Сценарии некорректного использования

Автор: Михаил Кривошеин (mikkri@mail.ru)

В современном мире программные системы приобретают все большее значение во всех сферах деятельности человека. В результате сбои в работе программ или их неправильное использование могут причинить значительный ущерб как компаниям, так и индивидуальным пользователям. В таком контексте востребованной становится забота об устойчивости программ к негативным воздействиям и ошибкам пользователей. В статье описан метод анализа сценариев некорректного использования (Misuse Cases), позволяющий позаботиться о корректности и стабильности работы программы еще на стадиях выявления требований и системного анализа. Метод основан на концепции метода сценариев использования, получившего широкое распространение и признание в сфере разработки программного обеспечения.

Концепция

Метод сценариев некорректного использования был предложен Guttorm Sindre и Andreas Opdahl в 2000 году. После чего в 2002 году Ian Alexander представил доработанную версию.

Идея заключается в том, что обычные модели сценариев использования дополняются сценариями использования системы некорректным образом или с нарушением ограничений, принятых при разработке. Выполнение действий сценариев некорректного использования инициируется актерами, возможно, враждебными по отношению к системе. Пример диаграммы сценариев некорректного использования приведен на рисунке №1.

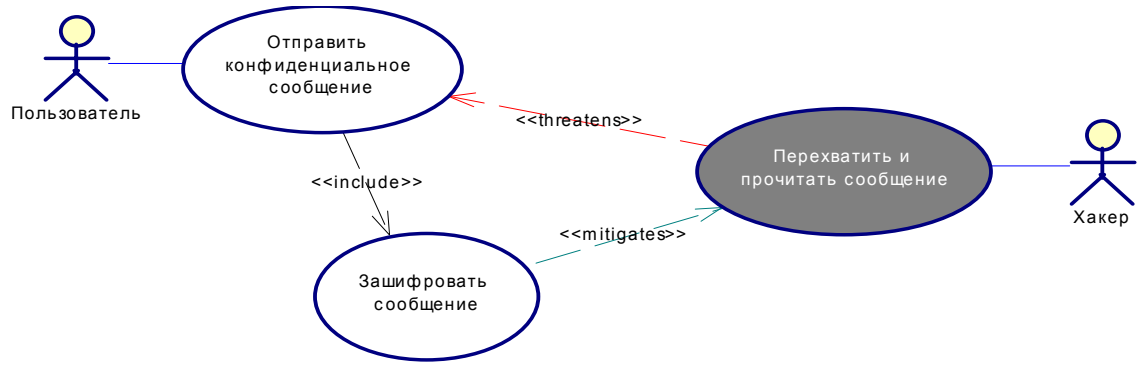

Рисунок № 1

Для большей контрастности сценарии некорректного использования закрашены темным цветом, в отличие от белых сценариев использования. Сценарии использования и сценарии некорректного использования образуют две модели. Их связывают зависимости между сценариями моделей. Типы зависимостей и примеры их использования будут рассмотрены далее.

Примеры

Примером будет сильно упрощенная модель сценариев для электронного магазина. Пусть у нас определено два актера – «Посетитель» и «Продавец». Посетитель может зарегистрироваться, просмотреть список товаров и сделать заказ. Продавец отвечает за обслуживание нормальных заказов (заказов, которые следует выполнить), игнорирование покупателей из черного списка и за предотвращение мошенничеств.

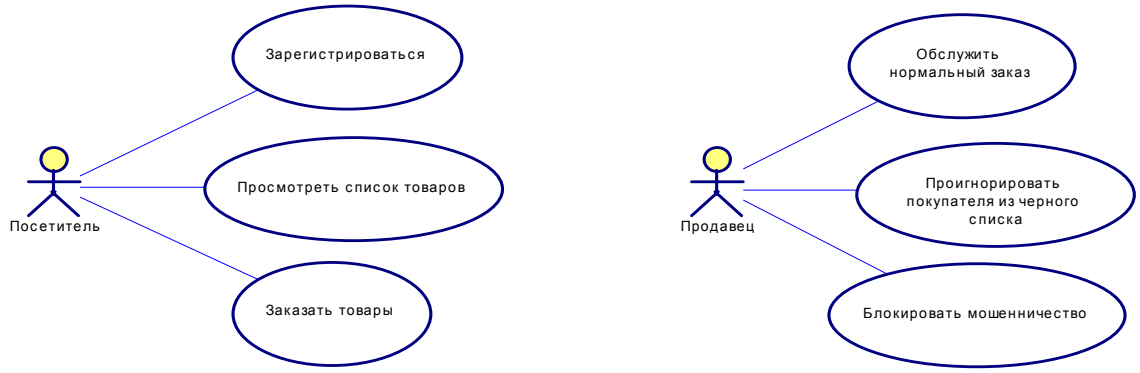

Рисунок № 2

Теперь применим метод сценариев некорректного использования для описания поведения системы в ряде нежелательных ситуаций.
Заметим, что если покупатель из черного списка сможет повторно зарегистрироваться в системе под новым идентификатором, задача продавца не допустить обслуживания покупателей из черного списка будет крайне затруднена (под угрозой).

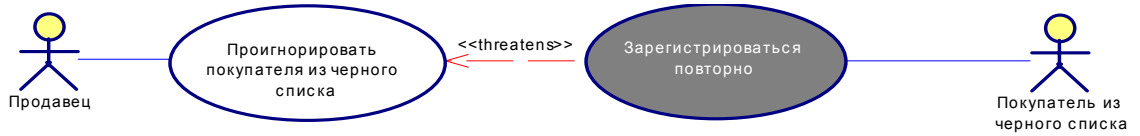

Рисунок № 3

Этот факт изображен на рисунке №3 в виде сценария «Зарегистрироваться повторно» и зависимости со стереотипом «threatens». Соответственно, раз выявлена такая угроза, следует разобраться, должна ли система ей противодействовать и, если да, то как. Пусть было решено в процессе регистрации посетителя в электронном магазине выполнять проверку на повторную регистрацию. Такое решение описано на рисунке №4.

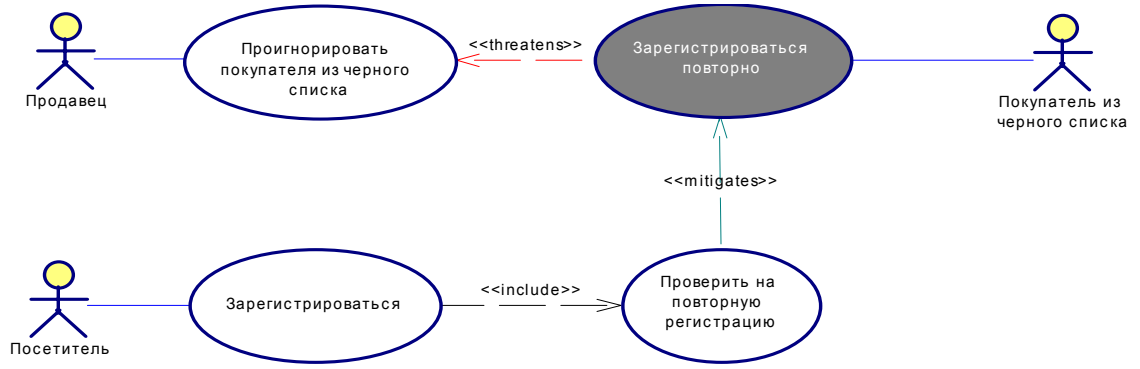

Рисунок № 4

На нем изображен только что выявленный сценарий использования «Проверить на повторную регистрацию», действия которого всегда выполняются при регистрации посетителя. Зависимостью со стереотипом «mitigates» указано, что реализация сценария в системе уменьшит негативный эффект от возможного выполнения действий сценария «Зарегистрироваться повторно».
Рассмотрим более сложный пример, изображенный на рисунке №5.

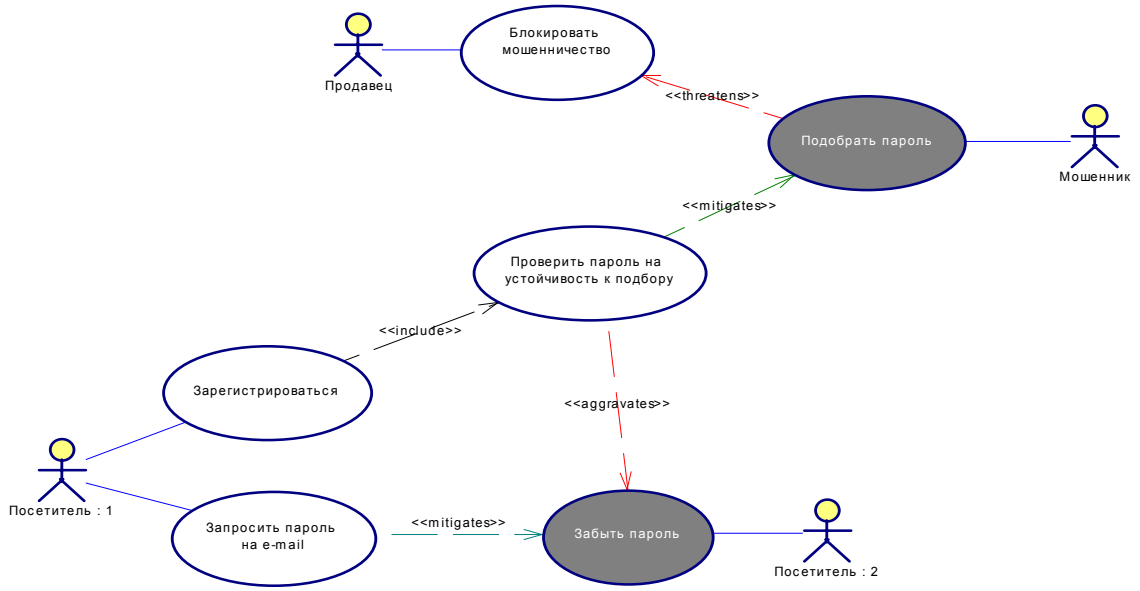

Рисунок № 5

На диаграмме изображено, что возможность подбора пароля зарегистрированного пользователя мошенником угрожает успешному выполнению продавцом действий по блокированию мошенничества. В связи с этим предлагается при первоначальной регистрации посетителя в электронном магазине выполнять проверку введенного пароля на устойчивость к подбору. Такая мера уменьшит возможность мошенника подобрать пароль и оказать негативное влияние на систему с его помощью.

В то же время, заставив посетителей использовать устойчивые к подбору пароли, разработчики системы увеличивают вероятность того, что посетитель забудет свой пароль. Этот факт продемонстрирован на диаграмме сценарием «Забыть пароль» и зависимостью со стереотипом «aggravates». Эта зависимость означает, что реализация сценария «Проверить пароль на устойчивость к подбору» приводит к увеличению влияния на систему сценария некорректного использования «Забыть пароль». Для борьбы с негативным эффектом сценария «Забыть пароль» на диаграмме предлагается реализовать функцию отправки пароля на введенный при регистрации адрес электронной почты.

Диаграмма на рисунке №5 интересна тем, что один и тот же актер «Посетитель» выступает на ней инициатором действий как обычных сценариев использования, так и сценариев некорректного использования. Причем сценарий некорректного использования не является непосредственно связанным с системой электронного магазина, и, на первый взгляд, не должен рассматриваться на этапах сбора требований и системного анализа. Но в данном случае применение метода сценариев некорректного использования позволило выявить необходимость реализации в системе дополнительной функции – отправки забытого пароля по электронной почте. Без использования этого метода требование могло быть упущено.

Допустим, рассматриваемый электронный магазин имеет склад в Москве, а специфика товаров такова, что его доставка в другие города затруднена и стоит дорого. В таком контексте доставка заказа в другой город без уверенности в том, что он будет полностью оплачен, крайне не желательна. Эта ситуация изображена на рисунке №6. Для ее обозначения используются сценарий некорректного использования «Сделать заказ с доставкой в другой город» и зависимость от него сценария «Блокировать мошенничество» со стереотипом «threatens» (угрожает успешному выполнению действий сценария использования).

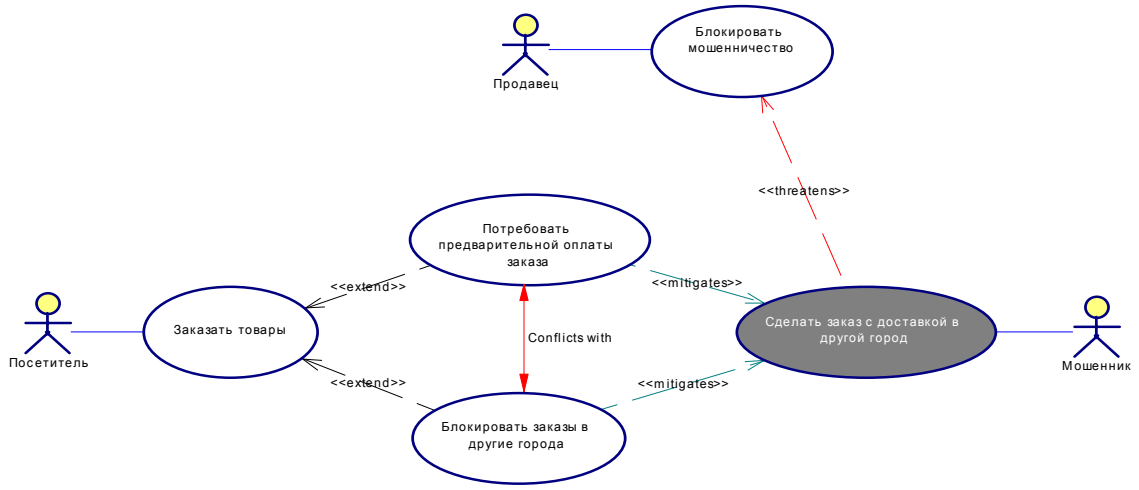

Рисунок № 6

Рассмотрим оставшуюся часть диаграммы. Для борьбы с заказами в другие города, которые делаются мошенниками, не желающими их оплачивать, в процессе анализа были предложены два решения: полностью отказаться от заказов из других городов или требовать от покупателей из других городов предварительной оплаты заказа и его доставки. Как нетрудно заметить, оба решения можно описать сценариями использования, расширяющими сценарий посетителя «Заказать товары». В то же время реализация обоих решений абсурдна, что показано на рисунке стрелкой отношения конфликтности между ними.

Метод применения

Выше были приведены примеры использования нотации, демонстрирующие все предлагаемые в ее рамках способы выражения. Теперь рассмотрим как можно применять метод сценариев некорректного использования на этапах сбора требований и системного анализа.

Сбор требований

В процессе сбора требований выявляются все участники работы системы (актеры) и основные выполняемые действия (сценарии). Таким образом появляется первое описание системы – состав актеров и преследуемые ими цели при работе с разрабатываемой системой.

При этом во время сбора требований можно выявить большинство актеров, которые могут оказать негативное или нежелательное воздействие на систему и наиболее очевидные и вероятные методы этого воздействия.

По результатам сбора требований должны быть построены две модели: модель сценариев использования системы и модель сценариев некорректного использования. На этом этапе достаточно иметь несколько диаграмм и краткие описания получившихся сценариев (в том числе и сценариев некорректного использования).

В завершение должны быть разработаны диаграммы, на которых обе модели (обычных сценариев использования и сценариев некорректного использования) объединяются для отображения их взаимосвязей. На этой стадии это будут зависимости угрозы успешному выполнению (со стереотипом «threatens») шагов сценариев использования и, возможно, небольшое количество зависимостей ослабления негативного влияния сценариев некорректного использования (со стереотипом «mitigates»).

Системный анализ

На этапе системного анализа собранные требования анализируются на полноту и согласованность. В частности, подготавливаются подробные описания для всех сценариев, включающие нормальную последовательность действий и альтернативные последовательности. Такие же описания следует составить для сценариев некорректного использования, по возможности, максимально точные.

После того, как основные элементы моделей сценариев подробно описаны, можно приступать к их анализу, в частности, к выявлению между ними зависимостей.

В первую очередь следует убедиться, что все зависимости угрозы выявлены. Дело в том, что один сценарий некорректного использования может угрожать успешному выполнению сразу ряда сценариев использования. На моделях следует указать все выявленные угрозы или, если их оказывается слишком много, описать зависимость на модели более высокого уровня абстракции.

Например, DoS атака Web-сервера хакером мешает выполнению посетителем любых действий с системой. Для описания этой угрозы разумно построить модель, где посетитель выполняет действия абстрактного сценария «Использовать Web-сервер», а хакер выполняет действия сценария некорректного использования «Применить DoS атаку», угрожающего выполнению действий сценария «Использовать Web-сервер».

После того, как все зависимости угрозы выявлены и обозначены, следует приступать к их анализу. В первую очередь, разумно выделить уже выявленные и описанные сценарии использования, уменьшающие эффект от выполнения действий сценариев некорректного использования. После чего следует проанализировать методы уменьшения влияния на систему остальных сценариев некорректного использования. В результате такого анализа в модель могут быть добавлены дополнительные сценарии использования, необходимость в которых изначально не была осознана. В заключение, все выявленные зависимости уменьшения эффекта сценариев некорректного использования помещаются на модель.

Последним шагом применения метода анализа некорректных сценариев использования является выявление и анализ отношений конфликтности между сценариями использования и дополнительный анализ того, что все угрозы от сценариев некорректного использования уменьшаются смоделированными сценариями использования адекватно их значимости для разрабатываемой системы.

В результате применения метода анализа некорректных сценариев использования должна получиться модель сценариев использования, учитывающая все значительные угрозы успешному функционированию системы.

Заключительный пример
В заключение хочется привести еще один пример применения метода. На рисунке №7 изображена модель, построенная в процессе последовательного анализа сценариев обоих типов.

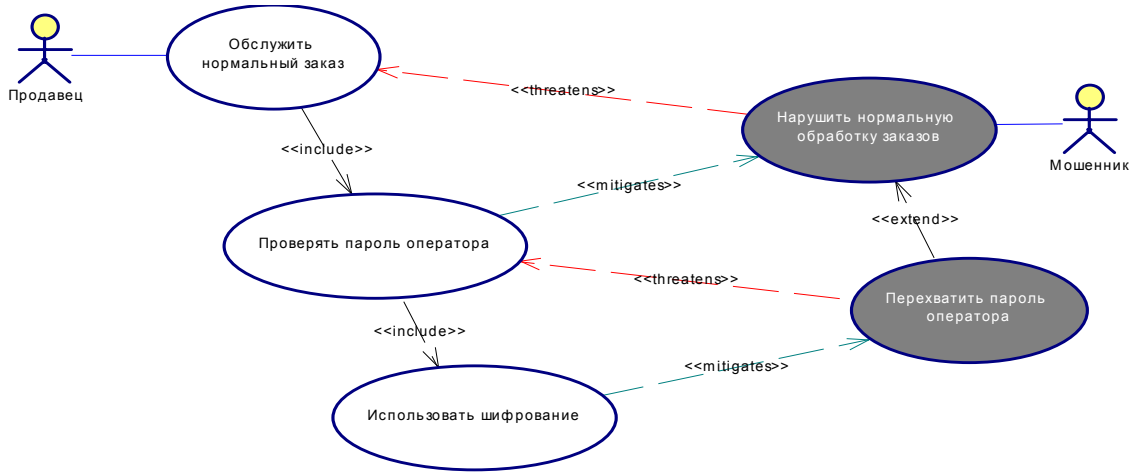

Рисунок № 7

Первым шагом на модель был помещен сценарий использования продавца «Обслужить нормальный заказ». После чего на модели было отмечено, что мошенник может попытаться нарушить нормальную обработку заказов, проникнув в систему.

Для уменьшения вероятности такого воздействия было решено добавить в систему обработки заказов проверку пароля оператора при обращении к системе. Такое расширение функциональности затруднило проникновение мошенника в систему.

После продолжения анализа некорректных сценариев использования было выявлено, что мошенник может попытаться перехватить пароль оператора, прослушав канал передачи данных. Такие действия со стороны мошенника делают малоэффективным использование паролей, так как чуть более опытный мошенник сможет проникнуть в систему под перехваченным паролем.

Для уменьшения вероятности, что мошенник все же узнает пароль, перехватив его, было решено обмениваться паролями в системе только с использованием шифрования. В результате применения шифрования перехват пароля мошенником практически потерял смысл, тем самым эффект от сценариев некорректного использования опять был уменьшен. После очередного этапа анализа было решено, что эффект от такого рода сценариев некорректного использования уменьшен до приемлемого уровня и анализ модели можно завершить.

Заключение

Метод описан, примеры рассмотрены. Надеюсь, его применение поможет вам в разработке качественных программ, стабильно и корректно работающих даже в не запланированных ситуациях, под воздействием злоумышленников, в руках неопытных пользователей.

В то же время нужно понимать, что рассмотренный метод всего лишь подход к структурированию и анализу информации о некорректном использовании системы, предполагаемых угрозах и негативных воздействиях. Он не отвечает на вопрос, что угрожает работе системы. Его задача – предоставить разработчикам инструмент для документирования и анализа нежелательных ситуаций на этапах сбора требований и системного анализа.

Описанный в статье метод очень новый, но, я уверен, он будет поддержан и найдет широкое применение. Если у вас возникли вопросы или замечания, буду рад их обсудить (mikkri@mail.ru).

Ссылки

Ian Alexander's Home Page: http://easyweb.easynet.co.uk/~iany/index.htm
Alistair Cockburn’s Home Page: http://alistair.cockburn.us/