Моя оборона, или Моделирование как стеклянный глаз информационной безопасности

С одной стороны, моделирование нельзя назвать модным трендом в сфере информационной безопасности. С другой — модель нарушителя и модель угроз не только темы постоянного обсуждения, но и источник восторгов для неофитов и нервных расстройств средней тяжести для действующих специалистов безопасности.

■ ДМИТРИЙ ОМСКИЙ,
эксперт по информационной безопасности

■ МИХАИЛ ЕЛАГИН,
советник директора ГАУ РК «ЦИТ»

Пластмассовый мир победил,
Макет оказался сильней…
Группа «Гражданская оборона»

Рассмотрим несколько проблем: что такое модель (и, соответственно, моделирование) в области информационной безопасности, какова цель такого моделирования (и, соответственно, создания моделей), какова цена и эффективность созданных моделей. И кому эти модели нужны. При этом неясно, какая из проблем более актуальна.

Модель полная

Для начала разберем «классические» модели. «Модель угроз безопасности информации должна содержать описание информационной системы и ее 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», — читаем в 17-м приказе ФСТЭК.

Ошибки, связанные с построением модели угроз с точки зрения регулятора (ФСТЭК), весьма полно описывают в своих блогах и статьях многие специалисты, в частности Алексей Лукацкий, и этой темы мы касаться не будем. Посмотрим на фразу «... должна содержать описание информационной системы и ее структурно-функциональных характеристик». При этом практически не выдвигается никаких требований к данному описанию.

В одной из работ, посвященных построению модели угроз, есть хорошая фраза: «Описание информационной системы должно раскладывать ее по полочкам настолько подробно, насколько это возможно». Но даст ли нам что-либо просто «максимально полное описание системы»? Например, цвет корпуса сервера, умные слова о его функциональном назначении (по проекту). Приведем аналогию в области экономической безопасности: информация о цвете детсадовского ночного горшка контрагента может в исключительных случаях послужить ценным элементом модели безопасности, но в случаях очень исключительных и за весьма высокую цену. При весьма сомнительной эффективности. Но заказчик часто все равно хочет «полную информацию».

То же самое можно сказать о «максимально полном» описании системы в рамках модели угроз, когда большое количество «информационного мусора» подменяет действительно важные, но, возможно, нестандартные или непривычные факторы.

Модель двуликая

При попытке разобраться с понятием «модель» мы сталкиваемся с тем, что этот термин как минимум двузначен, что вызывает определенную путаницу.

В первом случае модель — это некоторая упрощенная имитация моделируемой сущности, ее план, схема, карта. Здесь модель несет прежде всего объяснительные и описательные функции. Во втором случае модель несет предиктивные функции, то есть позволяет предсказывать поведение моделируемой системы в различных ситуациях и выявлять ее неявные свойства. Посмотрим на модели с другой стороны и увидим тот же дуализм.

Еще один взгляд на модели — модель боевых действий. В одном случае мы имеем дело с макетом театра боевых действий, скажем, городского квартала или иного ТВД, выполненным из пластика в определенном масштабе и включающим макеты рельефа, зданий и сооружений, солдат, боевой техники.

В другом случае перед нами имитационная или иная математическая модель, позволяющая провести оценку и оптимизацию процессов, проанализировать взаимовлияние факторов, выявив ключевые, сымитировать развитие процессов боевых действий в различных условиях.

Модель привычная

Вернемся к привычной нам модели угроз. Изначально задуманная как средство предсказания возможных последствий реализаций уязвимостей, анализа возможного поведения объектов защиты в условиях атаки и выработки оптимальных методов реагирования и противодействия, эта модель постепенно выродилась (особенно в случае модели угроз персональных данных) в жестко формальный систематизированный перечень угроз безопасности (в данном случае угроз безопасности персональных данных). В большинстве ситуаций модель угроз является слепком с результатов аудита защищаемой ИС и позволяет оценить соответствие системы формальным правилам регулятора. Но ни в коем случае не защититься от новых, нестандартных атак и воздействий.

В качестве одной из таких нестандартных угроз можно привести, например, класс так называемых семантических атак. Семантическая атака по Мартину Либики[1] — ситуация, при которой неправомерное вмешательство осуществляется не в деятельность и алгоритмы атакуемой системы, а в исходные, поступающие для обработки и анализа данные, что при знании алгоритмов работы системы может привести к выдаче заведомо неправильных результатов. Справедливости ради скажем, что задолго до Либики возможность такой атаки спрогнозировали братья Стругацкие. (Читаем «Великий КРИ»: «Дети, — сказал старик, — этот мошенник сделал в программе маленькое исправление. В задаче "Буриданов баран" он показал, что у барана семь ног. Мало того, этот

[1] «Что такое информационная война», 1995 г.

интеллектуальный пират убрал из программы все, что касается мозжечка барана!»)

Еще интереснее ситуация с моделью нарушителя. Такая модель, принципиально позволяющая существенно уменьшить риски любого вторжения, сегодня используется в первую очередь для решения вопроса о выборе уровня криптозащиты информации. Фактически это один из необходимых классификаторов, обеспечивающих выбор средств защиты, но не более того. Модели нарушителя, в соответствии с регламентирующими документами ФСБ, используются в целях определения необходимого уровня криптографической защиты, если для защиты информации требуется применение средств криптозащиты. То есть анализируется способность нарушителя к компрометации СКЗИ, но не более того.

Модель vs стандарт

Справедливости ради надо сказать, что регуляторы в сфере ИБ применяют лучшие мировые практики. Построение моделей безопасности тесно увязано с положениями ГОСТа Р ИСО/МЭК 18045, основанного на «Общих критериях».

Но есть один интересный момент. В большинстве случаев все, что касается моделей ИБ — будь то модель угроз или модель нарушителя, — оказывается жестко формализованным классификатором, перечнем систем, угроз и путей реагирования и предупреждения, «отлитым в бронзе» нормативно-методическим документом, фактическим стандартом... и в то же время пластиковым макетом театра предотвращения угроз (по аналогии с театром военных действий), позволяющим обеспечить надежнейшую защиту от известных угроз и атак (если, конечно, при подготовке модели не были забыты сколь-либо важные факторы и их взаимодействие), но бессильным перед обычнейшими событиями или их необычной совокупностью.

Бесплатный Wi-Fi-доступ в Интернет на 40 станциях был реализован одним из ведущих операторов связи Санкт-Петербурга за собственный счет

Есть еще один достойный внимания момент. Существующие методики подготовки моделей ИБ содержат жесткий и эффективный перечень требований к содержанию модели, но не дают никакого механизма верификации такой модели, выявления действующих факторов и их верификации, анализа адекватности модели. Все по принципу «написанному верить».

Модель нужная

При этом ответить на вопрос: «Какая модель нам нужна?» — в общем виде не представляется возможным. Хотя бы потому, что сначала надо сформулировать, кто это «мы» в конкретном случае, кто является реальным заказчиком и потребителем результатов моделирования, с какой точки зрения мы смотрим на проблему безопасности.

Во многих ситуациях действительно достаточно «фанерного макета». Это ни хорошо ни плохо. И нет смысла, по крайней мере в рамках этой статьи, обсуждать целесообразность и эффективность требований регулятора. Остановимся на том, что предлагаемые стандартные модели эффективны (возможно, на ограниченном пространстве) и безусловно необходимы. Но недостаточны для обеспечения безопасности объекта защиты в условиях быстро меняющегося мира.

Отдельный вопрос: а что мы защищаем или собираемся защищать? Фразы типа «защищать безопасность информации» напоминают солнечный зайчик стеклянного глаза агрессивно-депрессивной лирики Егора Летова. Защита ради защиты при хорошей аранжировке производит должное впечатление, но может привести к тому, что серьезный удар противника (или той самой случайности) будет пропущен в самое неподходящее время и приведет к печальным результатам.

В самом общем случае цель защиты можно определить как недопущение нежелательных последствий, связанных с вероятной реализацией уязвимостей и угроз на объекте защиты. А в качестве угроз может выступить и прямое попадание метеорита в ЦОД, и хакерская атака, и нарушение корпоративной этики сотрудниками, и неадекватное поведение администратора.

Игнорирование случайностей, нестандартных и неявных событий за счет представления максимально полной картины — возможно, эффективно, но... Как сказал Сталин после крушения аэровагона, в котором погибли инженер Абаковский, Артем и несколько иностранных коммунистов, «если случайность имеет политические последствия, то к такой случайности нужно присмотреться».

Модель современная

Итак, мы пришли к тому, что к недостаткам существующих базовых моделей ИБ следует отнести их формальный характер, невозможность смоделировать поведение системы в различных ситуациях, невозможность автоматически проанализировать описание моделируемой системы и набор действующих (влияющих) факторов в их взаимодействии. Для обеспечения реальной защищенности хочется добавить все эти возможности.

Что нам предлагает современная наука и техника? Оставим пока без внимания целый ряд диссертаций, традиционно начинающихся словами «возьмем интеграл» или «при нахождении сверток значения некоторых критериев необходимо предварительно инвертировать», отличающихся, вероятно, научной новизной, но мало пригодных для практической деятельности безопасника, и посмотрим на набор хорошо зарекомендовавших себя методов, таких как системная динамика, агентное и мультиагентное моделирование, когнитивное моделирование и анализ.

Эти методы действительно способны решить обозначенные проблемы, то есть создать систему имитационного моделирования систем защиты информации и информационной безопасности, позволяющие строить модели разного типа, оценивать эффективность воздействия на объекты защиты и противодействия таким воздействиям. Например, не составляет большого труда смоделировать прохождение воздействий и влияний различного типа на сложные системы и сети (как то: вирусные атаки, DDoS, атаки на сервисы и т. п.) либо оценить влияние различных факторов на уязвимость и защищенность объектов защиты, построив соответствующие когнитивные карты и модели. Существуют инструменты, разрешающие без принципиальных затруднений реализовать эти функции.

Вообще говоря, первоначально эту статью планировалось посвятить именно анализу существующих методов, систем и инструментов моделирования в приложении к ИБ (и такая статья будет подготовлена), но в процессе написания произошло несколько небольших событий, изменивших тему.

В частности, один из руководителей организации (и по совместительству автор этой статьи) дал команду отключить неправомерно (в соответствии с регламентом) созданный аккаунт нового сотрудника, не прошедшего проверку службой безопасности, работники технического подразделения выполнили следующие действия (в строгом соответствии с ошибками в регламенте):

- Провели проверку и выяснили, что аккаунт новому сотруднику не создавался и сообщения он отправлял с частного адреса.
- Получили подтверждение системы сервис-деск об официальном распоряжении руководителя об отключении аккаунта <сотрудника> (где-то здесь объект «сотрудник» исчез из цепочки исполнения).
- Поняли, что задача «отключить аккаунт N по распоряжению руководителя» неисполнима в связи с отсутствием аккаунта N.
- Устранили проблему, сведя задачу к исполнимой «отключить аккаунт <руководителя> по распоряжению руководителя».

И выполнили задачу, практически не нарушив регламент. «Пластмассовый мир победил, макет оказался сильней... Пластмассовый мир победил, ликует картонный набат», — играл проигрыватель в помещении техслужбы.