УДК 004

Ляпустин Е.М., Ахметзянов Д.И., Баязитов Т.Т.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Цифровизация и киберугрозы требуют эффективного управления информационной безопасностью (ИБ). Моделирование процессов ИБ – мощный инструмент анализа, проектирования и оценки защитных механизмов. В статье рассматриваются подходы к моделированию (формальные, имитационные, графические), области применения (анализ рисков, проектирование архитектуры безопасности), вызовы (сложность, нехватка данных) и перспективы (ИИ, гибридные модели, цифровые двойники).

Ключевые слова: информационная безопасность, моделирование, моделирование процессов, анализ рисков, формальные методы, имитационное моделирование.

Современный мир характеризуется беспрецедентным ростом информации и повсеместным внедрением ИТ, что неизбежно усложняет инфраструктуры и умножает количество и изощренность киберугроз. Сложность систем и многообразие задач информационной безопасности (ИБ) делают интуитивные подходы неэффективными, порождая острую потребность в инструментах формализации, анализа и прогнозирования. Ключевым таким инструментом является моделирование – создание абстрактных представлений реальных или гипотетических систем, атак и защит для их изучения. Модели упрощают сложность, выявляют скрытые связи, позволяют проводить анализ «что-если», сравнивать альтернативы и оптимизировать ресурсы, улучшая общее понимание ИБ.

Информационная безопасность определяется как состояние защищенности информации и инфраструктуры от угроз, обеспечивая конфиденциальность, целостность и доступность (CIA). Она поддерживается через взаимосвязанные процессы (управление рисками, инцидентами, уязвимостями) и системы ИБ, включающие организационные меры и программно-технические средства (МЭ, IDS/IPS, политики). Модель ИБ – это абстракция объекта ИБ, отражающая его существенные черты для конкретной цели. Исследования моделирования в ИБ эволюционировали от анализа рисков и политик к более сложным подходам, включая формальные методы, нотации бизнес-процессов (BPMN) и модели атак (деревья/графы атак). Однако проблемы стандартизации и интеграции моделей сохраняются.

Формальные методы, такие как Сети Петри, конечные автоматы и процессные алгебры, применяются для точного математического описания и строгого анализа политик безопасности, протоколов и моделей доступа. Они позволяют верифицировать корректность и выявлять логические уязвимости на этапе проектирования, анализируя потоки работ, жизненные циклы объектов и взаимодействие параллельных процессов.

Имитационное моделирование воспроизводит поведение систем во времени, учитывая случайность и динамику. Дискретно-событийное моделирование (DES) анализирует производительность систем ИБ. Агентное моделирование (ABM) изучает сложные эмерджентные явления, такие как распространение вредоносного ПО или поведение пользователей, через взаимодействие автономных агентов. Системная динамика (SD) исследует долгосрочные эффекты политик ИБ и инвестиций через потоковые диаграммы и петли обратной связи.

Графические модели используют визуальные языки для наглядного представления. BPMN помогает описывать и оптимизировать процессы ИБ. UML применяется для моделирования систем и их компонентов. Деревья и графы атак визуализируют пути компрометации системы, помогая выявить критические точки. Диаграммы потоков данных (DFD) отслеживают движение информации, указывая места, требующие защиты.

Модели на основе знаний, включая онтологии ИБ и экспертные системы, фокусируются на представлении и использовании экспертных знаний. Онтологии стандартизируют терминологию и интегрируют данные, а экспертные системы автоматизируют принятие решений на основе правил «если-то», например, при классификации инцидентов.

Применение моделирования в ИБ сталкивается со значительными вызовами. Сложность, масштаб и динамичность современных систем и угроз затрудняют создание точных, актуальных моделей. Недостаток достоверных данных для калибровки и сложность безопасной валидации на реальных системах являются существенными препятствиями. Точная формализация непредсказуемого человеческого фактора (пользователей и атакующих) остается серьезным ограничением. Интеграция различных типов моделей для комплексного анализа также представляет методологическую и техническую проблему.

Преодоление этих вызовов связано с перспективными направлениями. Важнейшим является интеграция с Искусственным Интеллектом и Машинным Обучением (AI/ML) для автоматизации построения и калибровки моделей, генерации данных для обучения систем защиты и моделирования адаптивного поведения AI-агентов. Развитие гибридных подходов, комбинирующих сильные стороны разных методов, также актуально. Концепция цифровых двойников (Digital Twins) обещает создание динамических моделей ИТ-инфраструктуры для мониторинга и симуляции. Необходимо улучшенное моделирование человеческого фактора с учетом когнитивных и социальных аспектов. Стандартизация языков и форматов моделирования ИБ упростит обмен моделями и интеграцию инструментов. Наконец, требуется адаптация и разработка методов моделирования для новых технологий: Интернета вещей (IoT), облачных вычислений, киберфизических систем.

Таким образом, моделирование – незаменимый инструмент для анализа и управления ИБ в условиях растущих угроз. Несмотря на прогресс, его применение ограничено сложностью среды, нехваткой данных и проблемой учета человеческого фактора. Дальнейшие исследования, особенно в области интеграции с AI/ML, гибридных моделей, цифровых двойников и моделирования поведения человека, критически важны для преодоления этих барьеров и повышения киберустойчивости.

Список использованных источников:

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Введ. 2008-02-01. М.: Стандартинформ, 2008. 16 с.

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 2022-04-01. М.: Стандартинформ, 2021. 39 с.

3. Мельников Д.А. Моделирование систем защиты информации: учебное пособие / Д.А. Мельников; Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет). М.: Издательство МГТУ им. Н.Э. Баумана, 2018. 87 с.

4. Баранов А..П. Формальные методы верификации и синтеза протоколов безопасности / А.П. Баранов // Труды Института системного программирования РАН. 2012. Т. 23. С. 319–334.

5. Максимов Д.Ю. Моделирование процессов управления информационной безопасностью организации с использованием BPMN / Д.Ю. Максимов, А.С. Марков // Бизнес-информатика. 2015. № 4 (34). С. 48–57.

6. Моделирование и оценка последствий компьютерных атак на критически важные информационные системы / И.В. Котенко, И.Б. Саенко, О.С. Лаута [и др.] // Информатика и автоматизация. 2019. Т. 18, № 1. С. 137–166.

Lyapustin E.M., Akhmetzyanov D.I., Bayazitov T.T.
Ufa University of Science and Technology, UFA

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MODELING OF INFORMATION SECURITY PROCESSES AND SYSTEMS

Abstract. Digitalization and cyber threats require effective management of information security (IS). Modeling of IS processes is a powerful tool for analyzing, designing and evaluating defense mechanisms. This article discusses modeling approaches (formal, simulation, graphical), applications (risk analysis, security architecture design), challenges (complexity, data scarcity) and perspectives (AI, hybrid models, digital twins).

Keywords: information security, modeling, process modeling, risk analysis, formal methods, simulation modeling.