Что же такое **модель угроз безопасности персональных данных**?! Для чего она нужна и как ее разработать?! Ответы на эти вопросы Вы найдете в этой статье.

В соответствии с Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (от 21 февраля 2008 года):

Модель угроз – это перечень возможных угроз.

Все просто и ясно. Хотя в ГОСТ Р 50922-2006 – «Защита информации. Основные термины и определения» дано более емкое определение:

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Итак, **модель угроз** – это документ, тем или иным способом описывающий возможные угрозы безопасности персональных данных.

Теперь разберемся что такое **угроза безопасности информации (персональных данных)**.

В документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» дано следующее определение:

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Проще говоря, угроза – это «дыра» в системе защиты.

Угроза может привести к утечке (уничтожению, модификации), а может и нет. Наличие угрозы свидетельствует лишь о наличии возможности несанкционированного доступа к данным.

Зачем нужна модель угроз

Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

В систему защиты включаются только те средства защиты информации, которые нейтрализуют актуальные угрозы.

В соответствии с пунктом 2 статьи 19 ФЗ «О персональных данных» обеспечение

безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз.

Разработка модели угроз безопасности персональных данных

Модель угроз (или как ее еще называют "Частная модель угроз") может разрабатываться ответственными за защиту персональных данных в организации. Также могут привлекаться сторонние эксперты. Разработчики модели угроз должны владеть полной информацией об информационной системе персональных данных, знать нормативную базу по защите информации.

При отсутствии экспертов разработку модели угроз лучше доверить сторонней организации.

Порядок разработки модели угроз определен в документах ФСТЭК:
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», Федеральная служба по техническому и экспортному контролю, 2008 год
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», Федеральная служба по техническому и экспортному контролю, 2008 год.

«Базовая модель» содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Многие эксперты по защите информации весьма скептически относятся к этому документу. Угрозы, приведенные в базовой модели, устарели и далеко не всеобъемлющи. Однако за неимением лучшего приходится довольствоваться текущей редакцией документа.

Документ **«Методика определения актуальных угроз»** содержит алгоритм оценки угрозы. Путем несложных расчетов определяется статус каждой вероятной угрозы.