Министерство науки и высшего образования

Российской Федерации

Федеральное Государственное

Автономное Образовательное Учреждение

Высшего Образования

Национальный ядерный университет «МИФИ»

Кафедра: «Финансовый Мониторинг»

Частное Техническое задание на разработку системы защиты

Студент Монастырский М. О.

Группа С21-703

Москва 2023г.

Оглавление

Принятые сокращения и определения

Система защиты информации (СЗИ) – средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.[1]

Информационная система(ИС)- совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[2]

ФСТЭК - Федеральная служба по техническому и экспортному контролю

ТЗ – Техническое задание

ЧТЗ – Частное Техническое задание

НПА – Нормативно-правовой Акт

ИБ – Информационная Безопасность

АС – Автоматизированная система, то же что ИС

[1] Согласно ст. 2 Закона РФ "О государственной тайне" от 21.07.1993 N 5485-1
[2] Согласно ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 02.11.2023) "Об информации, информационных технологиях и о защите информации"
Статья 2. Основные по

Введение

Создание всякой сложной системы вне зависимости от ее предназначения есть продукт множества сложных процессов, протекающих параллельно и независимо друг от друга, от исхода каждого такого процесса по отдельности зависит конечный результат в целом. Именно поэтому, для достижения высокой организованности всех задействованных процессов необходимо заранее иметь документ, который позволит всем участникам процесса выстроить образ результата, подкрепленный научно-техническим, организационным и нормативно правовым фундаментом. Только понимание результата может помочь всем участникам выстроить процессы взаимодействия во время разработки и стать базой для эксплуатации разрабатываемых систем. Таким документом может стать техническое задание, поскольку содержит всю необходимую информацию.

В настоящей работе будут рассмотрены организационно-правовые и технические вопросы составления частного технического задания на разработку системы защиты информации, включая такие необходимые для этого процессы как: Построение актуальной модели угроз защиты информации в соответствии с методикой ФСТЭК, построение модели нарушителя в соответствии с вышеупомянутой методикой, и прохождение аттестации ИС, а именно присвоение класса защищенности ИС при вводе таковой в эксплуатацию, также будут рассмотрены конкретные сертифицированные уполномоченными органами, и рассмотрен процесс разработки собственных решений в области защиты информации.

Основание разработки

Исходные данные модернизируемого объекта

Для определения исходных данных защищаемого объекта необходимо произвести оценку угроз безопасности исходя из требований Методики.

Учредить специальную комиссию, отвечающую рекомендациям согласно приложению 2 Методики, а именно:

> «В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от: подразделения по защите информации (обеспечения информационной безопасности); подразделения, ответственного за цифровую трансформацию (ИТ-специалистов); подразделения, ответственного за эксплуатацию сетей связи; подразделения, ответственного за эксплуатацию автоматизированных систем управления; подразделений обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов). 36 Состав экспертов по решению обладателя информации или оператора может быть дополнен или уточнен с учетом особенностей области деятельности, в которой функционируют системы и сети. В частности, для оценки угроз безопасности информации, реализация которых может привести к финансовым рискам, рекомендуется привлекать дополнительно специалистов экономических (финансовых) подразделений обладателя информации или оператора. Для организации работы экспертной группы рекомендуется определять специалиста по защите информации (обеспечению информационной безопасности), имеющего стаж работ не менее трех лет и практический

опыт оценки информационных рисков. В экспертную группу для оценки угроз безопасности информации рекомендуется включать специалистов, имеющих опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации. Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, так как это может негативным образом повлиять на результат определения угроз безопасности информации. В состав экспертной группы должны входить не менее трех экспертов»

В ходе оценки группа должна пройти следующие этапы:

Рисунок 1 Этапы проведения оценки согласно Методике

В качестве базы все этапы основываются на следующих документах:

- Список актуальных угроз (https://bdu.fstec.ru/)

- Открытые списки векторов атак, такие как ATT&CK
- Техническое задание на создание компьютерной сети, частные технические задания на создание ее компонентов
- Данные предоставляемые Оператору поставщиками услуг, в случае если инфраструктура организации основана на IaaS и базируется удаленно в облаке на базе сторонней организации
- И другие имеющие ценность в области ИБ

На первом этапе производится анализ потенциальных негативных последствий от реализации возможных угроз, например:

«1)если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является нарушение конфиденциальности персональных данных, в результате которого будут нарушены права субъектов персональных данных и соответствующие законодательные акты; 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является разлив нефти из нефтепровода, повлекший наступление экологического ущерба; 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредоставление услуг связи абонентам, повлекшее наступление ущерба в социальной сфере; 4) для оператора по переводу денежных средств одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств, в результате которого возможны финансовые и репутационные риски.»

Примеры типовых целей и пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации составляются согласно Приложениям 6 и 7 Методики.

На втором этапе проводится инвентаризация систем и сетей, для определения уязвимостей и векторов атаки специфичных для инфраструктуры предприятия.

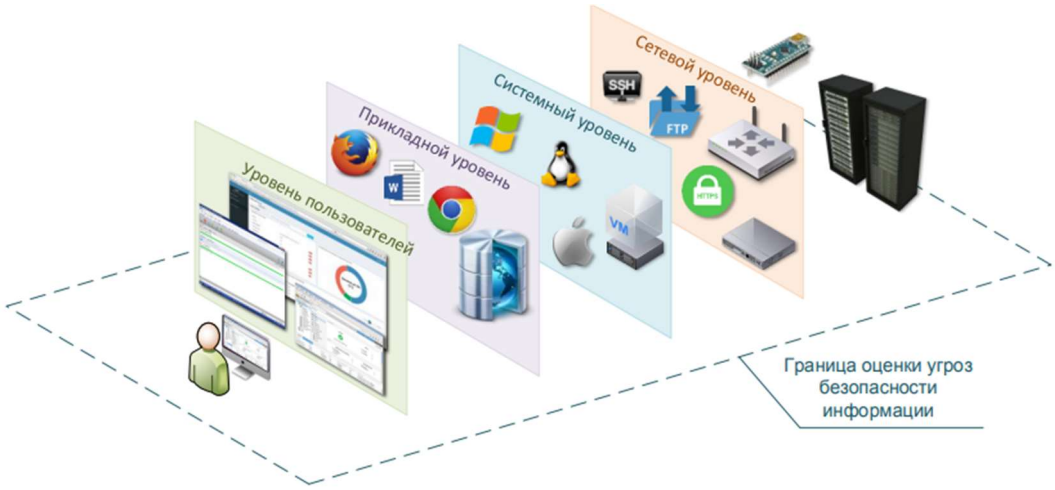

Рисунок 2. Уровни оценки инфраструктуры

На третьем этапе производится обобщение полученной информации и построение на ее основе модели угроз, модели злоумышленника, потенциальных сценариев реализации угрозы

Рисунок 3. Пример реализации угроз безопасности.

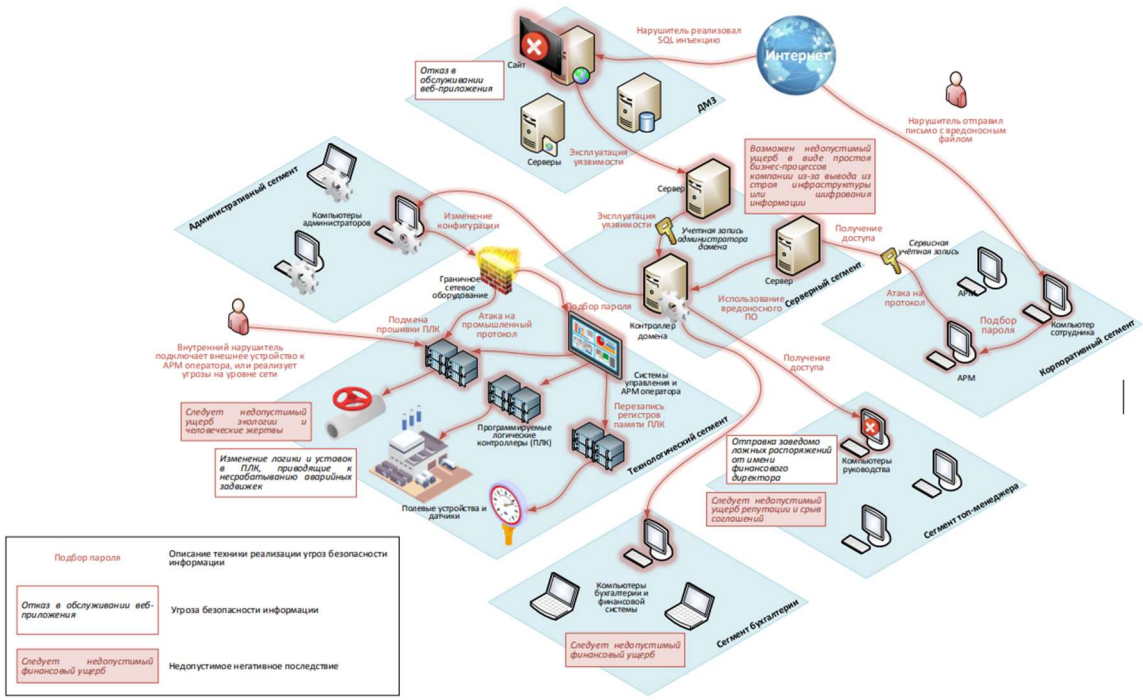

Рисунок 4. Реализация сценария угрозы безопасности

Оценка сложности таких угроз определяется согласно положениям Методики, указанным в приложениях.

По результатам построения полученная оценка может быть основой для выявления слабых мест в системах защиты организации и выработке мер по укреплению периметра контролируемой зоны.

Класс защищенности АС

Основополагающим документов в области определения класса защищенности АС является:
«Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации от 30 марта 1992 г.»

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.
- Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования в соответствии с пп. 2.4, 2.7 и 2.10. Подробно эти требования сформулированы в пп. 2.5, 2.6, 2.8, 2.9 и 2.11-2.15 РД

Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

- выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических

средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

- выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;
- организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;
- разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;
- осуществление приемки СЗИ НСД в составе АС.

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

не ниже 4 класса - для класса защищенности АС 1В;

не ниже 3 класса - для класса защищенности АС 1Б;

не ниже 2 класса - для класса защищенности АС 1А.

Таблица 1 «Требования к 3му классу защищенности»

Подсистемы и требования	Классы	
	3Б	3А
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-
к программам	-	-
к томам, каталогам, файлам, записям, полям записей	-	-
1.2. Управление потоками информации		
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	-
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-

3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

Таблица 2 «Требования ко 2му классу защищенности»

Подсистемы и требования	**Классы**	
	2Б	**2А**
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+
к программам	-	+
к томам, каталогам, файлам, записям, полям записей	-	+
1.2. Управление потоками информации	-	+
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+

доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	+
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	+
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	+
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

Таблица 3 «Требования к 1му классу защищенности»

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
в систему	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+	+	+	+
к программам	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
1.2. Управление потоками информации	-	-	+	+	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	+	+	+
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	-	-	-	+	+

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	-	+	+	+

Класс защищенности хоть и выбирается Заказчиком и Исполнителем, однако проверяется и вписывается в Технический Паспорт АС в ходе аттестационных мероприятий проводимых в соответствии с требованиями Приказа ФСТЭК России от 29.04.2021 N 77 "Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну"

Нормативные документы

Основанием для разработки технического задания является п. 15 Приказа ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"(Далее приказ № 17)

Также основанием для разработки ТЗ является практическая необходимость обеспечения состояния защищенности информации в соответствии с ст. 6,16 149 ФЗ, приказами № 17 и №524(если применим) ФСТЭК и ФСБ соответственно, а также ряда других НПА, таких как:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
- Постановление правительства РФ от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.).
- ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Помимо этого, основной базой для разработки СЗИ должна является актуальная модель угроз безопасности информации разработанная, содержащаяся и актуализируемая по мере необходимости в соответствии с требованиями Методики оценки угроз безопасности информации ФСТЭК, а также модель нарушителя, выработанная в соответствии с той же методикой, как это было описано выше. Кроме этого, в разработке СЗИ будут те же документы что и при разработке Методики и иные упомянутые в настоящей работе документы.

Требования к СЗИ

Перечень предполагаемых к использованию СЗИ

Основание на разработку собственных СЗИ

Состав, сроки и содержание проведения работ

Требования к подрядным организациям-исполнителям

Перечень предъявляемой заказчику научно-технической продукции и базы

Заключение

Источники