УДК 004.942

Р.С. Тимонин, К.А. Пшеничный
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Санкт-Петербург
E-mail cpshenichny@yandex.ru

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ МЕТОДА ДИАГРАММ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Тимонин Р.С, Пшеничный К.А. Исследование применимости метода диаграмм деятельности в сфере информационной безопасности. *Целью данной работы является исследование применимости метода диаграмм деятельности в сфере информационной безопасности. Результатом работы является модель представления анализируемого процесса на примере банковской деятельности. Такие модели можно применять в различных случаях, связанных с выявлением и анализом нетипичных значений, и в конечном счете прийти к формальной классификации информационных угроз в зависимости от свойств модели.*

Введение. Достижения в сфере информационных технологий и массовое внедрение средств автоматизации в различных сферах деятельности, наряду с очевидной пользой, многократно увеличивают разнообразие возможных каналов утечки информации и, соответственно, угроз несанкционированного доступа[1] (далее – НСД) к ней. Поэтому весьма полезной для обеспечения безопасности автоматизированной системы (далее – АС) представляется разработка наглядной, максимально исчерпывающей модели угроз информационной безопасности[1] (далее – ИБ) объекта информатизации. Вопрос обеспечения ИБ особенно остро стоит в банковской сфере, где ущерб от информационных угроз может быть исключительно велик[2].

Необходимость проведения настоящей работы вызвана вескими основаниями, изложенными в п.6 Доктрины ИБ РФ[3], полагать, что применяемые в настоящее время в отечественных системах обработки банковской информации организационные меры, а также аппаратно-программные средства защиты не могут обеспечить достаточную степень безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода угрозам с целью доступа к финансовой информации и дезорганизации работы автоматизированных банковских систем.

Существует множество методов для представления угроз объекта информатизации, однако каждый из них имеет свои ограничения, в частности, отсутствие динамической интерпретации процесса взаимодействия с защищаемым объектом. В данной работе угрозы ИБ, возникающие в банковской деятельности при НСД к АС, будут исследованы и наглядно представлены с помощью метода диаграмм деятельности (activity diagrams)[4]. Метод диаграмм деятельности применяется для моделирования динамических аспектов поведения систем[5]. Функционирование АС и воздействие на нее представляет собой динамическое состояния системы, поэтому исследование преднамеренных угроз безопасности АС с помощью метода диаграмм деятельности, изучающего динамические аспекты систем, представляет большой практический интерес.

Целью настоящей работы является исследование применимости метода диаграмм деятельности в сфере информационной безопасности. Для достижения данной цели необходимо разработать модель представления процесса, который может быть подвержен преднамеренным угрозам, с учетом всех тех его аспектов, которые необходимы для данного исследования.

Постановка задачи. В качестве преднамеренной угрозы для примера будет рассмотрена угроза НСД лицом, не имеющего доступа к конкретной АС или отдельным ее элементам, на примере ввода в систему текущих курсов валют. Получив доступ к АС, злоумышленник[6] может нарушить конфиденциальность,

целостность и доступность обрабатываемой в системе информации, в том числе исказить информацию (ввести ложный курс валюты) в целях получения собственной выгоды.

В автоматизированную систему банка каждый день вводят новые данные по курсам валют. При этом система сравнивает вновь вводимые значения курсов с аналогичными значениями, введёнными вчера. Если разница по модулю не превышает некоторого значения, принятого за предельно допустимую разницу и введённого в систему заранее, вновь вводимое значение принимается системой и может быть использовано при проведении банковских операций. Если превышает, система требует от пользователя подтверждения того, что данное значение является истинным.

Таким образом, если ввести в систему заведомо большее значение предельно допустимой разницы, чем то, которое может иметь место в действительности, и сообщить пользователю фиктивное значение курса, система может не потребовать от пользователя подтверждения при вводе заведомо ложного значения курса, которое, соответственно, будет использовано при проведении операций. Это открывает возможность для мошенничества и является преднамеренной угрозой информационной безопасности банка.

Построение вербальной модели. Теперь можно посмотреть, как эта ситуация может быть представлена с помощью метода диаграмм деятельности (рис. 1).

На рисунке рассматривается вербальная модель процесса (деятельности) установки в АС банка нового курса валют, наглядно отображающая с необходимой точностью последовательность атомарных действий для реализации поставленной задачи (от начала ввода курса и заканчивая его установкой в качестве текущего). Весь практический смысл составления модели заключается в анализе всех этих действий, чтобы проследить, на каком из этапов (действии) может возникнуть потенциальная угроза.

Деятельность, как составной элемент диаграммы, является совокупностью простых действий (в данном случае

последовательных)[7]. Начало диаграммы исходит из начального состояния[8]. Далее следует действие «Ввести курс валюты». Это действие влечет за собой ввод нового курса валюты в АС, который устанавливается текущим ежедневно (за исключением выходных и праздничных дней).

Казалось бы, что еще нужно для установки введенного курса валюты текущим курсом. Однако, есть еще несколько простых действий, призванных минимизировать возможные ошибки оператора АРМ в АС при вводе нового курса, а также предотвратить ввод ложного значения курса валюты злоумышленником.

Одним из таких защитных механизмов является следующий далее узел решения. Выполняя проверку на наличие непустого значения в форме ввода курса валюты, он, тем самым, предотвращает возникновение дальнейших ошибок при условии перехода к следующему действию. Естественно, при пустом значении в форме узел решения переведет процесс выполнения деятельности снова к действию «Ввести курс валюты». Этот цикл будет продолжаться до тех пор, пока оператор не введет значение курса, отличное от пустого.

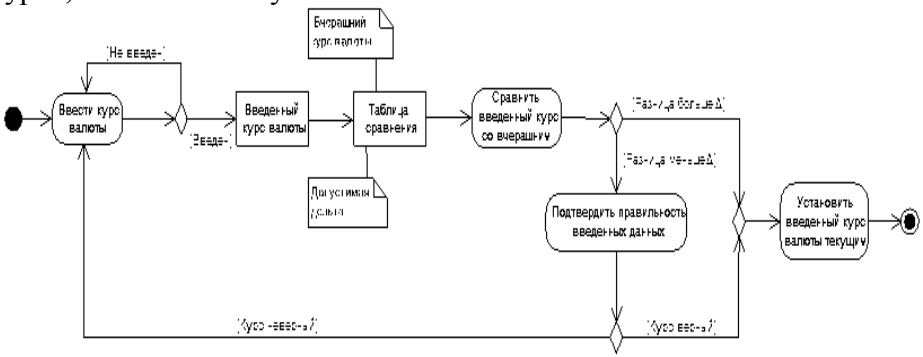

Рис. 1 – Метод диаграмм деятельности. Вербальная модель

За узлом решения в диаграмме следует объект «Введенный курс валют», который в действительности символизирует тот самый курс валют, введенный оператором АРМ.

Введенный курс попадает в таблицу сравнения, в которой помимо вчерашнего курса валют содержится значение, представляющее собой предельно допустимую разницу между вчерашним курсом валюты и только что введенным. То есть по сути это значение является дельтой ввода. Сама таблица сравнения отображается в виде одноименного объекта с прилагающимися к нему комментариями. Каждый из комментариев («Вчерашний курс валюты» и «Допустимая дельта») указывает на нахождение в таблице сравнения этих самых непустых значений.

Теперь, когда в диаграмме инициализированы все необходимые значения для сравнения, состояние деятельности переходит к действию «Сравнить введенный курс со вчерашним». Это действие находит разницу по модулю между значениями введенного курса валюты и вчерашним курсом.

На этом сравнение как таковое не заканчивается. Далее осуществляется переход к очередному узлу решения, который в зависимости от величины значения дельты, полученной в результате сравнения значений курса валют, принимает одно из решений. Либо состояние деятельности переходит к узлу объединения (для узла объединения только при выполнении того или иного действия осуществляется переход к следующему узлу управления) при полученной дельте меньше допустимой дельты, либо в ином случае переходит к еще одному проверочному действию.Следует рассмотреть второй случай. Дельта, полученная при сравнении введенного и вчерашнего курсов валют, оказывается больше допустимой. Здесь можно было бы выдать сообщение об ошибке и предложить заново ввести курс валюты, то есть, по сути, вернуться к начальному состоянию диаграммы и проделать весь путь до этого момента заново. Однако учитывая сложившуюся текущую обстановку с курсом рубля по отношению к таким крупным валютам, как европейская валюта и доллар США, когда курс может измениться в меньшую или большую сторону на несколько единиц или даже десятков значений, этого делать нельзя[9][10]. Допустимая дельта в стабильной экономической ситуации обычно равна десятым

долям, текущая же ситуация непредсказуема[11]. Поэтому даже если полученная дельта превышает допустимую, процесс не начинается заново с ввода нового курса валюты заново, а переходит далее к подтверждению правильности уже введенного курса. В этой ситуации может играть роль человеческий фактор, поэтому оператор, вводивший курс, должен перепроверить его значение. Соответственно, если оператор действительно ошибся, он переходит к начальному состоянию деятельности и начинает вводить курс валюты заново. Если он подтверждает правильность введенного уже курса, то состояние деятельности переходит к узлу объединения. В этом случае необходимо предельно осторожно подходить к реализации подобной системы подтверждения правильности введенных данных, так как вероятно возникновение ошибки второго рода. Если подтверждение правильности не вводить, то появляется вероятность появления ошибки первого рода.

Под ошибкой первого рода понимается ложная тревога, например, курс валюты введен верно, а установленные критерии защиты не позволяют этот курс установить текущим.

Под ошибкой второго рода понимается пропуск события, например, курс валюты введен неверно, но являясь злоумышленником, оператор, или другое лицо, несанкционированно получившее доступ к АРМ АС банка, подтверждает правильность ввода и устанавливает ложный курс текущим.Необходимость введения действия подтверждения данных при полученной дельта больше допустимой дельты должна исходить из текущей экономической ситуации в стране, о чем было сказано выше.

Итак, остается рассмотреть узел объединения. При правильности введенного курса (достоверность определяется либо автоматически при сравнении полученной дельты ввода с допустимой дельтой, либо непосредственно подтверждением оператором АРМ), определенной несколькими способами, состояние деятельности переходит к узлу объединения, который действительно объединяет доступные пути получения факта достоверности и приводит их к одному результату – переход к

следующему, последнему действию «Установить введенный курс валюты текущим». Это действие происходит без лишних подтверждений, условий, и т.п. и заканчивается конечным узлом (состоянием) деятельности.

Построение субъектно-предикатной модели

Можно исследовать преднамеренную угрозу банковской АС в той же ситуации с вводом курса валюты, но уже на примере субъектно-предикатной модели[12] (рис. 2).

На первый взгляд модели кажутся отдаленно похожими, сразу бросаются в глаза два конечных узла деятельности, в вербальной модели был один конечный узел. На самом деле модели, и вербальная, и субъектно-предикатная, отображают одну суть.

Прежде чем переходить уже к непосредственному сравнению моделей, необходимо пояснить условные обозначения, используемые на диаграмме. Если в вербальной модели субъектом проводимых операций (протекания процесса деятельности) был оператор АРМ АС банка, который вводил курс валют, сравнивал его со вчерашним курсом, а сам курс выступал объектом деятельности, то здесь в роли субъекта (сущности) выступает курс валюты. Поэтому все действия совершает как бы сам курс (он «содержится в голове», он «является введенным» и т.п.).

Еще одна особенность субъектно-предикатной модели представляет собой охват каждым одним действием всех действий (состояний) деятельности, но в соответствующий каждый отдельный момент рассматривается только действие (в редких случаях действия), выполняемое в данный момент. Остальные действия неактивны в настоящее время, либо они уже совершены, либо не совершены и будут совершены в дальнейшем (такие несовершенные действия обозначаются символом инверсии).

Касаясь самого предмета субъектно-предикатного динамического знания, необходимо условиться, что невозможно отрицание всех действий, ибо если все отрицается, то ничего и нет. Поэтому первым действием после начального состояния диаграммы деятельности является действие курса валют –

«Содержится в голове», которое на первый взгляд может показаться довольно странным. Это действие принимается как неоспоримое начальное действие деятельности.

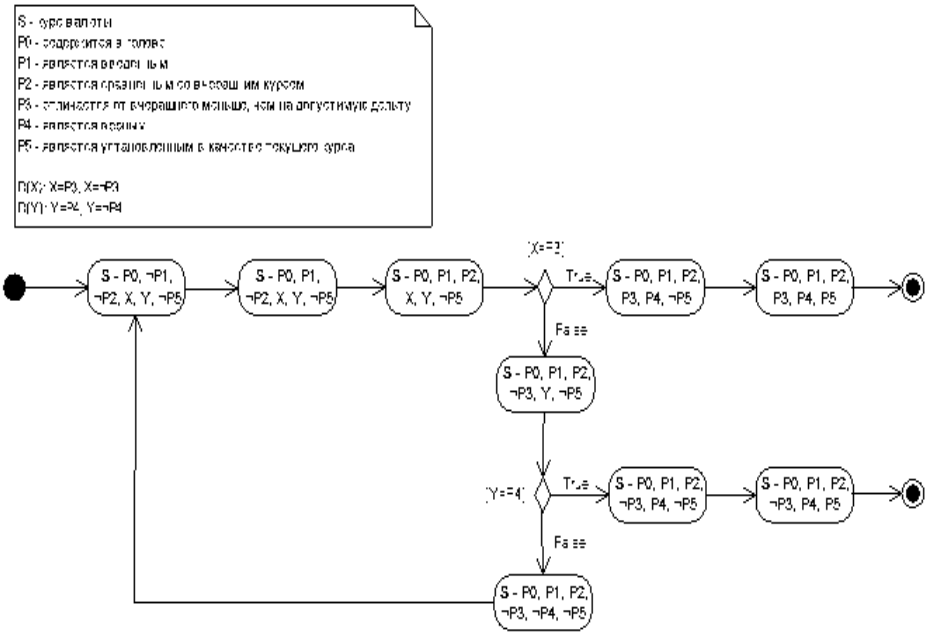

Рис. 2 – Метод диаграмм деятельности.

Субъектно-предикатная модельСимвол S является воплощением субъекта (сущности) курса валюты, в символе P находят свое отображение действия. X и Y – действия (состояния), которые могут быть как совершены, так и не совершены в данный момент времени, то есть по сути являются неизвестными состояниями. Это можно объяснить, как если бы чтобы узнать совершено ли это действие или нет, нужно выполнить еще несколько действий. Так действие X включает в себя два состояния: курс валюты «отличается от вчерашнего курса меньше, чем на допустимую дельту» и соответственно, отрицание предыдущего состояния, то есть курс валюты «не отличается…». Действие Y также включает два состояния: курс валюты «является верным» и «не является верным». Естественно,

нельзя заранее определить, является ли курс введенным верно, не проделав предварительно еще несколько действий.

Сравнение вербальной и субъектно-предикатной моделей. Теперь, когда особенности субъектно-предикатной модели рассмотрены, можно приступить к пошаговому сравнению модели с вербальной моделью.

Начальным действием вербальной модели является действие «Ввод курса валюты», в то время, как уже было замечено выше, диаграмма субъектно-предикатной модели начинается с действия курса валюты – «Содержится в голове». Причина такого различия заключается в особой предустановке субъектно-предикатной модели: невозможно отрицать все состояния сущности, иначе тогда ее самой не может существовать.

Далее, после действия ввода курса валюты в вербальной модели следует узел решения, подтверждающий факт ввода данных в АС банка. В случае с языком субъектно-предикатного знания, здесь такой необходимости нет, т. к. в отличие от вербального языка субъектно-предикатный язык является довольно строгим, не допускающим различного рода неоговоренности.

Объекты, «Введенный курс валюты» и «Таблица сравнения» вместе с приложенными комментариями, являются необязательными в вербальной модели, но опять же, используются для наиболее полного представления картины протекающий деятельности.

Действия сравнения и следующие за ними узлы решения, которые в зависимости от результата сравнения определяют дальнейший путь протекания деятельности, идентичны в обеих моделях.

Основное визуальное различие между диаграммами обеих моделей заключается в дальнейших развязках деятельности. В вербальной модели в случае положительного результата сравнения полученной дельты ввода и допустимой дельты, а также в случае подтверждения правильности отрицательного результата сравнения достаточно интегрировать эти потоки управления, исходящие с двух различных узлов, в одно действие,

с помощью узла объединения. Смысл понятен: если курс валюты является верным, то необходимо установить его в качестве текущего курса, что, собственно, и отображает диаграмма. С субъектно-предикатной моделью не все так просто. При проведении сравнения двух значений дельты, полученной и допустимой, на выходе получаются два различных состояния (полученная дельта меньше допустимой, или наоборот), которые в субъектно-предикатном языке уже нельзя объединить в одно состояния. Эта разница возникает в силу того факта, что каждое состояние субъектно-предикатной модели включает в себя все предыдущие и будущие состояния, которые на данный момент являются неактивными, но, тем не менее, они существуют (см. выше). Стоит заметить, что смысл от этого различия в моделях не меняется: и в субъектно-предикатной, и в вербальной модели в случае верно введенного курса он устанавливается в качестве текущего. Перед установкой курса в качестве текущего в субъектно-предикатной модели необходимо дополнительное состояние (действие): курс валюты «Является верным». Данное действие необходимо для того чтобы в случае неверно введенного курса (этот факт выявляется при подтверждении оператором правильности), можно было перейти на действие курса валюты – «Не является верным», уже от которого поток управления перейдет к начальному действию курса валюты – «Содержится в голове» – для введения курса валюты заново. Вербальная модель дополнительных разъяснений в данном случае не требует.

Заканчиваются диаграммы обеих моделей конечным состоянием. Разница лишь в том, что в вербальной модели одно конечное состояние, а в субъектно-предикатной, в силу особенностей ее языка, их два (см. предыдущий абзац).

Несмотря на визуальное отличие диаграмм обеих моделей, практический смысл их представления одинаков, различия же являются отражением особенности их языка (вербальный язык и язык субъектно-предикатного динамического знания).

Заключение. Для подведения итогов проделанной работы необходимо разъяснить практический интерес разработанной модели, а также перспективы их применения.

Ссылаясь на конкретную, разработанную в настоящей работе модель (две получившиеся модели, по сути, являются одной и той же моделью, только представлены с помощью разных «языков» – вербального и субъектно-предикатного), можно сделать вывод, что эта наглядная модель, раскладывающая весь процесс ввода курса валюты в автоматизированную систему банка на минимально возможные единицы деятельности – простейшие действия, облегчает выявление потенциальных угроз на всех этапах этого процесса. Таким образом, ответственное должностное лицо за обеспечение безопасности АС может проследить, какие конкретные действия совершаются оператором при течении процесса ввода курса валюты, и заблаговременно выявить возможные каналы утечки информации. Здесь необходимо смотреть на эту ситуацию с разных сторон, наблюдать и моделировать, что может происходить при различных вариантах развития событий, тем самым предугадывая возможные действия злоумышленника. Соответственно, после этого разработать превентивные меры.

Также разработанную модель можно применять и в других случаях. Следующие примеры показывают актуальность применения этой модели в совершенно разных сферах деятельности:

На производстве для автоматического контроля качества продукции сложных изделий, когда параметр вновь производимого изделия сравнивается с неким допуском, но в некоторых случаях может и выходить за его пределы (но если допуск задан неадекватно, система не распознает опасности брака);

В диспетчерских службах в авиации, когда в некоторых случаях, вероятно, диспетчер может разрешить тому или иному борту манёвр, формально выходящий за рамки допустимого (здесь встает вопрос, насколько корректно задано это самое "допустимое" значение), или в работе автопилота на борту, когда система не "призовёт на помощь" пилота, решив, что ситуация не выходит за рамки штатной, в то время как в действительности выходит (в этом случае неверно заданы "рамки");

При анализе большого количества данных (в самых разных областях), когда необходимо выявить и проанализировать "отскоки", нетипичные значения, лежащие вне поля "обычных" значений – границы этого поля задаются принимаемыми допущениями относительно значений статистических параметров (предельно допустимой "дельтой").

Таким образом, можно формально сформулировать тип информационных угроз, описываемых данной моделью. Далее, внутри этого типа можно анализировать опыт из разных областей – и передавать с требуемым обобщением, например, опыт банковских служащих авиадиспетчерам и наоборот.

Далее, если продолжить строить подобные модели одним и тем же методом, можно в результате прийти к формальной классификации информационных угроз в зависимости от свойств модели, описывающей каждый тип – наряду с теми сугубо утилитарными и не всегда безупречными классификациями, которыми сейчас описываются угрозы. А это выводит информационную безопасность на качественно новый уровень.

Список литературы

1. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992. – 13 с.;

2. Информационная безопасность предприятия: сущность [электронный ресурс]. – режим доступа: http://1fin.ru/?id=809, свободный (20.03.15);

3. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1897;

4. Википедия. Диаграмма деятельности [электронный ресурс]. – режим доступа: https://ru.wikipedia.org/wiki, свободный (20.03.15);

5. Г. Буч, Д. Рамбо, А. Джекобсон. Язык UML - Руководство пользователя. ЧАСТЬ IV - Основы моделирования поведения. Глава 19. Диаграммы деятельности [электронный ресурс]. – режим доступа:

http://dit.isuct.ru/ivt/books/CASE/case11/ch19.htm , свободный (20.03.15);

6. Информационная безопасность и защита информации. Учебное пособие. – Ростов-на-Дону, 2004 [электронный ресурс]. – режим доступа: http://window.edu.ru/library/pdf2txt/482/57482/27741, свободный (20.03.15).

7. Центр дистанционного образования. Лекция 9. Диаграмма деятельности [электронный ресурс]. – режим доступа: http://edu.dvgups.ru/METDOC/GDTRAN/YAT/ITIS/PROEK_INF_SIS/METOD/KURS_L/frame/frame_tema9.htm , свободный (20.03.15);

8. Национальный открытый университет Интуит. Лекция 5: Диаграмма активностей: крупным планом [электронный ресурс]. – режим доступа: http://www.intuit.ru/studies/courses/1007/229/lecture/5958 , свободный (20.03.15).

9. Центральный Банк Российской Федерации. Динамика официального курса заданной валюты [электронный ресурс]. – режим доступа: http://www.cbr.ru/currency_base/dynamics.aspx?VAL_NM_RQ=R01235&date_req1=20.11.2014&date_req2=20.03.2015&rt=1&mode=1 (20.03.15);

10. Википедия. Финансовый кризис в России (2014—2015) [электронный ресурс]. – режим доступа: https://ru.wikipedia.org/wiki, свободный (20.03.15);

11. Центр обмена СКВ Пушкарский. Покупка доллара - как формируется курс? [электронный ресурс]. – режим доступа: http://www.push52.ru/reader.aspx?ModeName=view&TypeNoteName=News&NoteName=pokupkadollara (20.03.15).

12. Pshenichny, C.A., and Mouromtsev, D.I., 2015. Grammar of Dynamic Knowledge for Collaborative Knowledge Engineering and Representation. In: Diviacco, P., Fox, P., Pshenichny, C., Leadbetter, A. (Eds): Collaborative Knowledge in Scientific Research Networks, IGI Global, pp 323-354.