МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«БЕЛОЯРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 1»

Приложение №2
к приказу МАОУ «Белоярская СОШ №1»
От 06.10.2021г. № 222/1-од

Утверждаю
Директор МАОУ «Белоярская СОШ №1»
_____ Е.А. Балеевских
«___» _____ 2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

п. Белоярский
2021г.

Содержание

запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Системный администратор – сотрудник учреждения, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Список контроля доступа (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля производства, разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Структурное подразделение – структурное подразделение учреждения с самостоятельными функциями, задачами и ответственностью.

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Удостоверяющий центр – автоматизированная система, включающая в себя аппаратно-программные средства, нормативно-методическую документацию и пользователей.

Узел – совокупность ЛВС МАОУ «БЕЛОЯРСКАЯ СОШ №1», расположенных в пределах одной контролируемой зоны.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность – достоверность и полноту информации и методов ее обработки.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации

информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководителем учреждения.

4.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ общества, корректировка моделей угроз и нарушителя.
- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей общества, а также повышать трудоемкость технологических процессов обработки информации.
- Контроль эффективности принимаемых защитных мер.
- Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4.3. Соответствие ПБ действующему законодательству

Правовую основу политик составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, МАОУ «БЕЛОЯРСКАЯ СОШ №1» и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

4.4. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию политик возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;
- в части, касающейся доведения правил политик до сотрудников МАОУ «БЕЛОЯРСКАЯ СОШ №1», а также иных лиц (см. область действия настоящей политики) – на администратора информационной безопасности;
- в части, касающейся исполнения правил политики, – на каждого сотрудника МАОУ «БЕЛОЯРСКАЯ СОШ №1», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

4.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников МАОУ «БЕЛОЯРСКАЯ СОШ №1»» в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по

- анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных процессов.
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.
- принятие руководством МАОУ «БЕЛОЯРСКАЯ СОШ №1» остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности МАОУ «БЕЛОЯРСКАЯ СОШ №1» и оценено их влияние на достижение целей деятельности МАОУ «БЕЛОЯРСКАЯ СОШ №1».

4.7.2. Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

- разработка плана обработки рисков ИБ;
- реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;
- реализация программ по обучению и осведомленности ИБ;
- обнаружение и реагирование на инциденты безопасности;
- обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. МАОУ «БЕЛОЯРСКАЯ СОШ №1» принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

4.7.3. Методы оценивания информационных рисков

Оценка информационных рисков МАОУ «БЕЛОЯРСКАЯ СОШ №1» выполняется по следующим основным этапам:

- идентификация и количественная оценка информационных ресурсов, значимых для работы МАОУ «БЕЛОЯРСКАЯ СОШ №1»;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы МАОУ «БЕЛОЯРСКАЯ СОШ №1» подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

4.8.5. Политика защиты АРМ

4.8.5.1. Назначение

Настоящая Политика определяет основные правила и требования по защите конфиденциальной информации МАОУ «БЕЛОЯРСКАЯ СОШ №1» от неавторизованного доступа, утраты или модификации.

4.8.5.2. Положения политики

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами предприятия, (согласно занимаемой должности), а именно: «Инструкция по обращению с носителями конфиденциальной информации», «Перечень сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом внедрения автоматизированных систем финансовых расчетов, и в соответствии с лицензионным соглашением с его правообладателем.

Действия администратора информационной безопасности и системного администратора при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями администратора информационной безопасности;
- Должностными обязанностями программиста.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС МАОУ «БЕЛОЯРСКАЯ СОШ №1», а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

4.9.3. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник МАОУ «БЕЛОЯРСКАЯ СОШ №1» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности МАОУ «БЕЛОЯРСКАЯ СОШ №1», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный МАОУ «БЕЛОЯРСКАЯ СОШ №1» в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники МАОУ «БЕЛОЯРСКАЯ СОШ №1» несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники МАОУ «БЕЛОЯРСКАЯ СОШ №1»» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

5. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники МАОУ «БЕЛОЯРСКАЯ СОШ №1» должны руководствоваться следующими законодательными нормативными документами:

5.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

- Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);
- Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 1 июля 1994 г. № 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»);
- Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300, в редакции Указа Президента РФ от 10 января 2000 г. № 24);
- Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

5.2. Законы Российской Федерации

- Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности» (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.);
- Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ (с изменениями от 26 января, 20 февраля, 12 августа 1996 г., 24 октября 1997 г., 8 июля, 17 декабря 1999 г., 16 апреля, 15 мая, 26 ноября 2001 г., 21 марта, 14, 26 ноября 2002 г., 10 января, 26 марта, 11 ноября, 23 декабря 2003 г., 29 июня, 29 июля, 2, 29, 30 декабря 2004 г., 21 марта, 9 мая, 2, 18, 21 июля 2005 г., 3, 10 января, 2 февраля, 3, 30 июня, 27 июля, 3 ноября, 4, 18, 29, 30 декабря 2006 г., 26 января, 5 февраля, 20 апреля, 26 июня, 19, 24 июля, 2, 25 октября, 4, 29 ноября, 1, 6 декабря 2007 г.);
- Закон РоссийскойФедерации от 27 ноября 1992 г. № 4015-I «Об организации страхового дела в Российской Федерации» (с изменениями от 31 декабря 1997 г., 20 ноября 1999 г., 21 марта, 25 апреля 2002 г., 8, 10 декабря 2003 г., 21 июня, 20 июля 2004 г., 7 марта, 18, 21 июля 2005 г., 17 мая, 8, 29 ноября 2007 г.);
- Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности» (с изменениями от 22 августа 1995 г., 18 апреля 1996 г., 24 января 1998 г., 7 ноября, 27 декабря 2000 г., 6 августа, 30 декабря 2001 г., 25 июля 2002 г., 10 января 2003 г., 10 мая, 29 июня, 22 августа, 29 декабря 2004 г., 1 апреля, 9 мая 2005 г., 2 февраля, 25 октября, 4, 18 декабря 2006 г., 26 апреля, 18 октября 2007 г.);
- Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г., 29 июня, 22 августа 2004 г., 2 декабря 2005 г., 24 июля 2007 г.);
- Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (с изменениями от 8 ноября 2007 г.);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г.);
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями от 23 декабря 2003 г., 22 августа, 2 ноября 2004 г., 9 мая 2005 г., 2 февраля, 3 марта, 26 июля, 29 декабря 2006 г., 9 февраля, 24 июля 2007 г.);
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» (с изменениями от 30 декабря 1999 г., 7 ноября 2000 г., 30 декабря 2001 г., 7 мая, 25 июля 2002 г., 10 января, 30 июня 2003 г., 22 августа 2004 г., 7 марта 2005 г., 15 апреля, 27 июля 2006 г., 5, 24 июля, 4 декабря 2007 г.);
- Федеральный закон от 9 января 1996 г. № 2-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О защите прав потребителей» и Кодекс РСФСР об административных правонарушениях» (с изменениями от 30 декабря 2001 г., 25 октября 2007 г.);
- Федеральный закон от 9 января 1996 г. № 3-ФЗ «О радиационной безопасности населения» (с изменениями от 22 августа 2004 г.);
- Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке» (с изменениями от 7 ноября 2000 г., 30 июня 2003 г., 22 августа 2004 г., 14 февраля 2007 г.);

- Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изменениями от 27 мая, 25 июня 1998 г., 9 февраля, 15, 18 марта, 9 июля 1999 г., 9, 20 марта, 19 июня, 7 августа, 17 ноября, 29 декабря 2001 г., 4, 14 марта, 7 мая, 25 июня, 24, 25 июля, 31 октября 2002 г., 11 марта, 8 апреля, 4, 7 июля, 8 декабря 2003 г., 21, 26 июля, 28 декабря 2004 г., 21 июля, 19 декабря 2005 г., 5 января, 27 июля, 4, 30 декабря 2006 г., 9 апреля, 10 мая, 24 июля, 4 ноября, 1, 6 декабря 2007 г.);
- Федеральный закон от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (с изменениями от 21, 31 июля, 17 декабря 1998 г., 19 ноября 1999 г., 10 апреля 2000 г., 26 июля, 8 августа, 27 ноября 2001 г., 25 июня, 25 июля 2002 г., 10 января, 30 июня, 8 декабря 2003 г., 26 апреля, 29 июня 2004 г., 18 июля, 29 декабря 2006 г., 24 июля 2007 г.);
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);
- Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля, 31 декабря 2005 г., 27 июля, 4, 29 декабря 2006 г., 5 февраля, 19 июля, 4, 8 ноября, 1, 6 декабря 2007 г.).

5.3. Указы и распоряжения президента Российской Федерации

- Указ Президента Российской Федерации от 14 января 1992 г. № 20 «О защите государственных секретов Российской Федерации»;
- Указ Президента Российской Федерации от 7 октября 1993 г. № 1607 «О государственной политике в области охраны авторского права и смежных прав»;
- Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» (с изменениями от 17 января 1997 г., 1 сентября 2000 г.);
- Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);
- Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изменениями от 25 июля 2000 г.);
- Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации» (с изменениями от 16 августа 1995 г., 4 января 1996 г., 28 мая 1997 г., 29 ноября 2004 г.);
- Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г., 6 июня, 10 сентября 2001 г., 29 мая 2002 г., 3 марта 2005 г., 11 февраля 2006 г., 24 декабря 2007 г.);
- Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);
- Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» (с изменениями от 10 января 2000 г.);

- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006 г.);
- Указ Президента Российской Федерации от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.);
- Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» (с изменениями от 12 октября 2007 г.).

5.4.Постановления и распоряжения правительства Российской Федерации

- Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности» (с изменениями от 5 мая, 3 сентября, 2 октября 2007 г.);
- Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г., 26 января 2007 г.);
- Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;
- Постановление Правительства РФ от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.);
- Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» (с изменениями от 15 января 2008 г.);
- Постановление Правительства Российской Федерациот 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного

- Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282);
- Приказ Минэнерго Российской Федерации от 13 января 2003 г. № 6 «Об утверждении Правил технической эксплуатации электроустановок потребителей»;
- Приказ Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст «О введении в действие межгосударственных стандартов»;
- Руководящий документ РД 50-082-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения», 1989 г.;
- Руководящий документ РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов», 1990 г.;
- Руководящий документ РД 50-680-88 «Методические указания. Автоматизированные системы. Основные положения», 1988 г.;
- Рекомендация Р 50-34.119-90 «Рекомендации. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения», 1990 г.;
- Рекомендация Р 50.4.002-2000 «Рекомендации по аккредитации. Инспекционный контроль за деятельностью в системе сертификации», 2000 г.;
- Рекомендация МИ 2377-98 «Рекомендация. Государственная система обеспечения единства измерений. Разработка и аттестация методик выполнения измерений», 1998 г.;
- Методические указания МИ 1317-86 «Методические указания. Государственная система обеспечения единства измерений. Результаты и характеристики погрешности измерений. Формы представления. Способы использования при испытаниях образцов продукции и контроля их параметров», 1986 г.;
- Строительные нормы и правила СНиП 23-03-2003 «Защита от шума» (введены в ействие постановлением Госстроя РФ от 30 июня 2003 г. № 136);
- Письмо Министерства промышленности и энергетики Российской Федерации и Министерства регионального развития Российской Федерации от 29 ноября 2006 г. № АР-6893/08, 12325-ЮТ/08;
- Постановление Главного государственного санитарного врача Российской Федерации от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» (с изменениями от 25 апреля 2007 г.);
- Нормы пожарной безопасности НПБ 88-2001 «Установки пожаротушения и сигнализации. Нормы и правила проектирования» (утверждены приказом ГУГПС МВД РФ от 4 июня 2001 г. N 31, с изменениями от 31 декабря 2002 г.);
- Строительные нормы и правила СНиП 2.01.15-90 «Инженерная защита территорий, зданий и сооружений от опасных геологических процессов. Основные положения проектирования» (утверждены постановлением Госстроя СССР от 29 декабря 1990 г. № 118);
- Строительные нормы и правила СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование» (приняты постановлением Госстроя РФ от 26 июня 2003 г. № 115);
- Строительные нормы и правила СНиП 21-01-97 «Пожарная безопасность зданий и сооружений» (утверждены постановлением Минстроя РФ от 13 февраля 1997 г. № 18-7, с изменениями от 3 июня 1999 г., 19 июля 2002 г.).

5.6.Государственные стандарты

- ГОСТ 2.051-2006 «Единая система конструкторской документации. Электронные документы. Общие положения» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст);
- ГОСТ 2.101-68 «Единая система конструкторской документации. Виды изделий» (утвержден Госстандартом СССР в декабре 1967 г.);
- ГОСТ 2.102-68 «Единая система конструкторской документации. Виды и комплектность конструкторских документов» (утвержден постановлением Госстандарта СССР от 28 июня 1968 г. № 1029, изменениями от 22 июня 2006 г.);
- ГОСТ 2.103-68 «Единая система конструкторской документации. Стадии разработки» (введен в действие Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);
- ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 118-ст);
- ГОСТ 2.111-68 «Единая система конструкторской документации. Нормоконтроль» (утвержден Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);
- ГОСТ 18321-73 «Статистический контроль качества. Методы случайного отбора выборок штучной продукции» (введен в действие постановлением Государственного комитета стандартов Совета Министров СССР от 9 января 1973 г. № 33);
- ГОСТ 2.109-73 «Единая система конструкторской документации. Основные требования к чертежам» (утвержден постановлением Госстандарта СССР от 27 июля 1973 г. № 1843, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.118-73 «Единая система конструкторской документации. Техническое предложение» (введен постановлением Госстандарта СССР от 28 февраля 1973 г. № 500, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.119-73 «Единая система конструкторской документации. Эскизный проект» (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 501, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.120-73 «Единая система конструкторской документации. Технический проект» (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 502, с изменениями от 22 июня 2006 г.);
- ГОСТ 19.001-77 «Единая система программной документации. Общие положения» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ 19.101-77 «Единая система программной документации. Виды программ и программных документов» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268, с изменениями от июня 1981 г.);
- ГОСТ 19.102-77 «Единая система программной документации. Стадии разработки» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ 19.103-77 «Единая система программной документации. Обозначения программ и программных документов» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);
- ГОСТ Р 50779.10-2000 (ИСО 3534.1-93) «Статистические методы. Вероятность и основы статистики. Термины и определения» (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);

- ГОСТ Р 50779.11-2000 (ИСО 3534.2-93) «Статистические методы. Статистическое управление качеством. Термины и определения» (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);
- ГОСТ 19.104-78 «Единая система программной документации. Основные надписи» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);
- ГОСТ 19.105-78 «Единая система программной документации. Общие требования к программным документам» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.106-78 «Единая система программной документации. Требования к программным документам, выполненным печатным способом» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.201-78 (СТ СЭВ 1627-79) «Единая система программной документации. Техническое задание. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от июля 1981 г.);
- ГОСТ 19.202-78 (СТ СЭВ 2090-80) «Единая система программной документации. Спецификация. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);
- ГОСТ 19.401-78 «Единая система программной документации. Текст программы. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от июля 1982 г.);
- ГОСТ 19.402-78 «Единая система программной документации. Описание программы» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.501-78 «Единая система программной документации. Формуляр. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351);
- □□ГОСТ 19.502-78 «Единая система программной документации. Описание применения. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);
- ГОСТ 19.601-78 «Единая система программной документации. Общие правила дублирования, учета и хранения» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);
- ГОСТ 19.602-78 «Единая система программной документации. Правила дублирования, учета и хранения программных документов, выполненных печатным способом» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);
- ГОСТ 19.603-78 «Единая система программной документации. Общие правила внесения изменений» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);
- ГОСТ 19.604-78 «Единая система программной документации. Правила внесения изменений в программные документы, выполненные печатным способом» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);
- ГОСТ 19.403-79 «Единая система программной документации. Ведомость держателей подлинников» (введен в действие постановлением Госстандарта СССР от 28 июня 1979 г. № 2335);

- ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования» (утвержден постановлением Госстандарта СССР от 28 января 1987 г. № 124, с изменениями от 24 марта 1989 г., 26 декабря 1990 г.);
- ГОСТ 2.004-88 «Единая система конструкторской документации. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ» (утвержден постановлением Госстандарта СССР от 28 ноября 1988 г. № 3843);
- ГОСТ 2.125-88 «Единая система конструкторской документации. Правила выполнения эскизных конструкторских документов» (утвержден постановлением Госстандарта СССР от 22 июля 1988 г. № 2714);
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем» (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 664, с изменениями от 29 декабря 1990 г.);
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы"(утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);
- ГОСТ 28195-89 «Оценка качества программных средств. Общие положения» (утвержден постановлением Госстандарта СССР от 28 июля 1989 г. № 2507);
- ГОСТ 28388-89 «Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 20 декабря 1989 г. № 3903);
- ГОСТ 28806-90 «Качество программных средств. Термины и определения» (утвержден постановлением Госстандарта СССР от 25 декабря 1990 г. № 3278);
- ГОСТ 19.701-90 (ИСО 5807-85) «Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 декабря 1990 г. № 3294);
- ГОСТ 19781-90 «Единая система программной документации. Обеспечение систем обработки информации программное. Термины и определения» (введен в действие постановлением Госстандарта СССР от 27 августа 1990 г. № 2467);
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утвержден постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399);
- ГОСТ 2.503-90 «Единая система конструкторской документации. Правила внесения изменений» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 апреля 1990 г. № 1031, с изменениями от 22 июня 2006 г.);
- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания» (утвержден постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469);
- ГОСТ 22505-97 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний» (утвержден постановлением Госстандарта России от 28 августа 1998 г. № 337);

- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем» (утвержден постановлением Комитета стандартизации и метрологии СССР от 17 февраля 1992 г. № 161);
- ГОСТ Р ИСО/МЭК ТО 9294-93 «Информационная технология. Руководство по управлению документированием программного обеспечения» (утвержденпостановлением Госстандарта России от 20 декабря 1993 г. № 260);
- ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению» (утвержден постановлением Госстандарта России от 28 декабря 1993 г. № 267);
- ГОСТ 2.001-93 «Единая система конструкторской документации. Общие положения» (введен в действие постановлением Госстандарта России от 3 марта 1994 г. № 50, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.123-93 «Единая система конструкторской документации. Комплектность конструкторских документов на печатные платы при автоматизированном проектировании» (введен в действие постановлением Госстандарта России от 2 марта 1994 г. № 44);
- ГОСТ Р ИСО 9127-94 «Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов» (принят постановлением Госстандарта России от 10 октября 1994 г. № 242);
- ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (принят постановлением Госстандарта России от 15 мая 1996 г. № 308);
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);
- ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний», Госстандарт России, 1995 г.;
- ГОСТ 2.105-95 «Единая система конструкторскойдокументации. Общие требования к текстовым документам» (введен в действие постановлением Госстандарта России от 8 августа 1995 г. № 426, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.602-95 «Единая система конструкторской документации. Ремонтные документы» (введен в действие постановлением Госстандарта России от 29 февраля 1996 г. № 131, с изменениями от 22 июня 2006 г.);
- ГОСТ 2.106-96 «Единая система конструкторской документации. Текстовые документы» (введен в действие постановлением Госстандарта России от 13 ноября 1996 г. № 620, с изменениями от 22 июня 2006 г.);
- ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 450);
- ГОСТ Р ИСО 9001-2001 «Системы менеджмента качества. Требования» (утвержден постановлением Госстандарта России от 15 августа 2001 г. № 333-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ 2.780-96 «Единая система конструкторской документации. Обозначения условные графические. Кондиционеры рабочей среды, емкости гидравлические и пневматические» (утвержден постановлением Госстандарта РФ от 7 апреля 1997 г. № 121);

- ГОСТ 2.784-96 «Единая система конструкторской документации. Обозначения условные графические. Элементы трубопроводов» (введен в действие постановлением Госстандарта России от 7 апреля 1997 г. № 124);
- ГОСТ Р 50923-96 «Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения» (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 451);
- ГОСТ 22505-97 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний» (введен в действие постановлением Госстандарта России от 28 августа 1998 г. № 337);
- ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);
- ГОСТ Р 51171-98 «Качество служебной информации. Правила предъявления информационных технологий на сертификацию» (введен в действие постановлением Госстандарта России от 12 мая 1998 г. № 184);
- ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);
- ГОСТ Р ИСО/МЭК 12207-99 «Информационная технология. Процессы жизненного цикла программных средств» (принят и введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 675-ст);
- ГОСТ Р 51320-99 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех» (введен в действие постановлением Госстандарта России от 22 декабря 1999 г. № 655-ст);
- ГОСТ Р 50779.72-99 (ИСО 2859-2-85) «Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 2. Планы выборочного контроля отдельных партий на основе предельного качества LQ» (введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 694-ст);
- ГОСТ Р 51319-99 «Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний» (введен в действие постановлением Госстандарта России от 28 декабря 1999 г. № 795-ст);
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», Госстандарт России, 2000 г.;
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования», Госстандарт России, 2000 г.;
- ГОСТ Р ИСО/МЭК 17025-2006 «Общие требования к компетентности испытательных и калибровочных лабораторий» (введен в действие постановлением Госстандарта России от 27 декабря 2006 г. № 506-ст);
- ГОСТ Р 40.002-2000 «Система сертификации ГОСТ Р. Регистр систем качества. Основные положения» (принят постановлением Госстандарта РФ от 13 апреля
- 2000 г. № 107-ст);
- ГОСТ Р ИСО/МЭК 65-2000 «Общие требования к органам по сертификации продукции» (утвержден постановлением Госстандарта РФ от 7 апреля 2000 г. № 96-ст);
- ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к

электромагнитным помехам. Требования и методы испытаний» (введен в действие постановлением Госстандарта России от 26 декабря 2000 г. № 417-ст);

- ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь»(принят постановлением Госстандарта России от 15 августа 2001 г. № 332-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ Р ИСО 9004-2001 «Системы менеджмента качества. Рекомендации по улучшению деятельности» (принят постановлением Госстандарта России от 15 августа 2001 г. № 334-ст, с изменениями от 7 июля 2003 г.);
- ГОСТ Р 50948-2001 «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности» (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);
- ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности» (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);
- ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);
- ГОСТ Р ИСО/МЭК 15408-2-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности» (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);
- ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» (принят и введен в действие постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);
- ГОСТ Р 40.003-2005 «Система сертификации ГОСТ Р. Регистр систем качества. Порядок сертификации систем менеджмента качества на соответствие ГОСТ Р ИСО 9001-2001 (ИСО 9001:2000)» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 14 ноября 2005 г. № 287-ст);
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст);