СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ

СОРОКИНА Алёна Евгеньевна
Московский государственный лингвистический университет, Москва, Россия,
lean99on@gmail.com

Научный руководитель: д-р физ.-мат. наук, доц. О. Л. Карелова

Аннотация. В современном мире, в эпоху цифровизации, информация является одним из наиболее критических ресурсов. Как следствие, информационные системы различных организаций становятся не только весьма ценными, но и достаточно уязвимыми активами. В связи с этим появляется необходимость создания системы защиты информации, что, в свою очередь, довольно затратно. Таким образом, прежде, чем приступить к построению системы защиты, следует смоделировать угрозы для каждой конкретной информационной системы и уже на основании готовой модели проектировать систему защиты информации. В данной работе представлен анализ методов моделирования угроз информационной безопасности.

Ключевые слова: угрозы, методы моделирования, информационная безопасность, сети Петри, деревья атак

COMPARATIVE ANALYSIS OF INFORMATION SYSTEM THREAT MODELING METHODS

SOROKINA Alyona Evgenievna
Moscow State Linguistic University, Moscow, Russia,
lean99on@gmail.com

Academic Advisor: Doctor of Physics and Mathematics (Dr. habil),
Ass. Prof. O. L. Karelova

Abstract. In the modern world, in the era of digitalization, information is one of the most critical resources. As a result, information systems of various organizations become not only very valuable but also quite vulnerable. In this regard, it becomes crucial to create an information security system, which, in turn, is quite expensive. Thus, before starting to build a security system, it is necessary to modulate threats for each specific information system and design an information security system based on a ready-made model. This paper presents an analysis of methods for modeling information security threats.

Keywords: threats, modeling methods, information security, Petri nets, attack trees

Модель – это объект или описание объекта, системы для замещения одной системы (оригинала) другой системой для лучшего изучения оригинала или воспроизведения каких-либо его свойств. Модель – результат отображения одной структуры (изученной) на другую (малоизученную). Любая модель строится и исследуется при определенных допущениях, гипотезах. Модель должна наиболее полно отображать и воспроизводить именно те качества объекта или системы, которые необходимо изучить в контексте поставленной цели. Модель создается для того, чтобы представить изучаемый объект в упрощенном и более наглядном виде для его дальнейшего изучения. Поэтому для каждого конкретного объекта могут быть созданы различные модели, классы моделей, применяемые для достижения различных целей. Необходимым условием моделирования является подобие объекта и его модели [Замятина, 2017].

В контексте информационной безопасности моделирование угроз позволяет определить актуальные для конкретной информационной системы угрозы, оценить их влияние на систему, а также обнаружить слабые места системы безопасности и устранить их в дальнейшем. Создание, взаимоналожение и комплексный анализ модели существующей системы безопасности и модели угроз задают вектор для развития и модификации системы с целью поддержания безопасности на должном уровне и избежания нежелательных потерь для организации. Такие модели позволяют оценить риски, которым система может быть подвержена. Методы моделирования угроз информационной системы являются инструментами для создания необходимых моделей. Несмотря на то, что существует множество различных методов моделирования угроз, и каждый вариант будет иметь свою собственную структуру, во время создания модели должны быть пройдены основные пять этапов:

1) мы должны определить то, над чем мы работаем, и для этого нам нужно разбить изучаемую нами систему на части и проанализировать как всю систему в целом, так и каждую ее часть в отдельности; на данном этапе мы анализируем поток данных, активы компании, а также участвующие в деятельности организации стороны (отделы, партнеры, клиенты) – всё, что может быть поставлено под угрозу;

2) необходимо определить перечень угроз, с которыми может столкнуться система, чтобы на основе этого выявить слабые места системы;

3) определить контрмеры, которые будут применены для борьбы с найденными ранее угрозами или для смягчения последствий их реализации в случае, если предотвратить угрозу нет возможности; на данном этапе мы определяем, какие технологии, планы реагирования на инциденты, средства контроля, инструменты минимизации угроз и рисков у нас уже есть и какие нужно добавить для успешного отражения той или иной атаки;

4) провести анализ рисков и оценить объем потерь от реализации той или иной угрозы;

5) нужно упорядочить угрозы (можно составить их список) и определить, какие из них являются актуальными для системы (в процессе моделирования может выясниться, что некоторые угрозы не актуальны; к примеру, в случае, если затраты на предотвращение угрозы превышают возможные потери от ее реализации, или если негативные последствия от ее реализации незначительны, то тратить ресурсы на противодействие нерационально).

Сети Петри. Модель на основе сети Петри позволяет в наглядной и хорошо формализованной форме проследить поведение параллельных систем с асинхронными взаимодействиями. В качестве таких систем могут быть рассмотрены информационная система и схема действий злоумышленника, который планирует совершить атаку на эту систему. Такая модель в компактном виде передает структуру взаимоотношений элементов системы и динамику изменения ее состояний при заданных начальных условиях. Одно из основных достоинств такого типа моделей заключается в высоком уровне абстрактности модели – взаимодействия в системе описываются всего лишь двумя понятиями: событие и условие [Проститенко, Халимон, Рогов, 2017].

В своей сущности сеть Петри – это двудольный ориентированный граф, состоящий из вершин двух типов – позиций (чаще всего представленных в виде кругов) и переходов (чаще всего представленных в виде прямоугольников или полос), которые соединены между собой дугами. Позиции могут содержать в себе маркеры (фишки), количество которых в каждой позиции определяет текущую маркировку (состояние) системы. Запуск перехода имитирует какое-либо действие, происходящее в реальной системе. Переход может быть запущен лишь в том случае, если все предварительные условия для того или иного действия выполнены (на входных позициях перехода достаточно доступных маркеров). После срабатывания перехода, маркеры из входных позиций удаляются, а вновь созданные маркеры добавляются в выходные позиции. Количество передаваемых маркеров определяется весом дуги, соединяющей переход с позицией. Стоить заметить, что позиции, как и переходы, не могу быть напрямую между собой связаны дугами.

Концепция сетей Петри изначально не учитывала такой параметр, как время, но на текущий момент он может быть введен для оценки и анализа производительности системы. Как правило, для моделирования дискретных событий могут быть использованы два типа переходов: немедленные переходы с нулевой задержкой срабатывания и переходы с детерминированной (задается время ожидания срабатывания) или стохастической (задаются параметры закона распределения времени ожидания срабатывания) задержкой срабатывания.

В научном исследовании «Petri Net-Based Approach for "Cyber" Risks Modelling and Analysis for Industrial Systems» предлагается использовать две модели для имитации воздействия угрозы на производственную систему – «номинальная» и «возбужденная» модели на основе сетей Петри. «Номинальная» модель отражает саму производственную систему в обычном для нее режиме функционирования. «Возбужденная» модель создается путем добавления в исходную модель действий-раздражителей, которыми как раз могут являться атаки злоумышленников на систему. На основе анализа «возбужденной» модели уже принимается решение об изменении исходной системы и применении к ней мер по снижению рисков и последствий реализации угрозы. Такой подход может применяться для моделирования угроз, анализа их воздействия на систему и снижения рисков, связанных с уязвимостями информационной безопасности и различными критическими сбоями в динамических системах [Labadi, Darcherif, El Abbassi, Hamaci URL].

Деревья атак. Деревья атак могут быть использованы в процессе анализа информационных рисков, предоставляя структуру для анализа воздействия атаки на систему - деревья атак предоставляют формальный методический способ описания безопасности систем на основе различных атак, что может быть очень полезно при оценке возможных угроз и их вероятностей во время оценки риска. 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 проектирования систем безопасности, защиты и их анализе.

Дерево атак обычно представляет собой графическое представление уязвимостей в информационной системе, но тем не менее оно может быть выражено в текстовом формате. Между этими двумя представлениями есть некоторое сходство. Каждый путь через дерево атак представляет уникальный вектор атаки в организации и показывает, какие уязвимости злоумышленник может использовать для получения доступа к конфиденциальным материалам. На каждом уровне или листе дерева атак существуют различные уязвимости, некоторые из которых должны быть объединены, чтобы вызвать нарушение, а некоторые способны вызвать нарушения сами по себе. Данные условия в деревьях атак выражаются через «и» и «или» и представлены по-разному в зависимости от того, используется ли графический, текстовый или комбинированный формат дерева атак. Создатель дерева атак самостоятельно определяет, сколько информации будет отображено в модели и в каких форматах представлены будут атрибуты, поскольку формальных стандартов не существует. Однако существуют некоторые рекомендации по созданию деревьев

атак, такие как измерение вероятностей каждого листа, удаление или маркировка маловероятных путей атаки, создание контрмер и применение наиболее подходящих контрмер к листьям. При графическом варианте представления каждый независимый уровень модели называется «листовым» узлом дерева атак, и уязвимости перемещаются во время атаки снизу вверх по схеме, достигая конечного узла, именуемого «корневым». Условия «и» и «или» на схеме могут быть представлены любым удобным способом. В текстовом формате дерево атак может быть представлено ранжированным маркированным списком, в котором «и» и «или» прописываются текстом.

Графический формат более удобен в использовании для восприятия и анализа информации, но он обладает существенным недостатком – при большом количестве узлов такую модель трудно масштабировать. Поэтому при работе с крупными системами чаще всего используют текстовый формат [Vitkus, Salter, Goranin, Ceponis, URL].

Сравнительный анализ деревьев атак и сетей Петри

Представим преимущества и недостатки каждого рассматриваемого способа моделирования в таблице 1 [Котенко, Котенко, Саенко, 2012].

Таблица 1

Сети Петри	Деревья атак
Схожие преимущества	
возможность графического представления модели, наглядность модели	
возможность использования вероятностных параметров	
Уникальные преимущества	
возможность использования временных параметров	масштабируемость
удобство моделирования параллельных процессов	адаптируемость
простота изучения и использования в силу наличия небольшого количества «примитивов»	простота изучения и использования
удобство использования для анализа различных аспектов безопасности компьютерной сети	удобство представления контрмер
Недостатки	
неспособность в явном виде описывать поведение нарушителя и атакуемого объекта	трудности моделирования циклических атак отсутствие возможностей динамического моделирования

Ввиду наличия определенных особенностей у каждого из приведенных методов, в контексте моделирования угроз они используются в разных целях. Сети Петри наиболее полезны для оценки поведения самой защищаемой системы во время или после внедрения в нее раздражителя, представленного атакой. Таким образом можно проследить и оценить влияние негативных факторов на саму систему и проследить динамику процессов во времени. Например, можно вычислить время простоя системы в случае проведения успешной атаки на нее. Деревья атак больше подходят для разработки и определения контрмер, которые необходимы для усовершенствования системы защиты. Оценив контрмеры, можно определить экономическое влияние рисков на систему, просчитать траты на защиту и потери количественно. Деревья атак могут быть представлены в различных вариациях: узлы дерева могут подразумевать конкретные атаки или же конкретные уязвимости. Первый тип моделей позволяет определить сценарий проведения атаки злоумышленником и найти все возможные способы остановить эту атаку или минимизировать последствия ее осуществления. Второй тип дает возможность определить возможные пути использования той или иной уже определенной уязвимости системы, построить цепочку последовательного использования известных уязвимостей для достижения конечной цели. Таким образом, деревья атак наиболее эффективны для поиска путей решения существующих проблем защиты информационной системы.

Список литературы

Замятина О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей: учебное пособие для магистратуры. М. : Юрайт, 2017.

Котенко Д. И., Котенко И. В., Саенко И. Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИ-РАН. 2012. № 22 (3). С. 5–30.

Простименко О. В., Халимон В. И., Рогов А. Ю. Моделирование дискретных систем на основе сетей Петри: учебное пособие. СПб. : СПбГТИ(ТУ), 2017.

Labadi K., Darcherif A.-M., El Abbassi I., Hamaci S. Petri Net-Based Approach for "Cyber" Risks Modelling and Analysis for Industrial Systems // E3S Web of Conferences 170, 0 0 (2020). EVF'2019. URL: https://doi.org/10.1051/e3sconf/202017002001

Vitkus D., Salter J., Goranin N., Ceponis D. Method for Attack Tree Data Transformation and Import Into IT Risk Analysis Expert Systems // Applied Sciences, 2020, 10, 8423. URL: https://www.mdpi.com/2076-3417/10/23/8423/htm