СТАНДАРТ

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ОБЕСПЕЧИВАЮЩИХ ОКАЗАНИЕ УСЛУГ В СФЕРЕ ОБРАЗОВАНИЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИКТ

Москва 2011

Содержание

Введение

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 «Стандартизация в Российской Федерации. Основные положения».

Стандарт устанавливает единые требования по обеспечению безопасности данных в информационных системах, обеспечивающих оказание государственных (муниципальных) услуг и сервисов сферы образования, предоставляемых в электронном виде.

Настоящий стандарт предназначен для добровольного использования всеми заинтересованными лицами и участниками процессов перевода оказания государственных (муниципальных) услуг в электронную форму и преследует следующие цели:

- предоставить аналитикам и разработчикам информационных систем методику структурированного описания накопленного ими полезного опыта (т.н. «хороших практик») для его последующего использования в других регионах;
- обеспечить потенциальных пользователей стандарта единым понятийным аппаратом, обеспечивающим однозначную интерпретацию текста стандарта и упрощающим практическое применение изложенных практик и методик.

1 Область применения

Настоящий стандарт устанавливает требования обеспечения безопасности данных информационных систем, обеспечивающих оказание услуг в сфере образования с использованием информационно-коммуникационных технологий

Применение стандарта является добровольным. В соответствии с Федеральным законом «О техническом регулировании» от 27.12.2002 N 184-ФЗ стандарт является стандартом организации – Министерства образования и науки Российской Федерации.

Перечень терминов

Конфиденциальность информации	обязательное требование для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия её обладателя
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Уничтожение персональных данных	действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в

	результате которых уничтожаются материальные носители персональных данных
Обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
Информационная система персональных данных	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
Межсетевой экран или сетевой экран	комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации
Модель угроз	содержит системное изложение вероятных угроз безопасности ПДн при их обработке в ИС

Перечень сокращений

ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ИС	Информационная система
СЗПДн	Система защиты персональных данных
АС	Автоматизированная система
СЗИ	Система защиты информации
СОП	Сеть общего пользования
НСД	Несанкционированный доступ
СТР-К	Специальные требования и рекомендации по технической защите конфиденциальной информации
ПЭМИН	Побочные электромагнитные излучения и наводки
ЭП	электронная подпись
МЭ	Межсетевой экран или сетевой экран

2 Нормативные ссылки

При разработке стандарта использовалась следующая нормативная документация:

– Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»;

– Федеральный закон от 27.12.2009 г. № 363-ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных»;

– Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ), гл. 14;

– Указ Президента Российской Федерации от 3 декабря 2008 года №1715 «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций»;

– Указ Президента Российской Федерации от 16 августа 2004 г. №1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;

– Указ Президента Российской Федерации от 11 августа 2003 г. №960 «Вопросы Федеральной службы безопасности Российской Федерации»;

– Постановление Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 6 июля 2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства Российской Федерации от 16 марта 2009 г. №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

– Порядок проведения классификации информационных систем персональных данных. Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №55/86/20. Зарегистрирован в Минюсте России 3 апреля 2008 г., регистрационный №11462;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (полная редакция). Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. ДСП;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г;

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;

– Положение о методах и способах защиты информации в информационных системах персональных данных. Приказ ФСТЭК России от 5 февраля 2010 г. №58, зарегистрировано в Минюсте РФ 19 февраля 2010 г. №16456;

– Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. №149/6/6-622, 2008 г., ФСБ России;

– Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. № 149/54-144, 2008 г. ФСБ России;

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Приказ ФСБ России от 9 февраля 2005 г. №66 (зарегистрировано в Минюсте Российской Федерации 3 марта 2005 г. №6382);

– Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) от 16 июля 2010 г. №482 «Об утверждении образца формы уведомления об обработке персональных данных»;

– Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Приказ Роскомнадзора от 1.12.2009 г. №630. Зарегистрирован Минюстом России 28 января 2010 г. № 16095;

– Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных». Утверждён приказом Министерства связи и массовых коммуникаций Российской Федерации от 30.01.2010г. №18. Зарегистрирован Минюстом России 24 марта 2010 г., № 16717;

– Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден руководством 8 Центра ФСБ России 8 августа 2009 г. № 149/7/2/6-1173;

– Приказ Министерства экономического развития Российской Федерации от 30 апреля 2009г. №141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». (Утверждает типовую форму журнала учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля (приложение 4).

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Основные положения

3.1 Цель создания единых стандартов обеспечения безопасности данных информационных систем

Целью разработки единых стандартов обеспечения безопасности данных информационных систем, обеспечивающих оказание услуг в сфере образования в электронном виде, является предоставление единой методической основы и достижение упорядочения посредством установления положений для всеобщего и многократного применения, и создания в организациях – операторах управляемого процесса обработки персональных данных, исключающего (существенно затрудняющего) возможности неправомерного обращения с персональными данными, и таким образом, нанесению ущерба субъектам персональных данных.

3.2 Назначение создания единых стандартов обеспечения безопасности информационных систем

Настоящий стандарт разработан в целях исполнения Распоряжения Правительства от 17 декабря 2009 г. N 1993-р (в ред. распоряжения Правительства РФ от 07.09.2010 N 1506-р) и предназначен для определения единых требований по безопасности данных в информационных системах, обеспечивающих предоставление 7 первоочередных региональных и муниципальных услуг и сервисов в сфере образования, в том числе:

- Прием заявлений, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования (детские сады);
- Предоставление информации о порядке проведения государственной (итоговой) аттестации обучающихся, освоивших образовательные программы основного общего и среднего (полного) общего образования, в том числе в форме единого государственного экзамена, а также информация из баз данных субъектов Российской Федерации об участниках единого государственного экзамена и о результатах единого государственного экзамена;
- Предоставление информации об организации общедоступного и бесплатного дошкольного, начального общего, основного общего, среднего (полного) общего образования, а также дополнительного образования в общеобразовательных учреждениях, расположенных на территории субъекта Российской Федерации;
- Предоставление информации об организации начального, среднего и дополнительного профессионального образования;
- Предоставление информации о результатах сданных экзаменов, тестирования и иных вступительных испытаний, а также о зачислении в образовательное учреждение;

− Предоставление информации о текущей успеваемости учащегося, ведение электронного дневника и электронного журнала успеваемости;

− Предоставление информации об образовательных программах и учебных планах, рабочих программах учебных курсов, предметах, дисциплинах (модулях), годовых календарных учебных графиках.

4 Требования к обеспечению безопасности данных информационных систем

4.1 Требования к защите информации

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

− обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

− соблюдение конфиденциальности информации ограниченного доступа;

− реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается Федеральным законом о персональных данных (ФЗ 2006 г. № 152 «О персональных данных»).

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, используемые в целях защиты

информации методы и способы её защиты должны соответствовать указанным требованиям.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

4.2 Требования по информационной безопасности

Требования по обеспечению информационной безопасности при взаимодействии информационных систем между собой и/или с федеральными информационными ресурсами на информационные системы, обеспечивающие оказание услуг в сфере образования с использованием информационно-коммуникационных технологий:

4.2.1 Для защиты электронных документов от подделки при обмене данными между взаимодействующими организациями, рекомендуется использовать электронную подпись (ЭП), позволяющую криптографически преобразовывать информацию с использованием закрытого ключа электронной подписи и позволяющую идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

4.2.2 Условия и порядок использования ЭП при осуществлении информационного взаимодействия определяются законодательством Российской Федерации в области применения ЭП.

4.2.3 Подсистема информационной безопасности каждой информационной системы, подключаемой к системе взаимодействия, должна обеспечивать установленные законодательством Российской Федерации уровни защищенности информации, обрабатываемой в этой системе.

4.2.4 Все каналы связи системы взаимодействия, выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям к средствам криптографической защиты информации класса не ниже КСЗ и находящихся в пределах контролируемых зон участников взаимодействия.

4.2.5 Доступ к электронным сервисам информационных систем участников взаимодействия должен осуществляться с использованием сертифицированных средств межсетевого экранирования.

4.2.6 Администрирование и сопровождение оборудования, обеспечивающего криптографическую защиту каналов связи, должно производиться только участником взаимодействия либо уполномоченными им лицами.

4.2.7 Доступ посторонних лиц ко всем техническим средствам системы взаимодействия, каналам связи и поддерживающим системам (электропитания, вентиляции, кондиционирования и т.п.) в контролируемой зоне участника взаимодействия должен быть исключен.

4.2.8 В целях обеспечения защиты информации, содержащейся в информационных системах, подключенных к системе взаимодействия, участники информационного взаимодействия:

- обеспечивают при обслуживании информационных систем, подключенных к системе взаимодействия, исполнение установленных требований по информационной, производственной, технологической и противопожарной безопасности;
- осуществляют контроль доступа посторонних лиц к техническим средствам и каналам связи в контролируемой зоне участника взаимодействия, включая время проведения ремонтных работ и уборки помещений;
- обеспечивают обслуживание информационных систем, подключенных к системе взаимодействия, только лицами, имеющими право доступа к информации, содержащейся в указанных информационных системах;
- принимают необходимые и достаточные меры, исключающие доступ посторонних лиц к защищаемой (в т.ч. парольной и ключевой) информации, хранящейся на используемых и отчуждаемых носителях информации;
- осуществляют учет лиц, имеющих доступ к оконечному оборудованию, обеспечивающему криптографическую защиту каналов связи системы взаимодействия, расположенному в контролируемой зоне участника взаимодействия, а также лиц, имеющих возможность изменения конфигурации информационных систем данного участника взаимодействия, подключенных к системе взаимодействия.

4.2.9 В целях обеспечения полноценного функционирования системы взаимодействия и подключенных к ней информационных систем каждый участник взаимодействия:

- обеспечивает возможность оперативного переключения на резервный канал с сохранением функций обеспечения безопасности информации для всех каналов связи, выход из строя которых может существенно повлиять на доступность информационных систем, подключенных к системе взаимодействия;
- обеспечивает возможность оперативной замены оборудования, обеспечивающего криптографическую защиту каналов связи, используемых участником взаимодействия для осуществления информационного обмена в рамках системы взаимодействия, в случае выхода такого оборудования из строя.

4.2.10 При взаимодействии с системой должна осуществляться идентификация и аутентификация информационных систем поставщиков и потребителей по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов или с использованием криптографических методов.

4.2.11 Программными средствами электронного сервиса должны протоколироваться факты приема и отправки каждого информационного сообщения в рамках системы взаимодействия с указанием уникального в рамках электронного сервиса идентификатора сообщения, направления (вида) сообщения (прием или отправка), даты, времени, адресата и контрольной суммы сообщения.

Требования к защите персональных данных определены в Постановлении Правительства Российской Федерации от 17 ноября 2007 г. №781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

4.3 Требования к организационным мерам для обеспечения безопасности данных информационных систем

В целях обеспечения информационной безопасности каждый Оператор должен устанавливать ответственность и излагать подход государственного или муниципального учреждения к управлению информационной безопасностью, который должен содержать следующие положения:

- определение информационной безопасности, ее цели и сферы действия, а также значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;
- изложение намерений, поддерживающих цели и принципы информационной безопасности в соответствии с целями предоставления государственных (муниципальных) услуг в электронном виде;
- основание для установки целей контроля и мер контроля, включая структуру оценки риска и менеджмент риска;
- краткое изложение наиболее существенных для государственного или муниципального учреждения политик безопасности, принципов, стандартов и требований, включающее:

а) соответствие законодательным, регулятивным требованиям и договорным обязательствам;

б) требования в отношении обучения и осведомлённости в вопросах безопасности;

в) управление непрерывностью предоставления государственных (муниципальных) услуг в электронном виде;

г) ответственность за нарушения политики информационной безопасности;

- определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

- ссылки на документы, дополняющие положения об информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика информационной безопасности должна быть доведена до сведения пользователей в рамках всего государственного или муниципального учреждения в уместной, доступной и понятной форме.

Руководство учреждения должно активно поддерживать безопасность внутри организации посредством ясных указаний, демонстрированных обязательств, чётких постановок задач и осведомлённости об обязанностях по обеспечению информационной безопасности.

Руководство государственного или муниципального учреждения должно:

- обеспечить, чтобы цели обеспечения информационной безопасности были определены, удовлетворяли организационным требованиям и были интегрированы в соответствующие процессы;

- формулировать, пересматривать и утверждать политику информационной безопасности;

- пересматривать эффективность реализации политики информационной безопасности;

- обеспечивать чёткое управление и зримую поддержку руководством инициатив в деле обеспечения безопасности;

- предоставлять ресурсы для обеспечения информационной безопасности;

- утверждать распределение специфических ролей и обязанностей по информационной безопасности в организации;

- инициировать планы и программы по поддержанию осведомлённости об информационной безопасности;

- обеспечивать координацию реализации мер контроля за информационной безопасностью учреждения.

Руководство государственного или муниципального учреждения должно определять потребность в консультации специалистов внутри организации или со стороны по вопросам информационной безопасности, просматривать и координировать результаты консультации по всей организации.

В зависимости от масштаба учреждения такие обязанности должны выполняться специальным собранием руководства.

4.4 Требования к обязанностям Оператора

Оператор персональных данных обязан:

- провести инвентаризацию информационных ресурсов, обрабатываемых в ИС и определить перечень обрабатываемых ПДн;
- урегулировать правовые вопросы обработки (использования) ПДн (уточнение правовых оснований обработки ПДн, получение согласия субъектов на обработку, пересмотр (при необходимости) договоров с субъектами, установление сроков обработки ПДн и др.);
- оформить и направить в территориальный орган уполномоченного органа по защите прав субъектов ПДн уведомление об обработке ПДн (при необходимости);
- разработать модель угроз (на основании результатов обследования ИСПДн);
- провести классификацию ИСПДн с оформлением соответствующего акта;
- определить требования по защите ПДн при их обработке в ИСПДн в соответствии с присвоенным классом и результатами моделирования угроз;
- осуществить проектирование Системы защиты персональных данных (СЗПДн);
- реализовать проект на создание СЗПДн;
- провести оценку соответствия ИСПДн требованиям безопасности согласно присвоенному классу (в форме проверки готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации);
- организовать эксплуатацию ИСПДн в соответствии с требованиями безопасности и контроль соблюдения использования СЗИ.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

− недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

− возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

− постоянный контроль за обеспечением уровня защищённости информации.

4.5 Требования к конфиденциальности персональных данных

4.5.1 Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением:

− обработка ПДн осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПДн и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

− обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

− обработка ПДн осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПДн;

− обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

− обработка ПДн необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

− обработка ПДн осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;

− осуществляется обработка ПДн, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

4.5.2 Обеспечение конфиденциальности персональных данных не требуется:

− в случае обезличивания персональных данных;

− в отношении общедоступных персональных данных.

4.6 Требования к принципам обработки персональных данных

4.6.1 Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.6.2 Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.6.3 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.6.4 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.6.5 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.6.6 При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4.6.7 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.7 Требования к мерам по обеспечению безопасности персональных данных при их обработке

4.7.1 Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.7.2 Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

− применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

− применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

− оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

− учетом машинных носителей персональных данных;

− обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

− восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

− установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

− контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5 Требования к порядку классификации информационных систем персональных данных

Целью классификации ИСПДн является определение по её результатам перечня организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности персональных данных при их обработке в конкретной информационной системе.

Проведение классификации ИСПДн обусловлено необходимостью реализации дифференцированного подхода к обеспечению безопасности ПДн в зависимости от объема обрабатываемых ПДн и угроз безопасности им с целью минимизации затрат на защиту информационных систем персональных данных.

Классификация ИСПДн проводится операторами (государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и

(или) осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн).

Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных (операторами), а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

5.1 Порядок проведения классификации ис персональных данных

Исходные данные для классификации:

- категория обрабатываемых в информационной системе персональных данных – $X_{ПД}$;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – $X_{ПДн}$;
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в ИС;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств ИС.

5.2 Требования к определению категории персональных данных

Персональные данные (общая категория) - 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.

Общедоступные персональные данные - 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.

Специальные категории персональных данных - персональные данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

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

Установлены следующие **категории ПДн ($X_{ПД}$)**:

- **Категория 1** - ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- **Категория 2** - ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;
- **Категория 3** - персональные данные, позволяющие идентифицировать субъекта ПДн;
- **Категория 4** - обезличенные и (или) общедоступные ПДн.

Категория обрабатываемых персональных данных определяется оператором в зависимости от целей обработки персональных данных.

5.3 Требования к определению категории ИСПДн

5.3.1 ИС, обрабатывающие ПДн, делятся по объему ПДн ($X_{НПД}$) на:

- $X_{НПД}$ **=3**, если в ИС одновременно обрабатываются ПДн менее чем о 1000 субъектах ПДн или ПДн субъектов в пределах конкретной организации;
- $X_{НПД}$ **=2**, если в ИС одновременно обрабатываются ПДн о 1000 – 100000 субъектах ПДн или ПДн субъектов, работающих в отрасли экономики, в органе государственной власти, проживающих в пределах муниципального образования;
- $X_{НПД}$ **=1**, если в ИС одновременно обрабатываются ПДн более чем о 100000 субъектах ПДн или ПДн субъектов субъекта РФ или РФ в целом.

При установлении оператором показателя $X_{НПД}$, равнозначным критерием является принадлежность субъектов персональных данных конкретной организации (органу государственной власти), отрасли или административно-территориальному образованию.

ИС, обрабатывающие ПДн, делятся на типовые и специальные:

Типовые ИС - информационные системы, в которых требуется обеспечение только конфиденциальности ПДн;

Специальные ИС - системы, в которых вне зависимости от необходимости обеспечения конфиденциальности ПДн требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Оператор при обработке ПДн обязан принимать необходимые организационные и технические меры, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

5.3.2 В зависимости от структуры ИСПДн подразделяются на:

- Автономные Комплексы технических средств;
- Локальные информационные системы;
- Распределенные информационные системы.

Возможные режимы обработки ПДн в ИСПДн:

- Однопользовательские ИСПДн;
- Многопользовательские ИСПДн.

5.3.3 По наличию подключений к сетям общего пользования (СОП) ИСПДн подразделяются на:

- ИСПДн, имеющие подключение к сетям международного обмена;
- ИСПДн, не имеющие подключения к сетям международного обмена.
- По разграничение прав доступа ИСПДн подразделяются на:
- ИСПДн, без разграничения прав доступа;
- ИСПДн, с разграничением прав доступа.

5.3.4 По местонахождению ИСПДн подразделяются на:

- ИСПДн, все технические средства которых, находятся в пределах Российской Федерации;

- ИСПДн, технические средства которых, частично или целиком находятся за пределами Российской Федерации

5.3.5 В зависимости от последствий нарушений заданной характеристики безопасности ПДн, типовой ИС присваивается один из классов:

- **Класс 1** (К1) - ИС, для которых нарушения могу привести к значительным негативным последствиям для субъектов ПД;

- **Класс 2** (К2) - ИС, для которых нарушения могут привести к негативным последствиям для субъектов ПД;

- **Класс 3** (К3) - ИС, для которых нарушения могут привести к незначительным негативным последствиям для субъектов ПД;
- **Класс 4** (К4) - ИС, для которых нарушения не приводят к негативным последствиям для субъектов ПД.

Класс типовой ИС выбирается по таблице (Таблица 1 - Выбор класса типовой ИС):

Таблица 1 - Выбор класса типовой ИС

Категория ПДн ($X_{ПД}$)	Показатель $X_{НПД}$ (объем $X_{ПД}$)		
	3 (менее 1тысячи)	2 (1-100 тысяч)	1 (более 100 тысяч)
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Класс специальной ИС определяется на основе модели угроз.

5.3.6 Рекомендации по классификации специальных ИСПДн

При определении требований по обеспечению безопасности персональных данных в специальных ИСПДн необходимо оценить возможность наступления и степень негативных последствий для субъектов ПДн, которые могут наступить в случае нарушения безопасности ПДн по следующей вербальной шкале:

- не приводят к негативным последствиям для субъектов;
- могут привести к незначительным негативным последствиям;
- могут привести к негативным последствиям;
- могут привести к значительным негативным последствиям.

Уровень требований по обеспечению безопасности специальных ИСПДн рекомендуется устанавливать на уровне требований, предъявляемых к типовым ИСПДн эквивалентного (соответствующего) класса с учётом результатов моделирования угроз.

5.3.7 Классификация сложных ИСПДн

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

Если классифицируемая АС интегрируется в состав вычислительной сети или системы, то классификации подлежит образуемая в результате интеграции

вычислительная сеть. Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС. Исключением является случай их объединения посредством межсетевого экрана (МЭ), когда каждая объединяющаяся АС может сохранять свой класс защищенности.

При разделении информационной системы при помощи межсетевых экранов на отдельные части для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.

Подключение информационной системы к информационной системе другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов.

5.3.8 Оформление результатов классификации ИСПДн

Результаты классификации информационных систем оформляются соответствующим актом оператора.

В акте классификации необходимо привести подробное описание всех исходных данных, используемых для классификации, с соответствующим обоснованием.

В качестве образца акта классификации целесообразно использовать Форму акта классификации АС (СТР-К, приложение Ж).

5.3.9 Порядок пересмотра класса ИСПДн

Класс информационной системы может быть пересмотрен:

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

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

6 Требования по созданию системы защиты персональных данных

Безопасность ПДн при их обработке в ИС обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации, а также используемые в ИС информационные технологии. Выбор и реализация методов и способов защиты информации в ИС осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности ПДн (модели угроз) и в зависимости от класса ИС.

Мероприятия по обеспечению безопасности персональных данных должны сочетать в себе реализацию правовых, организационных и технических мер защиты, причем все они одинаково значимы, а невыполнение одних требований может свести на нет результаты реализации других.

Применение технических мер защиты информации без правового урегулирования в организации – операторе вопросов обработки персональных данных никогда не сможет решить проблему обеспечения их безопасности.

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ по созданию ИСПДн.

Требуемый уровень безопасности персональных данных при их обработке в ИСПДн достигается обеспечением:

- локализации персональных данных;
- счётности субъектов и объектов ИСПДн;
- доверенности конфигурации и настроек ИСПДн;
- целостности всех элементов ИСПДн;
- подконтрольности всех действий субъектов;
- документированности всех событий в ИСПДн.

6.1 Требования к методам защиты ПДн

6.1.1 Правовые методы защиты ПДн

Требования к правовым методам включают в себя:

- правовую регламентацию порядка сбора, использования, предоставления и уничтожения ПДн;
- распределение полномочий между субъектами;
- нормативно-правовой контроль использования ПДн;
- установление ответственности за нарушения.
- Требования к организационно-административным методам включают в себя:

- формирование системы управления ПДн, в том числе управления доступом к ПДн (разграничение и контроль доступа к ПДн);
- регламентацию деятельности персонала по использованию ПДн;
- регламентацию порядка взаимодействия пользователей и администраторов ИС;
- контроль над деятельностью персонала.
- Требования к аппаратно-программным методам включают в себя:
- идентификация и аутентификация пользователей;
- обеспечение целостности ПДн;
- регистрация событий безопасности;
- межсетевое экранирование;
- антивирусная защита;
- защита каналов передачи ПДн.

6.1.2 Организационные методы защиты ПДн

Организационные методы предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации, в том числе:

- ограничение допуска персонала к ПДн (допуск персонала к ПДн на основании списка, утвержденного оператором или уполномоченным лицом и учёт лиц, допущенных к работе с ПДн в ИСПДн);
- учёт всех носителей ПДн с помощью их любой маркировки и с занесением учётных данных в журнал (учётную карточку);
- учёт применяемых СЗИ, эксплуатационной и технической документации к ним;
- обучение лиц, использующих СЗИ, правилам работы с ними;
- организация физической защиты средств обработки ПДн, помещений и носителей ПДн;
- контроль соблюдения использования СЗИ, предусмотренных эксплуатационной и технической документацией;
- организация системы реагирования на инциденты, связанные с нарушениями конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

6.1.3 Технические методы защиты ПДн

Технические методы предусматривают применение на объекте информатизации программно-технических средств и способов защиты информации, в том числе:

- средств защиты информации от НСД;

- специализированных средств антивирусной защиты;
- средств межсетевого экранирования;
- средств обнаружения вторжений;
- средств криптографической защиты (при необходимости);
- средств защиты от ПЭМИН (при необходимости).

Приложение А
Проект нормативного правового акта об утверждении стандарта безопасности данных информационных систем

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

_____
(субъект РФ)

ПОСТАНОВЛЕНИЕ

№_____ ___.___.201_ г.
(дата)

О стандарте безопасности данных информационных систем Министерства образования и науки (субъекта РФ)
Распоряжения Правительства от 17 декабря 2009 г. N 1993-р

В соответствии с Федеральным законом от 06.10.2003г. № 131 -ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Уставом [наименование муниципального образования] [наименование субъекта РФ]
ПОСТАНОВЛЯЮ:

Утвердить прилагаемые «Единые стандарты, определяющие требования к обеспечению безопасности данных в соответствии с законодательством Российской Федерации на информационные системы, обеспечивающие оказание услуг в сфере образования с использованием ИКТ» Министерства образования и науки (субъекта РФ) по исполнению Распоряжения Правительства от 17 декабря 2009 г. N 1993-р.

1. Отделу организационного обеспечения образования:

- Направить в Управление Министерства юстиции Российской Федерации по (субъекту РФ) копию настоящего постановления.

– Направить настоящее постановление в агентство связи и массовых коммуникаций (субъекта РФ) для официального опубликования.

– Разместить настоящее постановление на официальном портале органов государственной власти (субъекта РФ) .

2. Отделу правового обеспечения образования обеспечить включение настоящего постановления в электронную базу данных «ГАРАНТ» и «КонсультантПлюс».

3. Контроль за выполнением настоящего постановления возложить на заместителя министра - начальника управления по контролю и надзору за соблюдением законодательства и качеством образования министерства образования и науки (субъекта РФ) .

4. Настоящее постановление вступает в силу по истечении десяти дней со дня его официального опубликования.

Министр _____