

## **1 Тема: "Имитационное моделирование атак на вычислительную сеть"**

### **2 Введение.**

В современном мире средства вычислительной техники широко используются во многих отраслях деятельности человека. Основной их задачей является обработка и хранение информации поступающей из вне. Такие системы должны обеспечивать доступ к данным и гарантировать их актуальность. Для решения проблемы быстрого получения информации конечным пользователям, отдельные компьютеры объединяются в локальные сети. Подобное объединение можно проследить вплоть до глобальной сети интернет. Однако, решив проблему, связанную с доступностью информации, соединение компьютеров обострило проблемы связанные с безопасностью данных. В случае с локальной машиной не имеющей активного сетевого соединения проблема безопасности решается ограничением физического доступа к терминалу, однако объединив рабочие станции, зона, которую необходимо контролировать, резко возрастает. Кроме того, с внедрением беспроводных технологий, это зона не имеет четких границ, а существующее подключение сети к интернет открывает потенциальную возможность для атаки человеку из любой точки мира. В зависимости от сложности архитектуры, от используемого оборудования и уровня подготовленности сотрудников, имеющих подключение к локальной сети, обнаружение и ликвидация уязвимостей резко возрастает. Принимая во внимание вышеперечисленные факторы, инженеру, ответственному за построение локальной сети, необходимо иметь возможность оценки того или иного архитектурного или программного решения с точки зрения актуальности его применения для конкретной ситуации. Для подобного рода оценок существуют различные методы и средства моделирования.

Применение методов моделирования на этапе проектирования сети позволяет предугадать возможные проблемы при реализации выбранного решения, а также принять меры по обеспечению безопасного функционирования системы. К таким мерам относятся аппаратные средства, ограничивающие доступ к защищаемым ресурсам, протоколы криптографической защиты, программное обеспечение с возможностью мониторинга состояния сети.

Различные источники придерживаются разных определений процесса моделирования, так как крайне сложно подобрать такое определение,

которое в полной мере охватило деятельность по моделированию. Определение модели по А. А. Ляпунову: Моделирование – это опосредованное практическое или теоретическое исследование объекта, при котором непосредственно изучается не сам интересующий нас объект, а некоторая вспомогательная искусственная или естественная система (модель):

1. находящаяся в некотором объективном соответствии с познаваемым объектом;
2. способная замещать его в определенных отношениях;
3. дающая при еџ исследовании, в конечном счете, информацию о самом моделируемом объекте

По учебнику Советова и Яковлева : "модель (лат. *modulus* – мера) – это объект-заместитель объекта-оригинала, обеспечивающий изучение некоторых свойств оригинала." (с. 6) "Замещение одного объекта другим с целью получения информации о важнейших свойствах объекта-оригинала с помощью объекта-модели называется моделированием." (с. 6) "Под математическим моделированием будем понимать процесс установления соответствия данному реальному объекту некоторого математического объекта, называемого математической моделью, и исследование этой модели, позволяющее получать характеристики рассматриваемого реального объекта. Вид математической модели зависит как от природы реального объекта, так и задач исследования объекта и требуемой достоверности и точности решения этой задачи." (Прим. Формулировки взяты из Вики, однако, есть прямые ссылки на источники)

Основная сложность математического моделирования заключается в том, что исследуемые процессы необходимо формализовать математическими функциями, что не всегда возможно. Некоторые процессы, например, действия пользователя в системе, сложно свести к математическим функциям.

Имитационное моделирование – это метод, позволяющий строить модели, описывающие процессы так, как они проходили бы в действительности. Отличительными чертами данного метода является то, что у исследователя есть возможность изменять параметры системы, изучать процесс с одними входными данными или некоторым набором, исследовать развитие процесса во времени. Имитационное моделирование применяется тогда, когда неэффективно с точки зрения затраченных ресурсов и полученных результатов экспериментировать на реальном объекте. Невозможно построить математическую модель в связи с присутствующими в системе нелинейностями, стохастическими переменными или если необходимо исследовать систему во времени.

Существующие программные решения позволяют строить модели компьютерных сетей, и исследовать с помощью этой модели различные процессы, происходящие в системе. Однако большинство таких решений созданы для использования системными администраторами, и поэтому позволяют исследовать характеристики системы безотносительно к безопасности. Данные, полученные при использовании такой системы, могут быть абсолютно бесполезными для инженера по безопасности. Существующие решения, отражающие работу сети с точки зрения безопасности являются коммерческими, что затрудняет их использование в образовательных целях или являются свободно распространяемыми, но в этом случае, обычно, обладают малым числом возможностей и неудобным для использования графическим интерфейсом.

Таким образом целью данной работы является создание стенда для моделирования работы вычислительной сети с точки зрения информационной безопасности. Данный стенд должен предоставлять возможность построения сетей различных архитектур и топологий, выявлять "узкие" места в локальной сети замедляющие ее работу или представляющие собой уязвимость, а так же изучить состояние и поведение системы при различного рода атаках.

В качестве объекта исследования будем рассматривать процесс моделирования взаимодействия различных устройств, объединенных в вычислительную сеть. В рамках данной работы будет построена система, позволяющая моделировать алгоритмы работы устройств на различных уровнях эталонной модели взаимодействия открытых систем (OSI). Протоколы транспортного сетевого и канального уровней возможно моделировать без привлечения математических моделей и аппарата математической статистики. В то время как более высокие уровни взаимодействия связаны с действиями пользователя в системе и не могут быть точно воспроизведены. В связи с этим при моделировании генерации трафика в сети, то есть обычного режима работы, будут использованы математические модели, построенные при исследовании данного явления. При моделировании работы протоколов нижнего уровня и физической передачи данных возникают проблемы иного характера. Они связаны в первую очередь с наличием ошибки в канале связи. Учитывая то, что в реальных условиях эта ошибка носит, преимущественно, случайный характер, моделирование подобных инцидентов будет проводиться с использованием методов математической статистики.

Для построения модели вычислительной сети будет применен метод имитационного моделирования. Благодаря этому методу система будет иметь необходимую гибкость при настройке параметров. Наиболее удобным видом моделирования для данной задачи является метод агентного

моделирования, так как он позволяет описывать поведение каждого компонента системы в отдельности, а так же порядок их взаимодействия. Описанные преимущества позволяют произвести декомпозицию задачи и построить систему необходимого уровня сложности.

Для построения целевой системы необходимо разработать архитектуру будущего приложения. Она должна включать в себя возможности по построению моделей вычислительных сетей различной конфигурации, предусматривать механизмы настройки большинства компонентов системы, обладать гибкостью для возможного расширения используемого оборудования и протоколов.

Следующим этапом разработки является алгоритмизация математических моделей, описывающих генерацию трафика пользователем в вычислительной сети. Результатом данного этапа будет система, в достаточной степени точно отражающая реальные процессы, протекающие в вычислительной сети.

Третьим этапом разработки станет подсистема сбора статистической информации по различным устройствам. Данная подсистема занимается сбором данных со всех устройств, входящих в состав моделируемой сети и позволяет проследить динамику изменения состояний различных узлов.

Заключительным этапом является создание подсистемы, моделирующей различные виды атак на локальную сеть. В рамках данной подсистемы описываются устройства и программы(алгоритмы), используемые при атаках на вычислительные сети, определяются механизмы подключения к локальной сети, моделируются действия злоумышленника. По последнему пункту будет рассмотрено такое понятие, как мотивация злоумышленника, которая влияет на его заинтересованность в компрометации системы.

Для решения поставленных задач будет использоваться язык программирования JAVA с использованием различных расширений.

### **3 Статьи.**

Modeling network attacks Major Scott D. Lathrop, Lieutenant Colonel John M.D.Hill, Lieutenant Colonel John R. Surdu Information Technology and operations Center. Department of Electrical Engineering and computer science United states military academy

В статье описывается система моделирования атак, разработанная с целью моделирования вероятности успешной атаки с использованием локальной сети. В качестве модели используются деревья атак.(attack

tree). При моделировании учитывается точка, из которой производится атака(снаружи- через internet, изнутри - insider, беспроводная сеть), мотивы атакующего, этическая составляющая (тест на проникновение или промышленный шпионаж, и.т.д).

Attack trees. Диаграммы атак. Схожи с диаграммами угроз. На верхнем уровне находится угроза. Потомки представляют собой условия, которые должны быть достигнуты, чтобы реализовать угрозу.(Вики)

Simulation of computer network attacks. Carlos Sarraute, Fernando Miranda, Jose I. Orlicki CoreLabs, Core Security Technologies ITBA(Instituto Tecnológico de Buenos Aires)

Статья посвящена моделированию атак в компьютерной сети. Описываются реальные атаки, выделяются несколько фаз, характерных для проведения атаки (Поиск информации о системе, атака или проникновение, анализ внутренней информации, повышение привилегий, использование захваченной системы, удаление следов присутствия). Рассматриваются такие понятия как вектор атаки и эксплойты. В практической части статьи приведено моделирование различных атак с точки зрения атакующего

Agent-based modeling and simulation of malefactors attacks against computer networks. Igor Kotenko Mihail Stepashkin Alexaner Ulanov SPIIRAS, Intelligent System Laboratory. (На русском этой статьи не нашел)

В статье рассматривается агентное моделирование атак. Описывается так же система оценки существующих уязвимостей, включающая в себя оценки различных аспектов атаки, таких как уровень защищенности, уровень подготовленности атакующего и.т.д. Затем приводится пример моделирования DDoS атак.

Modeling modern network attacks and countermeasures using attack graphs. Kyle Ingols, Matthew Chu, Richard Lippmann, Seth Webster, Stephen Boyer. MIT Lincoln Laboratory.

В статье рассматривается моделирование современных атак и контрмер. Рассматриваются такие атаки, как атаки на клиента(Client-side attacks: на сервер загружается контент, который, незаметно для себя скачивает клиент, CSRF - может быть). Zero-Day атаки. В качестве контрмер предлагаются файрволы, Системы предотвращения вторжений. В качестве среды для моделирования выбрана NetSPA.

Моделирование противоборства программных агентов в интернете: общий подход, среда моделирования и эксперименты.

И.В. Котенко, А.В. Уланов Основной упор в статье сделан на рассмотрение атаки на распределенный отказ в обслуживании и принцип многоагентного моделирования.

Имитационное моделирование процессов передачи трафика в вычис-

лительных сетях

Рассматривается подход к имитационному моделированию локальных вычислительных сетей (ВС) на основе раскрашенных временных сетей Петри (СП) с очередями. Вводится понятие ролевых функционалов и операций над ними. Приводится пример построения СП для фрагмента локальной сети, предложен общий алгоритм работы имитационной модели.

Realistic modeling of Local network traffic. Stefan Karpinski Department of computer science University of California. Santa-Barbara.

Тезис: Существующие методы моделирования нагрузки неспособны точно воспроизводить или предсказывать характеристики производительности для реального поведения трафика в локальных вычислительных сетях. Синтетически генерировать трафик локальной сети, который точно отражает характеристики реального трафика возможно при выведении закономерностей поведения реальной системы и разработке математического фреймворка, описывающего модели трафика.

(Суть статьи - математические выкладки относительно того, как генерировать трафик. Рассматриваемая проблема заключается в том, что с точки зрения модели OSI прикладной, представительский, сеансовый, физический уровни являются сложными для моделирования, т.к. определяются в том числе поведением пользователя. В то время, как транспортный, сетевой, канальный уровни используют конкретные алгоритмы и могут быть смоделированы без особых сложностей)

Fluid modeling of pollution proliferation in P2P networks.

Моделирование атаки на p2p сеть. Атака заключается в подмене корректной информации на поврежденные копии. Построено несколько моделей, показывающих разрастание "области заражения" (т.е. количества peers раздающих поврежденный файл). Системы сводятся к нелинейным дифференциальным уравнениям для которых получено closed-form expression (могут быть выражены аналитически при условии конечного набора определенных "хорошо известных" функций). Применительно к системе было получено численное решение. Учтены так же различные варианты поведения пользователя (черные списки, отмена передачи и.т.д)

Active Worm Propagation Modeling in Unstructured P2P Networks.

Xiaosong Zhang, Ting Chen, Jiong Zheng and Hua Li Моделирование распространения червя в p2p сети. Рассматриваются различные аспекты атаки (выбор червем заражаемого хоста) и защиты (исключение зараженного хоста из сети)|

Моделирование алгоритма маршрутизации передаваемых данных в беспроводных сетях со смешанными типами коммутации. А.Г. Гайнулин

Нижегородский государственный технический университет.

В статье описываются принципы функционирования беспроводных соединений, приведены различные характеристики, используемые при оценке соединений. Интерес представляет описанный алгоритм маршрутизации.

Selected Methods of Measuring the Delay in Data Transmission Systems with Wireless Network Interfaces T. Topor-Kaminski, R. Zurkowski and M. Grygiel Institute of Measurement Science, Electronics and Control, Silesian University of Technology, Gliwice, Poland

В статье рассмотрены факторы из-за которых возникает задержка при передачи данных через беспроводную сеть, такие как время обработки пакета на отправляющей стороне, время передачи, время обработки на принимающей стороне. Проведены эксперименты касательно качества передачи данных, при различных длинах пакета и условиях (открытая сеть, открытая сеть + ping, сеть + защита WPA, TKIP)

Simulating the spread of a virus in a computer network Jihad Estrada and Zvi Drezner California state University Fullerton College of Business and Economics.

В статье поднимается тема скорости распространения вируса в компьютерной сети. В первой части описываются теоретические выкладки. Во второй части на имитационной модели проверяется справедливость. Рассматривается система из 50 взаимодействующих объектов, оценивается скорость распространения.

Есть еще статьи,но пока не уверен нужно ли их включать(перевожу)