УДК 681.3.06:519.248.681

А. В. СНЕГУРОВ, канд. техн. наук

ПЛАНИРОВАНИЕ ДЕЙСТВИЙ ПО РЕАГИРОВАНИЮ НА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Постановка проблемы

Способы и средства нарушения информационной безопасности критически важных информационных систем развиваются стремительными темпами. Нападающая сторона может осуществлять нападение в сложные для информационной системы моменты времени (период наибольшей нагрузки, выходные и праздничные дни, ночное время суток). Нападающая сторона может сначала определенное время изучать систему защиты как пассивными, так и активными способами, и только потом осуществлять нападение. Под активными способами можно понимать имитационные действия нападающей стороны, которые вынуждают систему защиты реагировать на вторжение, тем самым раскрывая свои возможности.

Нападающая сторона может организовывать комплексное нападение, при котором вместе с открытыми (имитационными) действиями может осуществляться скрытое проникновение в систему по разным каналам воздействия. Объективной реальностью является то, что разработка способов и средств нападения опережает разработку систем защиты, что делает сложным организацию противодействия новым угрозам.

В структуре обеспечения информационной безопасности информационных систем важную роль играют системы обнаружения вторжений (Intrusion Detection System (IDS)). Данные системы в дополнение к межсетевым экранам служат механизмами мониторинга и наблюдения подозрительной активности в сетях. Использование IDS позволяет выявлять факты неавторизованного доступа (вторжения или сетевой атаки) в информационную систему.

Системы обнаружения вторжений, построенные по методу аномалий, позволяют обнаруживать как атаки известных типов, так и атаки, сигнатуры которых еще не разработаны. Принцип функционирования таких систем основан на определении ненормального (необычного) поведения на хосте или в сети. Существенным недостатком таких систем является сложность описания параметров нормального и ненормального функционирования сети, а также большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности.

Все это существенн усложняет возможность адекватной реакции системы защиты на вторжение. На данный момент недостаточно проработаны методы определения факта нападения. Не разработаны эффективные механизмы распознавания аномальных состояний информационных систем, принятия решения относительно причин возникновения аномалий. Практически не решены вопросы выбора рационального поведения системы защиты при обнаружении атаки или аномального поведения информационной системы.

В современной литературе уделяется много внимания разработке систем защиты сложных информационных систем. Так, в [1] предлагается подход к построению интеллектуальной системы защиты, описываются пути построения подсистем поддержки принятия решения при функционировании системы защиты. В [2] предложен метод обнаружения угроз на основе теории последовательного анализа. Вопросы распознавания угроз и построения интеллектуальной системы защиты рассмотрены в [3, 4] и других источниках.

Однако проблемным остается планирование действий системы защиты при обнаружении аномалий в поведении информационной системы. Особенно это актуально, когда точно не выявлена причина аномального поведения информационной системы, которая может быть как результатом вторжения, так и результатом, например, нетипичного поведения авторизованных пользователей.

Цель статьи – разработка подхода по планированию действий системы защиты в условиях возникновения аномалий в поведении информационной системы.

Основной материал исследований

Важнейшей задачей после обнаружения вторжения является реализация комплекса мероприятий по защите информационной системы и ликвидации последствий данного вторжения. «Вся ваша работа по обеспечению инфраструктуры, которая может обнаружить вторжение, является ничего не стоящей, если ничто не будет сделано, когда вторжение действительно обнаружено» [5].

Расследования вторжений показали [5], что чрезвычайно полезным было наличие у должностных лиц структур информационной безопасности плана действий. План не охватывал все последующие события, но его наличие обеспечивало руководство последовательностью действий в условиях, когда эмоции были на пределе. Наличие такого плана позволяло в дальнейшем проанализировать свои действия, выработать более адекватный механизм реагирования на вторжение.

Особенностью планирования действий системы защиты при вторжении (обнаружении аномалий в работе информационной системы) является частичная неопределенность как в действиях нападающей стороны, так и в поведении защищаемой системы после вторжения.

К неопределенности относительно действий нападающей стороны относятся:

- время нападения;
- объект нападения;
- нападающая сторона;
- варианты действий нападающей стороны в разных складывающихся условиях обстановки.

В этих условиях планирование действий системы защиты должно подчиняться следующим правилам:

- планирование должно осуществляться заблаговременно, при этом должны определяться несколько вариантов действий системы защиты в зависимости от складывающихся условий;
- должен быть определен механизм классификации ситуаций нападения на основе четких или нечетких признаков, позволяющий соотнести для каждой сформулированной ситуации варианты действия системы защиты;
- планирование должно учитывать ситуативный характер действий системы защиты;
- при обнаружении факта нападения (аномалии в функционировании информационной системы) должен быть выбран рациональный вариант действия системы защиты, при этом план действий системы защиты должен корректироваться на основе результатов мониторинга действий нападающей стороны и состояния защищаемой системы;
- план действий системы защиты должен учитывать параллельное функционирование разных подсистем системы защиты, но которые могут взаимообеспечивать действия друг друга;
- временные интервалы действий системы защиты и нападающей стороны не могут быть жестко заданными и должны описываться нечеткими величинами.

Для решения поставленной задачи предлагается использовать математический аппарат нечеткого сетевого планирования. Данный математический аппарат позволяет выбрать последовательность действий системы защиты и задать продолжительность таких действий тогда, когда информация о последней априори плохо неизвестна и оценивается субъективно.

В сетевой модели действия системы защиты отображаются в виде сетевого графа. В данном графе вершины могут обусловливать события, определяющие начало и окончание отдельных действий, а дуги в этом случае будут соответствовать самим действиям. Пусть множество $\{Д_r\}_{r=1}^{R}$ – множество действий, которые должна (может) реализовать система защиты. Тогда, если множество $\{C_j\}_{j=1}^{J}$ будет представлять комплекс событий (состояний информационной системы), возникающих в процессе выполнения комплекса действий, то сетевая модель будет задаваться ориентированным графом, в котором элементы множества

$\{C_j\}_{j=1}^{J}$ играют роль вершин, а элементы множества $\{Д_r\}_{r=1}^{R}$ – роль дуг, соединяющих вершины. Каждой *r* дуге можно поставить в однозначное соответствие пару вершин, первая из которых будет определять момент начала действия *r*, а вторая – момент окончания этого действия.

Сетевая модель может быть представлена сетевым графиком, в табличной форме, в матричной форме или в форме диаграммы на шкале времени. Преимущество сетевых графиков и временных диаграмм перед табличной и матричной формами представления состоит в их наглядности. Однако это преимущество исчезает прямо пропорционально тому, как увеличиваются размеры сетевой модели.

Для каждого действия *r* задается множество его непосредственных предшественников $PRE(r) = \{pre(r)\}$ и последователей $POST(r) = \{post(r)\}$. Задается начальная вершина *start* и конечная вершина *fin*. Для каждого действия задается его продолжительность, представленная нечеткими числами $\tilde{Д}_r = \left\{t, \mu_{\tilde{Д}_r}(t)\right\}$, где t – возможная длительность действия системы защиты, $\mu_{\tilde{Д}_r}(t)$ – степень принадлежности величины t – нечеткому множеству $\tilde{Д}_r$ [6].

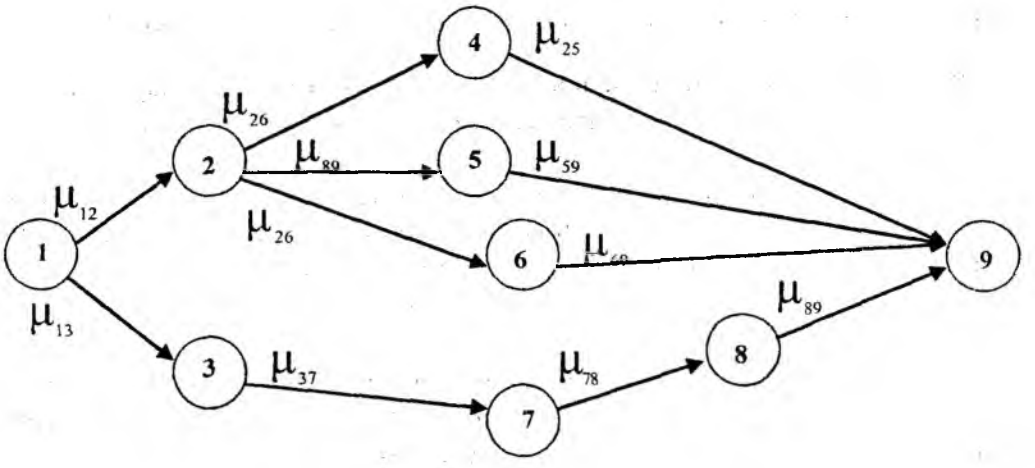
Существующие традиционные подходы к нечеткому сетевому планированию предусматривают задание тех работ (действий) которые нужно обязательно реализовать. Такое планирование предусматривает построение графика последовательности обязательных работ, и затем нахождение основных параметров реализации проекта: нечеткого критического пути, нечеткого резерва выполнения некритических работ и т.д.

Особенностью нечеткого сетевого планирования действий подсистемы защиты информационной системы, в отличие от традиционного планирования проекта, например строительства здания, является необходимость учитывать возможность ситуативного управления. То есть при реализации тех или иных действий должностные лица системы защиты должны осуществлять мониторинг состояния информационной системы. При этом в случае изменения ситуации, получения дополнительной информации о состоянии информационной системы и действий нападающей стороны необходимо оперативно уточнять свои действия. Это может привести как к отказу от одних действий, так и реализации других действий.

В статье для планирования действий системы защиты информационной системы предлагается доработать теорию нечеткого сетевого планирования для учета ситуативности управления. Считаем, что не каждый путь нечеткой сетевой модели может быть реализован. Реализация того или иного пути зависит от необходимости его реализации в складывающихся условиях обстановки и наличия ресурса на его реализацию.

Для учета данных предложений введем для каждого *i*-го состояния сетевой модели параметр $\mu_{ij}, i, j = \overline{1,J}$, $\mu_{ij} = [0,1]$, $\sum_{j=1}^{J} \mu_{ij} = 1$. Данный показатель имеет смысл степени необходимости (полезности) заданного действия системы защиты для *i*-го состояния для сложившейся ситуации. Пример сетевой модели, учитывающий возможность ситуативного планирования, представлен на рисунке.

Параметры μ_{ij} должны задаваться при планировании на основании имеющейся информации о возможных действиях нападающей стороны (информации из разглашенных вторжений, информации от структурных аналитических подразделений системы защиты). При обнаружении аномалии в работе информационной системы (обнаружении вторжения) данные параметры могут корректироваться на основании анализа сложившейся ситуации.



Из представленного примера сетевой модели видно, что в состоянии информационної системы 1 могут реализовываться действия 1-2 и 1-3 или одно из действий: 1-2 или 1-3. Аналогичная ситуация складывается и для состояния 2, когда могут начать реализовываться или все действия 2-9, 2-5, 2-6, или часть из них. Выбор тех или иных действий для реализации определяется складывающейся ситуацией, наличием ресурса для их реализации, коэффициентами μ_{ij}, которые выступают в качестве механизма поддержки принятия решению руководителю системы защиты информационной системы. Можно устанавливать определенное пороговое значение $\mu_{ij}^{пор}$, при превышении которого запланированное действие выбирается для реализации. Для пути 13789 показатели μ_{37}, μ_{78}, μ_{89} равны единице и, следовательно, данные действия системы защиты реализуются обязательно.

Выводы

Данный подход к планированию действий системы защиты критически информационной системы позволяет учесть наличие неполной информации относительно возможных действий нападающей стороны и реакции информационной системы на нападение. Такое планирование позволяет ситуативно менять варианты действий системы защиты в зависимости от складывающейся обстановки.

Список литературы: 1. *Петренко С. С., Беляев А .В.* Проблема обнаружения компьютерных атак в критически важных инфраструктурах // Защита информации. INSIDE. 2008. № 2. С. 32 – 36. 2. *Милокум Я. В.* Метод последовательного обнаружения угроз компьютерной сети // Наук. записки Укр. наук.-дослід. ін-ту зв'язку. наук.-вироб. зб. 2008. № 4(6). С. 79 – 88. 3. *Машкина И. В., Васильев В. И.* Подход к разработке интеллектуальной системы защиты информации // Информационные технологии. 2007. № 6. С.2 – 6. 4. *Душкин А. В.* Распознавание и оценка угроз несанкционированного воздействия на защищенные информационно-телекоммуникационные системы // Информ. Технологии.2008. № 3. С. 71 – 75. 5. *Безопасная* сеть вашей компании / Дж. Маллери, Дж. Занн, П. Келли, У. Нунан, Э. игрен, Пол Лав, Роб Крафт, Марк О'Нил; пер. с англ. Е.Линдеман. М.: НТ Пресс, 2007. 640 с. 6. *Слепцов А. И., Тыщук Т. А.* Метод нечеткого критического пути сетевого планирования и управления проектами на основе мягких вычислений // Кибернетика и системный анализ.1999.№ 3. С. 158 – 168.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.02.2009