МОДЕЛИРОВАНИЕ В ЦЕЛЯХ ОБЕСПЕЧЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ И ОПЫТ ПРИМЕНЕНИЯ

П.Ю. Филяк (Сыктывкар)

«Любая модель есть иллюзия, которую личность воспринимает как реальность, оживляя ее своим воображением»

(К. Кастанеда «Отдельная реальность»)

Роль и место моделей в нашей жизни трудно переоценить – ребенок, появившийся на свет, познает окружающий мир через модели. Модели это его игрушки, от простых до очень совершенных. В мире животных высшие млекопитающие при воспитании своих детенышей тоже используют модели – игрушки, правда, более примитивные, в основном естественного характера. В России и в СССР моделирование имеет глубокие корни и серьезные результаты. В настоящее время с развитием информационных технологий применение моделей становится все более массовым явлением, но, к сожалению, о повсеместном использовании моделей для решения широкого спектра задач говорить пока рано. Основные задачи, решаемые моделями, – задачи познания, обучения, анализа, производства, прогнозирования, инжиниринга, менеджмента (управления) – применительно к организациям. Согласно ГОСТ 15971-90 «Системы обработки информации. Термины и определения» **машинное моделирование** (Simulation) – реализуемый на вычислительной машине метод исследования, предполагающий замену реального процесса его математической моделью.

На сегодняшний день в сферах, где вопросы безопасности играют ключевую роль, а также где неверные управленческие решения могут вызывать серьезные социально-экономические последствия, модели применяются широко. Одной из таких сфер, где широко применяется моделирование, является обеспечение безопасности, по всем направлениям, которые являются составляющими национальной безопасности [1,2], в частности, информационной безопасности (ИБ). В законодательных и нормативных правовых актах, в стандартах, частности ГОСТах, дается определение понятий применяемых моделей и задается их статус и определенным образом регламентируется порядок их применения.

К таковым относятся – само понятие **модель, эмуляция, модель предприятия, информационная модель, модель жизненного цикла, модель угроз, модель нарушителя, модель защиты**. В частности, в соответствии с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

Помимо математических методов, позволяющих самостоятельно составить имитационную модель, что зависит от уровня математической подготовки и квалификации постановщика задач и лиц, реализующих поставленную задачу, разработано множество инструментов, позволяющих эффективно решать задачи ИБ на местах лицам, не имеющим специального математического образования. Приведем примеры использования таких инструментов.

UML – моделирование

Существуют различные средства моделирования систем [3-6]. Среди них – **языки моделирования**. Язык **UML** (Unified Modeling Language, унифицированный язык моделирования) – язык графического описания для объектного моделирования [7,8]. Для выбора UML есть несколько причин: UML универсален; на языке можно описать любую систему, моделировать в любой области; UML позволяет описать систему практически

со всех возможных точек зрения и разные аспекты поведения системы; диаграммы UML сравнительно просты для чтения после достаточно быстрого ознакомления с его синтаксисом; UML очень близок к методам программирования на современных объектно-ориентированных языках. Безусловно, для построения модели системы ИБ необходимо создавать отдельные диаграммы, которые вместе и будут составлять модель (рис. 1).

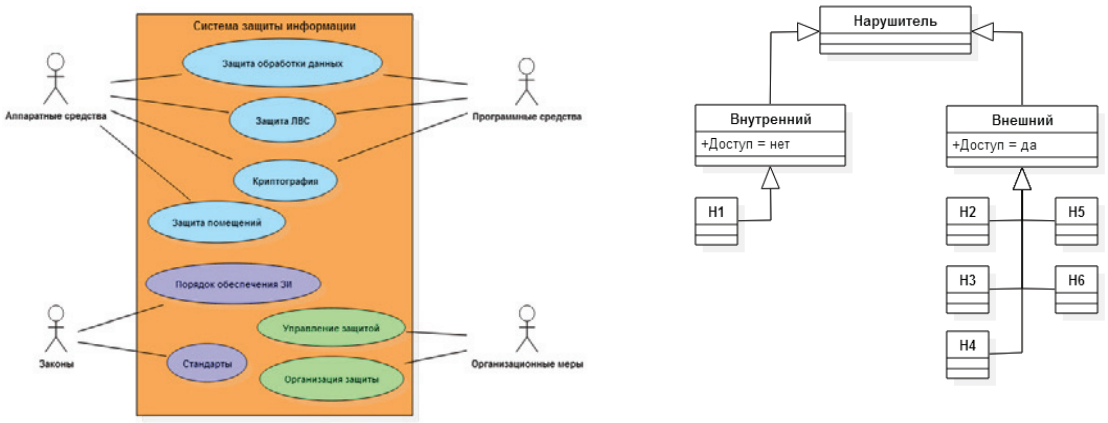

Рис.1. Система защиты информации и классификация нарушителей в UML

Модели UML являются артефактами, которые можно хранить и использовать как в форме электронных документов, так и в виде физической копии. С целью достижения более полного соответствия этому назначению специфицировано представление моделей UML в форме документов в формате XMI, что обеспечивает практическую интероперабельность при работе с моделями. Важным аспектом информационной безопасности является разработка политики ИБ. В этом случае удобно использование диаграммы классов (class diagram). С помощью неё можно классифицировать нарушителя при создании модели нарушителя (рис.1).

Таким образом, применение UML целесообразно при разработке и построении различных систем и политик, в нашем случае – это комплексная система обеспечения информационной безопасности.

Имитационное моделирование

Имитационное моделирование позволяет оптимизировать процесс с точки зрения обеспечения выполнения совокупности всех трех свойств защищенной информации – целостности, доступности, конфиденциальности. Имитационные модели (англ. simulation models) – соединение традиционного математического моделирования с новыми компьютерными технологиями. Целью построения имитаций является максимальное приближение модели к конкретному объекту и достижение максимальной точности его описания.

Агентное моделирование – метод имитационного моделирования, исследующий поведение децентрализованных агентов и то, как такое поведение определяет поведение всей системы в целом, оно предполагает сосредоточение непосредственно на отдельных объектах, их поведении и коммуникациях. Агентная модель – это ряд взаимодействующих активных объектов, которые отражают объекты и отношения в реальном мире [8,9].

На рынке продуктов, обеспечивающих анализ данных по методу агентного моделирования, одним из таких является **ORA** (Organization Risk Analysis) [9]. **ORA** - это инструмент мета-сетевого анализа, который определяет риски или уязвимости структуры организации. В **ORA** алгоритмы способны находить людей, типы навыков, знаний и задач, которые важны с точки зрения производительности и ИБ.

Разработанные меры вычисляются в программе **ORA** на основе сетевых данных. В **ORA** файлы, содержащие различные виды связей между так называемыми узлами связи информации, называются мета-сетями (Meta-networks).

Программа имеет инструменты для графического воспроизведения Мета-Матрицы для оптимизации структуры сети. Для визуализации также есть возможность просмотра Мета-сети в 3D, как показано на рис. 2.

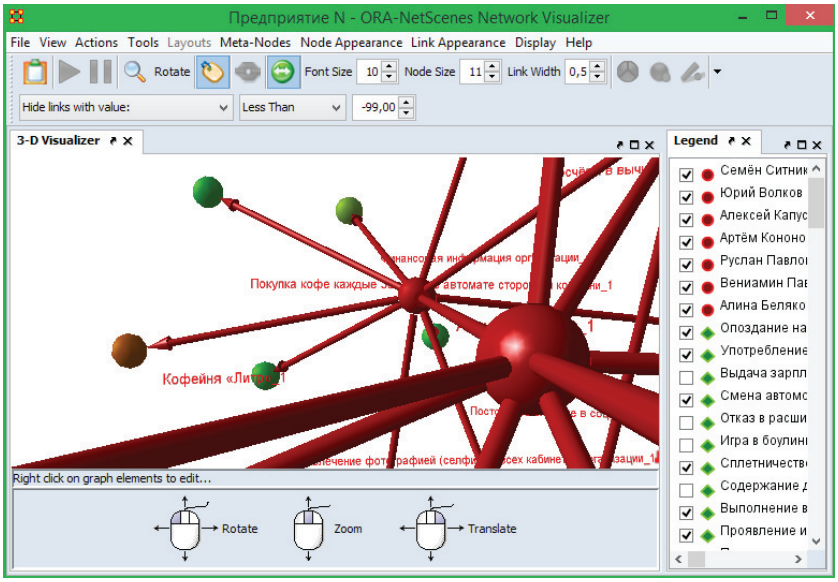

Рис. 2. 3D визуализация Мета-сети в ORA

ORA способна генерировать отформатированные отчёты по различным категориям анализа, доступные для просмотра на экране или в log-файлах, содержащие количественные оценки рисков и угроз. Эти оценки в дальнейшем могут стать основанием для уточнения качественных подходов обеспечения ИБ.

Чем больше информации используется в моделируемом анализе, тем больше угроз и событий ИБ может быть выявлено через отчётную аналитику, что позволит добавить новые уязвимости в модели угроз и уязвимостей организации и провести обновление политики безопасности организации. По сути, агентное моделирование, и ORA, как один из его инструментов, позволяет представить кинетостатику процессов обеспечения безопасности, а рассмотрение нескольких, множества или серии вариантов позволяет увидеть динамику безопасности любой системы, любой организации.

Мультиагентное моделирование

Сравнительно недавно возникшее направление в имитационном моделировании – так называемое агентное (мультиагентное) моделирование (agent-based modeling), имеет свои особенности [10]. Основные его задачи – строить простые модели сложных реальных систем. Инструментом мультиагентного моделирования может эффективно выступать система AnyLogic, позволяющая задать набор сущностей-моделей и шаблоны их поведения, рамки моделируемой системы и, запустив выполнение, наблюдать за происходящими в системе процессами и итоговым результатом.

AnyLogic является инструментом, реализующим многоподходное имитационное моделирование, который объединяет системную динамику, агентное и дискретно-событийное моделирование. Цель подобного моделирования – получить представление, как частные характеристики агентов и их изменение влияют на поведение системы в целом и

выстроить на его основе прогноз или объяснение событий [8,10]. Принципиальная модель процесса несанкционированной передачи конфиденциальной информации представлена на рис. 3. Полученные данные конкретизируют круг лиц, с которых следует начинать проверку, что принесет существенную пользу в проведении внутренних расследований в организации, а также в предупреждении подобных ситуаций в дальнейшем.

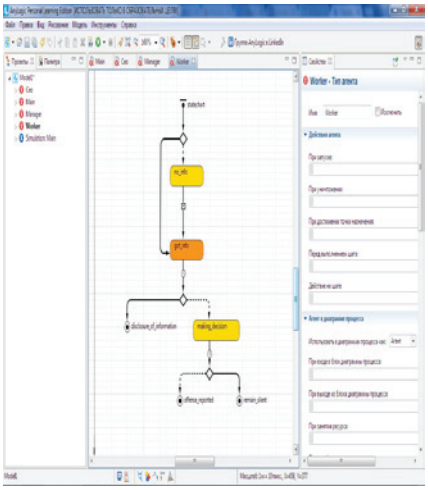

Рис.3. Принципиальная модель процесса несанкционированной передачи конфиденциальной информации

Применение AnyLogic на этапе проектирования информационных систем, позволяет смоделировать каждый из элементов сети информационной системы с позиций информационной безопасности, определить оптимальные требуемые для ее воплощения и сопровождения финансовые затраты.

Моделирование при работе с Big Data и Data Mining

Когда объемы данных и информации (Big Data), которыми приходится оперировать лицам, принимающим решения (ЛПР), стали значительно превышать величины, которые в состоянии переработать человеческий мозг [3], необходимо внедрять в практику подходы, позволяющие своевременно извлекать из огромных объемов структурированных и неструктурированных данных знания посредством интеллектуального анализа данных и информации – Data Mining [11].

В этой связи, заслуживает внимания информационно-аналитическая система (ИАС) PolyAnalyst [12], возможности которой были изучены при решении конкретных задач обеспечения безопасности. Источниками данных в PolyAnalyst могут служить: brandwatch, CSV файлы, FTP сервер, facebook, JSON, Lotus, Microsoft Access, Microsoft Excel, Numerical Sequence, Open Database Connectivity, OLEDB, RSS, SDL SM2, SPSS, twitter, XML, интернет-ресурсы, копии таблиц, объединённый поиск, ссылки и файлы. Информационно-аналитическая система PolyAnalyst имеет возможности анализа данных, анализа текста и многомерного анализа.

На рис. 4 представлен интерфейс системы PolyAnalyst. Рабочая область представляется в виде графов, где каждый узел имеет свою смысловую нагрузку.

Корневой узел – это, как правило, источник данных, а остальные узлы – это анализ, операция или графическое представление данных. PolyAnalyst позволяет моделировать потоки данных и информации, получаемые как от отдельных источников, так и в сетевых вариантах. Данная информационно-аналитическая система может эффективно применяться для решения проблем обеспечения информационной безопасности при работе на основе интеллектуального анализа (Data Mining) при работе с большими массивами данных (Big Data).

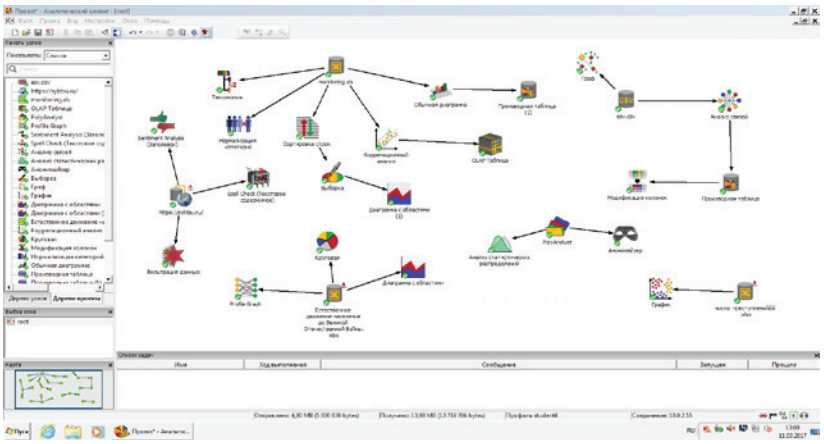

Рис.4. Моделирование в PolyAnalyst

Выводы «частного» и общего характера

1. Приведенные выше примеры реализации всего лишь малой толики арсенала инструментария в сфере моделирования, демонстрирующие хорошую сходимость с результатами, полученными на практике, эффективность, а подчас и незаменимость применения средств моделирования при решении задач, свидетельствуют о мощным потенциале возможностей у моделирования для масштабного внедрения его в экономике, социальной сфере в сфере безопасности и иных направлениях.

2. На настоящий момент нет единой универсальной модели и инструментального средства, позволяющего эффективно описывать все ситуации – каждая из моделей работает в определенном пространственно-временном и целевом диапазоне.

3. Задачи обеспечения ИБ, предполагающие рассмотрение множества разнообразных моделей, описывающих систему, механизм и процесс обеспечения ИБ, требующие комплексного подхода для решения данной проблемы, должны предусматривать применение различных методов моделирования и инструментальных средств для их реализации.

4. На настоящий момент не внедрено в широкую практику применение математического моделирования, во многих случаях в качестве модели применяется словесное описательное представление свойств или характеристик объектов и субъектов применительно к моделям, используемым в соответствии с нормативными документами (ГОСТами, руководящими документами) в сфере ИБ; последнее, с одной стороны, не противоречит требованиям, установленным регуляторами при прохождении организациями процедур аттестации, сертификации и лицензирования, установленным в области ИБ, а с другой стороны, негативно сказывается на качественном и количественном уровне обеспечения состояния ИБ.

5. Необходимо создание отечественной авторитетной общественной организации по типу саморегулируемой организации (СРО), своеобразного круга формального и неформального общения в сфере моделирования, в частности, по типу CASOS (США); с включением в состав такой организации наиболее авторитетных ученых, специалистов и разработчиков, теоретиков и практиков для решения на регулярной и систематической основе целого спектра задач, в частности:

• обобщение и изучение отечественного и зарубежного опыта в области моделирования, передовых разработок и проектов в целях глубокого, широкомасштабного использования его в отечественной практике;

• оказание услуг по информированию, обучению, повышению квалификации, консультированию, сопровождению при внедрении моделирования, отладке систем, механизмов и процессов моделирования;

• проведение классификации и кластеризации основных понятий в моделировании – понятий и видов моделей и моделирования с разработкой и принятием соответствующего нормативного правового документа со статусом стандарта (организации/ отрасли/ ГОСТа), декларирующего единство понимания определений и подходов в области моделирования в целом в масштабах государства – «хартия моделирования»;

• анализ, оценка и систематизация всех известных инструментальных средств моделирования отечественной и зарубежной разработки и перспективных разработок, их классификация и кластеризация;

• популяризация моделирования, постоянное повышение правовой культуры моделирования, качества моделирования;

• непрерывный мониторинг и анализ наработок и рынка программных средств в сфере моделирования;

• выявление антинаучных и популистских подходов в моделировании, информационная поддержка «ограждения» от негативных проявлений подобного рода;

• налаживание информационного взаимодействия с разработчиками инструментальных средств и инструментов моделирования;

• координация работ по доработке и сопровождению отечественных программных продуктов, имеющих высокую перспективность в сфере моделирования;

• разработка правовой базы для применения моделирования в различных сферах деятельности государства и общества (отечественных правовых документов – стандартов, руководящих документов, регламентов, технологических указаний), позволяющих внедрять на местах использование моделирование для решения реальных народнохозяйственных задач и использовать результаты моделирования в качестве официальных оценок и прогнозов;

• разработка единой правовой базы и критериев для классификации, аттестации и сертификации моделей и инструментальных средств моделирования, официально допустимых и/или рекомендуемых к применению в качестве официальных оценочно – прогнозных, обучающих, оценочно-тестирующих и иных средств в том числе в СППР и при принятии управленческих решений;

• разработка эксплуатационно-технических требований (ЭТТ), принципов и подходов к моделированию и моделям на основе использования устоявшихся, современных, передовых и перспективных практик;

• проводить единую политику совершенствования, непрерывного и опережающего развития требований и подходов к моделированию, в частности масштабного внедрения в практику современных средств эффективного и наглядного представления «входной» и отображения «выходной» информации – развитые интерфейсы, позволяющие использовать инфографику, мнемонику и иные эффективные способы подачи/получения информации на базе разработки развитых интерфейсов, современных средств мультимедиа, аудиолизации и визулизации контента, систем виртуальной реальности, n – мерных тренажеров, путем задействования всех каналов органолептической информации, – с учетом требований эргономики;

• информационное взаимодействие с государственными и негосударственными институтами реализации системы распределенных ситуационных центров (СРСЦ);

• оказание научно-методической помощи государственным органам в реализации государственной Стратегии и Программы развития информационного общества в Российской Федерации, задач государства при создании «цифровой экономики» - экономики XXI века – по части внедрения и развития моделирования в области анализа, проектирования, прогнозирования, управления.

Литература

1. Федеральный закон «О безопасности» от 28.12.2010. N 390-ФЗ.
2. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации».
3. **Филяк П.Ю.** Информационная безопасность и комплексная система безопасности: анализ, подходы. Информация и безопасность. 2016. Т. 19. № 1. С. 72–79.
4. **Андрей Голов** «Построение эффективной системы информационной безопасности» [Электронный ресурс] // URL: http://topsbi.ru/default.asp?artID=998 (дата обращения 18.08.2017).
5. Asher's Attic. Организационная структура системы обеспечения информационной безопасности. [Электронный ресурс] http://asher.ru/security/book/its/08 (Дата обращения 08.09.2017).
6. **Беляева О.В., Грицык В.А.** Имитационное моделирование систем защиты информации // Международный журнал экспериментального образования. 2010. № 5. С. 67–67.
7. «Моделирование на UML» [Электронный ресурс] // URL: http://book.uml3.ru (дата обращения 07.09.2017).
8. **Филяк П.Ю., Мишарин Г.Д., Уразов О.М., Золотарев В.В.** Обеспечение информационной безопасности организации методами моделирования. Информация и безопасность. 2015. Т. 18. № 4. С. 560–563.
9. CASOS. Project: ORA. Официальный сайт ORA. [Электронный ресурс] URL: http://www.casos.cs.cmu.edu/projects/ora/ (Дата обращения 25.08.2017).
10. AnyLogic. Многоподходное имитационное моделирование. Официальный сайт AnyLogic. [Электронный ресурс] URL: http://www.anylogic.ru/agent-based-modeling (Дата обращения 10.08.2017).
11. **Филяк П.Ю., Данилова Ю.Н., Растворов В.В., Бура М.А.** Обеспечение информационной безопасности с помощью информационно-аналитической системы PolyAnalyst. В сборнике: Современные проблемы и задачи обеспечения информационной безопасности сборник статей международной научно-практической конференции. 2017. С. 210–218.
12. Официальный портал компании Megaputer – разработчика PolyAnalyst [Электронный ресурс] URL: http://www.megaputer.ru/ (Дата обращения 27.08.2017).