Описание системы обеспечения информационной безопасности (СОИБ)

1. Исследование объекта СОИБ

Основными направлениями деятельности министерства информационных технологий и связи является осуществление функции по реализации государственной политики, оказанию государственных услуг и управлению государственным имуществом в сфере информационных технологий и связи. Организация активно развивает информационные технологии в Ростовской области, а так же сопровождает уже существующие, исполняя 17 приказ ВСТЭК Российской Федерации от 11 февраля 2013 года.

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначено структурное подразделение «Отдел защиты информации», ответственные за защиту информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- Неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- Неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);
- Неправомерного блокирования информации (обеспечение доступности информации).

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

- Разработка системы защиты информации информационной системы;
- Внедрение системы защиты информации информационной системы;

- Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;
- Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
- Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- Идентификацию и аутентификацию субъектов доступа и объектов доступа;
- Управление доступом субъектов доступа к объектам доступа;
- Ограничение программной среды;
- Защиту машинных носителей информации;
- Регистрацию событий безопасности;
- Антивирусную защиту;
- Обнаружение (предотвращение) вторжений;
- Контроль (анализ) защищенности информации;
- Целостность информационной системы и информации;
- Доступность информации;
- Защиту среды виртуализации;
- Защиту технических средств;

Модели угроз безопасности и модели нарушителя

17 приказ ВСТЭК Российской Федерации от 11 февраля 2013 года гласит что:

Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз безопасности информации и содержит:

- типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;
- возможные способы реализации угроз безопасности информации.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Определить требования и порядок создания СОИБ, в соответствии с которыми проводятся разработка СОИБ и ее приемка при вводе в действие.

В состав СОИБ входят следующие компоненты и подсистемы, тесно интегрированные между собой и с другими компонентами ИТ-инфраструктуры:

- подсистема защиты периметра сети;
- подсистема обеспечения безопасности межсетевых взаимодействий;
- подсистема мониторинга и аудита безопасности;
- подсистема обнаружения и предотвращения атак;
- подсистема резервного копирования и восстановления данных;
- подсистема анализа защищенности и управления политикой безопасности;
- подсистема контроля целостности данных;
- криптографическая подсистема;
- инфраструктура открытых ключей;
- подсистема защиты от вредоносного ПО;
- подсистема фильтрации контента и предотвращения утечки конфиденциальной информации;
- подсистема установки обновлений ПО;
- подсистема администрирования безопасности.

Процедура создания и сопровождения СОИБ.

Процедура создания и сопровождения системы обеспечения информационной безопасности включает в себя следующие этапы:

- предварительное обследование объекта информатизации с целью определения его текущего состояния, выработки требований по обеспечению безопасности, документирование информационной системы;
- создание Концепции обеспечения информационной безопасности;
- рабочее проектирование СОИБ (включая документацию на используемые средства защиты, план ввода СОИБ в эксплуатацию и организационно-распорядительных документов по обеспечению информационной безопасности), планирование обучения пользователей и обслуживающего персонала;
- поставка программных и технических средств защиты информации, ввод СОИБ в эксплуатацию, настройка всех компонентов и подсистем, проведение приемо-сдаточных испытаний;
- обучение пользователей и обслуживающего персонала;
- аттестация объекта информатизации по требованиям безопасности информации в системе сертификации ФСТЭК (в случае необходимости);
- сопровождение СОИБ, техническая поддержка, аутсорсинг информационной безопасности.

Целью проектирования системы обеспечения информационной безопасности является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях организации.

Техническое проектирование СОИБ является необходимым условием для реализации комплексного подхода к обеспечению ИБ. В отсутствии технического проекта возможно лишь

реализация фрагментарных мер и механизмов безопасности, за счет которых в современных условиях невозможно решение основных вопросов обеспечения информационной безопасности.

Порядок контроля и приемки

Для обеспечения соответствия внедряемой СОИБ необходимо предусмотреть на стадии ввода в действие СОИБ следующие виды испытаний:

- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания.

Испытания проводятся в соответствии с программой и методикой испытаний, разработанными до начала испытаний. Программа и методика испытаний должны устанавливать необходимый и достаточный объем испытаний и охватывать реализуемую функциональность и виды обеспечений.

Приемка СОИБ на соответствие проводится комиссией в составе уполномоченных представителей Министерства и ФСТЭК.

Предварительные испытания

- Предварительные испытания проводятся в соответствии с разработанными Программой и методикой испытаний.
- По результатам предварительных испытаний Исполнителем предоставляется Акт приемки в опытную эксплуатацию СОИБ.

Опытная эксплуатация

Опытная эксплуатация СОИБ проводится с целью определения фактических значений количественных и качественных характеристик и готовности персонала к работе в условиях функционирования СОИБ.

При необходимости изменения проектной и эксплуатационной документации, возникшие в период опытной эксплуатации, вносятся в нее без выпуска извещения на изменение и утверждаются Министерства и ФСТЭК.

На этапе опытной эксплуатации Исполнителем предоставляется следующая документация:

1) Рабочий журнал опытной эксплуатации, с выявленными в период проведения опытной эксплуатации замечаниями, в котором фиксируются:

а) произошедшие сбои и/или отказы, ложные срабатывания компонентов СОИБ;

б) дополнительные настройки компонентов СОИБ, вносимые по итогам отладки конфигурации и анализа регистрируемых событий;

2) Протокол об исправлении ошибок.

Опытная эксплуатация должна быть проведена в течение не более (трех) недель с даты проведения предварительных испытаний.

Приемочные испытания

Приемочные испытания проводятся в соответствии с разработанными Программой и методикой испытаний.

По результатам приемочных испытаний Исполнителем представляется следующая документация:

1) Протокол приемочных испытаний, который должен содержать:

а) назначение испытаний;

б) состав технических и программных средств, используемых при испытаниях;

в) указания методик, в соответствии с которыми проводились испытания;

г) условия проведения испытаний и характеристики исходных данных;

д) оцениваемые показатели, результаты испытаний и оценка выполнения программы испытаний;

е) обобщенные результаты испытаний;

ж) выводы о результатах испытаний и соответствии созданной системы требованиям данного ТЗ.

2) Акт приемки в промышленную эксплуатацию СОИБ.

По результатам приемочных испытаний Исполнителем предоставляется акт приемки в промышленную эксплуатацию СОИБ с протоколом приемочных испытаний, утверждаемый Заказчиком и Исполнителем.

Проектирование СОИБ.

Целью проектирования СОИБ является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях организации. Техническое проектирование СОИБ является необходимым условием для реализации комплексного подхода к обеспечению ИБ.

Технических проект СОИБ включает в себя:

- Спецификацию на комплекс технических средств СОИБ;
- Спецификацию на комплекс программных средств СОИБ.

Разработка технического проекта СОИБ, осуществляется на основе Приказа ФСТЭК России от 15.02.2017 N 27, а также существующей Концепции обеспечения ИБ.

Создание СЗПДн, пусть и в рамках более масштабной СОИБ, требовало соблюдения всех установок, заложенных в федеральное законодательство и методические документы регуляторов. Для того, чтобы адекватно реализовывать такие установки именно там, где это необходимо, потребовалось произвести уточнение границ объекта защиты. На основе определения, приведенного в Федеральном законе № 152-ФЗ «О персональных данных» были четко выделены и зафиксированы те элементы защищаемой ИС, которые образуют информационную систему персональных данных (ИСПДн). Как и следовало ожидать, границы ИСПДн не совпали с границами ИС в целом. Это обстоятельство позволило отказаться от некоторых избыточных технических решений, поскольку необходимость обеспечивать выполнение требований по защите ПДн в масштабах всей ИС сменилась необходимостью реализовать эти требования только в рамках ИСПДн как ее составной части. Дальнейшее проектирование СОИБ велось с учетом наличия в ней СЗПДн, а так же принципа «СОИБ – для защиты ИС в целом, СЗПДн – для защиты ИСПДн, сформированной в составе ИС».

Важный вопрос, который потребовалось решить совместно с оператором – установление необходимости обработки ПДн и определение их перечня. В рамках проектируемой СОИБ/СЗПДн необходимость обработки персональных данных продиктована как технологией обслуживания клиентов, так и положениями федерального закона № 126-ФЗ «О связи», устанавливающего возможность обработки телекоммуникационной компанией информации об абонентах. Положения статьи 53 упомянутого закона легли в основу перечня персональных данных, обрабатываемых в защищаемой ИСПДн, зафиксировавшего состав ПДн и правовые основания для их обработки.

Во главу угла при выполнении работ по защите ПДн ставится классификация ИСПДн. Разумеется, при создании СОИБ, имеющей в своем составе СЗПДн, это мероприятие в отношении последней имеет статус обязательного. Группа проектирования совместно со специалистами заказчика пришла к выводу, что защищаемая ИСПДн является специальной, поскольку в ней вне зависимости от необходимости обеспечения конфиденциальности ПДн требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности. Составленная в соответствии с методическими документами ФСТЭК частная модель угроз безопасности ПДн позволила, во-первых, адекватно определить класс системы и, во-вторых, выделить именно те угрозы, которые являются актуальными и от которых следует защищаться.

Собственно техническое проектирование СОИБ/СЗПДн проведено в классическом, хорошо зарекомендовавшем себя стиле, на основе выбора оптимальных вариантов реализации тех или иных подсистем (сервисов) информационной безопасности. Проблем с выбором сертифицированных СЗИ, отвечающих перечню актуальных угроз ПДн, так же не возникло: на рынке представлено достаточно большое число решений, и проектировщикам осталось подобрать наиболее подходящее по требованиям и условиям применения.

Особенностью рассматриваемого примера явилась разработка двух групп технических решений по обеспечению ИБ. Первая группа решений ориентировалась на защиту центрального ядра системы и головного филиала оператора, вторая – на защиту типового регионального филиала (их в структуре бизнеса насчитывается девять).

Знание существующей у заказчика системы мер по защите информации позволило использовать уже имеющиеся СЗИ и нормативные документы во вновь создаваемой системе обеспечения безопасности и тем самым снизить конечную стоимость СОИБ и длительность ее разработки, а так же избежать излишних трудностей для оператора при внедрении новых, ранее не использовавшихся СЗИ.

Важное место в проекте отведено организационным мерам, для чего были разработаны необходимые нормативные документы. Поскольку система защиты создавалась не в «чистом поле», важным моментом явилась гармоничная интеграция вновь разрабатываемых документов в существующую нормативную базу заказчика. Подробная информация об имеющихся в организации документах в области защиты информации не только обеспечила построение целостной взаимодополняющей нормативной базы, но и позволила использовать существующие положения при подготовке новых документов по защите информации, включая ПДн. Разумеется, особенности выполнения проекта, связанные с «инкапсуляцией» СЗПДн в СОИБ, внесли свой вклад в нормативную составляющую: помимо документов, обязательных к разработке и определенных требованиями ФСТЭК, были подготовлены дополнительные руководства, например – частная политика ИБ защищаемой системы.

Описание процедуры ввода СОИБ в действие.

Целью работ на стадии "Ввод в действие" является физическая реализация системы и передача ее в промышленную эксплуатацию. Основанием для начала работ по вводу АС служит готовность рабочей документации; они проводятся в соответствии с планом-графиком, утвержденным организацией-заказчиком и согласованным с организацией-разработчиком и соисполнителями. План-график работ по внедрению может предусматривать поочередный ввод системы.

Основные этапы работ: подготовка объекта к вводу АС, наладка и испытания системы, опытная эксплуатация, приемо-сдаточные испытания.

Подготовка объекта к вводу АС включает в себя организационно-технические работы (в том числе строительные работы и модернизацию технологического оборудования), комплектацию системы, монтаж оборудования АС. Комплектация системы производится в установленном порядке в соответствии с заказными спецификациями, разработанными на стадии рабочего проектирования. Монтаж оборудования АС производится специализированными организациями, привлекаемыми заказчиком на основании и в соответствии с рабочей документацией на систему. Завершение всех работ по монтажу технических средств АС в полном объеме фиксируется комиссией из представителей заказчика и исполнителя в виде двустороннего акта.

Наладка и испытания АС охватывают отладку комплекса технических средств системы, ее программного обеспечения и проведение предварительных испытаний системы до ее передачи в опытную эксплуатацию. В результате предварительных испытаний определяются количественные и качественные характеристики выполнения отдельных функций, выявляется возможность совместного функционирования всех подсистем и характеристики системы в целом.

Опытная эксплуатация АС проводится силами заказчика с участием исполнителя для проверки работоспособности системы и готовности оперативного и ремонтного персонала к работе в условиях промышленной эксплуатации системы. На этапе опытной эксплуатации выполняются следующие работы: включение системы в опытную эксплуатацию, определение эксплуатационных характеристик системы, дополнительная отладка программ и устройств, коррекция эксплуатационной документации. В ходе опытной эксплуатации осуществляется устранение ошибок в программах и внесение исправлений в техническую и эксплуатационную документацию.

Приемо-сдаточные испытания проводятся с целью проверки соответствия созданной системы общим техническим требованиям на АС, требованиям, содержащимся в ТЗ на создание системы, и приемки ее в промышленную эксплуатацию. Приемо-сдаточные испытания АС организуются и проводятся заказчиком, который совместно с исполнителем представляет комиссии следующую техническую документацию на систему: ТЗ, протокол опытной эксплуатации, проекты программ и методику проведения приемосдаточных испытаний, эксплуатационную документацию. Комиссия после изучения представленных материалов принимает решение о готовности (неготовности) АС для проведения приемо-сдаточных испытаний.

После окончания приемо-сдаточных испытаний составляется акт, в котором формируется заключение о соответствии (несоответствии) рассматриваемой АС предъявляемым к ней требованиям и целесообразности (нецелесообразности) передачи ее в промышленную эксплуатацию.