

Whitepaper

Требования регуляторов РФ по созданию модели
угроз кибербезопасности

Необходимость разработки модели угроз безопасности информации определяется различными требованиями регуляторов в сфере ИБ на территории РФ.

Однако, следует отметить, что формулировки, касающиеся необходимости разработки модели угроз – не во всех документах являются однозначными.

В качестве примеров проведем сравнительный анализ формулировок некоторых документов, в том числе:

1) **Приказ ФСТЭК №21** (Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных);

2) **Приказ ФСТЭК №17** (Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах);

3) **Приказ ФСТЭК №31** (Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды);

4) **Приказ ФСТЭК №235** (Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования);

5) **Приказ ФСТЭК №239** (Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации);

6) **Постановление Правительства от 01.11.2012 №1119** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

7) **Приказ ФСБ России от 10 июля 2014 г. №378** (Состав и содержание 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);

Наиболее логичным будет начать рассмотрение данного вопроса с документов, которые касаются защиты персональных данных, так как требования к защите ИСПДн применяются практически ко всем организациям (юр.лица и ИП) на территории РФ.

1. Согласно пункту второму Постановления Правительства №1119 (далее - **ПП №1119**):

– Безопасность персональных данных при их обработке в системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью **5 статьи 19 №152-ФЗ**;

– Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учётом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2. Согласно **пункту 6 ПП №1119**:

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

– Выделяются 3 (три) типа актуальных угроз для ИСПДн согласно **ПП №1119**:

1) Угрозы 1-ого типа, связанные с наличием недеklarированных возможностей в ОС;

2) Угрозы 2-ого типа, связанные с недеklarированными возможностями в прикладном ПО;

3) Угрозы 3-его типа, не связанные с предыдущими двумя типами (остальные угрозы, если они не связаны с наличием недеklarированных возможностей в ОС и прикладном ПО);

При этом в контексте **ПП №1119**, а также с учётом сложившейся практики, определение актуальных угроз в рамках **ПП №1119** осуществляется посредством утверждения Оператором (организацией) соответствующего Акта, об определении уровня актуальных угроз.

Также следует отметить, что определение актуальных угроз согласно **ПП №1119** никак не связано с необходимостью разработки модели угроз. Даже если рассуждать, исходя из логики: «что без моделирования угроз невозможно определить актуальность различных типов угроз» - **ПП №1119** в своем буквальном толковании не обязывает Оператора разрабатывать именно модель угроз, а при наличии используемого лицензионного системного и прикладного ПО, приобретенного на территории РФ на законных основаниях, Угрозы 1-ого и 2-ого типа – не принимаются Оператором в качестве актуальных на данных основаниях.

Что касается вопросов эксплуатации недеklarированных возможностей в лицензионном системном и прикладном ПО – данный аргумент возможно «закрыть» неактуальностью типа потенциального нарушителя (обладающего навыками выявления и эксплуатации уязвимостей «0-day»).

В таком случае сразу рождается вопрос: «А каким образом потенциальный тип нарушителя был определен без моделирования угроз?»

Ответ на данный вопрос кроется как раз-таки в буквальных формулировках **№152-ФЗ**, **ПП №1119**, и т.д. Регулятор говорит об «актуальных угрозах» и об «определении актуальных угроз», при этом способ, которым актуальность таких угроз должна быть определена – не указан. Равно как и необходимость разработки модели угроз или моделирования угроз – также не указана. Кроме того, как уже упоминалось ранее, относительно неактуальности типов потенциальных

нарушителей, в совокупности с определением типа актуальных угроз согласно **ПП №1119** – модель угроз в случае, если она будет разработана Оператором, в итоге не будет противоречить изготовленному Акту определения типа актуальных угроз для ИСПДн.

Фактически мы можем сделать вывод, что утвержденный Акт не будет противоречить несуществующей в организации модели угроз, если потенциально планируется разработка такой модели.

Переходим далее к **Приказу ФСТЭК №21** и **Приказу ФСБ №378**.

Согласно **пункту 3 Приказа ФСТЭК №21**, меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными **ПП №1119** и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

На данном этапе мы видим, что пока без изменений. **Приказ ФСТЭК №21** ссылается на **ПП №1119** и упоминает только «нейтрализацию актуальных угроз», про необходимость моделирования пока нам ничего не говорит. С учётом ссылки на **ПП №1119** – текущий вывод, что нужно определить актуальные угрозы исходя из 3 (трёх) типов, указанных в **ПП №1119**, ни о каком моделировании речи пока нет.

А вот теперь переходим к более интересному развитию событий. Обращаю внимание на **Приказ ФСБ №378**. Для начала следует напомнить, а что это за Приказ такой и для чего он нужен?

1. Документ предназначен для Операторов, использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах.

2. Документ определяет состав и содержание организационных и технических мер, необходимых для выполнения требований **ПП №1119**

3. Документ описывает, какие дополнительные меры нужно принять и каким образом, если Оператор использует СКЗИ для нейтрализации актуальных угроз.

Угрозы, которые нейтрализуются с использованием СКЗИ, обычно предполагают наличие информации, выходящей за пределы контролируемой зоны Оператора, иными словами – если данные передаются через сети общего пользования (интернет) и требуют обеспечения надежного, зашифрованного канала связи (или шифрования самих сведений при их передаче, например средствами ЭП), то для обеспечения безопасности информации используются СКЗИ (в контексте упомянутого **Приказа ФСБ №378** – персональные данные).

Согласно **пункту 5 Приказа ФСБ №378** и **подпункту «г» пункта 5 Приказа ФСБ №378**:

Для обеспечения 4-ого (четвертого) уровня защищенности персональных данных при их обработке в информационных системах необходимо использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности

информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Согласно **пункту 9 Приказа ФСБ №378** и **подпункту «б» пункта 9 Приказа ФСБ №378**:

Для выполнения требования, указанного в подпункте «г» пункта 5 Приказа ФСБ №378 (вышеуказанный абзац) необходимо в том числе: *«формирование и утверждение руководителем оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ»;*

Обращаю внимание, что формулировка *«формирование и утверждение совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учётом типа актуальных угроз требуемого класса СКЗИ»* - во первых **отличается** от «определения типа актуальных угроз» и конкретизирует формирование «совокупности предположений о возможностях....», а также **ссылается** «с учётом типа актуальных угроз», что на мой взгляд, объективно указывает на необходимость разработки именно «Модели угроз» в привычном нам понимании, а также разделяет процессы определения типа актуальных угроз согласно **ПП №1119** и моделирования угроз.

В итоге, если для нейтрализации актуальных угроз ИСПДн используются СКЗИ (при защите информации, выходящей за пределы КЗ), то применяется **Приказ ФСБ №378**, который предполагает разработку модели угроз для выполнения требований **ПП №1119**, так как **пункт 5 Приказа ФСБ №378** ссылается на обеспечение 4-ого (четвертого – минимального) уровня защищенности ПДн согласно **ПП №1119**. Это значит, что разработка модели угроз и применение **Приказа ФСБ №378** необходима всем организациям, инфраструктура которых предполагает использование СКЗИ для нейтрализации актуальных угроз ИСПДн (распределенная инфраструктура, наличие удаленных сотрудников без доменной техники, и т.д.).

Переходим к дальнейшему сравнительному анализу формулировок, касающихся необходимости разработки модели угроз. При изучении текста **Приказа ФСТЭК №17** (ГИС) создается уже совершенно иное впечатление, согласно тексту **Приказа ФСТЭК №17**:

– В рамках раздела **«Формирование требований к защите информации, содержащейся в информационной системе»**, в **пункте 14** указано, что формирование требований к защите информации включает «определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и **разработку на их основе модели угроз безопасности информации**;

– В **пункте 14.3.** вышеупомянутого раздела указано, что угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационных системы, возможных

способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности);

– **Пунктом 14.3.** также предусмотрено, что в качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

– **Абзац 3 пункта 14.3.:** *«При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности её функционирования»*

– **Абзацами 6 и 7 пункта 14.3.** указано:
«Модель угроз безопасности информации должна содержать описание информационной системы и её структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации»

«Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России»
(подразумевается методика ФСТЭК России, актуальный документ – «Методический документ от 05 февраля 2021 года «Методика оценки угроз безопасности информации»)

С учётом вышеизложенного, а также по результатам анализа содержания **Приказа ФСТЭК №17**, на мой взгляд не остается вопросов, связанных с сомнениями в части необходимости разработки модели угроз в случае, если информационная система – это ГИС. Выводы однозначные.

При этом важно, чтобы не запутаться, так как мы уже рассмотрели 2 глобальных сферы (ГИС и ПДн) в части необходимости разработки модели угроз по требованиям законодательства РФ и регуляторов, что если наша информационная система — это ГИС, то в любом случае формируем модель угроз. Если наша система – ИСПДн, то формирование модели угроз, на мой взгляд формально не обязательно, если говорить о вопросах требований регулятора. Но если наша ИСПДн является ГИС, то мы применяем **Приказ ФСТЭК №17** с учётом **ПП №1119**, и разработка модели угроз в таком случае будет необходимостью, но обусловленной тем, что ИС является ГИС и подпадает под требования **ФСТЭК №17**.

Также следует отметить, что с учетом содержания проверочного листа, утвержденного **Приказом Роскомнадзора от 24.12.202 №253**, со стороны РКН не предполагается проверка модели угроз, так как содержание данного документа может быть согласовано с точки зрения компетенций ФСТЭК и (или) ФСБ, возможно Минобороны в части касающейся, но не РКН.

В дополнение к примеру с **Приказом ФСТЭК №17** (ГИС) посмотрим аналогичную формулировку в части необходимости разработки модели угроз в другом Приказе – **ФСТЭК №31**.

Во-первых, следует отметить, что пункт 13.3. **Приказа ФСТЭК №31** крайне похож, а местами даже идентичен содержанию **Приказа ФСТЭК №17**. Для наглядности приведу конкретные примеры:

– «определение угроз безопасности информации должно включать выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей» (**подпункт «а» абзаца 1 пункта 13.3 Приказа ФСТЭК №31**);

– «определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации» (**подпункт «в» абзаца 1 пункта 13.3 Приказа ФСТЭК №31**);

– «В качестве исходных данных при определении угроз безопасности информации используется банк данных угроз безопасности информации.....» (**абзац 2 подпункта 13.3. Приказа ФСТЭК №31**);

«Модель угроз безопасности информации должна содержать описание автоматизированной системы управления и угроз безопасности информации для каждого из уровней автоматизированной системы управления, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования автоматизированной системы управления <*>» (**абзац 5 пункта 13.3 Приказа ФСТЭК №31**). В цитируемой формулировке также отмечен символ «*», означающий ссылку на методические документы ФСТЭК России (**подразумевается методика ФСТЭК России, актуальный документ – «Методический документ от 05 февраля 2021 года «Методика оценки угроз безопасности информации»**).

На данном этапе уже можно сделать вывод о том, что при наличии АСУ ТП, подпадающих под действие **Приказа ФСТЭК №31**, обязывает Оператора (владельца АСУ ТП) разработать модель угроз.

Рассмотрев вопросы разработки модели угроз в ИСПДн, ГИС, а также для АСУ ТП, переходим к сфере Критической информационной инфраструктуры (КИИ).

Требования по защите объектов КИИ регламентируются **Приказами ФСТЭК №239** и **№235**. Важно отметить, что **Приказ №239** содержит «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а **Приказ №235** содержит «Требования к созданию систем безопасности

значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Начнем с анализа формулировок **Приказа ФСТЭК №235**, я бы выделил лишь одну, содержащуюся в **подпункте «б» пункта 25 Приказа ФСТЭК №235**:

«25. Организационно-распорядительные документы по безопасности значимых объектов должны определять:

Б) планы мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, модели угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры,.....»

Промежуточный вывод таков, Приказ ФСТЭК №235 определяет требования к содержанию организационно-распорядительных документов значимых объектов КИИ (ЗОКИИ), в числе которых указаны модели угроз в отношении ЗОКИИ.

А теперь посмотрим, какая информация по нашему вопросу содержится в **Приказе ФСТЭК №239**:

1. **Пункты 11-11.3 Приказа ФСТЭК №239** по аналогии с ранее упомянутыми **пунктами 13-13.3. Приказа ФСТЭК №31 (АСУ ТП)** – крайне аналогичны **пунктам 14-14.3. Приказа ФСТЭК №17**.

2. Согласно **подпункту «а» пункта 11 Приказа ФСТЭК №239** разработка организационных и технических мер по обеспечению безопасности ЗОКИИ должна включать анализ угроз безопасности информации и **разработку модели угроз безопасности информации** или ее уточнение (при ее наличии).

3. Согласно **пункту 11.1 Приказа ФСТЭК №239** *«Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учётом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее – архитектура значимого объекта), а также особенностей функционирования значимого объекта».*

4. **Пунктом 11.1. Приказа ФСТЭК №239** также предусмотрено, что анализ угроз безопасности должен включать:

- Выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей (**подпункт «а» абзаца 2 пункта 11.1 Приказа ФСТЭК №239**);

- Определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации (**подпункт «в» абзаца 2 пункта 11.1 Приказа ФСТЭК №239**);

5. **Пункт 11.1. Приказа ФСТЭК №239** также предполагает:

- Что в качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации (БДУ ФСТЭК);

- Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;

- Требования к описанию каждой угрозы;

- Требования к применению методических документов ФСТЭК при разработке модели угроз.

С учётом всего вышеизложенного, важно помнить о различных отраслевых требованиях информационной безопасности, которые формируются регуляторами для организаций, функционирующих в определенной сфере деятельности, и речь не только о финансовых организациях, для которых регулятором по вопросам информационной безопасности будет ЦБ РФ, а также об организациях, работающих в определенных сферах (например, Минтранс, Минспорт, и т.д.).

Дополнительно можно обратиться к содержанию **ГОСТ 57580** (защита финансовых организаций), в котором также явно упоминается термин «модели угроз» и подразумевается необходимость её формирования и наличия в организации.

Вывод:

По итогам проведения сравнительного анализа формулировок различных документов, касающихся регулирования сферы ИБ в РФ, можно сделать однозначный вывод о необходимости разработки модели угроз в рамках построения системы защиты информации, если организация подпадает под действие Приказов ФСТЭК: №17, №31, №235 и 239, Приказа ФСБ №378, требований ЦБ РФ к финансовым организациям.

Исключением из данного вывода будет защита персональных данных, не выходящих за пределы контролируемой зоны Оператора, либо иные основания для **неиспользования СКЗИ** в целях нейтрализации актуальных угроз безопасности информации = организация не подпадает под действие Приказа ФСБ №378.

Также примеры случаев, когда модель угроз формально можно не разрабатывать:

1. Информационные системы не являются распределенными ИСПДн, передача ПДн за пределы КЗ из таких систем не осуществляется, применение СКЗИ для нейтрализации актуальных угроз не требуется, не подпадает под действие Приказа ФСБ №378.

2. В совокупности с пунктом 1 – организация не является владельцем значимого объекта КИИ (ЗОКИИ);

3. В совокупности с пунктом 1 и 2 – организация не является владельцем АСУ ТП, подпадающей под требования Приказа ФСТЭК №31 (не все АСУ ТП подпадают под действие данного Приказа);

4. В совокупности с пунктом 1,2,3 – организация не является Оператором ГИС (государственной информационной системы, или иных систем, подпадающих под требования ФСТЭК №17);

5. В совокупности с пунктом 1,2,3,4, – организация не подпадает под требования **ГОСТ 57580** (ЦБР – финансовые организации, указанные в

части первой статьи 76.1 ФЗ «О центральном банке Российской Федерации», а также субъекты национальной платежной системы)

6. ***Данный список можно дополнять и расширять всеми ситуациями, при которых организация должна разработать модель угроз, и которые необходимо исключить для принятия решения об отсутствии необходимости в разработке модели угроз.**

В заключение следует дополнить, что совокупность вышеуказанных ситуаций случается не часто, и лишь избавляет организацию от формальных требований регуляторов в части необходимости разработки именно модели угроз безопасности информации, но ничто не освобождает организацию от нейтрализации актуальных угроз безопасности информации, равно как и от определения актуальности угроз безопасности информации. Каким образом проводить данный анализ без разработки модели – каждый решает самостоятельно.

Также следует отметить, что банк данных угроз безопасности информации ФСТЭК России не является однозначным источником об угрозах, все Приказы предусматривают в том числе «иные источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

Так когда же нужно разрабатывать модель угроз?

Почти во всех случаях, за исключением указанных, но при этом не следует забывать о том, что указанный перечень не исчерпывающий и каждую конкретную ситуацию необходимо рассматривать в контексте организационно-правовой формы организации и сферы деятельности с учётом применимых к ней требований.

Субъективно я бы дополнил тем, что в «исключительных» случаях, разработка модели угроз значительно упрощается, и разработка модели принесет только пользу при построении системы защиты информации. Осознанное решение об отсутствии необходимости разработки модели угроз – скорее принесет больше вреда, чем пользы, и применимо только тогда, когда человеческих или финансовых ресурсов для разработки такой модели действительно недостаточно или разработка совсем нецелесообразна (например: организация – это ИП из одного человека, который все равно ничего не делает с ИБ, обработка данных ограничивается договорными отношениями с заказчиками).