

Вопрос 6. Документация на системы защиты информации автоматизированных систем

1. Организационно-распорядительная документация

Защита информации включает в себя комплекс организационных и технических мер, направленных на обеспечение безопасности свойств информации (конфиденциальность, целостность, доступность). Очевидно, что базисом системы защиты информации являются организационные меры, которые должны быть задокументированы в форме приказов, перечней, регламентов, инструкций, положений, руководств, регламентов, стандартов и т.д. Но и технические меры также предваряются разработкой документации, например: технический паспорт, модель угроз, техническое задание на разработку системы защиты информации, технический проект и т.д.

Разработка организационно-распорядительной и технической документации, отвечающей требованиям безопасности информации, регламентирующей процессы системы защиты информации на всех этапах её существования, сложная и трудоёмкая задача. Во многих организациях или отсутствует документация, или это набор документов — **шаблонов, наличие которых не влияет на процессы, связанные с деятельностью по защите информации.**

Перечень необходимых документов может меняться в зависимости от специфики объектов информатизации, на которых планируется обрабатывать защищаемую информацию. Первоначально определяются защищаемые объекты, назначаются лица, ответственные за организацию защиты информации, устанавливаются угрозы безопасности защищаемой информации, разрабатывается техническое задание на создание защищённого объекта информатизации. На следующих этапах выполняется проектирование, ввод в действие и сопровождение объекта. На каждом из этапов разрабатывается соответствующая документация: эскизный проект; технический проект; рабочая документация, материалы по аттестации объекта информатизации и т.д.

Основой для построения системы защиты информации являются требования законодательства РФ, нормативные акты ФСТЭК и ФСБ России, контрактные требования организации, а также условия ведения бизнеса, выраженные на основе идентификации защищаемых активов, построения модели нарушителей и угроз.

При формировании и разработке организационно-распорядительной и технической документации по защите информации задачами Руководства организации являются: инициализация, поддержка и контроль выполнения процессов. Степень выполнения указанной деятельности со стороны руководства организации определяется осознанием необходимости обеспечения информационной безопасности (ИБ) организации. Осознание необходимости обеспечения ИБ организации проявляется в использовании руководством организации бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса организации с допустимыми рисками. Осознание необходимости обеспечения ИБ является внутренним побудительным мотивом руководства организации постоянно **инициировать, поддерживать, анализировать и контролировать систему обеспечения информационной безопасности**, в отличие от ситуации, когда решение о выполнении указанных видов деятельности либо принимается в результате возникших проблем, либо определяется внешними факторами.

При разработке задокументированной политики информационной безопасности организации обычно рассматриваются четыре группы процессов (в соответствии с требованиями ГОСТ Р 51583-2014, ГОСТ Р ИСО/МЭК 27001-2006 и СТО БР ИББС-1.0-2014):

- планирование системы обеспечения информационной безопасности («планирование»);
- реализация системы обеспечения информационной безопасности («реализация»);
- мониторинг и анализ системы обеспечения информационной безопасности («проверка»);
- поддержка и улучшение системы обеспечения информационной безопасности («совершенствование»).

При документировании процессов рекомендуется разрабатывать следующие виды документов:

- **1 уровень:** документы, содержащие положения корпоративной политики (концептуальные, декларирующие или устанавливающие общие требования);
- **2 уровень:** документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности предприятия, планы работ по обеспечению ИБ;
- **3 уровень:** документы, содержащие требования, правила по выполнению технологических процессов (инструкции; матрицы доступа; методические указания; документы, содержащие требования к конфигурациям).
- **4 уровень:** документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ (журналы; карточки и т.д.) <1>

<1> Научно-технический центр «Велес» Статья: Разработка организационно-распорядительной документации (URL: <https://isafety.ru/?p=821>).



Документальное обеспечение ИБ АСУ <1>

<1> Домуховский Н. Презентация: Комплексная система обеспечения информационной безопасности АСУ ТП. М., 2015.

Примерный перечень организационно-распорядительных документов по защите персональных данных при их автоматизированной обработке может выглядеть следующим образом.

Уровень документов	Наименование документа	Процесс	Требования НМД по защите ПДн
1 уровень (Концептуальные, декларирующие или устанавливающие общие требования)		Политика в отношении обработки персональных данных информационной системы персональных данных «XXXXXX»	1;4 Статья 18.1 152-ФЗ «О персональных данных»
	Частная модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «XXXXXX»	1;4	Статья 19 152-ФЗ «О персональных данных», ПП РФ от 1.11.2012 № 119
	Перечень сведений о субъектах персональных данных, подлежащих защите при их обработке в информационной системе персональных данных «XXXXXX»	1;4	Статья 14.4 149-ФЗ «Об информации...», п 6 ПП РФ от 1.11.2012 № 119
	Акт классификации информационной системы персональных данных «XXXXXX»	1;4	ПП РФ от 1.11.2012 № 119, п 14.2, 14.3 Приказа ФСТЭК от 18.02.2013 № 17
	Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных «XXXXXX»	1;2	ФЗ «О персональных данных», ПП РФ от 1.11.2012 № 119
2 уровень Документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности организации, планы работ по обеспечению ИБ	План контролируемой зоны головного офиса	1,4	п. 13 ПП РФ от 1.11.2012 № 119, СТР-К, утв. приказом Гостехкомиссии России от 30 августа 2002г. № 282
	План действий в непредвиденных ситуациях и требования к обучению действиям в непредвиденных ситуациях.	1,2	
	Годовой план. Мероприятия по организации защиты персональных данных в информационной системе персональных данных «XXXXXX»	1-4	

Регламент. Физическая защита информационной системы персональных данных «XXXXXX»	2	Приказ ФСТЭК России от 11.02.2013 № 21СТР-К, утв. приказом Гостехкомиссии России от 30 августа 2002г. № 282
Регламент. Физическая защита информационной системы персональных данных «XXXXXX»	2	
Регламент. Управление доступом пользователей к ресурсам информационной системы персональных данных «XXXXX» и ресурсам сети интернет.	2	Приказ ФСТЭК России от 11.02.2013 № 21СТР-К, утв. приказом Гостехкомиссии России от 30 августа 2002г. № 282
Регламент. Порядок проведения ремонта и обслуживания технических средств информационной системы персональных данных «XXXXXX» и вывода их из эксплуатации.	2-4	Приказ ФСТЭК России от 11.02.2013 № 21СТР-К, утв. приказом Гостехкомиссии России от 30.08.2002 № 282
Регламент. Порядок проведения резервного копирования данных в информационной системе персональных данных «XXXXXX».	2	
Регламент. Объемы и периодичность проверок, контрольных испытаний информационной системы персональных данных «XXXXXX»	3	
Регламент. Порядок обеспечения безопасности обработки персональных данных при возникновении нештатных ситуаций в информационной системе персональных данных «XXXXXX»	2	
Регламент. Порядок управление инцидентами информационной безопасности в информационной системе персональных данных «XXXXXX»	2	
Регламент. Организация антивирусного контроля в информационной системе персональных данных «XXXXXX»	2,3	

3 уровень	Матрица разграничения доступа к ресурсам информационных систем персональных данных		
	Документы, содержащие требования, правила по выполнению технологических процессов: инструкции; матрицы доступа; методические указания; документы, содержащие требования к конфигурациям.	Инструкция по мерам безопасности при работе с криптографическими ключами.	2
		Инструкция пользователю информационной системы персональных данных	2
		Стандарт организации информационная система персональных данных «XXXXXX» программно-аппаратные средства АРМ и серверов. Требования	2-3 Приказ ФСТЭК России от 11.02.2013 № 21 СТР-К, утв. приказом Гостехкомиссии России от 30.08.2002 № 282
		Перечень работников, допущенных к обработке персональных данных	2-3 п. 13 ПП РФ от 1.11.2012 № 1119
		Положение о видеонаблюдении и звуковом контроле.	2-3 ТК РФ, 3-нРФ от 11.03.1992 № 2487-1
4 уровень		Технический паспорт на информационную систему персональных данных	2-3 СТР-К, утв. приказом Гостехкомиссии России № 7.2/02.03.2001
	Документы, содержащие свидетельства о выполненной деятельности по обеспечению ИБ	Ежеквартальные (ежемесячные) отчёты по ИБ информационных систем персональных данных	2-3
		Обязательства сотрудников о неразглашении сведений конфиденциального характера (персональных данных)	2-3
		Журнал учёта документов для служебного пользования	2-3 ПП РФ от 3 ноября 1994 г. № 1233
		Журнал позземплирного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.	2-3 Приказ ФАПСИ от 13 июня 2001 г. № 152
		Журнал учета посещения объектов информатизации сторонними лицами	2-3 —
		Журнал учета посещения серверного помещения	2-3 —

Журнал учета инцидентов информационной безопасности в информационной системе персональных данных «XXXXXX»	2-3	—
Журнал учета обращений субъектов персональных данных	2-3	—
Акты о стирании конфиденциальной информации, уничтожении машинных носителей конфиденциальной информации, машинных документов, числящихся на учете	2-3	
Журнал учёта резервного копирования	2-3	—
Журнал учета машинных носителей	2-3	ПП РФ от 3 ноября 1994 г. № 1233

Документация <1>

<1> Научно-технический центр «Велес» Статья: Разработка организационно-распорядительной документации (URL: <https://isafety.ru/?p=821>).

Более подробно с составом некоторых документов можно ознакомиться в модуле 5.

2. Эксплуатационная документация

Процесс создания технической документации на АСУ представляет собой совокупность взаимосвязанных стадий (этапов) работ, а именно:

№	Стадия	Рекомендуемые к разработке документы	Выполняемые работы
1.	Формирование требований к АС	отчеты по НИР	- обследование объекта и обоснование необходимости создания АСУ - формирование требований пользователя к АС - оформление отчёта о выполненной работе и заявки на разработку АСУ ТП (тактико-технического задания)
2.	Разработка концепции АС	концепция АС	- изучение объекта - проведение необходимых научно-исследовательских работ - разработка вариантов концепции АС, удовлетворяющего требованиям пользователя - оформление отчёта о выполненной работе
3.	Техническое задание (ТЗ)	техническое задание	Разработка и утверждение технического задания на создание АСУ
4.	Эскизный проект (ЭП)	- пояснительная записка к эскизному проекту - документы, аналогичные ТП, но с наименьшей детализацией	- разработка предварительных проектных решений по системе и её частям - разработка документации на АСУ ТП и её части
5.	Технический проект (ТП)	- описание автоматизируемых функций - описание постановки задач (комплекса задач) - описание информационного обеспечения системы - описание организации информационной базы - описание программного обеспечения - описание алгоритма (проектной процедуры)	- разработка проектных решений по системе и её частям - разработка документации на АСУ и её части - разработка и оформление документации на поставку изделий для комплектования АСУ и (или) технических требований (технических заданий) на их разработку - разработка заданий на проектирование в смежных частях проекта объекта автоматизации
6.	Рабочая документация (РД)	- описание технологического процесса обработки данных - программа и методика испытаний - руководство пользователя - паспорт	- разработка рабочей документации на систему и её части - разработка или адаптация программ
7.	Ввод в действие		- подготовка объекта автоматизации к вводу АСУ ТП в действие - подготовка персонала - комплектация АС поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями) - строительно-монтажные работы - пусконаладочные работы - проведение предварительных испытаний - проведение опытной эксплуатации - проведение приёмочных испытаний
8.	Сопровождение АС		- выполнение работ в соответствии с гарантийными обязательствами - послегарантийное обслуживание

Виды эксплуатационной документации

Полный перечень документов, разработка которых необходима при создании автоматизированной системы (АСУ ТП), указан в ГОСТ 34.201- 89.

1) Формирование требований к АСУ

Согласно ГОСТ 34.601-90, формирование требований к АСУ является первой стадией жизненного цикла автоматизированной системы управления. Эта стадия определяет направление дальнейших шагов по разработке системы – составления концепции, интеграции имеющихся и создаваемых средств ПО, предварительной оценки стоимости работ.

Этапы

Формирование требований к автоматизированной системе предполагает выполнение следующих этапов работ (в соответствии с указанным выше ГОСТ):

1. Анализ объекта, подтверждение необходимости создания АС.
2. Выработка пользовательских требований к автоматизированной системе.
3. Составление отчета о выполненной работе и оформление тактико-технического задания (заявки на разработку АС).

Документы

Результатом выполнения первого этапа является один из документов:

- Аналитический отчет;
- Техничко-экономическое обоснование;
- Тактико-техническое задание;
- Заявка на разработку автоматизированной системы управления.

Действия

В рамках анализа объекта автоматизации необходимо произвести сбор и изучение данных о его функционировании, а также сведений об организации, структуре производства. В качестве источника информации могут быть использованы регламенты и устав компании, а также государственные нормативно-правовые акты. Также в ходе исследования анализируют уже имеющиеся на объекте автоматизированные системы и степень интеграции создаваемой АС с ними. Производится сбор и анализ информации об отечественных и импортных аналогах автоматизированной системы, которую нужно разработать.

На основании полученных сведений выявляют пользовательские и функциональные требования к АСУ.

Отчет, составленный по результатам анализа, содержит следующие данные:

- Информация об объекте;
- Цель и методика обследования;
- Основные параметры: технические, технологические, эксплуатационные, конструктивные;
- Пользовательские требования;
- Указания по внедрению, степень интеграции;
- Сфера применения;
- Подтверждение экономической целесообразности разработки автоматизированной системы управления;
- Предложения и прогнозы развития объекта.

2) Разработка концепции АСУ

Согласно ГОСТ 34.601-90 одной из стадий создания АСУ является разработка концепции АС. На данной стадии, исходя из результатов обследования объекта автоматизации, разрабатывается концепция АСУ.

На стадии разработки выполняются следующие работы:

- получение первичных сведений об объекте автоматизации;
- проведение необходимых научно-исследовательских работ;
- разработка вариантов концепции АС;
- оформление итогового отчёта о проделанной работе.

Концепция АС – первоначальный и основной документ, описывающий подходы к построению автоматизированной системы предприятия. Концепция автоматизированной системы управления описывает предполагаемый результат, который будет достигнут от внедрения АСУ. **Так же концепция даёт ответы на такие вопросы как:**

- насколько эффективно будет организовано взаимодействие подразделений организации;
- как повысится результативность деятельности подразделений организации;
- и другие.

Наличие утвержденной концепции очень сильно облегчает дальнейшее взаимодействие между заказчиком и исполнителем - особенно для больших корпоративных заказчиков, так как для ответов подавляющего большинства вопросов можно сослаться на утвержденную концепцию.

3) Техническое задание на автоматизированную систему (АСУ)

Техническое задание на автоматизированную систему управления (ТЗ на АС) – основной документ, предъявляющий требования к создаваемой автоматизированной системе и устанавливающий порядок, в соответствии с которым будет проводиться разработка АСУ ТП и ее прием при вводе в эксплуатацию.

ТЗ может разрабатываться как на всю систему, так и на составные части:

- составные части АС (по ГОСТ 34.602);
- технические средства (компоненты) входящие в состав АС (по ГОСТ ЕСКД);
- программные средства (компоненты) входящие в состав АС (по ГОСТ ЕСПД).

Современное техническое задание на разработку автоматизированной систему АСУ должно разрабатываться с учётом требований современного уровня развития науки и технического прогресса, а так же с учётом лучших мировых практик в области предъявляемых требований на разрабатываемые автоматизированные системы управления АСУ.

Структура и разделы

ТЗ на АСУ может содержать следующие разделы:

- 1) общие сведения;
- 2) назначение и цели создания (развития) системы;
- 3) характеристика объектов автоматизации;
- 4) требования к системе;
- 5) состав и содержание работ по созданию АС;
- 6) порядок контроля и приемки системы;
- 7) требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие;
- 8) требования к документированию;
- 9) источники разработки.

Допускается разделение указанных разделов на подразделы. В зависимости от функционального назначения и условий, в которых будет функционировать АСУ, допускаются следующие действия с разделами ТЗ:

- ввод дополнительных разделов (подразделов);
- исключение разделов (подразделов);
- объединение разделов (подразделов).

В отдельных случаях допускается оформление и разработка ТЗ в виде приложения.

4) Эскизный проект

Эскизным проектом называют пакет конструкторской документации, создаваемый на стадии разработки автоматизированной системы. Цель создания этих документов – установить принципиальные, конструктивные решения, представить их для ознакомления с принципами работы и устройством разрабатываемой системы. Также этим проектом может рассматриваться несколько вариантов устройства АСУ.

Эскизный проект на автоматизированную систему разрабатывают перед техническим проектом или вместе с ним. Эта документация может и не оформляться в случае, если ею не может быть предоставлено никаких новых данных – ее необходимость устанавливается тех заданием.

Разработка эскизного проекта

Эскизный проект программного продукта или автоматизированной системы разрабатывается в соответствии со следующими этапами:

1. **Декомпозиция АС на комплексы и проработка архитектурных решений**
На этом этапе выбирается уровень автоматизации. Анализируются аналогичные системы. Выбирается схема взаимодействия оператора с системой, оцениваются алгоритмы и процессы обработки данных. По итогам этого этапа разработки эскизного проекта получают более точные требования к АС, а также функциональную внешнюю спецификацию ее комплексов
2. **Разработка операционной среды или требований к ней**
На этом этапе составляются требования к конфигурации оборудования и операционной среды, выбирается операционная система
3. **Разработка методов анализа качества системы**, с соответствующими метриками показателей качественной оценки, необходимыми для проведения испытаний
4. **Планирование перспектив создания АСУ**
На данном этапе выбираются основные концепции технологий разработки, уточняются требования к программным средствам, создается база данных по автоматизации и контролю работ, а также проходит оформление пояснительной записки.

Перечень документов эскизного проекта

- Эскизный проект на автоматизированную систему состоит из такой документации как:
 - Ведомость ЭП
 - Пояснительная записка
 - Структурная схема комплекса техсредств
 - Функциональная схема структуры автоматизированной системы управления
 - Перечень заданий, составленных для разработки специальных дополнительных техсредств

- Схема автоматизации
- Технические задания по разработке дополнительных средств.

Эскизный проект может не содержать некоторых документов, приведенных в данном списке, а также может быть дополнен иной документацией. **Полный список документов выбирается в зависимости от специфики конкретной системы, требований заказчика и регламентируется техническим заданием.**

5) Технический проект на автоматизированную систему (АСУ ТП)

Технический проект на АСУ – это пакет документации, который описывает окончательные решения по проектированию автоматизированной системы управления.

Информация, представленная в техническом проекте, должна быть достаточной для того, чтобы на ее основе составить рабочий проект. Технический проект автоматизированной системы должен содержать данные об общесистемных проектных решениях, алгоритмах решения задач, расчет экономических показателей будущей автоматизированной системы. Технический проект на АСУ составляется на основании требований технического задания (ТЗ).

Этапы разработки

Разработка технического проекта регламентируется государственным стандартом ГОСТ 34.601-90. Этим документом предусматриваются следующие этапы работ:

- Разработка общих проектных решений по АСУ и проектных решений для отдельных ее составляющих
- Разработка проектных документов на систему и ее элементы
- Разработка и оформление пакета документов на поставку комплектующих системы или техзадания на их разработку
- Разработка проектных заданий на смежные части проекта.

Технический проект на автоматизированную систему разрабатывается по определенным стадиям. Сначала проходит составление общего проекта, а на его основании составляются технические проекты первой и второй очереди. Причем работы по разработке документов первой и второй очереди могут вестись независимо друг от друга.

Что входит в пакет документов?

Список необходимых документов, которые включает тех проект, регламентируется государственным стандартом, требования к их содержанию описываются в руководящей документации по стандартизации. Согласно этим стандартам, технический проект на АСУ состоит из таких документов:

- Ведомости ТП
- Схема организационной структуры
- Схема функциональной структуры
- Ведомости покупаемых дополнительных изделий
- Перечня данных и сигналов на входе
- Перечня сигналов на выходе
- Задания по разработке дополнительных разделов, необходимых для разработки АСУ
- Пояснительной записки, с планом подготовительных работ для ввода АСУ в использование

- Описаний функций автоматизации, поставленной задачи, информационного обеспечения, организации базы информации, системы кодировки и классификации, информационных массивов, комплектов техсредств, ПО, проектных процедур, структуры организации

- Плана расположения
- Ведомости на материалы и оборудование
- Локального сметного расчета

Технический проект на автоматизированную систему должен содержать все эти документы, если иное не предусмотрено ТЗ. <1>

<1> Статья: Документация на автоматизированную систему (АСУ ТП) (URL: <http://www.swrit.ru/dokumentaciya-na-as.html>).