Е.В. Иванов[1]
А.И. Иванова[2]

МЕТОДЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ ПРОЦЕССИНГОВОГО ЦЕНТРА

В данной статье описываются методы и средства имитационного моделирования, дается их классификация. Приводится краткий обзор существующих средств имитационного моделирования. Рассматривается модель работы службы безопасности на предмет зависимости затрачиваемых средств от поставленных задач, разъясняется необходимость применения моделирования для решения подобных задач. Также анализируется одна из зарубежных моделей.

Ключевые слова: *информационная безопасность, анализ защищенности, имитационное моделирование, системная динамика, процессинговый центр, причинно-следственная диаграмма, потоковая диаграмма.*

E.V. Ivanov
A.I. Ivanova

IMITATION MODELING METHODS OF SECURITY SUBSYSTEMS OF A PROCESSING CENTER

In this article, authors describe methods,classification and tools of simulation modeling. Authors observe the existing simulation tools and chose system dynamics to explore the field of information security. The analysis of security department model and how costs depend on goals is given. Also the necessity of the model implementation to solve security problems in financial organization is explained. One of the foreign models that explore insider threats to informationinfrastructure is investigated.

Keywords: *information security, security analysis, simulation modeling, system dynamics, processing center, causual loop diagram, levels and flows diagram.*

Исследование подсистемы безопасности с помощью имитационного моделирования состоит в организации и проведении компьютерного эксперимента на имитационной модели. Такой компьютерный эксперимент заключается в построении и выполнении модели и наблюдении за ее поведением при заданных значениях входных факторов, то есть в проведении экспериментов вида «что если». Инструмент имитационного моделирования в этом случае должен обеспечить удобный интерфейс для задания значений исходных параметров (факторов) и регистрации соответствующих значений выходных показателей и их изменения во времени [1].

Вопросы моделирования обеспечения информационной безопасности активно исследуются на протяжении десятков лет. В большинстве случаев используется имитационное моделирование как средство модуляции поведения, прогнозирования и последующего анализа результатов работы той или иной системы. Имитационное моделирование имеет ряд преимуществ по сравнению с аналитическим или иными типами моделирования, а именно:

- возможность быстро просчитывать различные варианты будущего (смоделировать сценарии), изменяя исходные данные, полученные экспертным путем;
- выявление наиболее критических факторов (например, что важнее: усиление проверки трафика на вредоносное содержимое или его пропускная способность), таким образом их можно ранжировать по степени важности рисков и возможностей, появляющихся в моделируемой среде;
- использование большого количества причинно-следственных связей между элементами имитационной модели, которые объективно существуют в моделируемой среде (например, уменьшение бюджета на средства защиты (причина) – увеличение количества атак и уменьшение уровня защищенности (следствие) и т.д.);
- наглядность вводимых данных и получаемых результатов.

Динамическую модель можно назвать «живой» в том смысле, что каждое ее состояние за-

[1] Аспирант кафедры информационной безопасности банковских систем факультета информационной безопасности НИЯУ МИФИ.

[2] Аспирант кафедры теории и технологии управления факультета государственного управления МГУ.

висит от ее предшествующих состояний в каждый момент времени, то есть модель развивается, «живет» в соответствии с заложенными в ней законами, правилами.

Динамическая модель является динамической в том смысле, что в каждый момент времени одно состояние напрямую или косвенно зависит от другого или нескольких. Изменение каждого состояния соответствует заложенным в него законом и правилам.

Однако существует ряд ограничений при использовании имитационного моделирования. Во-первых, изменения разных систем происходят с разной скоростью, когда эти скорости накладываются друг на друга, возникают проблемы восприятия. Например, несанкционированное копирование базы данных происходит определенное время, а анализ подключений – моментом. Во-вторых, изменения в одном элементе системы обычно влекут трудно предсказуемые изменения в остальных элементах, система переходит в новое состояние, меняется ее поведение. Например, внешний *firewall* прекратил фильтрацию, и система работает с новыми свойствами. В-третьих, из-за нелинейности многих процессов предсказывать поведение системы невозможно, используя лишь экстраполяцию ее тренда поведения в прошлом. Причина и следствие растянуты во времени, что затрудняет их выявление, поэтому эффективное решение часто не очевидно на первый взгляд.

Разработано большое количество разнообразных формальных и неформальных моделей отдельных механизмов защиты. Однако если подняться на уровень выше и посмотреть шире, то моделей, связанных с необходимостью применения тех или иных механизмов защиты, выделения ресурсов для этого – крайне мало. Вполне очевидно, что легче решить конкретную задачу защиты, смоделировать процесс атаки, построить математическую модель, нежели комплексно смоделировать задачи, стоящие перед службой информационной безопасности, провести имитационное моделирование поведения подсистемы защиты.

В данной работе, приведена попытка разъяснить особенности имитационного моделирования, провести классификацию существующих средств и построить модель на примере службы информационной безопасности процессингового центра (ПЦ).

Классификация средств имитационного моделирования

Традиционно математические модели разделяют на аналитические и имитационные. Аналитические модели представляют собой уравнения или системы уравнений, записанные в виде алгебраических, интегральных, дифференциальных, конечно разностных и иных соотношений и логических условий. Они записаны и решены в буквенном виде. Аналитическая модель, как правило, статическая. Аналитическое представление подходит лишь для очень простых и сильно идеализированных задач и объектов, которые, как правило, имеют мало общего с реальной действительностью, но обладают высокой общностью. Данный тип моделей обычно применяют для описания фундаментальных свойств объектов, так как фундамент прост по своей сути. Сложные объекты редко удается описать аналитически. Альтернативой аналитическим моделям являются имитационные модели (динамические). Основное отличие имитационных моделей от аналитических состоит в том, что вместо аналитического описания взаимосвязей между входами и выходами исследуемой системы строят алгоритм, отображающий последовательность развития процессов внутри исследуемого объекта, а затем имитируют поведение объекта на компьютере. К имитационным моделям прибегают тогда, когда объект моделирования настолько сложен, что адекватно описать его поведение математическими уравнениями невозможно или затруднительно. Имитационное моделирование позволяет разлагать большую модель на части (объекты, «кусочки»), которыми можно оперировать по отдельности, создавая другие, более простые или, наоборот, более сложные модели. Таким образом, основным преимуществом имитационного моделирования по сравнению с аналитическим является возможность решения более сложных задач, так как имитационную модель можно усложнять, при этом результативность модели не падает [2]. Для наглядности представим виды моделирования на схеме, см. рис. 1.

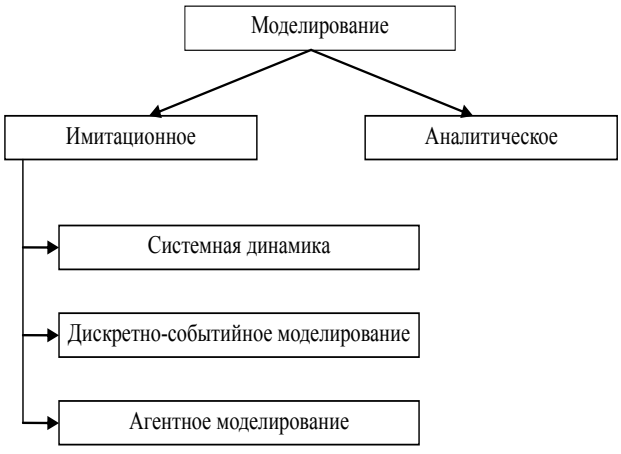

Рис. 1. Виды моделирования

Рассмотрим подробнее имитационное моделирование, оно подразделяется на три основных подхода:

• системная динамика;

• дискретно-событийное моделирование;

• агентное моделирование.

Первые два подхода являются «традиционными» методами имитационного моделирования. Агентное моделирование – относительно новый метод, получивший широкое распространение только после 2000 года. Системная динамика и дискретно-событийное моделирование рассматривают систему сверху вниз, работая на так называемом системном уровне. Агентное моделирование сфокусировано на физическом уровне, где важны отдельные физические объекты, их индивидуальное поведение и физические связи, точные размеры, расстояния, временны́е промежутки.

Системная динамика предполагает наивысший уровень абстракции, когда исследователь абстрагируется от индивидуальных объектов и их поведения. Дискретно-событийное моделирование оперирует на среднем уровне, то есть работает с отдельными объектами, но их физическими размерами пренебрегает (значения скоростей, времени усредняются или используются их стохастические значения). Что касается агентного моделирования, оно может применяться практически на любом уровне абстракции и в любых масштабах. Агенты могут представлять компьютеры, средства защиты, сеть или ПО в физическом пространстве (низкий уровень), администратора или злоумышленника на среднем уровне, или же компанию или финансовый институт на высоком уровне [3].

При имитационном моделировании используют как отечественные, так и зарубежные программные продукты. Для построения моделей, основываясь на подходах системной динамики, используют *STELLA* или *iThink*, *Powersim*, *Vensim* или *AnyLogic* [4]. При дискретно-событийном моделировании существует большее количество средств, например *AnyLogic*, *Arena*, *Extend*, *Witness*, *SimProcess*, *AutoMod*, *PROMODEL*, *Enterprise Dynamics*, *FlexSim*, *eMPlant*, *Simul*8 и другие. Для агентного моделирования конкретного программного продукта нет, существуют программные продукты, которые включают данный вид моделирования, например *AnyLogic* или академические разработки – *SWARM*, *RePast*, *AScape*.

Приведем пример имитационной модели для работы службы информационной безопасности процессингового центра.

Актуальность проблемы информационной безопасности ПЦ велика. По сути ПЦ отводится вся техническая сторона операций с банковскими картами, а именно:

• платежи по банковским картам через терминалы самообслуживания и банкоматы;

• выдача наличных через банкоматы;

• платежи через *POS*-терминалы в магазинах, организациях сфер услуг и др.

Также ПЦ занимается внедрением и сопровождением:

• внедрение и поддержка банкоматов, терминалов самообслуживания, *POS*-терминалов;

• контроль работоспособности устройств;

• обновление программного обеспечения устройств;

• внедрение дополнительных услуг.

Мониторинг транзакций на предмет мошеннических операций:

• блокирование карт при обнаружении инцидента;

• отмена транзакции при обнаружении инцидента;

• экспертиза по изъятым поддельным картам;

• разбор претензионных ситуаций со стороны клиентов банков и др.

Вдобавок, ПЦ – это та организация, в которую обращаются клиенты по всем вопросам, связанным с пластиковыми картами, – потеря карты, захват карты банкоматом, установка лимитов по карте, эммисия дополнительной карты и др.

ПЦ работает с персональными данными клиентов банков, что, безусловно, накладывает определенные обязанности на службу информационной безопасности центра. И проблема инсайдеров актуальна вдвойне, по сравнению с другими финансовыми организациями. А соответствие стандарту *PCI DSS*() необходимо в режиме «*Complained*», чтобы ПЦ имел право работать с платежными системами, такими, как *VISA*, *MASTER CARD* и др.

Исходя из вышесказанного, специалисту по информационной безопасности очевидно, что проблемы и задачи в качественной организации системы безопасности и слаженности работы службы безопасности со всеми остальными службами ПЦ имеют высокий приоритет, и этим проблемам отводится немалое количество ресурсов ПЦ.

По причинам ограниченности бюджета руководство ПЦ не может выделять бесконечные ресурсы на работу службы информационной безопасности. Следовательно, происходит следующая ситуация: руководство обращается к начальнику службы информационной безопасности с просьбой огласить бюджет, необходимый ему, чтобы

покрыть максимальное количество рисков информационной безопасности. Начальник службы информационной безопасности должен оценить работу своей службы и потребовать столько средств, сколько ему необходимо, причем обосновать размер запрашиваемых средств.

Интуитивно понятно, что решить такую задачу «на пальцах» невозможно. Довольно сложно предсказать, сколько понадобится средств для тех или иных задач, особенно если одни задачи зависят от других напрямую или косвенно.

Для решения подобной задачи предлагается использовать метод имитационного моделирования (системная динамика в рамках данной работы) зависимости запрашиваемых ресурсов (бюджета) от задач, стоящих перед службой информационной безопасности [5].

Итак, перейдем непосредственно к процессу моделирования задач информационной безопасности. В качестве метода имитационного моделирования будем использовать метод системной динамики. Системная динамика как инструмент принятия решений сегодня используется такими ведущими корпорации, как *General Motors*, *Hewlett-Packard*, *McKinsey&Co*., *Prudential*, *McMillan-Bloedel*, *A.T. Kearney*, *Ford*, *Smith Kline Beecham*, *Dow-Corning*, *Intel*, *British Petroleum*, *Statoil*, *Shell* и другими крупными компаниями. Родоначальником метода принято считать американского ученого Дж. Форрестора (США, Массачусетский технологический институт, 1950-е гг.). Сегодня системная динамика как метод имитационного моделирования применяется успешно уже более полувека. В России к ней стали проявлять активный интерес около пяти лет назад. В Санкт-Петербурге группа разработчиков-консультантов создала самый продвинутый программный продукт на мировом рынке для имитационного моделирования на данный момент – *AnyLogic*, который сочетает системную динамику с дискретным и агентным имитационным моделированием, позволяя создавать комбинированные имитационные модели. Однако в рамках данной работы мы будем рассматривать модель, построенную на языке системной динамики в программном продукте – *Vensim*, обучающая версия которого находится в свободном доступе.

Процесс моделирования можно подразделить на пять этапов. В первую очередь создается причинно-следственная диаграмма. Данная диаграмма помогает выявить ключевые факторы, будущие переменные модели, а также взаимосвязи между ними, определить полярность связей. Переменная *А* оказывает положительное влияние на переменную *Б*, если при прочих равных условиях изменение переменной *А* приводит к изменению переменной *Б* в том же направлении. Если изменение переменной *А* приводит к изменению переменной *Б* в противоположном направлении, то такая связь называется отрицательной. На диаграмме специалистом должно быть учтено как можно больше косвенных и прямых обратных связей. На языке системной динамики такие подсистемы именуются контурами обратной связи. На этом подготовительном этапе моделирования следует выявить балансирующие и самовоспроизводящиеся контуры обратной связи для комплексного анализа моделируемой системы.

Вторым этапом моделирования будет создание потоковой диаграммы, где ключевые параметры системы будут представлены в виде переменных-накопителей. «Потоки» – темп изменения состояния системы, некий процесс во времени. «Накопители» – состояние системы, своеобразный «резервуар», накапливает определенный материальный или нематериальный фактор с течением времени. Принцип аккумуляции: динамическое поведение возникает, когда «потоки» аккумулируются (накапливаются) в «накопителях» [6].

Третий этап – создание компьютерной модели в выбранной среде моделирования, с заданием законов взаимосвязей между переменными на основе потоковой диаграммы.

На четвертом этапе происходит проверка адекватности модели на основе статистических данных прошлых периодов времени и накопленных данных в целом в этой области.

И наконец, пятый этап, ради чего и создается модель – это серия компьютерных (имитационных) экспериментов («прогонов» модели), в ходе которых становится понятным поведение системы в динамике, разрабатываются сценарии и ищутся оптимальные значения ключевых параметров, слабые места, пограничные значения (если необходимо) и т.д.

Рассмотрим на конкретном примере [5] первый этап моделирования работы отдела информационной безопасности, см. рис. 2.

На диаграмме рассматриваются четыре основных балансирующих контура.

1. Контур развития информационной безопасности – П1.

2. Формальный уровень управления – П2.

3. Внедрение новых физико-логических методов защиты – П3.

4. Затраты, связанные с дополнительными анализами рисков, – П4.

Потоковая диаграмма для данной проблемы может выглядеть следующим образом (см. рис. 3).

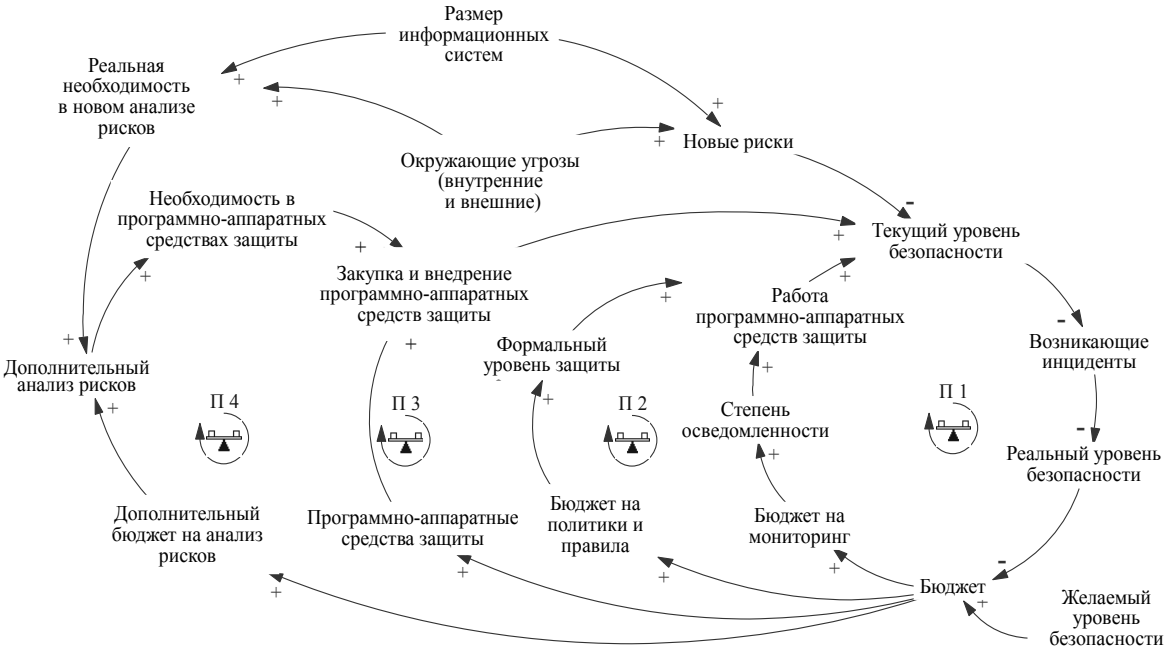

Рис. 2. Причинно-следственная диаграмма выделения бюджета для службы информационной безопасности

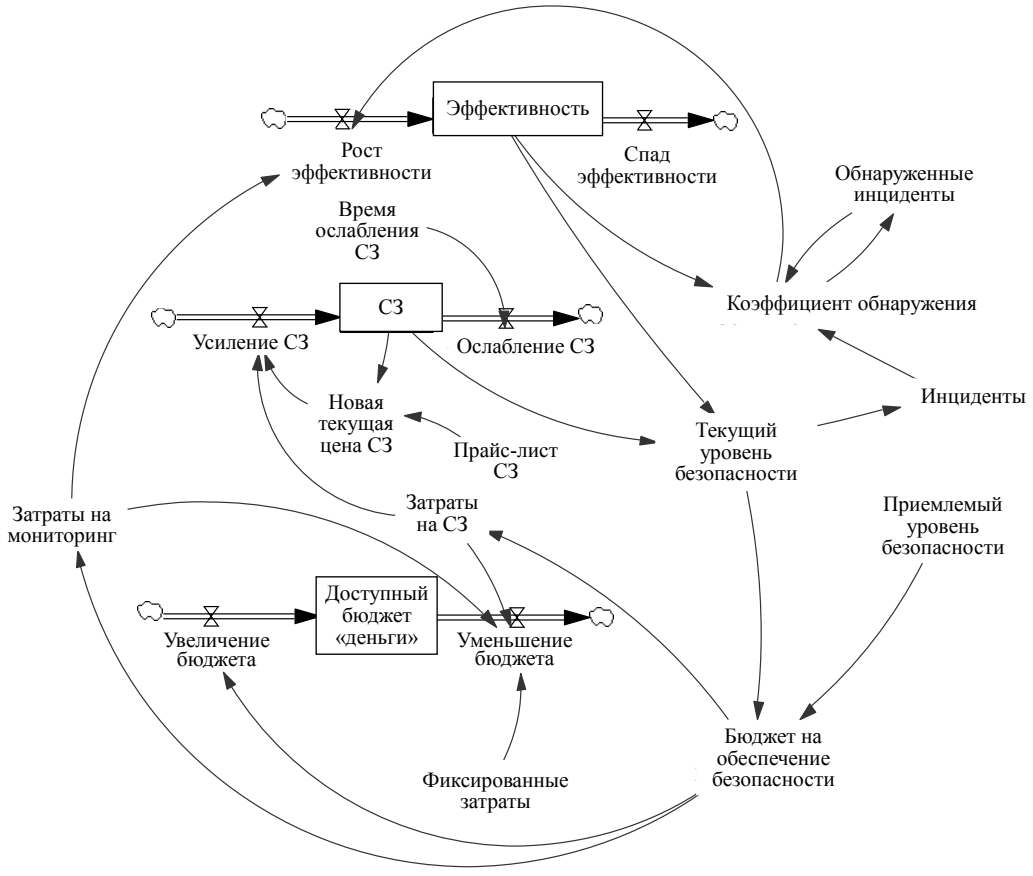

Рис. 3. Потоковая диаграмма работы службы информационной безопасности

Построенная модель основана на доработанной автором зарубежной модели [5] и не означает конечную, точную модель. Модель, построенная на данном этапе этой работы, должна быть выверена и доказана. Но даже на текущий момент она очень полезна для демонстрации способностей системной динамики для получения лучшего понимания того, как связаны те или другие объекты между собой и как одни влияют на другие. После прогона модели на компьютере эксперт службы безопасности получает результаты работы модели и выделяет из них резонные, также он принимает решение о необходимости добавления большего количества переменных в модель, если посчитает нужным. После этого результаты отдаются руководителю службы информационной безопасности.

Пример зарубежного опыта применения имитационного моделирования

Поскольку автор использует зарубежный опыт в основе представленной модели, следует сказать о проблемах адаптации любой имитационной модели к российской среде. При использовании готовой модели можно столкнуться с «подводными камнями», а именно:

• модель ориентирована не на те переменные, которые требуют анализа;

• какими уравнениями связаны переменные – неизвестно;

• актуальность модели в связи с этапом развития человечества;

• человеческий фактор: одно дело проектировать модель под себя, а другое дело – настраивать готовую модель, имея ограниченное количество параметров.

Рассмотрим универсальную модель [7] (см. рис. 4), ориентированную на анализ зависимости применения мер безопасности от атак со стороны сотрудников (инсайдерские атаки, далее – атаки).

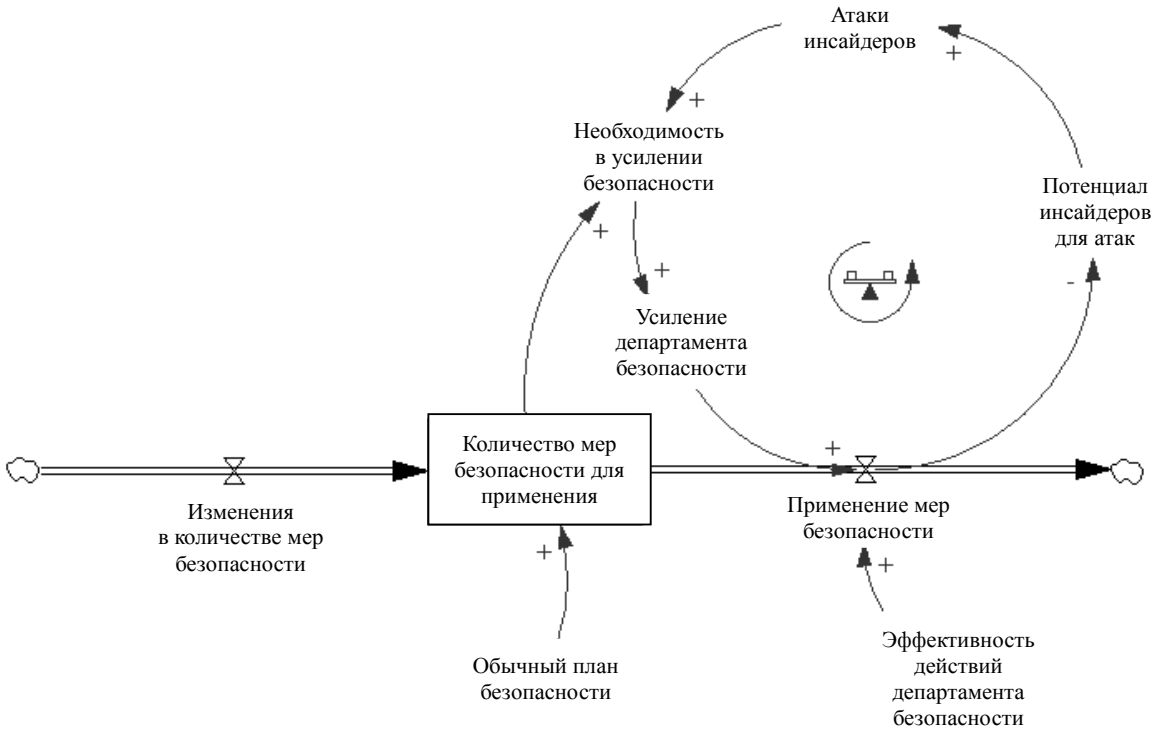

Рис. 4. Универсальная модель

В представленной модели организация имеет план работ по обеспечению безопасности. Этот план описывает количество и типы мер, необходимых, чтобы предотвратить атаки. В модели «департамент информационной безопасности» внедряет меры, чтобы снизить уровень атак. Чем больше мер безопасности будет внедрено, тем ниже будет потенциал атак; таким образом, число атак тоже снизится. Далее, так как число атак снизится, необходимость в усилении безопасности тоже снизится, следствием чего станет уменьшение внедрения средств безопасности. Этот механизм обратной связи имеет эффект балансировки, потому что результатом увеличения внедрения средств безопасности станет уменьшение в дальнейшем внедрения средств безопасности. Меры безопасности уменьшают потенциал атак. Например, способ заполучить неавторизированный до-

ступ к файлам или системам и возможность угадать пользовательские пароли может считаться ресурсом для атаки. Меры безопасности ограничивают эти способы или уменьшают возможности использования этих атак в дальнейшем.

Заключение

Управление информационной безопасностью в организации – динамическая и сложная проблема, которая включает огромное количество переменных и различных факторов. Эффективное управление безопасностью требует баланса между различными факторами. Управление этим динамическим балансом, который включает различные факторы, сложно измерить или предугадать. Процесс моделирования предоставляет расширенные возможности для лучшего понимания всей системы в комплексе. Моделирование способно предсказать, каким будет результат для того или другого фактора, когда на начальном этапе результат совсем неочевиден. Процесс моделирования полезен в области информационной безопасности.

Литература

1. Хабибуллин, Р.Г., Макарова, И.В., Беляев, А.И., Буйвол, П.А. Использование пакета моделирования систем *AnyLogic* для обучения студентов автомобильных специальностей : 4-я Всероссийская научно-практическая конференция по имитационному моделированию ИММОД. – СПб., 2009.

2. Бабина, О.И., Хабибуллин, Р.Г., Макарова, И.В., Беляев, А.И., Буйвол, П.А. Сравнительный анализ имитационных и аналитических моделей : материалы конференции ИММОД. – СПб., 2009.

3. Многоподходное моделирование : электронный ресурс – http://www.xjtek.ru/anylogic/approaches/

4. Борщев, А. Имитационное моделирование : клиенты, модели, разработчики : 2-я Всероссийская конференция ИММОД. – СПб., 2005.

5. Jose M. Sarriegi, Javier Santos, Jose M. Torres, David Imizcoz, Angel L. Plandolit. Modeling Security Management of Information Systems: Analysis of an Ongoing Practical Case : Conference Proceedings : the 24th International Conference of the System Dynamics Society. – 2006 Nijmegen, the Netherlands.

6. Сидоренко, В.Н. Системная динамика. – М. : ТЕИС, 1998. – С. 27–31, 38–40.

7. Ignacio J. Martinez-Moyano, Michael E. Samsa, James F. Burke, Bahadir K. Akcam. Toward a Generic Model of Security in an Organizational Context: Exploring Insider Threats to Information Infrastructure : Proceedings of the 41st Hawaii International Conference on System Sciences – 2008.