УДК 004.056.53

Д.И. Котенко, И.В. Котенко, И.Б. Саенко

МЕТОДЫ И СРЕДСТВА МОДЕЛИРОВАНИЯ АТАК В БОЛЬШИХ КОМПЬЮТЕРНЫХ СЕТЯХ: СОСТОЯНИЕ ПРОБЛЕМЫ

Котенко Д.И., Котенко И.В., Саенко И.Б. **Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы.**

Аннотация. Работа посвящена анализу проблем моделирования атак в больших компьютерных сетях с использованием различных моделей, методов и инструментальных средств. На основании особенностей больших сетей как объектов информационной безопасности и объектов атак детально рассмотрены известные модели, а также методы и средства моделирования атак, а также приведены направления их дальнейшего развития. Показана роль требований к информационной безопасности в итерациях моделирования атак. Приведены примеры исследований проблем моделирования атак, связанных с различными видами НЕ-факторов.

Ключевые слова: моделирование атак, большие компьютерные сети, графы атак, многоагентные системы, нейронные сети, экспертные системы, НЕ-факторы, вычислительная сложность, циклы моделирования, система анализа защищенности.

Kotenko D.I., Kotenko I.V., Saenko I.B. **Methods and tools for attack modeling in large computer networks: state of the problem.**

Abstract. The paper is intended to analyze attack modeling problems in large computer networks with the use of different models, methods and tools. The famous models, as well as methods and tools for attack modelling are examined in detail on the basis of the characteristics of large networks as information security related objects and objects of attack, and directions for further development are provided. The role of information security requirements in attack modeling iterations is shown. Examples of attack modeling problems associated with different types of NOT-factors are presented.

Keywords: attack modeling, large computer networks, attack graphs, multi-agent systems, neural networks, expert systems, NOT-factors, computational complexity, modeling cycles, security analysis.

1. Введение. Проблемы безопасности, которые достаточно успешно решаются в небольших компьютерных сетях с использованием разнообразных инструментальных средств, в том числе поддерживающих моделирование атак, не удается также эффективно решать для больших сетей. Сложности моделирования атак в больших компьютерных сетях связаны с неполнотой и неопределенностью информации, доступной для использования средствами моделирования, а также большой вычислительной сложностью алгоритмов построения и анализа моделей атак.

Данная работа посвящена анализу проблемы моделирования атак в больших компьютерных сетях с использованием различных моделей, методов и инструментальных средств. На основании особенностей

больших сетей как объектов информационной безопасности и объектов атак достаточно детально рассмотрены известные модели, методы и средства моделирования атак, а также приведены направления их дальнейшего развития. При этом следует отметить, что перечень работ, использованных для анализа, не претендует на полноту, но он, по мнению авторов, содержит наиболее важные работы.

2. Особенности больших компьютерных сетей как объектов обеспечения информационной безопасности. Рассмотрим особенности больших компьютерных сетей, связанные с обеспечением информационной безопасности. В работах [1, 2] показано, что большим сетям свойственны следующие отличительные черты в этой области:

1) большая сеть имеет сложную и не всегда ясную структуру;

2) серьезные проблемы при построении интегрированных систем безопасности в больших сетях возникают в связи с различием скоростей передачи данных на разных участках информационных трактов;

3) закупка и внедрение большого количества разнообразных аппаратно-технических сетевых устройств производятся в разное время разными специалистами, которые не только имеют свои предпочтения к характеристикам, производительности, аппаратным платформам и базовыми технологиям, но и по-разному представляют информационную структуру сети;

4) наличие специфических проблем, связанных с совместимостью различных платформ и версий операционных систем, средств и технологий прикладного программного обеспечения приводит к необходимости разработки решений по интеграции этих технологий, что в свою очередь требует значительных усилий по моделированию ситуаций, отработке надежных сценариев миграции и высокой квалификации специалистов;

5) решению проблем информационной безопасности часто придают второстепенное значение по сравнению с другими проблемами, решаемыми в процессе создания и развития большой сети;

6) отсутствие плана сети с документально закрепленными зонами ответственности затрудняет любое серьезное вмешательство в ее инфраструктуру, в частности, усложняет внедрение средств безопасности в работающую сеть;

7) в больших компьютерных сетях происходит размывание зон ответственности, связанное с разным административным подчинением и наличием пограничных участков, что приводит к возникновению

«белых пятен» в структуре сети, следовательно, к серьезным уязвимостям в системе безопасности;

8) неполнота и неопределенность исходных данных, имеющие место из-за наличия нескольких слабо связанных друг с другом документов, описывающих идеологию построения и развития компьютерной системы, приводят к характерным проблемам, одной из которых является неопределенность в вопросах обеспечении безопасности компьютерной сети;

9) территориальная удаленность инфраструктурных объектов больших сетей влечет за собой ресурсоемкие проблемы одновременного использования каналов связи различного типа;

10) велика вероятность возникновения временных интервалов неработоспособности некоторых компонентов системы безопасности, реализованных на базе разнородных аппаратно-технических средств или средств, географически расположенных в определенных местах.

Для территориальных сетей (Wide Area Network, WAN) следует выделить ряд дополнительных проблем безопасности, связанных с глобальным масштабом таких сетей. Самая известная глобальная сеть — это Интернет. Кроме нее к глобальным сетям относятся FidoNet, CREN, EARNet, EUNet, а также распределенные системы боевого управления, интеллектуальные транспортные системы, распределенные сети здравоохранения, сети контроля мировых запасов нефти и разведки газа, научно-исследовательские сети, сети мониторинга авиационного трафика и другие. Среди особенностей WAN следует отметить избыточность оборудования и программного обеспечения. С одной стороны, такая избыточность повышает устойчивость к сбоям, особенно для сетей, которые должны функционировать в реальном времени, с другой — усложняет сети и увеличивает объем привлекаемых ресурсов, в частности, для обеспечения безопасности, что в целом снижает эффективность использования сетей. Другой особенностью WAN является коллективное управление, которое приводит к дополнительным проблемам по обеспечению безопасности сети.

Пожалуй, наиболее серьезные проблемы безопасности WAN связаны с их уязвимостью к *распределенным атакам*. Рассмотрим более подробно это понятие.

3. Понятие атаки и распределенной атаки. При рассмотрении проблем уязвимостей к атакам больших компьютерных сетей важно определить сам термин «атака» (нарушение безопасности, вторжение, проникновение, нападение и др.), который в связи с его многозначностью по-разному трактуется специалистами по безопасности.

В отечественных стандартах в области информационных технологий нет четкого определения этого термина, однако в ГОСТ [3] данный термин применяется при пояснении значения термина *угроза* с помощью примеров *инцидентов информационной безопасности* (атаки хакера на систему, злонамеренный код, упущения и другие). Таким образом, на основании терминологии ГОСТ под *атакой* на информационную систему следует понимать один или несколько инцидентов информационной безопасности, связанных с *человеческим фактором*, которые в совокупности могут привести к реализации угроз путем использования *уязвимостей* этой информационной системы.

При определении термина «атака» использован целый ряд других терминов, также требующих определений. Так, *инцидент информационной безопасности* — это любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Для удобства далее вместо термина «инцидент информационной безопасности» будет использоваться термин «инцидент».

Объектом атаки будем называть размещенное в компьютерной сети средство обработки информации, в котором могут происходить инциденты. *Средством обработки информации* является любая система обработки информации, сервис или инфраструктура, или их физическое место размещения.

С понятием «атака» тесно связано понятие *угроза*, под которой понимается потенциальная причина инцидента, способного нанести ущерб системе или организации. *Ущерб* — это физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде. Исследователи обычно отдельно выделяют угрозы раскрытия информации, нарушения целостности и отказа в обслуживании (DoS). Первые два вида угроз являются наиболее частыми в локальных сетях, а в WAN на первое место выходит последний класс угроз.

Наконец, *уязвимость* информационной системы — это некая ее слабость, которая делает возможным возникновение угрозы.

В общем случае атака состоит из следующих этапов: исследование информационной системы, разработка программной реализации, осуществление атаки. В частном случае *пассивной атаки* последний этап может стать завершающим, однако в общем случае он может обеспечивать поддержку проведения других атак.

В больших сетях, особенно в WAN, подавляющее число возникающих атак перерастают в *распределенные атаки.* Для распределенных атак характерно синхронное возникновение большого количества инцидентов. Распределенные атаки относятся к типам "многие–к–

одному" и "многие–ко–многим". Так как распределенные атаки для больших сетей вызывают наибольший интерес, то далее в основном будет рассматриваться только этот класс атак, и для краткости вместо термина «распределенная атака» будет применяться термин «атака».

4. Модели атак в больших компьютерных сетях. Обычно классификация атак ориентирована на отдельные аспекты моделирования атак [4]. Такими аспектами могут быть формализмы представления данных и знаний об атаках, уровни модели OSI (Open Systems Interconnection) или модели DoD (Department of Defense), типы атак, возможности масштабирования, способность учитывать динамические характеристики атак (например, время, параллельные процессы, цепочки взаимосвязанных инцидентов) и т.д. С точки зрения формального представления данных и знаний, наиболее популярные типы моделей атак — это табличные и матричные модели, логические модели, модели, основанные на графах, а также модели, использующие объектно-ориентированный подход (рис. 1). Рассмотрим подробнее особенности каждого из этих типов.

Рис. 1. Типы моделей атак в больших компьютерных сетях.

Наиболее простые подходы к моделированию атак основаны на *табличном* или *матричном представлении информации*. Табличное представление трудно использовать при моделировании большого количества связей между возможными инцидентами или соответствующими действиями нарушителя. Кроме того, такой тип модели не удобен для анализа циклических атак. Однако, очевидно удобство таких моделей в тех случаях, кода информация представляет собой набор малосвязанных друг с другом образцов инцидентов или правил обнаружения атак.

Более универсальными являются *логические модели*, среди которых чаще всего используются модели атак, основанные на логике первого порядка и нечеткой логике. Преимуществами такого подхода являются возможности обработки цепочек взаимосвязанных инцидентов и использования языков представления знаний о предметной области, которые максимально приближены к естественному языку. Дополнительно к этому использование нечеткой логики позволяет учитывать случаи неопределенности исходных данных о моделируемых атаках. К недостаткам можно отнести необходимость использования специальных программных средств, обеспечивающих механизмы *логического вывода*. Примерами реализации механизмов вывода для логики первого порядка являются средства поддержки языка программирования Пролог. В случае нечеткой логики требуется поддержка *нечеткого вывода*. Следует отметить, что для моделирования логического вывода обычно используется *виртуальная машина*, что требует значительных вычислительных мощностей для обработки информации, необходимой для моделирования атак в больших компьютерных сетях.

Пожалуй, наиболее распространенными являются *модели атак, основанные на графах* [5]. Среди них широко известны графы атак, байесовские сети, сети Петри, а также различные расширения этих формализмов.

Рассмотрим модели атак, основанные на графах. Под *графом атак* понимается граф, содержащий все известные траектории (сценарии, пути) реализации нарушителем угроз (целей). Анализ такого графа может выполняться для решения следующих задач: анализ инцидентов; обнаружение возможных атак, не выявляемых системами обнаружения атак в реальном времени; оценка адекватности реализуемых мер безопасности и уровня защищенности сети; определение мер защиты для критических уязвимостей и программ, не имеющих обновлений; минимизация рисков и ресурсов для обеспечения безопасности компьютерной сети.

Ключевой проблемой построения графа атак для больших сетей является масштабируемость, связанная с формированием графа атак для сетей с большим числом хостов и уязвимостей.

Одним из распространенных подходов к моделированию атак с помощью графов является подход с использованием *деревьев атак*. В деревьях атак вершины могут быть типа И и ИЛИ. В расширениях деревьев атак вершинам и ребрам назначаются различные параметры, характеризующие объемы используемых нарушителем ресурсов (например, время, стоимость, сложность). Встречаются также модели, в которых вводятся дополнительные типы вершин, например, Order AND, показывающие, что подцели, соответствующие дочерним вершинам, должны достигаться нарушителем в строго определенном порядке.

Модели, основанные на деревьях атак, имеют следующие преимущества: наглядность, универсальность, адаптируемость, масштабируемость. К недостаткам моделей, основанных на деревьях атак, следует отнести трудности моделирования циклических атак и отсутствие возможностей динамического моделирования.

Кроме деревьев атак для моделирования используется ряд других формальных представлений атак, основанных на графах, к которым можно отнести рассмотренные выше преимущества и недостатки деревьев атак. К ним относятся:

1) *графы с перечислимым множеством состояний*, в которых вершинам соответствуют тройки $\langle s, d, a \rangle$, где s — источник атаки, d — цель атаки, a — элементарная атака, а дуги обозначают переходы из одного состояния в другое;

2) *графы зависимостей*, описанные в терминах ограничений доступа и угроз, в которых ограничения доступа представлены вершинами, а угрозы — связями; если вершины рассматриваются как условия, нарушения которых позволяют реализовать угрозу, то такие графы называют *ориентированными на условия,* если же вершины рассматриваются как предусловия и постусловия реализации угроз, то такие графы называются *ориентированными на угрозы (exploit-orientated);*

3) *графы путей реализации атак*, в которых вершины соответствуют инцидентам (элементарным атакам), а дуги отражают переходы от одного инцидента к другому, что обеспечивает удобство анализа атак в тех случаях, когда путь выполнения одной атаки охватывает несколько различных хостов, портов, программ, конфигурационных файлов и других объектов, расположенных на различных узлах компьютерной сети.

Примером моделирования атак с помощью байесовских сетей являются *байесовские графы атак*, которые представляют собой направленные ациклические графы, где вершины ассоциируются с инцидентами, рассматриваемыми также как элементарные условия, а ребра моделируют конъюнкцию или дизъюнкцию элементарных условий. Направление каждого ребра указывает на тот инцидент, который может возникнуть, если будет выполнена конъюнкция или дизъюнкция предшествующих ему условий. Байесовский граф атак имеет одну целевую вершину, которую можно ассоциировать с конкретной атакой. Значения вероятности, которые задаются для каждой вершины, кроме целевой, отражают возможную вероятность возникновения инцидента. Для расчета вероятности возникновения атаки или инцидента при условии возникновения предшествующих инцидентов можно использовать формулу условной вероятности.

Преимущества и недостатки байесовских графов атак такие же, как у рассмотренных ранее деревьев атак. Однако, в отличие от деревьев атак байесовские графы атак имеют дополнительные преимущества, так как они представляют собой вероятностные модели, которые позволяют учитывать случаи неопределенности исходных данных о моделируемых атаках.

Среди разновидностей байесовских сетей следует выделить *скрытые марковские модели*, которые часто используются при моделировании атак из-за удобства исследования путей в пространстве состояний, каждое из которых характеризуется заданной вероятностью.

Сети Петри являются одним из широко используемых формализмов при моделировании атак в компьютерных сетях. В терминах теории множеств *сеть Петри* можно определить как четверку $\langle \mathbf{P}, \mathbf{T}, I, O \rangle$, где $\mathbf{P} = \{p_1, p_2, ..., p_n\}$ — конечное множество *мест,* $n \geq 0$; $\mathbf{T} = \{t_1, t_2, ..., t_m\}$ — конечное множество *переходов,* $m \geq 0$, причем множество мест и множество переходов не пересекаются ($\mathbf{P} \cap \mathbf{T} = \varnothing$); $I : \mathbf{T} \to \mathbf{P}$ — отображение множества переходов во множество мест (I называется *входной функцией*); $O : \mathbf{T} \to \mathbf{Q}$ — отображение множества переходов во множество $\mathbf{Q}$ (O называется *выходной функцией*), где множество $\mathbf{Q}$ зависит от класса сетей Петри, например, в простых (*ординарных*) сетях Петри $\mathbf{Q} = \mathbf{P}$.

Маркировка сети Петри есть функция, отображающая множество мест $\mathbf{P}$ во множество $\mathbf{N}$, которое зависит от класса сети Петри. Маркировка сети Петри предназначена для моделирования ее динамиче-

ских характеристик. Множество **N** может быть *комплектом,* т.е. конечной совокупностью объектов, в которой возможно присутствие одинаковых объектов. Выходная функция сети Петри может содержать *пост-операцию* D, т.е. операцию изменения структуры сети Петри путем вставки или удаления мест или переходов.

Элементы множества **T** могут иметь время задержки либо вес, определяющий приоритет перехода по отношению к другим переходам, начинающимся в одном и том же месте. Также переходы могут сами быть сетью более низкого уровня.

Таблица 1. **Сети Петри, используемые для моделирования атак**

Тип маркировки	**Тип выходной функции**	**Способ задания свойств переходов**	**Классы сетей Петри**
$\mathbf{N} = \{\text{true,false}\}$	$O: \mathbf{T} \to \mathbf{P}$		Системы «условие–действие» Машина состояний
N — множество целых чисел	$O: \mathbf{T} \to \mathbf{P}$	$\mathbf{T} = \mathbf{G}$	Сети «место–переход»
		$\mathbf{T} = \mathbf{W}$	Стохастические сети Петри Сети Петри–Маркова
N является комплектом	$O: \mathbf{T} \to \mathbf{P}$		Раскрашенные сети Петри Скрытые раскрашенные сети Петри Мобильные сети Петри Нечеткие сети Петри Сети Петри высокого уровня Сети «окружение–отношение» Сети изделий (Product Nets) Сети «предикат–переход»
N является комплектом	$O: \mathbf{T} \to \mathbf{P}$	$\mathbf{T} = \mathbf{W}$	Временные раскрашенные сети Петри
N является комплектом	$O: \mathbf{T} \to \mathbf{P}$	$\mathbf{T} = \mathbf{L}$	Иерархические раскрашенные сети Петри
N является комплектом	$O: \mathbf{T} \to \mathbf{D}$, $\mathbf{T} \to \mathbf{P}$		Динамические сети Петри

Для более адекватного моделирования атак применяются различные расширения формализма сетей Петри. Так как существует большое количество таких расширений, удобно их классифицировать по типу маркировки и типу выходной функции [6]. В табл. 1 данная

классификация дополнена группировкой по способам задания свойств переходов и примерами расширений сетей Петри, используемых при моделировании атак.

Множество переходов, для которых определен приоритет, обозначено как **G** . Множество переходов, для которых задано время задержки, имеет обозначение **W** . Множество переходов, которые являются сетями более низкого уровня, обозначено как **L** .

Для моделирования атак наиболее часто используются такие расширения как *раскрашенные сети Петри, стохастические сети Петри* и *нечеткие сети Петри*. Важной особенностью последних является то, что элементами множества **N** являются значения функций принадлежности, позволяющих моделировать атаки с учетом неопределенности данных о безопасности сети. Примером функции принадлежности может быть функция оценки степени нарушения конфиденциальности, зависящая от типа атаки и текущей маркировки сети Петри.

Кроме рассмотренных выше преимуществ отдельных классов сетей Петри, в целом у них всех есть ряд параметров, делающих их использование удобным для моделирования атак в компьютерной сети.

К их числу, в частности, относятся: возможность графического представления модели; удобство моделирования динамических и параллельных процессов; способность отражения вероятностных процессов; возможность использования временных параметров; наличие большого количества инструментальных средств поддержки данного формализма; простота изучения и использования в силу наличия небольшого количества «примитивов»; удобство использования для анализа различных аспектов безопасности компьютерной сети.

К недостатку сетей Петри, который не компенсируется ни одним ее расширением, можно отнести неспособность в явном виде описывать поведение нарушителя и атакуемого объекта, т.е. динамическую смену их состояний. Такого недостатка лишены модели, в которых используются *агенты*.

Моделирование поведения нарушителя и атакуемого объекта удобно осуществлять с помощью *имитационного моделирования*, для которого специалисты используют четыре следующих основных подхода: дискретно–событийное моделирование, непрерывное динамическое моделирование, системная динамика, моделирование с помощью *агентов*. Необходимо отметить, что современные системы моделирования являются объектно-ориентированными, тем самым обеспечивая объединение всех четырех подходов.

Рассмотрим некоторые особенности моделей атак, реализуемых с использованием *агентов* [7, 8]. Типичными примерами агентов в больших сетях являются *вирусы* и *черви*. Если требуется моделировать поведение нарушителя и атакуемого объекта, то использование для этого искусственных агентов позволят отразить целый набор поведенческих характеристик, включая активность, реактивность, автономность, общительность, целенаправленность, интенциональность. Такой набор свойств агентов делает их особенно удобными для моделирования распределенных атак, а также случаев соперничества нарушителей друг с другом. Чаще всего при моделировании атак с помощью агентов выполняется построение *многоагентных систем*, в которых агенты разделены по роду деятельности и объединены в команды.

Для примера рассмотрим многоагентную модель распределенной атаки типа «распределенный отказ в обслуживании» (DDoS). Для проведения данной атаки нарушитель должен предварительно скомпрометировать большое количество хостов и установить на них атакующие агенты, которые, в свою очередь, будут либо одновременно посылать атакуемым хостам большое количество сетевых пакетов или трудных для обработки запросов, либо передавать через промежуточные узлы слишком длинные или некорректные пакеты.

Одним из вариантов построения и применения многоагентной системы при моделировании DDoS-атак является работа [7], где рассматриваются *агенты атаки* и *агенты защиты*.

Агенты атаки разделены на два следующих класса: «демоны», непосредственно реализующие атаку, и «мастера», выполняющие действия по координации остальных компонентов системы.

Агенты защиты разбиты на следующие классы: агенты обработки информации («сэмплеры»); агенты обнаружения атаки («детекторы»); агенты фильтрации и балансировки нагрузки («фильтры»); агенты идентификации и выведения из строя агентов атаки («агенты расследования»).

В целом при моделировании атак с помощью агентов, в частности, таких, как агенты атаки и защиты, могут быть использованы языки программирования общего назначения, например, C++, Java и другие, а также специальные языки описания и реализации агентов, например, ACL, KQML и AgentTalk. Разнообразие таких языков, а также готовых библиотек и инструментальных средств разработки агентов обеспечивает специалистам по безопасности широкие возможности для моделирования атак в сетях большого масштаба.

5. Методы моделирования атак в больших компьютерных сетях. Рассмотрим существующие методы моделирования распределенных атак и проблемы их использования для анализа безопасности в больших компьютерных сетях. В общем случае моделирование атак состоит из итераций, включающих следующие группы взаимосвязанных процессов (рис. 2): определение (переопределение) задачи, построение модели, запуск модели, анализ результатов. Особенности каждой из этих групп рассмотрены ниже.

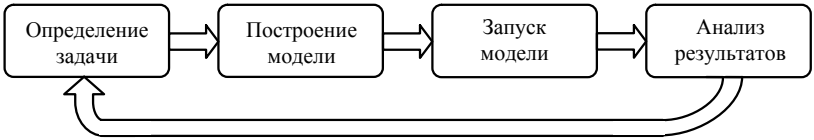

Рис. 2. Взаимосвязь групп процессов моделирования атак.

Под группой процессов определения задачи подразумевается подготовка требований, необходимых для выполнения последующих процессов моделирования, и получение исходных данных для построения модели. Данные требования включают, прежде всего, совокупность *требований к информационной безопасности*, отвечающих специфическим запросам потребителя, которые принято называть *профилем защиты*. В случаях неопределенности требований или исходных данных для успешного моделирования атак процессы определения задачи также должны включать приобретение знаний, позволяющих управлять построением модели атак. Такая неопределенность может быть связана с рассмотренными выше проблемами больших сетей, имеющих не всегда ясную структуру, «размытые» зоны ответственности, удаленные друг от друга на большие расстояния. Поэтому использование знаний, извлекаемых из различных источников, может иметь первостепенное значение при построении моделей атак для сетей, где решение проблем безопасности является критически важным.

Требования к информационной безопасности определяются особенностями конкретной предметной области и могут содержать как данные, так и метаданные, необходимые для решения задач обеспечения безопасности компьютерной сети, в частности, с использованием методов моделирования атак. Извлечение и представление таких требований являются отдельными задачами, некоторые решения которых рассмотрены в работе [9], где предложено использование *мета-*

моделей для представления целей, задач, рисков, ответственности и окружения.

Исходные данные для построения моделей атак обычно содержатся в документации, описывающей идеологию построения и развития информационной системы, структуру компьютерной сети, распределение зон ответственности и прочую информацию. Для больших сетей особенно характерна недостаточность документированных данных. Поэтому для построения моделей атак необходимо использовать информацию, извлеченную из других источников. Такими источниками могут быть журналы, формируемые типовыми сетевыми приложениями и системами мониторинга, примеры атак, выявленных сетевыми сканерами, и другие.

Группа процессов построения модели предназначена для формализации исходных данных и знаний об атаках в исследуемой компьютерной сети. При этом конкретные формализмы, методы и средства построения модели выбираются в зависимости от конкретных требований к модели, т.е. целей, задач, рисков, ответственности, окружения и т.д., а также неполноты и неопределенности исходной информации.

Задачи, решаемые в этой группе процессов, для больших сетей связаны с проблемами вычислительной сложности. Так как эти задачи различаются в зависимости от требований, исходных данных и способов формализации данных и знаний, они образуют множество сложных вычислительных задач, включающее NP-трудные и NP-полные задачи. Примерами являются следующие задачи:

построение графа атак в условиях неполноты исходных данных для атак типа «многие–к–одному» и «многие–ко–многим»;

оптимальное размещение вершин отображаемого графа атак для обеспечения эффективности его дальнейшего анализа;

планирование скоординированного поведения агентов с использованием *графов зависимостей агентов.*

Группа процессов запуска модели необходима при моделировании динамических характеристик нарушителей или объектов атаки и предназначена для изучения ее поведения и последующего анализа результатов моделирования. При запуске моделей также могут иметь место задачи большой вычислительной сложности, решение которых обычно зависит от выбранных инструментальных средств моделирования. Кроме того, задачи большой вычислительной сложности возникают при мониторинге уже запущенных моделей. Примером является NP-полная задача распознавания плана поведения агентов [10]. В тех случаях, когда динамические характеристики не существенны, анализ

результатов обычно осуществляется путем непосредственного исследования модели атак, т.е. без запуска модели.

Группа процессов анализа результатов в зависимости от требований к текущей итерации может быть ориентирована на выявление возможных или реализованных угроз, определение эффективных средств защиты с точки зрения имеющихся ресурсов, подготовку требований для следующих итераций моделирования и т.д. Как и при построении модели атак, анализ результатов моделирования может потребовать больших вычислительных затрат. Наибольшие трудности вызывают, например, следующие NP-трудные и NP-полные задачи: поиск наиболее длинного пути в матрице инцидентов; поиск наиболее длинного пути в графе атак; поиск атак, для проведения которых требуются заданные ресурсные ограничения (поиск осуществляется по графу атак); определение с помощью графа атак минимального набора инцидентов, идентифицирующих нарушителя; определение минимального покрытия узлов сети средствами трассировки пакетов (*tracers*) или средствами трассировки событий (*sensors*); идентификация плана поведения атакующих агентов в иерархии планов, учитывающей различные уровни абстракции и порядок следования.

Являясь составной частью итерации моделирования, анализ результатов может приводить к изменениям требований, необходимых для проведения новых итераций. При этом модели атак, построенные на предыдущих итерациях, могут рассматриваться как исходные данные для построения новых моделей.

Чтобы сократить объемы вычислений для задач, алгоритмическое решение которых обладает большой вычислительной сложностью, используются различные эвристики. Например, эвристикой для сокращения перебора при построении моделей на основе графов атак может быть фильтрация заранее подготовленных шаблонов с планами атак на основе различных *метрик риска*, характеризующих усилия, стоимость, время и другие необходимые ресурсы.

В качестве эвристик для снижения сложности вычислений при решении различных задач анализа графов атак могут выступать, например, агрегация элементов графа, кластеризация матрицы смежности графа, «жадный» эвристический алгоритм, генетические алгоритмы и другие. Под *агрегацией* понимается отображение различных фрагментов графов атак, характеризуемых заданными уровнями абстракции и определенными значениями свойств элементов графа.

Если требования являются не достаточно определенными, или сети имеют так много узлов и связей, что объем исходных данных ока-

зывается настолько большим, что уже нельзя использовать существующие алгоритмические решения, успешно применяемые для сетей небольшого размера, то задача моделирования может быть отнесена к классу *неформализованных задач*. Данный класс включает задачи, которые обладают одной или несколькими из следующих характеристик [11]: задачи не могут быть заданы в числовой форме; цели не могут быть выражены в терминах точно определенной числовой функции; не существует алгоритмического решения задач; алгоритмическое решение существует, но его нельзя использовать из-за ограниченности ресурсов (время, память).

Для решения неформализованных задач могут быть полезны модели и методы извлечения, представления и обработки знаний, методы инженерии знаний, используемые в области искусственного интеллекта. Для интеллектуальной поддержки моделирования атак чаще всего используются экспертные системы, искусственные нейронные сети и интеллектуальные агенты, примеры которых рассмотрены ниже.

Один из характерных примеров использования экспертных (ЭС) для систем интеллектуальной поддержки моделирования атак описан в [12], где рассматривается ЭС, созданная в среде Java Expert System Shell (JESS). В качестве источника знаний ЭС были использованы обобщенные шаблоны атак, которые преобразованы в правила и сохранены в базе знаний ЭС на языке представления знаний CLIPS. Созданное решение позволяет учесть атаки типа «один–к–одному» и «один–ко–многим». Предусмотрено его развитие для учета распределенных атак за счет введения маркировки узлов в графе атак для моделирования захвата узлов несколькими нарушителями.

Преимуществом использования ЭС для построения моделей атак в больших компьютерных сетях является не только их ориентированность на решение неформализованных задач, но и возможность представления знаний на языке, близком к естественному. Недостатком ЭС является необходимость привлечения экспертов по обеспечению безопасности компьютерных сетей в качестве первичного источника знаний. Однако, возможно использование вторичных источников, например, баз данных и текстовых документов.

Рассмотрим особенности использования искусственных нейронных сетей при моделировании атак. Искусственная нейронная сеть может рассматриваться как направленный граф, в узлах которого находятся искусственные нейроны, а связи имеют заданные веса. С точки зрения архитектуры связей, различают сети прямого распространения, в которых графы не имеют петель, и с обратными связями

(рекуррентные сети). Возможны различные подходы к моделированию атак с помощью искусственных нейронных сетей. Например, в работе [13] предложено обучать нейронные сети на примерах атак, отнесенных к определенным классам, чтобы в дальнейшем использовать для распознавания атак соответствующих классов, выявляя аномальные последовательности изменений параметров объектов информационной системы.

Более сложный подход к моделированию атак в больших сетях с использованием нейронных сетей предложен в работе [14]. В данной работе нейронная сеть типа *Graph Neural Networks* применяется для ранжирования узлов в графе атак, в результате чего осуществляется выделение в графе атак наиболее важных групп узлов. Параметры ранжирования могут меняться, что позволяет добиваться требуемой эффективности метода. Примерами таких параметров могут быть среднее или максимальное расстояние между узлами.

Преимуществами моделей, основанных на нейронных сетях, являются гибкость, адаптивность, способность анализировать неполные и искаженные данные, высокая скорость обработки данных и возможность распознавания не встречающихся ранее ситуаций. К недостаткам относятся невозможность точного описания поведения моделируемой системы в целом и отдельных ее элементов. Кроме того, для обучения нейронной сети требуется подготовить большую выборку примеров атак, а достоверность модели полностью зависит от эффективности обучения нейронной сети.

Как отмечено ранее, для моделирования распределенных атак, а также случаев соперничества нарушителей друг с другом удобно использовать агенты. Если задача моделирования является неформализованной, то целесообразно применение *интеллектуальных агентов*, которые обладают развитой моделью внешнего мира благодаря наличию у них базы знаний, механизмов решения и анализа действий. В качестве примера рассмотрим *агентно-ориентированную систему моделирования атак*, предложенную в работе [15]. Распределенные скоординированные атаки на компьютерную сеть в данной системе представляются в виде сценариев совместных действий агентов-хакеров, которые осуществляются с различных хостов. Отличительные черты рассматриваемого подхода заключаются в использовании спецификации задач хакеров, учете иерархии их намерений, выделении нескольких уровней описания атак, использовании онтологии предметной области «Атаки на компьютерные сети» при разработке планов действий и моделей отдельных атак, применении стохастиче-

ских атрибутных грамматик для формализации сценариев, возможности моделирования поведения агентов в реальном масштабе времени.

Знания, необходимые для интеллектуальной поддержки процессов моделирования атак, могут быть извлечены из различных первичных и вторичных источников. Используя эти знаний при моделировании процессов, происходящих в больших компьютерных сетях, исследователи сталкиваются с тем, что доля «дефектов знаний» и различных форм незнания оказывается достаточно большой. Поэтому для адекватного моделирования атак требуется учитывать *НЕ-факторы*.

Термин *НЕ-факторы* был предложен А.С. Нариньяни для комплекса свойств, характерных для реальной системы знаний, но плохо представленных в формальных системах (неполнота, неточность, недоопределнность, некорректность, нечеткость и другие) [16]. Среди известных в настоящее время НЕ-факторов в формализмах представления моделей атак исследователи учитывают только *неточность*, *недоопределенность* и *нечеткость*, кроме того, в некоторых методах построения моделей атак учитываются также *неоднозначность* и *неполнота*. Проблемы учета других видов НЕ-факторов в данной области мало исследованы.

Неточность значения означает, что его величина может быть получена с точностью, не превышающей некоторый порог, определенный природой соответствующего параметра.

Недоопределенность величины означает, что она по своей природе является более точной, чем позволяет установить доступная нам в данный момент информация. В работе [17] различают *недоопределенность первого типа,* когда удается установить, что значение принадлежит некоторому множеству, *и недоопределенность второго типа*, когда известна вероятность того, что некоторый атрибут (переменная, параметр и т.п.) принимает определенное значение.

Нечеткость означает отсутствие точных границ области определения, свойственных большинству понятий. Для учета данного НЕ-фактора используются *лингвистические переменные*.

Неоднозначность значения означает, что существует множество альтернатив, оцениваемых неравномерно с точки зрения конкретной семантики.

Неполнота характеризуется отсутствием необходимой для решения задачи информации [17].

Примеры исследований проблем моделирования атак, связанных с различными видами НЕ-факторов, представлены в табл. 2.

Таблица 2. **Примеры исследований проблем моделирования атак**

НЕ-фактор	Пример исследования
Неточность	[18]
Нечеткость	[19]
Недоопределенность первого типа	[20]
Недоопределенность второго типа	[5]

6. Средства построения моделей атак в больших компьютерных сетях. В настоящее время существуют программные средства, ориентированные на моделирование атак в больших компьютерных сетях (табл. 3). Рассмотрим некоторые примеры более подробно.

Таблица 3. **Программные средства моделирования атак**

Название средства	Производитель	Тип формализма	Учет DDoS
COMNET III	CACI Product, USA	Графы	
NeuSecure	NetIQ, USA	Графы	
Система анализа защищенности АС	СПИИРАН, Россия	Графы	
NeuSecure	NetIQ, USA	Графы	
NS-2	ACIMS, USA	Графы	Да
OPNET Modeler	OPNET Technologies, USA	Графы	Да
OMNeT++	OMNeT++ Community	Графы	Да
NNID	University of Texas at Austin, USA	Графы (нейронные сети)	Да
Cannady's tool	Nova Southeastern University, USA	Графы (нейронные сети)	Да
Security Manager	Intellitactics, USA	Таблицы	Да
LogLogic	LogLogic, USA	Таблицы	Да
Enterprise Security Manager	ArcSight, USA	Таблицы, графы	Да
Sentinel	Novell, USA	Таблицы, графы	
Security Information Manager	Symantec, USA	Таблицы, графы	Да
eTrust Security Command Center	Computer Associates, USA	Таблицы, графы	
Security Center	ActiveWorx, USA	Таблицы, графы	Да
Tivoli Risk Manager	IBM, USA	Таблицы, графы	Да
Eventia	Check Point Software Technologies	Таблицы, графы	Да
ESM	ArcSight, USA	Таблицы, графы	Да
MulVAL	Kansas State University, USA	Графы, логические	Да

		модели	
nFX Open Security Platform	NetForensics, USA	Логические модели	
ASAX	University of Namur, Belgium	Логические модели	Да
Агент-07	Пермский государственный университет	Агенты	
AAFID	Purdue University, West Lafayette, USA	Агенты	Да
	СПИИРАН, Россия	Агенты	Да

Программное средство «Система анализа защищенности АС» [21], разработанное в СПИИРАН, предназначено для анализа защищенности автоматизированных систем (АС) путем имитации действий нарушителя, построения и анализа дерева атак. Входными данными для моделирования являются спецификации анализируемой АС, модель нарушителя и исходные показатели защищенности, включая интегральный показатель «уровень защищенности АС», на основе которых система строит дерево атак и обеспечивает его графическую визуализацию с целью дальнейшего анализа. Выходными данными являются показатели защищенности, рассчитанные с использованием деревьев атак, а также другая информация об анализируемой сети в виде журналов регистрации событий, отчетов и т.д. Система разработана на языке Java.

Также в СПИИРАН проведен ряд исследований по созданию многоагентных моделей, ориентированных на моделирование распределенных атак [7, 15]. Кроме того, значительная часть проблем разработки средств моделирования атак в Интернете рассмотрена в работе [8], где в качестве основных требований к используемому инструментарию моделирования выделены следующие: детальная реализация протоколов, используемых в DDoS-атаках; возможности расширения функциональности агентов путем добавления новых компонент; наличие средств изменения параметров моделирования во время проведения исследований; совместимость с различными операционными системам, как минимум с Windows и Linux; развитый графический интерфейс; возможность получения права бесплатного использования в исследовательских целях.

В данных исследованиях выбран инструментарий моделирования OMNeT++ INET Framework как наилучшим образом соответствующий перечисленным требованиям. С помощью данного средства созданы модели антагонистического взаимодействия команд агентов–злоумышленников и агентов защиты. Показана эффективность разработанных средств на примере сценария моделирования DDoS-атаки.

7. Направления дальнейшего развития методов и средств моделирования атак в больших компьютерных сетях. Потребность в создании новых методов и средств моделирования атак вызвана, прежде всего, необходимостью максимального сокращения вычислительной сложности алгоритмов построения и анализа моделей атак, что особенно актуально для больших компьютерных сетей. Такая гибкость может быть обеспечена, если пользователям средств моделирования атак не только будет предоставлена возможность применять известные эвристические методы сокращения вычислительной сложности, например, основанные на использовании метрик риска, агрегации элементов графа, кластеризации матрицы смежности графа, «жадного» алгоритма, генетического алгоритма и т.д., но и будет дана возможность самостоятельно создавать новые и модифицировать существующие правила построения и анализа моделей атак в зависимости от текущих требований безопасности.

Также при моделировании атак в больших компьютерных сетях важно учитывать, что процессы моделирования атак, а также другие процессы, связанные с обеспечением безопасности сетей, имеют итерационный характер. Однако, как показал анализ существующих инструментальных средств моделирования атак, такие средства обычно слабо ориентированы на поддержку замкнутых циклов моделирования, при которых результаты предшествующих итераций можно было бы полностью или частично использовать в новых циклах.

Многие трудности моделирования атак в больших компьютерных сетях связаны с наличием различных видов НЕ-факторов. В рамках примеров, приведенных в табл. 2, учтены отдельные виды НЕ-факторов. Однако до настоящего времени не проводились исследования с целью создания универсальных моделей атак, ориентированных сразу на несколько видов НЕ-факторов.

В настоящее время проводятся активные исследования в области построения нового поколения систем управления информацией и событиями безопасности (Security Information and Event Management, SIEM) [22, 23]. В качестве возможных областей применения SIEM-систем нового поколения рассматриваются распределенные крупномасштабные сети, а также критические инфраструктуры. Компонент моделирования атак и анализа безопасности (Attack Modeling and Security Evaluation Component, AMSEC) считается неотъемлемой частью таких SIEM-систем.

Так как области применения SIEM-систем в общем случае относятся к классу больших сетей, то задачу разработки компонента AM-

SEC также следует рассматривать как дальнейшее направление развития методов и средств моделирования атак в больших компьютерных сетях. Рассмотрим некоторые предложения по ее решению.

Основная проблема реализации компонента AMSEC видится в обеспечении реального или достаточно близкого к реальному масштаба времени. Как известно, результаты работы системы моделирования атак зачастую не могут быть получены в реальном времени. Однако преодолеть это ограничение можно, если учесть, что построенные графы атак сохраняют актуальность достаточное время. Благодаря этому предлагается использовать в рамках AMSEC построенные заранее графы атак, которые могут применяться как предсказания действий нарушителя в период, следующих за моментом возникновения атаки, так и для анализа и выявления его предыдущих действий, приведших систему к текущему состоянию.

Кроме того, для повышения эффективности функционирования AMSEC предлагается использовать не отдельные текущие события, а инциденты, выявленные в результате осуществления процесса корреляции хранимых в SIEM-системе событий безопасности.

Предсказание последующих действий нарушителя должно осуществляться на основании обработки следующих исходных данных: 1) целей атак, которые задаются их графами; 2) моделей нарушителя, позволяющих построить графы атак, наиболее близкие к реальным; 3) использованных нарушителем классов атак и уязвимостей.

Таким образом, учет данных, полученных от компонента AMSEC, позволит делать выводы о взаимной корреляции обнаруженных и еще не обнаруженных инцидентов безопасности.

Кроме того, для повышения результативности работы компонента AMSEC предлагается дополнить его функционал решением следующих задач: 1) выявлением наиболее слабых мест в топологии сети, т.е. узлов, через которые проходит наибольшее число графов атак; 2) формированием и выбором контрмер, направленных на снижение возможного количества графов атак, проходящих через узлы сети; 3) оценкой возможных последствий реализации контрмер, учитывающих зависимости между защищаемыми сервисами.

Реализация перечисленных предложений позволит существенно повысить эффективность функционирования SIEM-системы и ее возможности предсказывать, обнаруживать и идентифицировать атаки в больших компьютерных сетях и вырабатывать меры противодействия им за счет использования методов и средств моделирования атак.

8. Заключение. Рассмотренные модели, методы и средства моделирования атак показывают, что, несмотря на их многочисленность, проблема моделирования атак в больших компьютерных сетях остается нерешенной и актуальной. Результаты анализа направлений дальнейшего развития методов и средств моделирования атак предопределяют необходимость первоочередной разработки новой методики моделирования атак в больших компьютерных сетях, ориентированной на решение рассмотренных выше проблем и задач. Вместе с этим необходима разработка комплекса программно-инструментальных средств для автоматизированной поддержки данной методики.

Литература

1. *Федотов А. М.* Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций. М.: ВИНИТИ, 2008. № 2. С. 88–101.
2. *Лахно В.А., Петров А.С., Скрипкина А.С.* Построение дискретных процедур распознавания и поиска уязвимостей информации // Інформаційна безпека, 2010. № 2 (4). С. 5–13.
3. ГОСТ Р ИСО/МЭК. 13335-1 — 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий / М.: Стандартинформ, 2007. 18 с.
4. *Сердюк В. А.* Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: НИУ ВШЭ, 2011.
5. *Zhang S., Song S.* A. Novel Attack Graph Posterior Inference Model Based on Bayesian Network // Journal of Information Security, 2011. № 2. P. 8–27.
6. *Рыбина Г.В., Смирнов В.В.* Методы и алгоритмы верификации баз знаний в интегрированных экспертных системах // Известия РАН. Теория и системы управления. 2007. № 4. С. 91–102.
7. *Котенко И. В., Уланов А. В.* Команды агентов в кибер-пространстве, моделирование процессов защиты информации в глобальном Интернете // Тр. ин-та системного анализа РАН. Проблемы управления кибербезопасностью информационного общества. М: КомКнига, 2006. Т. 27. С. 108–129.
8. *Котенко И. В., Уланов А.В.* Моделирование противоборства программных агентов в Интернете: общий подход, среда моделирования и эксперименты // Защита информации. INSIDE. 2006. № 5. С. 2–10.
9. *Faily S.I., Fléchais I.A.* Meta-Model for Usable Secure Requirements Engineering // Workshop on Software Engineering for Secure Systems, 2010. SESS ’10, ICSE / IEEE Computer Society Press, 2010. P. 126–135.
10. *Banerjee B., Kraemer L., Lyle J.* Multi-Agent Plan Recognition: Formalization and Algorithms // Proceedings of AAAI, 2010. P. 1059-1064.
11. *Попов Э. В., Фоминых И.Б., Кисель Е.Б., Шапот М.Д.* Статические и динамические экспертные системы. М.: Финансы и статистика, 1996.
12. *Danforth M.* EVA: A Framework for Network Analysis and Risk Assessment // USENIX Systems Administration Conference (LISA'09), Baltimore, MD, US, November 1–6, 2009. P. 65–77.

13. *Гамаюнов Д.Ю., Качалин А.И.* Методика настройки интеллектуальных распознавателей компьютерных атак для работы в корпоративных сетях // Искусственный интеллект, 2006. № 2. С. 30–34.
14. *Lu L., Safavi-Naini R., Hagenbuchner M., Susilo W., Horton J., Yong S.L., Tsoi A.C.* Ranking attack graphs with graph neural networks // Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics. LNCS, 2009. P. 345–359.
15. *Котенко И.В.* Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью: Труды Института системного анализа РАН. М.: УРСС, 2009. Т. 41. С. 74–103.
16. *Нариньяни А.С.* НЕ-факторы: state of art // Научная сессия МИФИ, 2004. Т. 3. С. 26-30.
17. *Рыбина Г.В., Душкин Р.В., Козлов Д.А., Левин Д.Е., Смирнов В.В., Файбисович М.Л.* Вопросы извлечения и представления неточных и недоопределенных знаний при автоматизированном построении баз знаний для интегрированных экспертных систем // Третья международная летняя школа-семинар по искусственному интеллекту для студентов и аспирантов (Браславская школа) / Сборник научных трудов. Мн.: БГУИР, 1999. С. 191–198.
18. *Abdulla S.M., Al-Dabagh N.B., Zakaria O.* Identify Features and Parameters to Devise an Accurate Intrusion Detection System Using Artificial Neural Network // World Academy of Science, Engineering and Technology. 2010. Issue 70. P. 627–631.
19. *Huang G., Zhang B.* An Approach to Fuzzy Petri Attack Net and Its Automatic Generating Algorithm Based on Fuzzy Petri Net // Proceedings of the Sixth Wuhan International Conference on E-Business (WHICEB2007), May 26-27, Wuhan, China, 2007. P. 1370–1379.
20. *Kichkaylo T., Ryutov T., Orosz M.D., Neches R.* Planning to Discover and Counteract Attacks // Informatica (Slovenia), 2010, № 34(2). P. 159–168.
21. *Котенко И.В., Степашкин М.В., Чечулин А.А., Дойникова Е.В., Котенко Д.И.* Инструментальные средства анализа защищенности автоматизированных систем // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года / СПб.: Изд-во Политехнического университета. 2010. С. 115–116.
22. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012.
23. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012.

Котенко Дмитрий Игоревич — аспирант кафедры МО ЭВМ Санкт-Петербургского государственного электротехнического университета «ЛЭТИ». Область научных интересов: информационная безопасность в компьютерных сетях. Число научных публикаций — 6. dmitrykotenko1986@gmail.com; СПбГЭТУ«ЛЭТИ», каф. МО ЭВМ, ул. проф. Попова, д. 5, Санкт-Петербург, 197376, РФ; р.т. +7(812)234-9668. Научный руководитель — Молдовян А.А.

Kotenko Dmitry Igorevich — postgraduate student of Computer Software Department of Saint Petersburg State Electrotechnical University «LETI» (ETU). Research interests: network information security. The number of publications — 6. dmitrykotenko1986@gmail.com;Saint

Petersburg State Electrotechnical University «LETI» (ETU), 5, Professor Popov st., Saint-Petersburg, 197376, Russia; office phone +7(812)234-9668. Scientific adviser — Moldovjan A.A.

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Professor, Head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more than 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Саенко Игорь Борисович — д-р техн.наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность. Число научных публикаций — 250. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security of SPIIRAS. Research interests: automated information systems, information security. The number of publications — 250. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812)328–2642, fax +7(812)328–4450.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ (проекты 10–01–00826–а, 11–07–00435–а), программой фундаментальных исследований ОНИТ РАН (проект 2.2) и проектами Седьмой рамочной программы Европейского Союза SecFutur и MASSIF.

Рекомендовано лабораторией криптологии, заведующий лабораторией Молдовян Н.А., д–р техн.наук, проф., заслуженный изобретатель РФ.
Статья поступила в редакцию 3.05.2012.

РЕФЕРАТ

Котенко Д.И., Котенко И.В., Саенко И.Б. **Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы.**

Работа посвящена анализу проблем моделирования атак в больших компьютерных сетях с использованием различных моделей, методов и инструментальных средств. Исходя из рассмотрения особенностей больших сетей как объектов информационной безопасности и объектов атак, детально рассмотрены известные модели, а также методы и средства моделирования атак, а также приведены направления их дальнейшего развития.

Особенности больших сетей как объектов информационной безопасности обусловлены структурными факторами, различием скоростей передачи данных, разнообразием аппаратных и программных средств, организационными факторами, неполнотой и неопределенностью исходных данных, а также территориальной удаленностью инфраструктурных объектов.

В больших сетях подавляющее число возникающих атак перерастают в распределенные атаки, для которых характерно синхронное возникновение большого количества инцидентов. Распределенные атаки относятся к типам "многие–к–одному" и "многие–ко–многим" и для больших сетей вызывают наибольший научный интерес.

С точки зрения формального представления данных и знаний, наиболее популярными типами моделей атак в больших сетях являются табличные модели, логические модели, модели, основанные на графах, а также модели, основанные на агентах. К недостатку моделей, основанных на графах, относится неспособность в явном виде описывать динамическую смену состояний. Такого недостатка лишены модели, основанные на агентах.

Показана роль требований к информационной безопасности в итерациях моделирования атак. В общем случае эти итерации включают определение задачи, построение модели, запуск модели и анализ результатов.

Для решения неформализованных задач моделирования атак используются модели и методы извлечения, представления и обработки знаний, а также методы инженерии знаний. Для интеллектуальной поддержки моделирования атак чаще всего используются экспертные системы, искусственные нейронные сети и интеллектуальные агенты.

Для адекватного моделирования атак требуется учитывать НЕ-факторы, которые характеризуют свойства, характерные для реальной системы знаний, но плохо представленные в формальных системах.

В настоящее время существуют программные средства, включая отечественные, ориентированные на моделирование атак в больших компьютерных сетях. Однако потребность в разработке новых методов и средств моделирования атак в больших сетях сохраняется, что вызвано, в частности, необходимостью максимального сокращения вычислительной сложности алгоритмов.

SUMMARY

Kotenko D.I., Kotenko I.V., Saenko I.B. **Methods and tools for attack modeling in large computer networks: state of the problem.**

The paper is intended to analyze attack modeling problems in large computer networks with the use of different models, methods and tools. The famous models, as well as methods and tools for attack modelling are examined in detail on the basis of the characteristics of large networks as information security related objects and objects of attack, and directions for further development are provided.

Features of large networks as objects of information security are caused by structural factors, variation in data transfer speed, a variety of hardware and software, organizational factors, incomplete and uncertain input data as well as territorial remoteness of infrastructure objects.

In larger networks, the vast majority of emerging attacks are growing into distributed attacks, for which a large number of incidents occur synchronously. Distributed attacks are the types of "many-to-one" and "many-to-many" relationship which arouse scientific interest for large networks.

In terms of formal data and knowledge representation, the most popular types of attack models on large networks are a tabular model, logic models, models based on graphs and models based on agents. Failure to explicitly describe the dynamical states refers to lack of graph-based models. Agent-based models are deprived of such shortcoming.

The role of information security requirements in attack modeling iterations is shown. In general, these iterations include task definition, developing model, launching model and analysis of results.

To provide modeling tasks, models and methods of extraction, representation and processing of knowledge, as well knowledge engineering techniques are used. For intellectual support of modeling attacks the expert systems, artificial neural networks and intelligent agents are used most often.

For the adequate attacks simulating NOT-factors that characterize the properties specific to a real system knowledge, but are poorly represented in formal systems must be taken into account.

Currently, there are software tools, including domestic, oriented on simulation of attacks on a large computer networks. However, there's the need to develop new methods and tools for modeling attacks on large networks, due to, inter alia, the need to minimize the computational complexity of algorithms.