DOI 10.37882/2223-2966.2023.08.13

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE COMPARATIVE ANALYSIS OF MODELING METHODS AGAINST INFORMATION SECURITY THREATS

O. Karelova
E. Alyushina

Summary. The article provides a comparative analysis of modeling methods against information security threats in organization. The graphic methods for visualizing potential information security threat scenarios are overviewed (Petri nets and attack trees), as well as the FSTEC methodology for threat modeling.

Keywords: threats; modeling methods; information security; threats to information security.

Карелова Оксана Леонидовна
Доктор физико-математических наук, доцент, профессор, Московский Государственный Лингвистический Университет;
Профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ (Москва)
okarelova@yandex.ru
Алюшина Екатерина Романовна
Московский государственный лингвистический университет
alusinaekaterina@gmail.com

Аннотация. В статье проводится сравнительный анализ методов моделирования угроз информационной безопасности организации. Рассмотрены графические методы представления сценариев угроз безопасности информации (сети Петри и деревья атак), а также методика ФСТЭК построения модели угроз.

Ключевые слова: угрозы, методы моделирования, информационная безопасность, угрозы информационной безопасности.

Обеспечение высокого уровня информационной безопасности является одним из требований реализации деятельности любой организации. Для определения актуальных угроз, соответствующих информационным ресурсам организации, необходимо создание модели угроз информационных ресурсов организации.

Модель угроз (безопасности информации) представляет собой физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [1]. Угроза безопасности информации представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2]. Таким образом, модель угроз представляет собой документ, назначение которого — определить угрозы, актуальные для исследуемой системы.

Содержимое модели угроз описано новой методикой оценки Федеральной службы по техническому и экспортному контролю (ФСТЭК), выпущенной 5 февраля 2021, которая сменила устаревшую базовую модель угроз 2008 года. Новая методика диктует следующие требования к содержанию модели [3]:

— определить негативные последствия, которые могут возникнуть в случае реализации угроз безопасности информации;
— провести инвентаризацию систем и сетей и определить возможные объекты воздействия угроз безопасности информации;
— определить источники угроз безопасности информации и оценить возможностей нарушителей по реализации угроз безопасности информации;
— оценить способы реализации угроз безопасности информации, вероятных для исследуемой системы;
— оценить возможности реализации угроз и определить актуальность угроз;
— оценить вероятные сценарии атак в системах и сетях.

Ключом к моделированию угроз безопасности информации является определение слабых точек и уязвимостей, где следует прилагать наибольшие усилия для обеспечения безопасности системы. Однако, данные параметры изменяются по мере добавления новых элементов в информационные системы, их удаления или модернизации, а также изменения, связанные с пользовательскими требованиями, законодательными актами или с требованиями регуляторов в области информационной безопасности.

В данной работе рассмотрены наиболее эффективные, с точки зрения авторов, методы графического представления сценариев реализации угроз безопасности информации — сети Петри и деревья атак.

Сети Петри являются простым и удобным средством для моделирования разнообразных распределенных систем и процессов.

Сеть Петри представляет собой двудольный ориентированный граф, содержащий вершины двух типов — места и переходы. Последовательности событий отображаются срабатываниями переходов. Соглашения о правилах срабатывания переходов является способом выражения причинно-следственных связей между условиями и событиями в системе. Последовательность событий образует моделируемый процесс. Данный метод позволяет дать количественную оценку информационной безопасности корпоративной системы [4].

Деревья атак представляют собой описание вариантов проведения атаки для достижения некоторой цели, которая ставится во главу дерева атаки (является его вершиной). Для каждой информационной системы может быть определено достаточно большое количество угроз, для каждой из которых строится своё собственное дерево атак. Каждый узел в дереве атак представляет собой некоторую подцель, достижение которой, в случае выполнения ряда условий, позволяет злоумышленнику подняться по дереву на более высокий уровень и так до тех пор, пока злоумышленник не достигнет вершины дерева. В последнем случае считается, что злоумышленник успешно реализовал атаку.

Основная цель деревьев атак — моделирование угроз безопасности, рассмотрение возможных атак на систему и анализ векторов атак. Деревья атак также успешно используются в анализе рисков информационной безопасности, в процессах анализа и проектирования систем безопасности и защиты информации.

Применение деревьев атак позволяет несколько упростить задачу аналитиков при исследовании проблемы безопасности и защищённости информационной системы. Деревья атак обладают высокой наглядностью и позволяют хорошо структурировать всевозможные варианты потенциальных проблем для каждого из активов.

Для каждого актива следует построить его дерево атак, в котором попытаться перечислить все возможные пути осуществления атак на этот актив. Актив (или, скорее, его свойство безопасности — конфиденциальность, целостность, доступность, аутентичность и т.д.) ставятся во главу дерева, в самом дереве перечисляются пути и, по возможности, средства компрометации (нарушения) этого свойства безопасности [5].

Представим сравнение методов моделирования угроз информационной безопасности информационных систем организации в виде таблицы, отметив преимущества и недостатки каждого из рассмотренных методов в Таблицах. (таблица 1, 2, 3)

Таблица 1.

Достоинства и недостатки Методики оценки угроз безопасности информации ФСТЭК для моделирования угроз информационной безопасности

Достоинства	Недостатки
Переход на сценарный подход моделирования угроз ИБ	Отсутствие инструментальной поддержки.
	Методика оторвана от БДУ. ФСТЭК, что требует ручного анализа актуальных угроз
Оценка угроз экспертной группой, а не отдельным специалистом	Отсутствие частной модели угроз, только наличие отдельных примеров, а также структуры документа модели угроз ИБ
Основой для моделирования угроз являются негативные последствия, необходимость защиты от наступления которых определена заинтересованными лицами. Это упрощает проблему убеждения бизнеса в необходимости обеспечения безопасности и снижает требования к специалисту	Приложение 11 ФСТЭК посвящено основным тактикам и соответствующим им типовым техникам, используемых для построения сценариев реализации угроз безопасности информации, однако со временем список станет невозможно расширить, так как его расширение требует создания новой Методики.
Оценивается только возможность реализации угрозы — экспертам не требуется оценивать, с какой вероятностью нарушитель способен реализовать угрозу	Модель не учитывает применение мер по защите, используя составленную модель оценки угроз безопасности информации, останавливается на создании сценариев

Таблица 2.

Достоинства и недостатки Деревьев атак для моделирования угроз информационной безопасности

Достоинства	Недостатки
Гибкость	Проблема полного охвата проблемы безопасности
Удобство представления контрмер	Проблема глубины обзора каждого варианта атаки
Наглядность	Проблема оценки значимости вариантов атак
Легкость дальнейшей формализации и алгоритмизации и наличие инструментальной поддержки для этого	Отсутствие возможности динамического моделирования
Дедуктивный характер выявления причинно-следственных связей исследуемых явлений	Трудность моделирования цикличных атак
Доступность для статистического моделирования и количественной оценки изучаемых явлений, процессов и их свойств	

Таблица 3.

Достоинства и недостатки Сетей Петри для моделирования угроз информационной безопасности

Достоинства	Недостатки
Мощное средство моделирования асинхронных, параллельных распределенных и недетерминированных процессов	Отсутствие информации о причинно-следственных связях между событиями в системе
Возможность отображения на одной модели взаимодействия нескольких параллельно— последовательных процессов системы	Затруднения, связанные с моделированием обширных систем
Свойство иерархического вложения сетей Петри	Неспособность в явном виде описывать поведение нарушителя и атакуемого объекта
Возможность использования таких параметров, как время, приоритет переходов, цвет	Отсутствие качественных бесплатных программно-инструментальных средств для моделирования систем средствами сетей Петри
Удобство использования для анализа различных аспектов безопасности компьютерной сети	Анализ не предоставляет количественных характеристик, определяющих состояние системы
	Чрезвычайно сложно отразить преобразование информации при срабатывании переходов сети Петри

Таблица 4.

Сравнение методов моделирования угроз информационной безопасности

Методика оценки угроз безопасности информации ФСТЭК	Деревья атак	Сети Петри
Возможность графической реализации		
	+	+
Возможность инструментальной поддержки		
	+	+
Возможность включения в модель контрмер		
	+	
Наличие информации о причинно-следственных связях между событиями		
+	+	
Масштабируемость		
	+	
Способность описывать поведение нарушителя и атакуемого объекта		
+	+	
Возможность статического моделирования		
+	+	
Возможность динамического моделирования		
		+

Ввиду наличия определенных особенностей у каждого из рассмотренных методов, для моделирования угроз информационной безопасности организации более универсальным методом будет являться построение деревьев атак для визуализации как конкретных атак, так и возможных уязвимостей, использование которых может являться подцелью атакующего наравне с возможностью установления причинно-следственных связей и количественной оценки изучаемых явлений. Также сценарный подход к моделированию угроз, представленный в методике ФСТЭК, позволяет одновременно решить сразу несколько задач обеспечения информационной безопасности: охватить максимально возможный спектр угроз, актуальных для данной информационной системы; разработать детальные требования к мерам безопасности, препятствующим каждому возможному действию нарушителя; определить индикаторы компрометации, которые позволят обнаружить применение сценария реализации угрозы; заблаговременно разработать меры оперативного реагирования на каждый сценарий; в ходе реагирования на атаку — прогнозировать возможные следующие действия нарушителя и оперативно противодействовать им. Таким образом применение деревьев атак и методики ФСТЭК является одним из лучших вариантов моделирования угроз информационной безопасности организации.

Важно отметить, что без моделирования угроз и нарушителя может быть построена избыточная система защиты, защищающая от многочисленных угроз, реализация которых невозможна в данной организации, либо неэффективная система защиты, не охватывающая все актуальные угрозы.

ЛИТЕРАТУРА

1. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 01.10.2009 // Национальный стандарт Российской Федерации
2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» от 01.02.2008 // Национальный стандарт Российской Федерации
3. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз безопасности информации». [Электронный ресурс] — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 16.05.2023).
4. Проститенко, О.В. Моделирование дискретных систем на основе сетей Петри: учебное пособие / О.В. Проститенко, В.И. Халимон, А.Ю. Рогов. — СПб.: СПбГТИ(ТУ), 2017 — 69 с.
5. Д.И. Котенко, И.В. Котенко, И.Б. Саенко, Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы, Тр. СПИИРАН, 2012, выпуск 22, 5–30.
6. R-Vision SGRC // R-Vision [Электронный ресурс]. — URL: https://rvision.ru/products/sgrc (дата обращения: 16.05.2023).
7. Kaspersky Security CAD // Лаборатория Касперского [Электронный ресурс]. — URL: https://scad.kaspersky.com/ (дата обращения: 16.05.2023).