилучшие условия для реализации в ней ценностей примирения. В результате, стороны начинают понимать друг друга, находят приемлемое для всех участников решение и принимают ответственность за его реализацию без внешнего принуждения.

Ценности примирения:

1) принятие самими участниками конфликтной ситуации на себя ответственности по ее урегулированию, исключающей насилие и дальнейшее причинение вреда;

2) восстановление у участников конфликта способности понимать последствия ситуации для себя, своих родных, второй стороны;

3) прекращение взаимной вражды и нормализация отношений;

4) ответственность обидчика перед жертвой (если в ситуации был правонарушитель) состоит в заглаживании причиненного вреда (или принесенной обиды) насколько возможно силами самого нарушителя;

5) выход из состояния жертвы тех, кому были причинены вред, обида или несправедливость (если такие были в ситуации) за счет заглаживания обидчиком причиненного жертве вреда, и ответы на волнующие жертву вопросы со стороны обидчика и его близких;

6) планирование сторонами конфликта их конкретных действий - кто и что именно будет делать, что позволит избежать повторения подобных ситуаций в дальнейшем и не допустить клеймения и отвержения кого-либо из участников;

7) помощь близких и уважаемых сторонами конфликта людей в актуализации нравственных ориентиров и ценностей, поддержка ими позитивных изменений и выполнение заключенного примирительного договора (плана).

Деятельность ШСП осуществляется с учетом:

нейтрального отношения ведущего и самостоятельного нахождения решения самими участниками ситуации. Ведущий не может побуждать стороны к принятию того или иного решения по существу конфликта. Ведущий не является защитником, советчиком или обвинителем для какой-либо из сторон, не выносит решения и в равной степени поддерживает действия участников, направленные на урегулирование ситуации в рамках восстановительного подхода и ценностей примирения;

добровольного участия в восстановительной программе. Допускается направление участников ситуации на предварительную встречу, но итоговое решение об участии в общей встрече люди принимают добровольно;

конфиденциальности восстановительной программы - за ее пределы выносится только то, на что стороны дали свое согласие (договор, соглашение, план действий по решению конфликта и иные договоренности);

информированности сторон ведущим восстановительной программы о сути программы, ее процессе и возможных последствиях;

ответственного отношения сторон за результат, а ведущего - за организацию процесса и за безопасность участников на встрече;

заглаживание вреда - при совершении общественно опасных деяний ответственность состоит, в том числе, в заглаживании причиненного вреда.

Основные восстановительные программы

В качестве восстановительной программы рекомендуется использовать восстановительную медиацию, в которой помимо ведущих обычно участвуют от 2 до 6 человек. Для работы с группами (класс, родительское собрание) больше подходят технологии Семейный совет и Круги сообществ. Ниже представлены основные программы и типичные ситуации, в которых они применяются.

_____

http://sprc.ru/wp-content/uploads/2018/11/Sbornik-2018-web.pdf; http://sprc.ru/wp-content/uploads/2012/11/Круги-сообществ.pdf

С ситуациями, отмеченными в таблице звездочками (*), рекомендуется работать специалистам ШСП в сотрудничестве с территориальными службами примирения.

Ситуация	Восстановительная программа

Конфликт между обучающимися, в том числе с участием их родителей (законных представителей). Пример: обучающиеся и их родители (законные представители) изначально не хотят мириться, настроены жаловаться, враждовать и так далее.	Восстановительная медиация.
Конфликт между родителем обучающегося и педагогом.*	Восстановительная медиация.
Многосторонний конфликт с участием большинства учеников класса. Конфликт среди группы родителей обучающихся класса. Класс "поделился" на враждующие группировки или большая часть класса объединилась против одного (травля).*	Круг сообщества.
Отсутствие партнерства школы и родителей. Развитие класса как команды. Профилактика возможных конфликтов. Формирование нового класса, слияние классов и т.д.*	Профилактические восстановительные программы.
Конфликт между педагогами.*	Восстановительная медиация.
Конфликт на стадии эскалации с большим числом участников. В конфликт включились группы родителей обучающихся, представители администрации образовательной организации, средств массовой информации, иногда уполномоченный по правам ребенка в субъекте Российской Федерации, правоохранительные органы.*	Школьно-родительский совет
Конфликт в семье.*	Восстановительная медиация.
Отсутствие взаимопонимания между родителями и ребенком, ребенок совершает правонарушения, систематически пропускает по неуважительным причинам занятия в образовательной организации, находится в социально опасном положении и т.д.*	Семейный совет (семейная конференция).
Совершение несовершеннолетним общественно опасного деяния, в том числе с возбуждением уголовного дела либо при отказе в его возбуждении, с последующим рассмотрением ситуации на заседании комиссии по делам несовершеннолетних и защите их прав. Несовершеннолетний, находящийся в трудной жизненной ситуации, в конфликте с законом.*	Восстановительная медиация. Семейный совет (семейная конференция).
Напряженные отношения в "педагогической команде" (объединение разных педагогических коллективов в единый образовательный комплекс, назначение нового директора образовательной организации и т.п.).*	Круг сообщества.

Кроме того, может применяться комплекс восстановительных программ. Восстановительный подход помогает в управлении дисциплиной в классе, при потере управления классом с помощью проведения Круга сообщества.

ШСМ также может: организовывать мероприятия по снижению конфликтности учеников, повышать квалификацию педагогов и специалистов в рамках

восстановительного подхода, создавать пространство для конструктивного партнерства родителей обучающихся и педагогов (классных руководителей), поддерживать атмосферу сотрудничества в образовательной организации, укреплять связи в сообществе.

Примерные этапы примирительной программы:

1) получение информации о происшествии или запроса;

2) проведение индивидуальной/предварительной встречи (или серии встреч) с каждой из сторон;

3) проведение общей совместной встречи всех заинтересованных участников для обсуждения ситуации, поиска выходов и разработки согласованного решения, соглашений или плана;

4) обратная связь от участников по выполнению принятых ими решений.

Взаимодействие служб примирения образовательных организаций и территориальных служб примирения может способствовать профилактике безнадзорности и правонарушений несовершеннолетних на территории субъектов Российской Федерации. Оценка качества проведения восстановительных программ на соответствие деятельности ведущего концепции и ценностям восстановительного подхода осуществляется внутри профессионального сообщества.

4. Функционирование и развитие сети служб медиации/примирения

Службы медиации и службы примирения, как и их участники, могут образовывать сообщества, ассоциации, объединения, которые будут входить в сеть служб медиации/примирения (далее - Сеть). Цель функционирования и развития Сети, заключается в обеспечении взаимодействия между службами медиации/примирения (далее - Сетевое взаимодействие). Сетевое взаимодействие направлено на обеспечение содержательной и организационной поддержки развитию служб.

В целях Сетевого взаимодействия представляется целесообразным:

включить работу школьных служб медиации/примирения в региональные грантовые программы (при их наличии);

обеспечить обучение специалистов по программам повышения квалификации в сфере восстановительного подхода и медиации в системе образования с

обязательным привлечением к проведению обучения специалистов, имеющих восстановительную и/или медиативную практику в сфере образования;

поддержать обучение основам восстановительного подхода и медиации заинтересованных обучающихся;

включить темы школьных служб медиации/примирения в конкурсы профессионального мастерства педагогических работников;

осуществлять мониторинг основных показателей проведения восстановительных программ и медиации;

поддерживать профессиональное сообщество специалистов медиативных и восстановительных практик в сфере образования, проводить регулярные региональные конференции, семинары и другие мероприятия;

рассмотреть возможность включения работы по проведению восстановительных программ и медиации в существующие в субъекте Российской Федерации формы отчетности работы специалистов образовательной сферы.

Приложение

Таблица

"Рекомендуемые техники и инструменты, используемые в работе СШМ"

Индивидуальные, раздельные встречи (консультации, подготовка к совместным встречам) с участниками образовательных отношений	Совместные встречи с участниками образовательных отношений			Обучение в "группах равных"
	Отдельные участники образовательных отношений (например: между обучающимся и обучающимся, педагогом и обучающимся, родителем обучающегося (законным представителем) и классным	Семьи, близких родственников, заинтересованных лиц из социального окружения обучающегося	Групп участников образовательных отношений (группы: родителей, одноклассников, коллег и иных)	

	руководителем, заместителем руководителя по воспитательной работе и специалистом образовательной организации и иными)			
1	2			3
техника активного слушания (петля понимания, резюмирование, обобщение, рефрейминг); техника работы с интересами; техника работы с чувствами; техника задавания вопросов; медиативная беседа; восстановительная беседа	техника активного слушания; техника задавания вопросов; техника работы с интересами; техника работы с чувствами; медиативная беседа; восстановительная беседа	техника активного слушания; техника задавания вопросов; техника работы с интересами; техника работы с чувствами; семейная конференция	техника активного слушания; техника задавания вопросов; техника работы с интересами; техника работы с чувствами; круги сообществ	техника активного слушания; техника задавания вопросов; техника работы с интересами; техника работы с чувствами круги сообществ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО

от 26 декабря 2017 года N 07-7657

О направлении методических рекомендаций

Департамент государственной политики в сфере защиты прав детей Минобрнауки России направляет для использования в работе методические

рекомендации по внедрению восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций, разработанные во исполнение пункта 31 плана мероприятий по реализации в 2016-2020 годах Стратегии развития воспитания в Российской Федерации на период до 2015* года, утвержденной распоряжением Правительства Российской Федерации от 29 мая 2015 г. N 996-р.

_____

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

Заместитель
директора Департамента -
начальник отдела
Л.П.Фальковская

Методические рекомендации по внедрению восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций

1. Введение

Настоящие методические рекомендации по внедрению восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций (далее - Методические рекомендации) разработаны во исполнение пункта 31 плана мероприятий по реализации в 2016-2020 годах Стратегии развития воспитания в Российской Федерации на период до 2015* года, утвержденной распоряжением Правительства Российской Федерации от 29 мая 2015 г. N 996-р Центром медиации и общественного взаимодействия федерального государственного бюджетного образовательного учреждения высшего образования "Российский государственный социальный университет" и Всероссийской ассоциацией восстановительной медиации.

_____

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

Методические рекомендации включают научно-практический опыт Межрегиональной общественной организации "Общественный центр "Судебно-правовая реформа" и Всероссийской ассоциации восстановительной медиации по разработке и внедрению программ восстановительного правосудия. Данный опыт может быть использован образовательными организациями в воспитательной деятельности.

2. Актуальность внедрения восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций

В процессе взросления и последующей жизни современный человек осваивает множество различных ролей и вступает в отношения с многообразным социальным окружением: членами семьи, коллегами, соседями, малознакомыми людьми. Для того, чтобы выстраивать такие сложные отношения без реакции, разрушающей человеческие связи, необходимо обладать определенными умениями, прививаемыми с детства. Важнейшей задачей воспитательной деятельности образовательных организаций в современных условиях является формирование у обучающихся навыков конструктивного разрешения возникающих конфликтов, основанных на гуманистических ценностях

человеческой жизни и семьи, уважении личности и интересов другого человека, взаимопонимании и сотрудничества для достижения общих результатов.

К сожалению, в современных условиях дети, зачастую, не в полной мере получают от взрослых (родителей и педагогов) поддержку, обеспечивающую конструктивный выход из конфликтных и, даже, подчас криминальных ситуаций. Порой, в условиях, когда ребенок срывает уроки, совершает рукоприкладство, и его поведение становится достоянием полиции, образовательная организация старается перевода несовершеннолетнего на домашнее обучение, в другую школу или специальное учебно-воспитательное учреждение.

Данная проблемная ситуация в воспитательной деятельности усугубляется социальным расслоением обучающихся. Дети, чьи родители не столь благополучны в материальном и социальном плане, отягощенные сложной семейной ситуацией, не всегда могут завоевать авторитет у сверстников и учителей только за счет успешного овладения учебными предметами. Одни из них приобретают статус "отверженных", другие - становятся школьными "авторитетами", которые испытывают тяготение к криминальной субкультуре и, зачастую, занимаются вымогательством, применяют силовые способы поднятия своего статуса среди ровесников. В то же время успевающие дети невольно попадают под влияние соответствующей подростковой субкультуры, поскольку и их возможности самоутвердиться в школе, особенно в подростковом возрасте, часто ограничены.

Детский рэкет, драки (на жаргоне подростков - "стрелки") и участие в них значительной части обучающихся демонстрирует недостатки современной системы воспитания. В свою очередь, подобные явления способствуют формированию подростковых группировок с криминально ориентированными образцами поведения. Такие формы организации молодежи, как правило, основаны на ценностях силового взаимодействия и состоят из молодых людей, в силу различных причин, фактически вытолкнутых из социальной среды образовательных организаций и семьи. Пространство современной подростковой жизни наполнено двумя активностями: с одной стороны, учебной активностью школьников, занятием в кружках и секциях, с другой - силовой активностью, направленной на завоевание статуса и авторитета различными, но, прежде всего, силовыми методами.

В таких условиях происходит нерегулируемое расслоение детей и примитивизация их взаимоотношений, нередко выражается в том, что сплетни, манипуляции, насилие и угрозы насилием, выяснение "кто сильнее", "с кем и против кого дружить", "клеймение" изгоев, травля (преследование, издевательство, систематическое вербальное и физическое унижение одноклассников со стороны сильных и агрессивных детей и растянутое во времени психологическое подавление, ущемление достоинства, особенно слабых) определяют направление социализации части обучающихся.

Не имея поддержки со стороны взрослых, не осваивая навыки конструктивного выхода из конфликтных ситуаций, не участвуя в анализе и нормировании отношений с другими детьми и воспитателями, многие подростки начинают все богатство отношений и различные способы их регулирования подменять одним силовым взаимодействием. Более того, замыкаясь в собственной среде и оказываясь выключенными из пространства культурных регуляторов поведения и отношений, они несут свои разрушительные навыки дальше в социум.

В условиях нарушенных взаимоотношений детей от родителей все больше и больше свободного времени несовершеннолетних занимает коммуникация в чатах, социальных сетях. Однако, и интернет является пространством, где в

отношениях подростков нередко демонстрируется силовое взаимодействие. Такие отношения и действия, зачастую, коррелируют с нормами, принятыми в криминальной субкультуре.

Также опасность кроется в размытости воспитательных стратегий образовательной организации, что в таком случае фактически сводит воспитание к определенному набору мероприятий, формально маркируемых как воспитательные.

Учитывая тот факт, что именно подростковое сообщество играет важную роль в социализации школьников, в освоении "взрослых" форм отношений между ними, значимым является умение педагогов выстраивать контакт с обучающимися. Любовь, дружба, выработка отношения к людям и событиям, а также постановка общих целей, задач, выбор и согласование способов их достижения - все эти аспекты жизни составляют основу человеческого существования. Подростковое общество в процессе непрерывной коммуникации детей друг с другом позволяет им примерить эти отношения на себя, зачастую, путем преодоления искусственно создаваемых самими подростками экстремальных ситуаций. Таким образом, подростковое сообщество становится формой коллективности, в которой посредством такого "примеривания" вырабатывается коллективное, а также индивидуальное отношение подростков к миру и людям.

Для того чтобы подростки осваивали действительно конструктивные формы общения и деятельности, необходимо управление процессами, происходящими в детских и подростковых сообществах со стороны взрослых (родителей), прежде всего, через трансляцию, в том числе в семье, коммуникативно-ориентированных (понимающих и одновременно развивающих) способов разрешения конфликтов и, соответственно, способностей понимать другого, рефлексии собственных действий и осмысления собственной позиции в различных ситуациях. Безусловно, процессу восстановления цивилизованных межличностных коммуникаций благоприятствуют восстановительные технологии, в ходе которых разнообразные отношения и поступки детей, их родителей и учителей при поддержке специалистов становятся предметом конструктивного обсуждения со стороны самих подростков.

В связи с вышесказанным большое значение приобретает восстановление включенности родителей и социального окружения ребенка, в том числе совершившего правонарушения, в процесс "воспитательного взаимодействия".

В последние годы в воспитательной деятельности образовательных организаций все большую значимость приобретает работа с детско-родительскими сообществами, формирующимися вокруг школьных классов. Способом оперативного контакта в данных социальных группах выступают популярные мессенджеры Viber или WhatsApp. Благодаря возможности быстрых коммуникаций любая конфликтная ситуация в классе (с кем бы из участников образовательного процесса она ни возникла) уже вечером того же дня становится достоянием широкой общественности и темой для обсуждения родителей всех обучающихся, и, нередко, становится причиной последующего уже группового конфликта.

Зачастую установки родителей, высказываемые ими резкие суждения по отношению к тем или иным жизненным ситуациям, социальным группам и меньшинствам, предопределяют последующие поступки детей. Подобная ситуация актуальна для инклюзивных классов, где проблематика принятия детей с особыми образовательными потребностями часто касается не только учащихся, но и их родителей. Кроме того, в детских и подростковых коллективах образовательных организаций нередки случаи ксенофобии, что является вопиющим фактом для такого многонационального многоконфессионального

государства как Россия. В подобные конфликты, начавшиеся в классе, часто включаются и родственники конфликтующих сторон - представители той или иной диаспоры, чьи национальные или религиозные чувства были задеты. В сложившейся ситуации взаимодействие с такими сообществами как пример конструктивного разрешения конфликтных ситуаций, основанного на их публичном обсуждении, становится важным компонентом воспитательной деятельности образовательных организаций и требует особых навыков.

В связи с вышесказанным одной из приоритетных стратегических задач образовательных организаций становится применение подходов к воспитанию, базирующихся на гуманистических и традиционных способах управления конфликтами, направленных на преодоление криминализации подрастающего поколения, профилактику правонарушений несовершеннолетних, включение семейного и более широкого социального окружения ребенка к решению его возможных проблем, формирование в подростковых сообществах лидеров, несущих позитивные ценности; а также активном применении форм групповой работы с родительскими и детскими сообществами; профилактику и разрешение этноконфессиональных и межкультурных конфликтов в детской и подростковой среде.

Одним из ключевых инструментов реализации данной воспитательной стратегии является внедрение восстановительных технологий и принципов медиации в образовательное пространство, предусмотренное Стратегией развития воспитания в Российской Федерации на период до 2025 года, утвержденной распоряжением Правительства Российской Федерации от 29 мая 2015 г. N 996-р, которое может быть выражено в широком информировании педагогического состава образовательных организаций Российской Федерации о возможностях восстановительных технологий и медиации в воспитательном процессе; внедрении восстановительных технологий и медиации в воспитательную деятельность образовательных организаций путем формирования соответствующих компетенций у педагогического состава; использовании ресурса школьных служб примирения/служб школьной медиации для реализации восстановительных технологий (в том числе медиации).

3. Нормативные основы, цель и задачи внедрения восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций

Методические рекомендации разработаны во исполнение пункта 31 плана мероприятий по реализации в 2016-2020 годах Стратегии развития воспитания в Российской Федерации на период до 2025 года, утвержденного распоряжением Правительства Российской Федерации от 12 марта 2016 г. N 423-р, а также, с учетом опыта деятельности по реализации Указа Президента Российской Федерации N 761 от 1 июня 2012 г. О Национальной стратегии действий в интересах детей на 2012-2017 годы. В данном Указе предусматривается создание и развитие сети служб медиации/примирения в целях реализации восстановительного правосудия, организация школьных служб медиации/ примирения, нацеленных на разрешение конфликтов в образовательных организациях, профилактику правонарушений детей и подростков, улучшение отношений в образовательной организации.

Методические рекомендации опираются на ряд нормативный и правовых актов, определяющих ключевые задачи в системе образования.

Стратегию развития воспитания в Российской Федерации на период до 2025 года, утвержденную распоряжением Правительства Российской Федерации от 29 мая 2015 г. N 996-р. Одним из ее механизмов является "развитие инструментов

медиации для разрешения потенциальных конфликтов в детской среде в рамках образовательного процесса, а также при осуществлении деятельности других организаций, работающих с детьми".

Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2020 года", утвержденная распоряжением Правительства Российской Федерации от 22 марта 2017 г. N 520-р, в качестве своих ключевых задач, предусматривает в том числе:

снижение количества правонарушений, совершенных несовершеннолетними, в том числе повторных;

укрепление института семьи;

защиту прав несовершеннолетних, создание условий для формирования достойной жизненной перспективы;

совершенствование имеющихся и внедрение новых технологий и методов профилактической работы с несовершеннолетними, в том числе расширение практики применения технологий восстановительного подхода с учетом эффективной практики субъектов Российской Федерации;

а также, в рамках развития единой образовательной (воспитывающей) среды предполагает "обеспечение организационно-методической поддержки развития служб медиации в образовательных организациях", и "совершенствование системы взаимодействия с родителями по вопросам профилактики асоциального поведения обучающихся".

Федеральный государственный образовательный стандарт основного общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. N 1897, в том числе, направлен на формирование российской гражданской идентичности обучающихся; духовно-нравственное развитие, воспитание обучающихся и сохранение их здоровья, определяющий, что личностные результаты освоения основной образовательной программы должны отражать, в том числе:

формирование осознанного, уважительного и доброжелательного отношения к другому человеку, его мнению, мировоззрению, культуре, языку, вере, гражданской позиции, к истории, культуре, религии, традициям, языкам, ценностям народов России и народов мира; готовности и способности вести диалог с другими людьми и достигать в нем взаимопонимания;

освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;

развитие морального сознания и компетентности в решении моральных проблем на основе личностного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;

формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

нахождение общего решения и разрешения конфликтов на основе согласования позиций и учета интересов.

Метапредметные результаты освоения основной образовательной программы должны отражать, в том числе:

умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; работать индивидуально и в группе: находить общее

решение и разрешать конфликты на основе согласования позиций и учета интересов; формулировать, аргументировать и отстаивать свое мнение;

умение осознанно использовать речевые средства в соответствии с задачей коммуникации для выражения своих чувств, мыслей и потребностей; планирования и регуляции своей деятельности; владение устной и письменной речью, монологической контекстной речью.

В качестве организационной основы для реализации процесса интеграции восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций данные Методические рекомендации учитывают:

опыт Межрегиональной общественной организации "Общественный центр "Судебно-правовая реформа" и Всероссийской ассоциации восстановительной медиации по разработке и внедрению программ восстановительного правосудия;

ресурс сети служб примирения/медиации, созданных во исполнение Концепции развития до 2017 года сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная ответственность в Российской Федерации, утверждённой распоряжением Правительства Российской Федерации от 30 июля 2014 г. N 1430-р.

Целью внедрения восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций является формирование у подрастающего поколения навыков конструктивного поведения в конфликте как способа профилактики девиантного поведения подростков, преодоления их криминализации; укрепления института семьи посредством включения ее в воспитательный процесс; формирования коммуникативной компетентности детей, педагогов и родителей.

Достижение поставленной цели обеспечивается путем решения следующих задач:

широкого информирования педагогического состава образовательных организаций Российской Федерации о возможностях восстановительных технологий и медиации в воспитательной деятельности;

внедрения восстановительных технологий и медиации в воспитательную деятельность образовательных организаций путем формирования соответствующих компетенций у педагогического состава посредством реализации дополнительных профессиональных программ (повышения квалификации);

использования ресурса школьных служб примирения/медиации для реализации восстановительных технологий (в том числе медиации) в воспитательной деятельности образовательных организаций;

регламентации и организации взаимодействия образовательных организаций с территориальными службами примирения/медиации для их привлечения к проведению процедур медиации и программ восстановительного правосудия в отношении несовершеннолетних в рамках воспитательной деятельности.

Концептуальной основой Методических рекомендаций являются Стандарты восстановительной медиации, утвержденные Всероссийской ассоциацией восстановительной медиации в 2009 году.

Методические рекомендации учитывают положения действующего законодательства Российской Федерации и иных нормативных правовых актов Российской Федерации, затрагивающих сферы образования, физической культуры и спорта, культуры, семейной, молодежной, национальной политики, а

также международных документов в сфере защиты прав детей, ратифицированных Российской Федерацией.

4. Концептуальные основания использования восстановительных технологий (в том числе медиации) в воспитательной деятельности образовательных организаций

Концепция восстановительного разрешения конфликтов и криминальных ситуаций (и шире - восстановительного подхода) разрабатывается сегодня в мире как система теоретических представлений и набор способов, процедур и приемов работы, используемых в ситуации преступления, всплеска насилия, конфликта, в обстоятельствах эскалации взаимонепонимания, отчуждения и напряженности в отношениях между людьми. Использование восстановительного подхода необходимо тогда, когда межличностные отношения насыщаются ненавистью и мстительностью, что мешает нормальной человеческой жизни. Восстановительное разрешение конфликтов и криминальных ситуаций помогает людям самим исправить зло, причиненное конфликтами и преступлениями. Восстановительный подход в разрешении конфликтов и криминальных ситуаций с помощью ведущих восстановительных технологий помогает реализовать важные для общества ценности: исцеление жертв преступлений, заглаживание вреда силами обидчиков, участие в этом процессе ближайшего социального окружения участников конфликта.

Восстановительные технологии возникли как ответ на критику современного западного правосудия и формального юридического подхода к конфликтам и криминальным ситуациям. На острие данной критики оказались "приватизация конфликта" системой государственного правосудия, смещение ответственности за решение конфликтов из сообществ людей в руки профессионалов и, как следствие, утрата людьми способности самим искать выход из конфликтных ситуаций. Чем значительнее роль профессионалов правосудия, тем больше они уверены в том, что знают, что именно происходит, что относится к делу, что нет, и как разрешать данную ситуацию.

В итоге, при профессиональном разборе конфликтной или криминальной ситуации ее участники все меньше могут влиять на собственную жизнь, а профессиональные решения в сфере правосудия - иметь отношение к реальным ситуациям людей и сообществ в контексте ценностей общества и развития личности.

Напротив, важнейшей характеристикой восстановительного подхода в правосудии является возвращение способности разрешить конфликт самими его сторонами. Данный подход осуществляется посредством реализации технологий восстановительного правосудия: восстановительной медиации, Кругов сообщества, семейных конференций (советов), восстановительных профилактических программ, проводимых с целью разрешения конфликтных ситуаций, в том числе возникающих на этноконфессиональной почве.

Одним из видов восстановительных технологий являются программы восстановительной медиации.

Под медиацией понимается способ урегулирования споров при содействии беспристрастной третьей стороны (медиатора) на основе добровольного согласия сторон в целях достижения ими взаимоприемлемого решения.

Процедура медиации проводится на основе принципов добровольности, конфиденциальности, сотрудничества и равноправия сторон, беспристрастности и независимости медиатора.

Коммуникация в условиях соблюдения вышеперечисленных принципов предполагает поиск взаимоприемлемых решений в ситуации разности позиций и интересов людей, находящихся в конфликтном взаимодействии.

Представленная выше идеология восстановительного правосудия позволяет дополнить идею классической медиации рядом фундаментальных положений и сформулировать концепцию восстановительной медиации.

Восстановительная медиация - процесс, в котором медиатор создает условия для восстановления способности людей понимать друг друга и договариваться о приемлемых для них вариантах разрешения проблем (при необходимости - о заглаживании причиненного вреда), возникших в результате конфликтных или криминальных ситуаций. В ходе восстановительной медиации важно, чтобы стороны имели возможность освободиться от негативных состояний и обрести ресурс для совместного поиска выхода из ситуации. Восстановительная медиация включает обязательные предварительные встречи медиатора с каждой из сторон по отдельности и общую встречу сторон с участием медиатора.

В отличие от бытового восприятия конфликта, рассматриваемого как нечто, действующее на людей разрушающе, для медиатора конфликт - точка, с которой может начаться диалог сторон, направленный на прояснение их позиций, т.е. - переход от столкновения к взаимопониманию.

В процессе восстановительной медиации происходит:

перевод ситуации от столкновения людей в форме конфликта или криминальной ситуации к обсуждению ее последствий самими участниками конфликта (криминальной ситуации). При этом в случае криминальной ситуации важно опираться на интересы жертв преступления;

определение оснований прошлых и будущих действий участников конфликта или криминальной ситуации (проблем, интересов, потребностей, ценностей, целей) и содействие изменению данных оснований в направлении общественно значимых ценностей. В случае криминальной ситуации необходимо содействовать изменению поведения правонарушителя с целью профилактики будущих преступлений;

Медиатор поддерживает в равной степени все стороны в движении к восстановительным действиям. Кроме того, в криминальной ситуации важное значение приобретает содействие восстановительным действиям участников конфликта (взаимопониманию, извинению, прощению и заглаживанию вреда). В восстановительных программах принятие решений сторонами опирается на их самоопределение: стороны сами вырабатывают и исполняют принятое решение. В некоторых сложных и травматических случаях для этого требуется поддержка социального окружения сторон, социальных работников и психологов.

Основными принципами восстановительной медиации являются:

добровольность участия сторон. Стороны участвуют во встрече добровольно, принуждение в какой-либо форме сторон к участию недопустимо. Стороны вправе отказаться от участия в медиации как до ее начала, так и в ходе самой медиации;

информированность сторон. Медиатор обязан предоставить сторонам всю необходимую информацию о сути медиации, ее процессе и возможных последствиях;

нейтральность (беспристрастность и независимость) медиатора. Медиатор в равной степени поддерживает стороны и их стремление в разрешении конфликта. Если медиатор чувствует, что не может сохранять нейтральность, он должен передать дело другому медиатору или прекратить медиацию. Медиатор не может принимать от какой-либо из сторон вознаграждение или иные виды поощрений, поскольку это может вызвать подозрения в поддержке одной из сторон.

конфиденциальность процесса медиации. Медиация носит конфиденциальный характер. Медиатор или служба медиации обеспечивает конфиденциальность медиации и защиту от разглашения документов, касающихся процесса медиации. Исключение составляет информация, связанная с возможной угрозой жизни либо возможности совершения преступления. При выявлении этой информации медиатор ставит участников в известность, что данная информация будет разглашена. Медиатор передает информацию о результатах медиации в структуру, направившую дело на медиацию. Медиатор может вести записи и составлять отчеты для обсуждения в кругу медиаторов и кураторов служб примирения/ медиации. При публикации имена участников должны быть изменены;

ответственность сторон и медиатора. Медиатор отвечает за безопасность участников на встрече, а также за соблюдение принципов и стандартов. Ответственность за результат медиации несут стороны конфликта, участвующие в медиации. Медиатор не может советовать сторонам принять то или иное решение по существу конфликта;

заглаживание вреда обидчиком. В ситуации, где есть обидчик и жертва, ответственность обидчика состоит в заглаживании вреда, причиненного жертве;

самостоятельность служб примирения/ медиации. Служба примирения/медиации самостоятельна в выборе форм деятельности и организации процесса медиации.

Службы примирения/медиации в Российский Федерации, реализующие программы восстановительного правосудия, в том числе, опираются на "Стандарты восстановительной медиации", разработанные Всероссийской ассоциацией восстановительной медиации в 2009 году (http://sprc.ru/wp-content /uploads/2012/08/ Стандарты-восстановительной-медиации.pdf).

В России существует успешный опыт проведения восстановительной технологии "Семейная конференция" ("Семейный совет"). В результате многих проведенных Семейных конференций родственникам удается при поддержке специалистов изменить ситуацию, восстановить родственные связи и, тем самым, не допустить изъятия его из семьи. Важным здесь является не столько создание правового благополучия несовершеннолетнего, сколько восстановления взаимоотношений родственников для помощи ребенку. Например, формальное восстановление прав ребенка на жилплощадь без контроля и поддержки со стороны взрослых может привести к использованию квартиры в качестве пункта сбора криминальной группировки.

Таким образом, восстановительные технологии становятся актуальным способом воспитательной деятельности в ситуациях нарушенных семейных связей, когда первоочередной задачей семьи становится объединение близких ради социального благополучия ребенка.

Для решения задач работы с сообществами существует восстановительная технология "Круг сообщества", базирующаяся на традиционных для большинства россиян практиках крестьянского общинного правосудия - разрешения групповых конфликтов с включением социального окружения всех конфликтующих сторон, принимающих на себя ответственность за принятое решение и его последующее выполнение. Применение таких технологий урегулирования спорных ситуаций, апеллирующих к исторической памяти разрешения конфликтов "всем миром", становится способом возрождения данных традиций. Не менее важное значение в отношении конфликтов на этноконфессиональной почве приобретает владение сотрудниками образовательных организаций знаниями о национальных, религиозных особенностях участников данных конфликтов.

Восстановительная профилактическая программа - программа помощи в ситуациях, имеющих риск развития (эскалации) конфликта или совершения правонарушения, в рамках которой участники берут на себя ответственность за его/их предотвращение и/или улучшение отношений и реализуются принципы восстановительного правосудия (восстановительной медиации).

В Российской Федерации с 1998 года реализацию программ восстановительного правосудия осуществляют команды и службы примирения, создаваемые в школах, центрах социально-психологической помощи и на базе социально ориентированных некоммерческих организаций при поддержке Межрегиональной общественной организации "Общественный центр "Судебно-правовая реформа". В рамках данной работы создаются ассоциации специалистов, складываются местные модели межведомственного взаимодействия различных структур, работающих с несовершеннолетними и их семьями, куда включаются и службы примирения, развивается инструментарий восстановительных программ.

Развитие восстановительного правосудия в отношении несовершеннолетних осуществляется в том числе при поддержке Всероссийской ассоциации восстановительной медиации посредством формирования региональных сообществ, куда входят представители муниципальных учреждений социальной сферы и сферы образования. Данные группы реализуют восстановительную практику по уголовным делам и конфликтам с участием несовершеннолетних во взаимодействии с судами, комиссиями по делам несовершеннолетних и защите прав, образовательными организациями.

Службы примирения/медиации способствуют воспитательному процессу, поскольку становятся каналом трансляции цивилизованных норм взаимоотношений между детьми, а также между детьми и взрослыми. При этом часть детей, участвующих в работе служб (как медиаторы, так и стороны процедуры медиации) сами являются проводниками таких норм, используя их в последующем в ходе разрешения своих собственных конфликтных ситуаций.

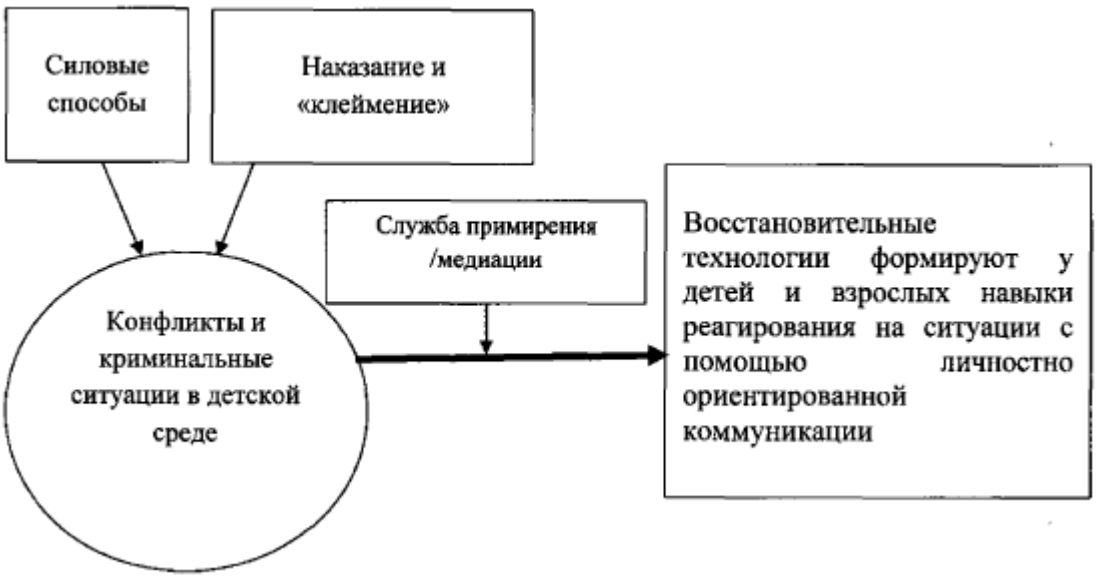
Социокультурная функция службы служб примирения/медиации состоит в обеспечении воспроизводства способа и навыка осуществления действия по разрешению конфликтов посредством личностно ориентированной коммуникации. Личностно ориентированная коммуникация побуждает участников размышлять над последствиями своих действий, понимать ситуацию и основания действий других людей и самим принимать решения и осознавать их ценностные основания, что позволяет строить и сохранять конструктивные взаимоотношения в постоянно меняющихся условиях.

Общественно значимая и воспитательная функция служб примирения/ медиации состоит в создании оппозиции силовым способам разрешения конфликтов, наказанию и клеймению через организацию программ восстановительной медиации, кругов сообществ и семейных конференций (схема 1). Деятельность служб примирения/медиации можно также использовать как элемент управления конфликтами в работе с подростковыми криминальными группировками.

Классическая и восстановительная медиация отличаются концептуальными основами и технологией проведения процедуры. Выбор в пользу классической или восстановительной медиации, а также конкретного инструмента восстановительной медиации, зависит от типа конфликтной ситуации. В частности, отдельные методы восстановительной практики ("Круги сообщества", "Семейные конференции") будут представлены в соответствующих разделах.

Схема 1. Воспитательная функция служб примирения/медиации

Реагирование детей и взрослых



5. Круг сообщества как традиционная практика разрешения конфликтов и криминальных ситуаций

Восстановительные технологии основаны на двух принципах - прекращении конфликта между людьми и вовлечении в этот процесс ближайшего социального окружения конфликтующих. Данные принципы исторически сложились в общинных формах жизни. Издревле в сельских сообществах существовали механизмы преодоления вражды, воспроизводились различные формы взаимопомощи, являющиеся важной питательной средой для развития конструктивных форм реагирования на конфликты, проступки и преступления, позволяющие целым сообществам и отдельным людям выжить, избежав кровной вражды или кары официального правосудия. Ценность общинных практик базировалась на сохранении мира в сообществе (поселке, деревне), да и сама сельская община носила название "миръ", где сохранение мира как преодоление раскола между людьми в конфликтных и криминальных ситуациях являлось ключевой задачей старейшин. В ситуациях правонарушений важной ценностью в общинах было не столько наказание, сколько компенсация вреда потерпевшему или его семье. Эти традиции, поддерживаемые людьми во многих селениях и городах, до сих пор существуют на Кавказе в форме маслаата (примирения кровников - находящихся в отношениях кровной мести).

Подобный подход находил поддержку общественного мнения, опиравшегося, в том числе, и на религиозные принципы. И сегодня во многих странах мира не умерли народные традиции примирения, которые в некоторых местных сообществах активные граждане используют для восстановления и нормализации жизни. В России также сохранилась традиция, когда участники конфликтной или криминальной ситуации, обращаясь к традициям примирения в кризисные моменты своей жизни, сообща решают, как изменить ситуацию в интересах каждого так, чтобы это способствовало реализации нравственных ценностей. Во многих малых поселениях восстанавливаются сельские сходы, помогающие

людям различные вопросы решать силами сообществ. В последние годы и в крупных городах происходит повышение гражданской активности, в рамках которой граждане объединяются для решения беспокоящих их вопросов, как правило, коммунальной направленности (капитальный ремонт домов, благоустройство придомовой территории). Отмечается также и активное формирование родительских сообществ вокруг школьных классов, объединенных на платформе известных мессенджеров, становящихся площадкой для обсуждения новостей класса, включая случившиеся за день конфликты.

В сложившейся ситуации разрешение конфликтных ситуаций с участием всего сообщества становится важнейшей задачей образовательных организаций, реализация которой возможна с применением инструментов, базирующихся на традиционных для большинства россиян практиках крестьянского общинного правосудия, независимо от места их географического проживания и вероисповедания.

На базе данных традиций специалистами Всероссийской ассоциации восстановительной медиации была разработана восстановительная технология - Круг сообщества. Важнейшей особенностью Круга сообщества является привлечение к обсуждению конфликтной ситуации всех заинтересованных людей, что обеспечивает их активное участие в принятии решения и разделении ответственности за его последующее выполнение. Процесс Круга сообщества позволяет включать в работу с конфликтами и криминальными ситуациями значительное число участников. Поскольку в ситуациях конфликта отношения людей отличаются враждебностью, возникает необходимость привлечения нейтрального посредника - ведущего Круга сообщества.

Показанием к проведению Круга сообщества в образовательной организации могут быть любые конфликты, возникающие в образовательном пространстве преимущественно с несколькими участниками или группами участников: конфликты между детьми; педагогами и детьми; педагогами и родителями; педагогами, родителями и детьми. Работа по построению конструктивного взаимодействия в сообществе, формирующемся вокруг школьных классов (сообщество детей, родителей, работников образовательной организации) приобретает особую значимость в случае необходимости разрешения конфликтов, возникающих на этноконфессиональной почве (раздел "Этноконфессиональная медиация в образовательных организациях"), а также в связи со становлением инклюзивного образования.

Одно из направлений развития воспитания в соответствии со Стратегией развития воспитания в Российской Федерации на период до 2025 года предполагает формирование деятельного позитивного отношения к людям с ограниченными возможностями здоровья и детям-инвалидам, преодоление психологических барьеров, существующих в обществе по отношению к людям с ограниченными возможностями здоровья для обеспечения равного доступа к образованию для всех обучающихся с учетом разнообразия особых образовательных потребностей и индивидуальных возможностей, гарантированного Федеральным законом от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации".

Одним из способов преодоления данных барьеров в детско-родительском сообществе является технология Круга сообщества.

С помощью ведущего и добровольцев-помощников ведущего в Круге сообщества реализуются такие ценности как:

помощь, взаимная поддержка и сопричастность людей;

мирное сосуществование;

свободное и безопасное для участников обсуждение проблем;

восстановление и укрепление позитивных связей между людьми;

развитие способностей членов сообщества в работе с травматическими и болезненными ситуациями;

принятие участниками ответственности за происходящее.

Проведение Круга сообщества возможно в образовательных организациях как самими педагогами, прошедшими обучение данной методике, так и с привлечением специалистов служб примирения/медиации.

6. Семейные конференции как инструмент укрепления института семьи

Как известно, девиантное поведение детей и подростков зачастую происходит на фоне семейного неблагополучия, когда ребенок выпадает из зоны родительского контроля с последующим возможным вовлечением в криминальные ситуации. Одним из важнейших компонентов воспитательной работы по профилактике правонарушений несовершеннолетних в случае выявления фактов девиантного поведения ребенка является осознание его родителями сложившейся ситуации и сотрудничество всех членов семьи с педагогами образовательной организации.

Когда ребенок в силу тех или иных причин фактически оказывается без родительского попечения, помощь ему могут оказать иные родственники (брат, сестра, бабушки, дедушки, тети, дяди).

Для того, чтобы вовлечь все семейное окружение ребенка в процесс воспитательного воздействия, проводится программа восстановительного правосудия "Семейная конференция" ("Семейный совет"). Данная технология базируется на традиции различных народов в виде помощи родственников друг другу в условиях потери контроля за поведением ребенка и используется в случаях, когда семья не справляется с воспитанием ребенка.

Важной составляющей семейной конференции является активизация потенциала семьи и ее ближайшего социального окружения для выработки самостоятельного решения по поводу кризисной ситуации у кого-либо из ее членов. Кроме представителей ближайшего социального окружения, в таких программах могут участвовать представители органов и учреждений системы профилактики правонарушений и безнадзорности несовершеннолетних. Решения принимаются в результате обсуждений и при достижении консенсуса.

В ходе реализации программы Семейной конференции ее ведущий работает над созданием условий для совместного решения проблем ребенка самими родственниками. Основой работы ведущего Семейной конференции является подготовка и проведение встречи круга родственников, которые могут помочь родителям и детям изменить сложившуюся ситуацию. В данных программах ведущий собирает членов семьи и родственников, обращаясь к традициям коллективного принятия решений, настраивает участников на конкретные шаги по оказанию помощи ребенку, и это создает возможность конструктивного преодоления чувства стыда. Например, если мать ребенка страдает алкогольной зависимостью, обсуждается не ее личная ситуация, ее не пытаются "воспитывать", а обсуждается вопрос о том, что может семья сделать в этой ситуации для ребенка, и что делать, чтобы ребенок не был изъят из семьи. Осуществляя подготовку родственников к семейному совету, специалисты ставят своей основной целью не изменить людей и их жизненные обстоятельства, а способствовать восстановлению отношений между ними с помощью постановки основного вопроса Семейной конференции, связанного с необходимостью принятия решения в интересах благополучия ребенка.

Функция специалистов в Семейной конференции заключается в том, чтобы создать уникальные и подходящие для данного случая конфигурацию людей и условия для личностно окрашенной коммуникации, помогающей самим участникам Семейной конференции принять решение по исправлению ситуации. Специалисты помогают состояться ценным для человеческого сообщества восстановительным действиям: заглаживанию вреда, раскаянию, осознанию, прощению, планированию своего будущего, восстановлению отношений и опеки над детьми - действиям, которые в силу определенных обстоятельств (например, травмы, обиды или болезни) люди без посторонней помощи порой сделать не в состоянии. Поэтому в такой ситуации важно участие нейтральных ведущих, профессиональные действия которых позволяют принять решения участникам конференции в интересах сохранения ребенка в кровной семье или под опекой родственников.

Семейные конференции могут проводиться обученными специалистами служб примирения/медиации в образовательной организации с целью оказания воздействия на того или иного ребенка в случае его девиантного поведения или низкой успеваемости.

7. Этноконфессиональная медиация в образовательных организациях

Проявления ксенофобии, неуважительного отношения к традициям и вероисповеданию людей иной национальности или конфессии, к сожалению, не является сегодня редкостью в образовательной среде. Участниками подобных конфликтов зачастую становятся не только обучающиеся, но и их родственники - представители диаспоры, требующие немедленного извинения и наказания стороны, виновной, по их мнению, в конфликте.

Помимо традиционных способов профилактики ксенофобии посредством этнокультурного воспитания подрастающего поколения, а также его воспитания в духе поликультурности и толерантности образовательные организации могут обеспечивать эффективное урегулирование подобных конфликтов с использованием технологий этноконфессиональной медиации.

Под этноконфессиональной медиацией понимается способ урегулирования конфликта с учетом его межэтнической и межконфессиональной составляющей с участием независимого нейтрального посредника. Данный способ может быть реализован как в формате классической медиации с участием двух конфликтующих сторон, так и посредством проведения Круга сообщества с участием двух и более сторон конфликта, а также их родственников и других представителей социального окружения.

Специалисту образовательной организации (службы примирения/медиации), принимающему на себя функции медиатора этноконфессиональных конфликтов, помимо технологий проведения классической медиации и Круга сообщества важно обладать комплексом специфических знаний, позволяющих эффективно работать с подобными конфликтами, в частности иметь знания о:

предметном наполнении конфликтов этноса или конфессиональной группы, описываемым основными эпосами, притчами, священными текстами той или иной конфессиональной группы;

исторически сложившихся (традиционных) методах урегулирования конфликтов данным этносом/ конфессиональной группы, а также с их правовой оценкой;

особенностях смысловых нагрузок тех или иных словесных формулировок;

тендерных, возрастных и родственных барьеров и их роли в коммуникации данного этноса/конфессиональной группы, в межэтнических/межрелигиозных взаимоотношениях, а также их месте в конфликтах с участием данного этноса/ конфессиональной группы и/или внутри его/их.

8. Организационные модели и направления внедрения восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций

Основой для внедрения восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций могут стать существующие и вновь создаваемые школьные и территориальные службы примирения/медиации.

Школьная служба примирения/служба школьной медиации (служба примирения/медиации образовательной организации) - утвержденная приказом директора образовательной организации детско-взрослая команда, которая в рамках образовательной организации под руководством взрослого куратора осуществляет деятельность по профилактике и разрешению конфликтных ситуаций, возникающих в ходе учебно-воспитательной деятельности посредством применения методов медиации и восстановительных технологий.

Служба примирения/медиации образовательной организации осуществляет:

обучение школьников и педагогов конструктивным способам общения, способности принимать согласованные решения и сотрудничать - прежде всего, через опыт решения реальных конфликтных ситуаций;

первичную профилактику, когда явного конфликта нет, но есть риск его возникновения в дальнейшем (например, проведения Кругов сообщества с детьми при слиянии двух классов в один, с родителями первоклассников, с детьми и их родителями при переходе в среднюю школу и так далее);

первичную профилактику (конфликта еще нет, но участниками чувствуется напряженность, например, по результатам исследования межэтнической напряженности или по запросу классного руководителя/родителей);

урегулирование конфликтов между школьниками (учащимися), а также учащимися и педагогами;

урегулирование конфликтов между педагогами и родителями;

согласование позиций и интересов детей, родителей и педагогов по отношению к образовательному процессу, большей включенности родителей и ответственному поведению детей;

вторичную профилактику и работу с правонарушениями (в том числе по делам, переданным в комиссии по делам несовершеннолетних и защите их прав);

сложным многосторонним конфликтам между всеми участниками образовательного процесса (когда в конфликт так или иначе включены дети, родители, педагоги, администрация, органы управления образованием, средства массовой информации и так далее) - с привлечением территориальных и городских служб примирения /медиации.

В большинстве субъектов Российской Федерации куратором службы примирения/медиации образовательной организации является специалист данной организации (социальный педагог, психолог), осуществляющий указанную деятельность в рамках функциональных обязанностей.

Работа школьной службы примирения/службы школьной медиации обычно регламентируется Положением о соответствующей службе, утвержденным приказом руководителя образовательной организации, а также методическими рекомендациями по созданию соответствующих служб.

Деятельность по применению восстановительных технологий школьными службами примирения/службами школьной медиации может также основываться на следовании "Стандартам восстановительной медиации" (http://sprc.ru/wp-content/uploads/2012/08/Стандарты-восстановительной-медиации.pdf).

Территориальная служба примирения/медиации является структурой, занимающейся проведением восстановительных программ (в том числе медиации) на территории (в районе, в городе, в регионе).

Под службой понимаются различные варианты организации такой деятельности, в частности посредством:

создания подразделения внутри организации, оказывающего услуги детям и семьям (например, социального, медико-психологического или иного центра);

передачи данного функционала конкретному сотруднику организации;

организации службы примирения/медиации в организации, которая занимается комплексной работой с несовершеннолетними правонарушителями, где медиация и восстановительные технологии являются одним из видов деятельности;

включения восстановительных технологий (в том числе медиации) в круг инструментов социально ориентированной практики некоммерческих организаций.

Территориальные службы примирения/медиации проводят восстановительные программы (медиацию, семейные конференции, Круги сообщества) по следующим категориям случаев:

преступления, совершенные несовершеннолетними (информация о случаях поступает из судов, комиссий по делам несовершеннолетних и защите их прав, органов предварительного расследования, непосредственно от граждан, иногда - из образовательных организаций, от адвокатов);

общественно опасные деяния, совершенные детьми, не достигшими возраста уголовной ответственности - ООД (информация о случаях поступает из комиссий по делам несовершеннолетних и защите их прав, отделов по делам несовершеннолетних органов внутренних дел, непосредственно от граждан, образовательных организаций, от адвокатов);

семейные конфликты: детско-родительские конфликты; гражданские дела, связанные с разводом родителей и определением места проживания ребенка; ситуации невыполнения родителями своих обязанностей по отношению к детям и пр. (информация о случаях поступает из судов по гражданским делам, комиссий по делам несовершеннолетних и защите их прав, непосредственно от граждан, иногда - из образовательных организаций, от адвокатов);

конфликты в образовательных организациях (информация о случаях поступает из образовательных организаций и от граждан);

профилактические программы в образовательных организациях.

Поскольку в деятельности по применению программ восстановительного правосудия и медиации, в целом, заложены ценности участия сообщества, самоопределения людей, открытости к переговорам, то и внедрение данных технологий должно соответствовать этим целям, то есть быть процессом добровольным и открытым для коммуникации между разными его участниками. Важнейшую роль в такой работе должны играть региональные сообщества (ассоциации) медиаторов и кураторов служб примирения/медиации. Для этого в субъектах Российской Федерации могут образовываться сообщества, ассоциации, объединения, сети. Сетевое взаимодействие обеспечивает содержательную и организационную поддержку развитию служб примирения/медиации с учетом их организационно-правовых региональных особенностей.

Важнейшими признаками сетевого взаимодействия является добровольное присоединение участников, свободное распространение информации внутри сети, самостоятельность выбора организационно-правовой формы (ассоциации, объединения, в том числе без образования юридического лица), стратегия развития и поиск партнеров на региональном уровне, обмен опытом и взаимная поддержка участников объединения. В таких ассоциациях представители различных ведомств и некоммерческих организаций встречаются для обсуждения теории и практики восстановительного правосудия, что создает основу для подлинного межведомственного взаимодействия.

Сетевое взаимодействие обеспечивает содержательную и организационную поддержку восстановительных технологий на уровне субъекта Российской Федерации.

В целях поддержки сети служб примирения/медиации органам управления образованием совместно с другими субъектами системы профилактики безнадзорности и правонарушений несовершеннолетних рекомендуется на региональном уровне разработать и утвердить региональную модель развития сети служб примирения/медиации, позволяющую обеспечить:

разработку программ повышения квалификации в сфере восстановительной медиации и восстановительного подхода в системе образования, привлечение к проведению обучения специалистов, имеющих практику медиации и урегулирования конфликтов;

поддержку различных форм обучения основам медиации и восстановительных технологий заинтересованных школьников в качестве медиаторов-ровесников;

включение тем, связанных с деятельностью служб примирения/медиации в конкурсы профессионального мастерства педагогов (при их наличии);

включение направления служб примирения/медиации в региональные грантовые программы (при их наличии);

проведение мониторинга основных показателей проведения восстановительных программ;

разработку регламентов (соглашений) о взаимодействии школьных и территориальных служб примирения/медиации с комиссий по делам несовершеннолетних и защите их прав с целью эффективного проведения восстановительных программ;

поддержку профессионального сообщества специалистов служб примирения/медиации, проведение регулярных региональных конференций, семинаров и других мероприятий, поддерживающих сетевое взаимодействие.

Повышение профессионального мастерства ведущих восстановительных программ/медиаторов может происходить в профессиональном сообществе в форме супервизий (консультирования медиатора более опытным коллегой, имеющим соответствующую квалификацию, с целью разбора практических случаев, анализа и корректировки профессиональных умений, и развития умений профессионального самоанализа супервизируемого специалиста), мастер-классов и в иных формах.

Критерии анализа и оценки деятельности ведущего восстановительные программы разрешения конфликтов и криминальных ситуаций/медиатора разрабатывает профессиональное сообщество.

Профессиональное сообщество осуществляет методическую поддержку деятельности специалистов служб примирения/медиации, а также, при необходимости, помогает им в сложных ситуациях, выходящих за рамки стандартной процедуры. Методистом, т.е. лицом, оказывающим подобную поддержку, может быть только человек, имеющий собственную практику проведения медиации и/или восстановительных программ в системе образования.

Стратегия развития служб примирения/медиации на территории и документы, регламентирующие организацию деятельности данных служб должны разрабатываться и приниматься с учетом мнения профессионального сообщества.

Интеграция восстановительных технологий (в том числе медиации) в воспитательную работу образовательных организаций может осуществляться с использованием ресурса существующих служб примирения/медиации в рамках их сетевого взаимодействия посредством реализации организационных мероприятий, приведенных ниже в таблице.

Направление интеграции восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций	Мероприятия по интеграции восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций
Повышение уровня информированности	Проведение информационных семинаров

всех работников образовательной организации о возможностях восстановительных технологий как компонента воспитательной работы	в образовательных организациях специалистами школьных и территориальных служб примирения/медиации
Приобретение компетенций по применению восстановительных технологий (восстановительной медиации, "Кругов сообщества", "Семейных конференций") а также принципов этноконфессиональной медиации специалистами школьных и территориальных служб примирения/ медиации	Прохождение специалистами школьных и территориальных служб примирения/медиации программ дополнительного профессионального образования (повышения квалификации) с обучением применению восстановительных технологий (восстановительной медиации, "Кругов сообщества", "Семейных конференций") а также этноконфессиональной медиации
Привлечение специалистов территориальных служб примирения/ медиации к разрешению конфликтов в образовательных организациях в случае наличия угрозы соблюдению принципа нейтральности медиатора, являющегося работником	Проведение восстановительных технологий (восстановительной медиации, "Кругов сообщества", "Семейных конференций") в образовательных организациях силами специалистов территориальных служб примирения/медиации образовательной организации
Управление реализацией восстановительных технологий в воспитательной деятельности образовательных организаций	Поддержка создания региональных сообщества (ассоциаций). Регламентация их деятельности на уровне субъектов Российской Федерации и на уровне образовательных организаций

9. Список нормативных правовых документов и литературы для самостоятельного ознакомления с методологией интеграции восстановительных технологий (в том числе медиации) в воспитательную деятельность образовательных организаций

1. Зачем нужны службы школьной медиации? [Электронный ресурс]//Портал "Слово". - 10 февраля 2014 г. (http://portal-slovo.ru/topic/47714.php?sphrase_id=89012)

2. Зер Х. Восстановительное правосудие: новый взгляд на преступление и наказание. Перевод с английского/общая редакция Л.М.Карнозовой. - М.: МОО Центр "Судебно-правовая реформа", 2002.

3. Интернет-ресурсы:

www.fedim.ru - сайт ФГБУ "Федеральный институт медиации"

www.sprc.ru - сайт общественного центра "Судебно-правовая реформа"

www.школьные-службы-примирения.рф - сайт школьных служб примирения

4. Карнозова Л.М. Введение в восстановительное правосудие (медиация в ответ на преступление). - М.: Проспект, 2014.

5. Коновалов А.Ю. Школьные службы примирения и восстановительная культура взаимоотношений/Практическое руководство. Под общей редакцией Карнозовой Л.М. - М.: МОО "Судебно-правовая реформа", 2012.

6. Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2020 года (утверждена распоряжением Правительства Российской Федерации от 22 марта 2017 г. N 520-р).

7. Концепция развития до 2017 года сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная

ответственность в Российской Федерации (утверждена распоряжением Правительства Российской Федерации N 1430-р от 30 июля 2014 г.).

8. Кристи Н. Конфликты как собственность.//Правосудие по делам несовершеннолетних. Перспективы развития. Вып.1. М.: МОО Центр "Судебно-правовая реформа", 1999. С.28-45.

9. Методические рекомендации по созданию и развитию служб примирения в образовательных организациях, разработаны Всероссийской ассоциацией восстановительной медиации, Москва, 2015.

10. Методические рекомендации по созданию и развитию служб школьной медиации в образовательных организациях, разработаны ФГБУ "Федеральный институт медиации", Москва, 2015.

11. Максудов Р.Р. Программы восстановительного разрешения конфликтов и криминальных ситуаций: от уникальных эпизодов к заживлению социальной ткани/под общей редакцией Н.В.Путинцевой/М.: МОО Центр "Судебно-правовая реформа", 2012.

12. Национальная стратегия действий в интересах детей на 2012-2017 годы (утверждена Указом Президента Российской Федерации от 1 июня 2012 года N 761).

13. Стандарты восстановительной медиации. \\ Вестник восстановительной юстиции. Концепция и практика восстановительной медиации. Выпуск 7. - М.: Центр "СПР". 2010.

14. Создание и поддержка служб примирения в регионах (сборник материалов). Ч.1/Сост. Л.М.Карнозова, А.Ю.Коновалов. - М.: МОО Центр "Судебно-правовая реформа", 2016 (электронный сборник), http://sprc.ru/

15. Создание и поддержка служб примирения в регионах (сборник материалов). Ч.2/Сост. Л.М.Карнозова. - М.: МОО Центр "Судебно-правовая реформа", 2016 (электронный сборник), http://sprc.ru/

16. Стратегия развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 29 мая 2015 г. N 996-р).

17. Территориальные службы примирения: условия функционирования и организационное устройство/Сборник материалов/Сост. Л.М.Карнозова. М.: МОО Центр "Судебно-правовая реформа", 2015 (электронный сборник). http://sprc.ru/

18. Технология разрешения конфликтов. // Газета "Вести образования", N 5 (114), 25 марта 2015 года. (http://vogazeta.ru/ivo/info/14511.html)

19. Федеральный государственный образовательный стандарт основного общего образования (утвержден приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. N 1897).

20. Федеральный закон от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации".

21. Шамликашвили Ц.А., Семенова О.А. Почему ребенку трудно учиться и как ему помочь? М.: МЦУПК, 2010. - 400 с.

22. Шамликашвили Ц.А., Харитонов С.В., Графский В.П., Пчелинцева Д.Н. Причины споров между детьми и действенные способы их урегулирования с точки зрения сотрудников образовательных учреждений//Вестник Федерального института медиации. 2017. N 2. С.22-27.

23. Шамликашвили Ц.А., Хазанова М.А. Метод "школьная медиация" как способ создания безопасного пространства и его психологические механизмы//Психологическая наука и образование. 2014. N 2. С.26-33.

24. Шамликашвили Ц.А. Что такое "школьная медиация" в теории и на практике?//Медиация и право. Посредничество и примирение. 2008. N 2. с.16.

25. Школьная медиация как действенный инструмент в защите прав детей. [Электронный ресурс]//Информационно-правовой портал "Гарант". - 30 августа 2013 г.

Министерство образования и науки Российской Федерации
ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ ЗАЩИТЫ ПРАВ ДЕТЕЙ

ПИСЬМО

от 18 декабря 2015 года N 07-4317

О направлении методических рекомендаций

Во исполнение пункта 2 межведомственного плана комплексных мероприятий по реализации Концепции развития до 2017 года сети служб медиации в целях реализации восстановительного правосудия в отношении детей, в том числе совершивших общественно опасные деяния, но не достигших возраста, с которого наступает уголовная ответственность, утвержденной распоряжением Правительства Российской Федерации от 30 июля 2014 года N 1430-р, Минобрнауки России направляет методические рекомендации* по созданию и развитию служб школьной медиации в образовательных организациях, разработанные ФГБУ "Федеральный институт медиации", а также методические рекомендации* по созданию и развитию школьных служб примирения, разработанные специалистами Всероссийской ассоциации восстановительной медиации, для возможного использования в работе.

_____

* Приложения см. по ссылке. - Примечание изготовителя базы данных.

Дополнительная информация размещена на официальном сайте ФГБУ "Федеральный институт медиации" (www.fedim.ru), а также на информационных сайтах www.sprc.ru и www.школьные-службы-примирения.рф

Заместитель директора Департамента
В.Л.Кабанов

Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ПИСЬМО

от 22 октября 2009 года N 17-187

Об обеспечении защиты персональных данных

_____

В дополнение к настоящему документу см. письмо Рособразования от 15 февраля 2010 года N 17-50.

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* N 152-ФЗ "О персональных данных".

---

* Вероятно, ошибка оригинала. Следует читать "от 27.07.2006". - Примечание изготовителя базы данных.

В дополнение к письму Федерального агентства по образованию от 29.07.2009 N 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 N ФАО-6748/52/17-02-09/72, просим вас в срок до 15 ноября 2009 года 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* N 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.

---

* Вероятно, ошибка оригинала. Следует читать "от 27.07.2006". - Примечание изготовителя базы данных.

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 по 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 года N 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 года 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 года N 55/86/20.

Количество субъектов ПДн в системе Категория ПДн, обрабатываемых в электронном виде	Более 100 тыс. ПДн	В объеме		От 1000 до 1000 00 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,	**1 класс (К1)**			***2 класс (К2)***				3 класс (К3)	

за исключением ПДн, относящихся к категории 1			
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 года N 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 в виду, что в соответствии с Федеральным законом от 27 июля 2006 года N 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 года N 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 в виду, 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 года N 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.

_____

* Вероятно, ошибка оригинала. Следует читать "от 27.07.2006". - Примечание изготовителя базы данных.

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 то же 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 N 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.

АКТ
классификации информационной системы, обрабатывающей персональные данные

наименование информационной системы

Комиссия, в соответствии с N в составе:
приказом от
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 года 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 в виду, 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 N 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* N 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);

_____

* Вероятно, ошибка оригинала. Следует читать "от 27.07.2006". - Примечание изготовителя базы данных.

- 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);

Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных, 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* N 152-ФЗ "О персональных данных" за исключением случаев, предусмотренных данным Федеральным законом, имеет право

_____

* Вероятно, ошибка оригинала. Следует читать "от 27.07.2006". - Примечание изготовителя базы данных.

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 N 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 года N 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 года N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 года N 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 учету. 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

N 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 персональных данных в структурном подразделении _____ Подпись

Пример формы журнала учета съемных носителей

ЖУРНАЛ
учета съемных носителей персональных данных

_____
наименование структурного подразделения

Начат " ____ " _____ 200 ___ г.
Окончен " ____ " _____ 200 ___ г.

Должность и Ф.И.О. ответственного за хранение _____ Подпись

N 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 (N и дата отправки адресату или распоряжения о передаче, N 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 _____ N _____ в составе:
(должности, Ф.И.О.)
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

N п/п	Дата	Учетный номер съемного носителя	Пояснения
1	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
(Ф.И.О.) 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, соответствующим 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.

Приложение 3

СВЕДЕНИЯ
о характеристиках информационных систем, обрабатывающих персональные данные (ИСПДн)
(примеры заполнения)

N п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное)	Индекс и почтовый адрес	Отраслевая (ведомственная) принадлежность	Исходные данные классификации ИСПДн					Категория ПДн	Класс ИСПДн	Наличие администраторов ИСПДн и регламентов обработки ПДн	Примечание
					Структура ИСПДн	Наличие подключений к сетям общего пользования	Режим обработки ПДн	Разграничение доступа пользователей	Местонахождение технических средств ИСПДн				
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Автоматизированная информа-	..... государст-	индекс, регион, гор	Рособразование	Распределен-	Да	Многопользо-	Да	РФ	2/1	К2	Да	

	ционная система "Университет"	венный технический университет (...ГУ)	од, улица, дом		ная		вательский						
2	Система расчета и начисления зарплаты сотрудникам	.……химико-технологический техникум (...ХТТ)	индекс, регион, город, улица, дом	Рособразование	Автономная	Да	Одно-пользовательский	Нет	РФ	2/2	К3	Нет	
3	Система ведения кадрового учета и расчета зарплаты	.……государственный технический университет (...ГУ)	индекс, регион, город, улица, дом	Рособразование	Локальная	Нет	Много-пользовательский	Да	РФ	2/1	К2	Да	
4	Система организации приемной компании "Абитуриент"	.……государственный технический университе	индекс, регион, город, улица, дом	Рособразование	Локальная	Да	Много-пользовательский	Да	РФ	2/2	К3	Да	

		т (...ГУ)											
5	Система организации учебного процесса "Контингент"	.……… государственный технический университет (...ГУ)	индекс, регион, город, улица, дом	Рособразование	Локальная	Да	Многопользовательский	Да	РФ	3/2	КЗ	Да	
6	Система расчета стипендии	.……… государственный технический университет (...ГУ)	индекс, регион, город, улица, дом	Рособразование	Локальная	Нет	Многопользовательский	Нет	РФ	2/2	КЗ	Да	

Заместитель руководителя учреждения,
ответственный за защиту персональных данных подпись

Обязательные требования:

Ввод информации осуществляется только в табличном виде (Microsoft Excel) с расширением xls.

Данные вводятся в таблицу через пробел, без знака переноса слов и без перевода строки. Шрифт Times New Roman, размер 10, нежирный.

Выравнивание по горизонтали: по левому краю, выравнивание по вертикали: по верхнему краю. Отступ: 0.

Пробел не ставится перед номером, скобкой, точкой, запятой, кавычками, двоеточием, точкой с запятой, вопросительным и восклицательным знаком.

Заполнение таблицы:

Графа 1. Порядковый номер: заносится порядковый номер ИСПДн.

Графа 2. Наименование ИСПДн: заносится наименование ИСПДн или составной части.

Графа 3. Наименование объекта (полное и сокращенное): заносится наименование организации (юридического лица), где находится ИСПДн.

Например: Тульский государственный университет (ТулГУ). ГОУ ВПО, ГОУ СПО, ГОУ НПО ...не указываются.

Графа 4. Индекс и почтовый адрес: заносится почтовый адрес местонахождения системы (без указания помещений, аудиторий, комнат.....), включая территориально удаленные подразделения и филиалы.

Например: 426069, Удмуртская Республика, г.Ижевск, ул.Студенческая, д.7

Графа 5. Отраслевая (ведомственная принадлежность): Рособразование

Если не Федеральное агентство по образованию - указать ведомственную принадлежность объекта.

Графа 6. Структура ИСПДн - выбрать из вариантов:

- Локальная (сеть в пределах здания или близко расположенных зданий)

- Автономная (автоматизированные рабочие места, не подключенные к иным информационным системам)

- Распределенная (с использованием технологии удаленного доступа по сети).

Графа 7. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена, в т.ч. Интернет: Да, Нет.

Графа 8. Режим обработки ПДн: Однопользовательский, Многопользовательский.

Графа 9. Разграничение доступа пользователей: Да, Нет.

Графа 10. Местонахождение технических средств ИСПДн: РФ или перечислить страны, где находится ИСПДн.

Графа 11. Наиболее высокая категория ПДн из числа обрабатываемых в ИСПДн (1,2,3,4) указывается через дробь: Категория ПДн в электронном виде/Категория ПДн в бумажном виде. Например: 3/2. (В соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" и с учетом рекомендаций по проведению работ в подведомственных Рособразованию учреждениях по обеспечению защиты

информационных систем персональных данных).

Графа 12. Класс ИСПДн: К1, К2, К3, К4, специальный. (приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных").

Графа 13. Наличие администраторов ИСПДн и регламентов (Положения и инструкций) по обработке ПДн: Да, Нет.

Графа 14. Примечание (не более 100 символов): при необходимости указывается дополнительная информация.

Примечание:

Заполненную форму необходимо отправить до 15.11.2009 по E-mail: ispd@ministry.ru, в теме сообщения указать наименование Вашего учреждения. (Например: Тульский государственный университет).