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

РСП – Режимно-Секретное Подразделение

НСД – Несанкционированный Доступ

РД - Руководящий Документ

СВТ – Средство Вычислительной Техники

НДВ – Не декларированные Возможности

ГК – Гражданский Кодекс

ОИВ – Орган Исполнительной Власти

[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"

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 подготовить 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 единой 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 обсуждаться конкретные сертифицированные уполномоченными органами СЗИ и будет изложен процесс разработки собственных решений в области защиты информации.

Основание разработки

Основанием для разработки ЧТЗ СЗИ является распоряжение руководителя РСП, выработанное на основании приказа руководителя учреждения и НПА, таких как Приказ №77 ФСТЭК, требования 149-ФЗ;152-ФЗ, ГОСТов, регулирующих сферу ИБ и иных НПА, регулирующих вопросы защиты информации, например, приказы ФСБ, в случае, если имеет место шифрование.

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). 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.

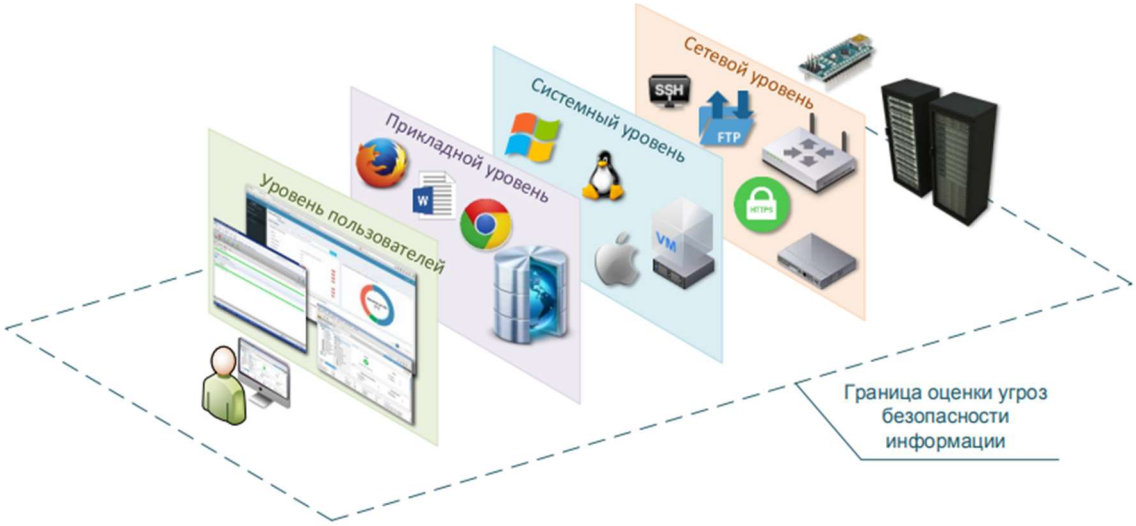

Рисунок 2. Уровни оценки инфраструктуры.

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.

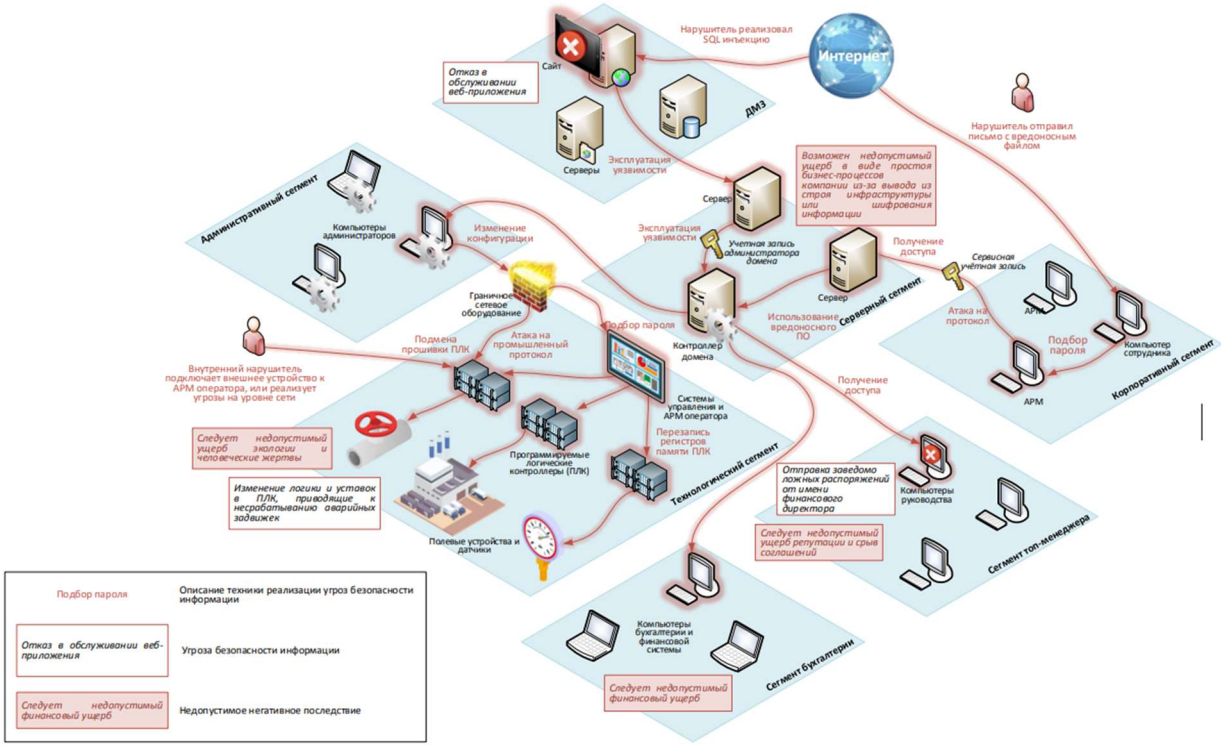

Рисунок 4. Реализация сценария угрозы безопасности.

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 3-му 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 2-му 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 1-му 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	-	-	+	+	+

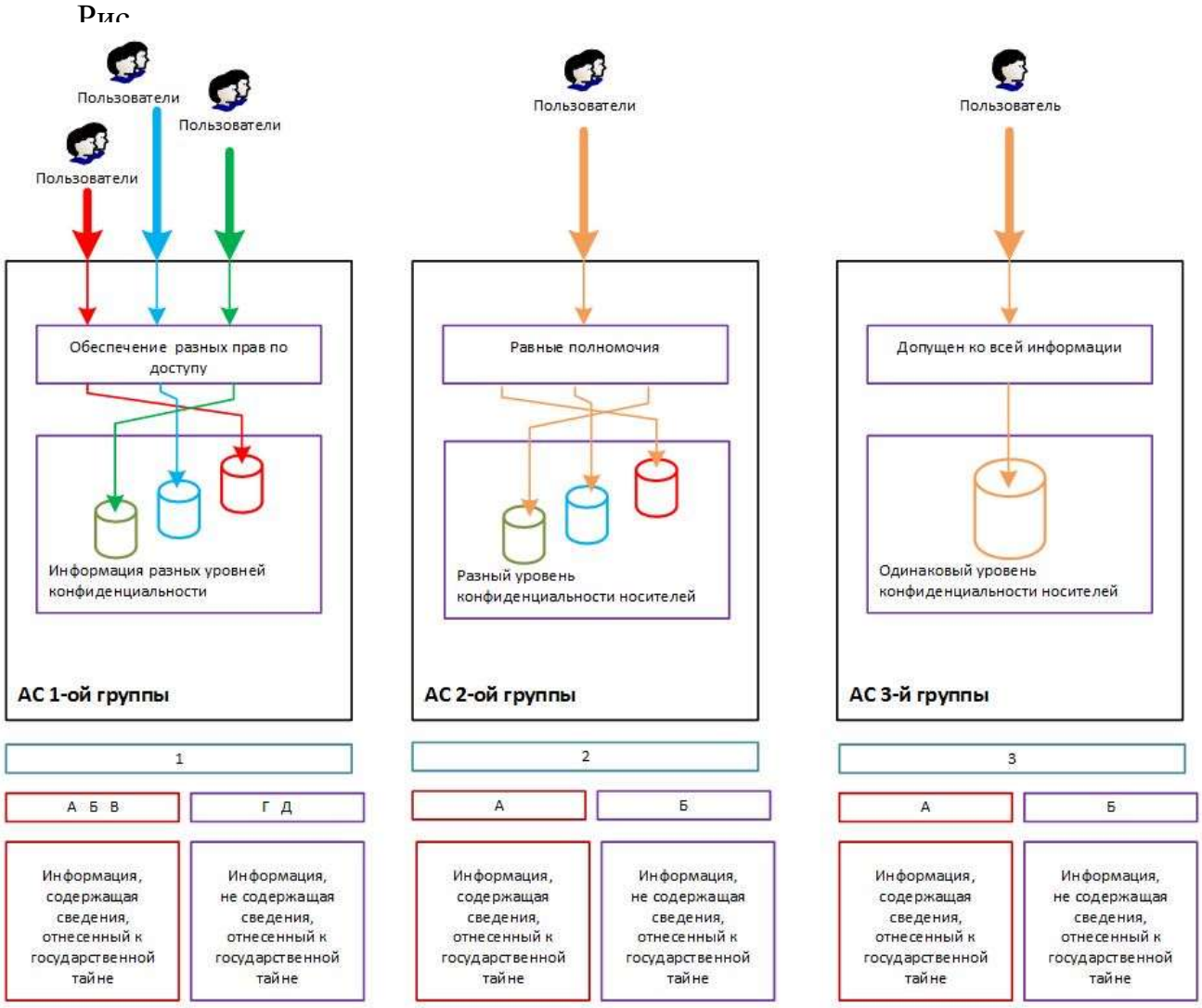

Рисунок 5. Классы защищенности АС

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).

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».

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 использованы те же документы, что и при разработке Методики и иные документы, упомянутые в настоящей работе.

Требования к СЗИ

По поручению Правительства Российской Федерации разработаны Требования по защите информации в информационных системах общего пользования. В них, в частности, определены такие виды средств защиты информации, как СЗИ от неправомерных действий (в том числе средства криптографической защиты информации), средства обнаружения вредоносных программ (в том числе антивирусные средства), средства контроля доступа к информации (в том числе средства обнаружения компьютерных атак), средства фильтрации и блокирования сетевого трафика (в том числе средства межсетевого экранирования). Использование таких СЗИ должно обеспечить требуемый уровень защищенности. Виды средств криптографической защиты информации, Средства защиты информации, реализующее алгоритмы криптографического преобразования информации, относят к криптографическим средствам защиты информации (по ГОСТ Р 50922-2006). Разработка, изготовление и распространение их является

лицензируемым видом деятельности. Согласно Положения о лицензировании принято различать: средства шифрования; средства имитозащиты; средства электронной подписи; средства кодирования; средства изготовления ключевых документов; ключевые документы; аппаратные шифровальные (криптографические) средства; программные шифровальные (криптографические) средства; программно-аппаратные шифровальные (криптографические) средства. В первом случае речь идет о криптографических СЗИ, обеспечивающих возможность разграничения доступа к ней. Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций, называют средствами кодирования. Электронные документы, содержащие ключевую информацию, необходимую для выполнения криптографических преобразований с помощью средств шифрования, принято называть ключевыми документами. Средства шифрования, обеспечивающие создание ключевых документов, называют средствами изготовления ключевых документов. Защиту от навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов предоставляют средства имитозащиты. Криптографические СЗИ, обеспечивающие создание электронной цифровой подписи с использованием закрытого ключа, подтверждение с использованием открытого ключа подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи относят к средствам электронной подписи. Суть различий последних трех видов шифровальных средств, указанных выше, очевидно следует из их названий. Более подробная информация, касающаяся криптографических СЗИ, отражена в утвержденном ФСБ России документе «ПКЗ-2005». Классификация криптографических средств защиты информации ФСБ России определены классы криптографических СЗИ: КС1, КС2, КС3, КВ и КА. К основным особенностям СЗИ класса КС1 относится их

возможность противостоять атакам, проводимым из-за пределов контролируемой зоны. При этом подразумевается, что создание способов атак, их подготовка и проведение осуществляется без участия специалистов в области разработки и анализа криптографических СЗИ. Предполагается, что информация о системе, в которой применяются указанные СЗИ, может быть получена из открытых источников. Если криптографическое СЗИ может противостоять атакам, блокируемым средствами класса КС1, а также проводимым в пределах контролируемой зоны, то такое СЗИ соответствует классу КС2. При этом допускается, например, что при подготовке атаки могла стать доступной информация о физических мерах защиты информационных систем, обеспечении контролируемой зоны и пр. В случае возможности противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ говорят о соответствии таких средств классу КС3. Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то речь идет о соответствии классу КВ. Если к разработке способов атак привлекались специалисты в области использования НДВ системного программного обеспечения, была доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то защиту от таких атак могут обеспечивать средства класса КА. Классификация средств защиты электронной подписи Средства электронной подписи в зависимости от способностей противостоять атакам принято сопоставлять со следующими классами: КС1, КС2, КС3, КВ1, КВ2 и КА1. Эта классификация аналогична рассмотренной выше в отношении криптографических СЗИ.

Помимо этого, существует классификация защищенности СВТ, на которую опирается ФСТЭК при утверждении Требований по безопасности информации. Утверждены приказом ФСТЭК России от 2 июня 2020 г. N 76

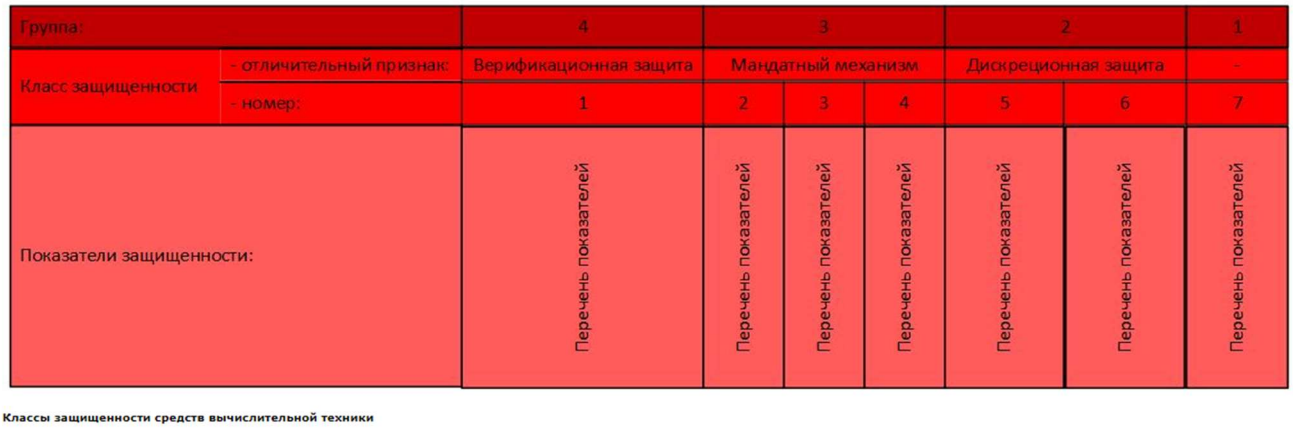

Рисунок 6. Классы защищенности средств вычислительной техники.

Здесь регулятор определил перечень классов защищенности, где первый считается наивысшим классом, а низшим — седьмой. Классы защищенности разделены на группы (рис. 6). Первая группа образована 7 классом. Он устанавливается тем средствам вычислительной техники, которые должны содержать механизмы защиты от НСД к информации, но итоговая защищенность которых ниже защищенности средств 6-го класса. Вторую группу образовывают 6 и 5 классы защищенности. Они отличаются наличием дискреционного управления доступом. Этот механизм позволяет задавать правила доступа пользователей к различным ресурсам, таким как файл, программа и прочее, в которых явно указано, что именно можно делать субъекту: читать содержимое файла, выполнять запуск программы и т. д. Образующие третью группу 4, 3 и 2 классы отличаются реализацией мандатного управления доступом, основанным на использовании классификационных меток. Они позволяют пользователям и ресурсам назначать т. н. классификационные уровни, например, категории секретности обрабатываемой информации. Так, создается иерархическая структура, в

которой пользователь может получить доступ к ресурсу в том случае, если его уровень в созданной иерархии не ниже уровня иерархии требуемого ресурса. В случае неиерархической структуры в классификационный уровень пользователя включают те классификационные уровни ресурсов, доступ к которым этому пользователю должен быть обеспечен. При этом в этих средствах вычислительной техники присутствует механизм дискреционного управления доступом, дискреционные правила служат дополнением мандатных. А в состав четвертой группы входил только 1 класс, характеризующийся наличием верифицированной защиты. Реализованный механизм защиты должен гарантированно обеспечивать перехват диспетчером доступа всех обращений субъектов доступа к объектам. «Средства, соответствующие 6 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 3 категории[1], в государственных информационных системах 3 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[****].

Средства, соответствующие 5 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 2 категории[*], в государственных информационных системах 2 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных[****].

Средства, соответствующие 4 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 1 категории[*], в государственных информационных системах 1 класса защищенности[**], в автоматизированных системах управления

производственными и технологическими процессами 1 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных[****], в информационных системах общего пользования II класса[2][*****].

5. При проведении сертификации средства защиты информации должно быть подтверждено соответствие средства настоящим Требованиям.

Устанавливается следующее соответствие классов средств защиты информации и средств вычислительной техники уровням доверия:

средства защиты информации 6 класса должны соответствовать 6 уровню доверия;

средства защиты информации 5 класса должны соответствовать 5 уровню доверия;

средства защиты информации 4 класса и средства вычислительной техники
5 класса должны соответствовать 4 уровню доверия.

6. Средство соответствует уровню доверия, если оно удовлетворяет требованиям к разработке и производству средства, проведению испытаний средства, поддержке безопасности средства

1 Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955).

[*] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

[**] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 30 июня 2017 г., регистрационный № 32919) и приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

[***] Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

2 Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736),

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955).

** Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

*** Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 30 июня 2017 г., регистрационный № 32919) и приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

**** Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

***** Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

Таблица 4а. Требования к СЗИ с уровнем доверия 4-6.

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1.	Требования к разработке и производству средства:			
1.1.	требования к разработке модели безопасности средства			+
1.2.	требования к проектированию архитектуры безопасности средства	+	=	=
1.3.	требования к разработке функциональной спецификации средства	+	+	+
1.4.	требования к проектированию средства	+	=	=
1.5.	требования к разработке проектной (программной) документации	+	+	+
1.6.	требования к средствам разработки, применяемым для создания средства	+	=	=
1.7.	требования к управлению конфигурацией средства	+	+	+

1.8.	требования к разработке документации по безопасной разработке средства	+	=	+
1.9.	требования к разработке эксплуатационной документации	+	=	=
2.	Требования к проведению испытаний средства:			
2.1.	требования к тестированию средства	+	+	+
2.2.	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	+	+	+
2.3.	требования к проведению анализа скрытых каналов в средстве			+
3.	Требования к поддержке безопасности средства:			
3.1.	требования к устранению недостатков средства	+	+	+
3.2.	требования к обновлению средства	+	+	+
3.3.	требования к документированию процедур устранения недостатков и обновления средства	+	=	=
3.4.	требования к информированию об окончании производства и (или) поддержки безопасности средства	+	=	=

Таблица 4б. Требования к СЗИ с уровнем доверия 1-3.

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+

ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа			
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации			
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему			
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы			+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через	+	+	+

	внешние информационно-телекоммуникационные сети			
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники		+	+
III. Ограничение программной среды (ОПС)				
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			

IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			
ЗНИ.7	Контроль подключения машинных носителей информации			
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+	+	+
V. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+

РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе			
VI. Антивирусная защита (АВЗ)				
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
VII. Обнаружение вторжений (СОВ)				
СОВ.1	Обнаружение вторжений		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Контроль (анализ) защищенности информации (АНЗ)				

АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)				
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы			
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной		+	+

	информации, не относящихся к функционированию информационной системы (защита от спама)			
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы			
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему			+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему			
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			
X. Обеспечение доступности информации (ОДТ)				
ОДТ.1	Использование отказоустойчивых технических средств			+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы			+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации		+	+

ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала		+	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов			
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации		+	+
XI. Защита среды виртуализации (ЗСВ)				
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		+	+

ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры		+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+	+	+
XII. Защита технических средств (ЗТС)				
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+

ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)			+
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы		+	+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами			

ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		+	+
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи		+	+
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации		+	+
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю		+	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя		+	+
ЗИС.14	Использование устройств терминального доступа для обработки информации			

ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации		+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+	+	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы			+
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы		+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными		+	+

	системами и информационно-телекоммуникационными сетями			
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения		+	+
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)			
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем			
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации			
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы			
ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы			
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	+	+	+

Перечень предполагаемых к использованию СЗИ

Перечень предлагаемых к использованию СЗИ должен отвечать потребностям организации, выявленным во время оценки угроз безопасности информации, перечень одобренных уполномоченными органами расположен на сайте (https://reestr.fstec.ru/reg3) в сети интернет.

ODS Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 | 139 КБ | 428187

Текст для поиска

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Предназначение средства (область применения), краткая характеристика параметров / (оценка возможности использования в информационных системах персональных данных (ИСПДн))	Схема сертификации
3754	23.06.2017	23.06.2020	программное изделие «Kaspersky Endpoint Security 10 для Android»	Соответствует требованиям документов: Требования к САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ)	серия
3764	28.06.2017	28.06.2020	EcoRouterOS версии 3.2	Операционная система EcoRouterOS версии 3.2 - по 5 классу РД СВТ, по 4 уровню отсутствия НДВ и ТУ	серия
3765	30.06.2017	30.06.2020	Avanpost IDM	программное обеспечение «Avanpost IDM» - по 4 уровню РД НДВ и ТУ	серия
3766	30.06.2017	30.06.2020	ДФГ152	программное обеспечение «ДФГ152» - по 4 уровню РД НДВ и ТУ	серия
3767	30.06.2017	30.06.2020	Система управления. Аналитика-BI	программный комплекс «Система управления. Аналитика-BI» - по 4 уровню РД НДВ	50

Фрагмент реестра сертифицированных СЗИ

Рисунок 7. Фрагмент реестра сертифированных СЗИ.

Аналогичный перечень в рамках своей компетенции поддерживает и ФСБ

Основание на разработку собственных СЗИ

Согласно Приказу №17:

«При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.»

Следовательно, при невозможности применения имеющихся аттестованных решений, либо изменения архитектуры системы таким образом, чтобы они стали применимы руководитель РСП, либо руководитель организации должен выработать распоряжение о разработке собственного СЗИ, на основании этого приказа должно быть разработано Техническое задание, которое на основании того же приказа ФСТЭК ложится в основу разработки.

Состав, сроки и содержание проведения работ

Так как ЧТС СЗИ согласно приказу №17 ФСТЭК должно соответствовать требованию ГОСТ 34.602

«техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (далее - ГОСТ 34.602). То, согласно выше указанному ГОСТу, сроки и состав работ определяются в соответствующем разделе ТЗ, либо в Договоре на проведение работ и является результатом

договоренностей между Заказчиком и Исполнителем согласно статье 708 ГК РФ.

Из ГОСТ 34.601 в общем случае состав работ определяется п.2 и прил.1 указанного стандарта. Но также является предметом договора Исполнителя и Заказчика.

Требования к подрядным организациям-исполнителям

Согласно Постановлению Правительства РФ от 03.02.2012 N 79 (ред. от 03.02.2023) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации».

«Не допускается осуществление деятельности, указанной в абзаце первом настоящего пункта, иностранными юридическими лицами.

4. При осуществлении лицензируемого вида деятельности лицензированию подлежат:

а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

в средствах и системах информатизации;

в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

в помещениях со средствами (системами), подлежащими защите;

в помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации:
е) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации)».

Перечень предъявляемой заказчику научно-технической продукции и базы

Согласно приказу №17 ФСТЭК Исполнитель предоставляет заказчику эксплуатационную документацию
Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

- структуры системы защиты информации информационной системы;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.

Внедрение системы защиты информации информационной системы организуется обладателем информации (заказчиком).
Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной

документацией на систему защиты информации информационной системы и в том числе включает:

- установку и настройку средств защиты информации в информационной системе;
- разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);
- внедрение организационных мер защиты информации;
- предварительные испытания системы защиты информации информационной системы;
- опытную эксплуатацию системы защиты информации информационной системы;
- анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;
- приемочные испытания системы защиты информации информационной системы.

А также сведения об аттестации разработанной СЗИ в уполномоченном органе «Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

По решению заказчика (оператора) аттестационные испытания могут быть совмещены с проведением приемочных испытаний информационной системы.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний».

Заключение

В настоящей работе обсуждались организационно-правовые моменты, связанные с разработкой частного технического задания на создание средства защиты информации, процесса принятия такого решения, выработки своих собственных решений в случае, если принятые стандартные решения не подходят под задачи и невозможно изменить уже отлаженную архитектуру таким образом, чтобы можно было использовать существующее на рынке аттестованное решение без ущерба производственным процессам, а также процесс аттестации таких решений и результатов разработки.

Помимо этого, в работе были затронуты вопросы, касающиеся обязанностей и требований к исполнителю заказов на выработку подобных решений, вопросы лицензирования деятельности исполнителя.

Все обсуждаемые вопросы были подкреплены соответствующими НПА и руководящими документами регулирующих ОИВ.

Источники

1. ГОСТ 34.602— 2020
2. МЕТОДИЧЕСКИЙ ДОКУМЕНТ МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИ
3. Приказ ФСТЭК №17
4. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации
5. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)
6. https://www.anti-malware.ru/analytics/Market_Analysis/infosecurity-systems-classification-fsb-fstek
7. https://bdu.fstec.ru/
8. https://reestr.fstec.ru/reg3
9. Приказ ФСТЭК №77
10. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
11. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
12. Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 03.02.2023) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации.
13. Приказ ФСТЭК №76
14. ГОСТ 34.601
15. ГК РФ 708
16. ГОСТ 34.201
17. ГОСТ Р 51624