УДК 519.854

ЛИСТРОВОЙ С.В., д.т.н., профессор,
МОЦНЫЙ С.В., аспирант (УкрГАЖТ)

# Подходы к предотвращению угроз в компьютерных сетях на основе решения задачи о наименьшем покрытии

*В статье рассматривается модель предотвращения угроз в компьютерных сетях на основе решения задачи о минимальном вершинном покрытии, которая позволяет снизить стоимость построения компьютерных сетей и сложность планирования, не снижая при этом эффективность функционирования систем обнаружения и предотвращения вторжений. В результате проведенного анализа показана актуальность и необходимость использования оптимизированных алгоритмов нахождения минимального вершинного покрытия в связи с высоким темпом расширения компьютерных сетей.*

***Ключевые слова**: компьютерные сети, фильтры Блума, вершинные покрытия, системы обнаружения вторжений, системы предотвращения вторжений, временная сложность, степенное распределение.*

## Постановка проблемы

С каждым годом происходит расширение масштабов использования компьютерных сетей, возрастает количество информации, нуждающейся в надежной защите. Наряду с этим возрастает количество угроз нарушения сетевой безопасности, которые могут выражаться в распространении различного вредоносного программного обеспечения, рассылки фишинговых сообщений посредством электронной почты, разрушении сетевой структуры и уничтожении важных файлов, взломе ключевых серверов и т.д. Вследствие этого возникает острая необходимость в создании эффективных систем, способных противостоять угрозам подобного вида.

На сегодняшний день применяются системы, которые производят мониторинг и анализ сетевого трафика в режиме реального времени на предмет наличия подозрительной активности, обозначаемые как СОВ – «Системы обнаружения вторжений» (англ. *Intrusion Detection Systems*) [5]. Данные системы относят к пассивной технологии защиты, поскольку они лишь предоставляют информацию о найденных угрозах. Также широко используются активные системы, называемые «Системы предотвращения вторжений» (англ. *Intrusion Prevention Systems),* которые позволяют производить ответные действия при обнаружении вторжения в компьютерную сеть (к примеру, сброс соединения или перенастройка межсетевого экрана). Самым распространенным способом реализации подобных систем является аппаратное совмещение их функционала с маршрутизаторами (англ. Routers). В таком исполнении система получает доступ к анализируемому трафику сразу после его поступления на сетевой интерфейс.



Очевидно, что установка сенсоров перечисленных систем на каждом сетевом узле будет характеризоваться чрезмерной стоимостью как непосредственно оборудования, так отладки и последующего обслуживания компьютерной сети. В особенности, если взять во внимание широкие масштабы современных сетей.

Таким образом, данный факт выводит на первый план необходимость разработки эффективного подхода, который позволяет снизить стоимость и сложность разработки и поддержки компьютерной сети, сохраняя при этом достаточную эффективность обнаружения и предотвращения существующих угроз.

## Анализ последних исследований и публикаций

На сегодняшний день известны различные подходы к построению эффективных систем обнаружения и предотвращения вторжений.

Резауль Карим предложил подход на основе байесовского метода для построения гарантировано эффективных систем применительно к беспроводным децентрализованным самоорганизующимся сетям [16].

Тсонг Сонг совместно с коллегами [17] сформировал трехуровневую архитектуру построения систем обнаружения и предотвращения вторжений, в состав которой входят «белый список», «черный список» и «классификатор данных методом опорных векторов».

Гюнез Кайесик и др. [18] усовершенствовали технику, основанную на моделировании поведения известных атак, которая помогает экспертам по вопросам безопасности определять сходство между различными атаками. При тестировании данного подхода специалистами обычно используется самоорганизующаяся карта (англ. Self-organizing map — SOM), позволяющая визуализировать сходства

между отдельно взятыми атаками на компьютерную сеть.

Однако, не смотря на наличие различных подходов, у многих используемых систем при этом также существуют и общие черты, такие как, к примеру, использование базы сигнатур известных угроз и координация работы совместно с установленными межсетевыми фильтрами. В данном контексте сигнатуры представляют собой особенности и характерные черты известных на сегодняшний день угроз безопасности компьютерной сети.

Подобные сигнатуры необходимо сверять с существующей базой при каждом прохождении нового пакета по сети. Таким образом, легко заметить, что необходимы достаточно эффективные методы анализа трафика, особенно, в связи с постоянным возрастанием скоростей и масштабов компьютерных сетей.

По способу функционирования системы обнаружения вторжений можно разделить на системы обнаружения злоупотреблений (misuse detection) и системы обнаружения аномалий (anomaly detection) [6].

Детекторы злоупотреблений анализируют деятельность системы, каждое событие или множество событий, происходящих в переделах системы, на соответствие заданному заранее шаблону, другими словами, образцу, который описывает известную на данный момент атаку. Форма определения злоупотреблений, используемая в коммерческих продуктах, специфицирует каждый образец событий, соответствующий атаке, как отдельную сигнатуру в наиболее общем случае [7]. Однако детекторы злоупотреблений могут определить только те атаки, о характеристиках которых уже известно. Таким образом, необходимо постоянно обновлять базы данных для получения сигнатур новых атак.

Детекторы аномалий определяют такие действия программного обеспечения, которые вызывают подозрение и являются своего рода «ненормальными». Они предполагают, что атаки отличаются от «законной» деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой допустимое поведение пользователей, хостов или сетевых соединений. Подходы определения аномалий часто требуют, чтобы система проходила обучение, во время которого определяются характеристики нормального поведения.

В основе некоторых популярных техник систем обнаружения и предотвращения вторжений лежит метод приблизительного сравнения строк, который, однако, не может быть адаптирован к потребностям расширяемых сетей, поскольку имеет слишком низкую производительность, лежащую в основе их алгоритмов. К примеру, как показывают проведенные исследования [8], временная сложность при их использовании может равняться $\underline{O}(n^3 m)$ (где $n$ - размер паттерна сигнатуры, $m$ – размер общей базы).

Наиболее эффективным подходом к решению различного спектра задач, связанных с анализом трафика в переделах компьютерной сети (к примеру, для выявления принадлежности пакета к базе вредоносных сигнатур), является использование фильтров Блума [9]. Фильтр Блума - это вероятностная структура данных, позволяющая хранить некое множество элементов, а также быстро отвечать на вопрос о том, есть ли данный элемент во множестве или нет. Как показано в работе [10], поиск по множеству при помощи фильтра Блума происходит с константной временной сложностью. Таким образом, при рациональном применении данных фильтров в пределах существующей сети, представляется возможным производить анализ трафика за полиномиальное время.

## Выделение нерешенных ранее частей общей проблемы

Несмотря на многочисленные проведенные исследования специалистов по безопасности в компьютерных сетях, на сегодняшний день отсутствует универсальный подход к конфигурированию компьютерной сети, который позволил бы с одной стороны эффективно обнаруживать и предотвращать любые возможные угрозы, исходящие от злоумышленников, а с другой стороны сохранить приемлемый уровень стоимости построения, отладки и обслуживания сети. Особенно, учитывая постоянно возрастающие масштабы компьютерных сетей. Также в существующих исследованиях отсутствует детальный анализ относительно применимости того или иного метода обеспечения безопасности в пределах сети к различным вариантам сетевых топологий.

## Цель статьи

Целью данной работы является разработка оптимальной модели предотвращения угроз в компьютерных сетях на основе решения задачи о минимальном вершинном покрытии, а также проведение анализа сетевой топологии, в пределах которой предполагается использование данной модели.

## Изложение основного материала

Весь интернет можно представить в виде совокупности автономных систем. Под автономной системой (англ. Autonomous System — AS) понимается независимая и равноправная система IP-сетей и маршрутизаторов, управляемая какой-либо крупной зарегистрированной организацией (к примеру, интернет-провайдер). Полное определение автономной системы отражено в документации RFC 1930 (англ.

Request for Comments – Рабочее предложение). Форма записи номера автономной системы может быть представлена в виде 16-ти или 32-битного числа (32-битная форма была введена в связи с исчерпанием количества номеров) [1].

Для того чтобы автономные системы могли быть на связи друг с другом, необходимо сконфигурировать роутер, который будет предоставлять информацию об автономной системе по протоколу BGP (англ. Border Gateway Protocol - Протокол граничного шлюза) [2]. BGP представляет собой протокол динамической маршрутизации, согласно правилам которого BGP-маршрутизатор держит в своей памяти карту маршрутов ко всем остальным маршрутизаторам в сети и сообщает другим узлам интернета через какие маршруты достижимы управляемые им самим блоки IP-адресов. Исследования проведенные в [3][4], показывают, что наиболее эффективной топологией для построения данных систем является топология на основе модели безмасштабных сетей. Данная топология в сравнении с другими позволяет проводить динамическую переконфигурацию сети со значительно меньшей сложностью и затратами.

Термин безмасштабные сети (scalefree networks) может быть применен ко многим коммуникационным системам.[11]. Гипотеза о безмасштабных сетях была высказана в 1967 г. социологом из Гарвардского университета С. Милграмом [12]. Он утверждал, что каждого человека можно связать с любым другим человеком на земном шаре в цепочку из шести знакомых. Его эксперименты получили название «Мир тесен» (англ. «small world»). С тех пор, благодаря бурному развитию информационных технологий во второй половине XX века, было неоднократно доказано, что этим свойством обладают многие технические и социальные системы.

Данные сети обладают важным свойством, выделяющим их на фоне остальных, которое проявляется в том, что степени вершин распределены по степенному закону или закону, приближающемуся к степенному в асимптотике.

Принимая, что $k$ является числом связей, выходящих из данного узла и $P(k)$ это вероятность [13], что степень случайно выбранной вершины равняется $k$, для безмасштабной сети будет выполним следующий *закон степенного распределения*:

$$P(k) \sim ck^{-\gamma} \qquad (1)$$

где: $\gamma$ – показатель степени (индивидуальная компонента сети),

c – нормализующий параметр.

Показатель степени в приведенной выше формуле не зависит от размера сети, таким образом, степенным структурам свойственна масштабная инвариантность. Исходя из данных соображений, подобные сети и назвали безмасштабными.

Безмасштабным сетям характерна кластерная структура. Значение коэффициента кластеризации у них намного выше, чем у случайных сетей, имеющих такую же размерность. При этом особенно высокая мера кластеризации наблюдается в упорядоченных сетях.

Барабаши и Альберт сформулировали возможную модель возникновения и эволюции безмасштабных сетей. Как было показано в их работе, для возникновения безмасштабных сетей необходимо наличие следующих условий [4]:

1. *Рост (англ. Growth).* При небольшом числе $m_0$ узлов на каждом временном шаге добавляется один новый узел с $m$ ($m \leq m_0$) связями. Данные связи соединяют этот новый узел с $m$ различными узлами, о которых известно на момент проведения операции.

2. *Предпочтительное присоединение (англ. Preferencial attachment).*

Проведенные вычисления показали, что принцип предпочтительного присоединения действительно приводит к безмасштабной сети с показателем степени $\gamma = 3$. Подобное явление редко встречается в реальных сетях, но ценность этой модели заключается в том, что она показывает реальную возможность образования безмасштабной сети на основе простых предположений [14].

Если произвольно удалять узлы из пуассоновской случайной сети Эрдеша-Реньи в определенный момент возникает критическое значение, измеряемое отношением числа удаленных узлов к общему числу узлов в сети, выше которого сеть распадается на отдельные фрагменты. Для безмасштабных сетей, у которых наблюдается показатель степени $\gamma \leq 3$, такого критического числа не существует [15]. Подобные безмасштабные сети очень устойчивы к случайным повреждениям или внешним случайным воздействиям.

Для анализа трафика на наличие угроз в таких сетях предлагается использовать средства на основе фильтров Блума. Данный выбор обоснован их эффективностью и способностью предоставлять результат за полиномиальное время [10]. Рассмотрим, каким образом можно снизить стоимость и сложность компьютерной сети, используя подход на основе концепции безмасштабных сетей и задачи о наименьшем покрытии.

Средства на базе фильтров Блума предлагается устанавливать только в узлах, образующих минимальное вершинное покрытие в графе, отображающем структуру проектируемой сети. Физически в качестве вершин, входящих данное покрытие, будут выступать роутеры автономной системы. Под ребрами понимается распределенная среда между роутерами (воздушная среда, оптоволокно, коаксиальный кабель и т.д.).

Рассмотрим граф G = (V, E) произвольной сети приведенный на рис. 1. V – множество вершин (роутеров), E – множество ребер (распределенная среда). Найдем последовательно минимальное вершинное покрытие с помощью приближенного алгоритма.

На первом шаге выбирается ребро BC (выбор делается на основании предположения о том, что роутеры B и C содержат большую степень связности по сравнению с другими). После этого удаляются соответственно покрытые ребра AB, EC и DC.

На следующих шагах проделаем точно такие же действия над ребрами EF и DE. В результате чего получим вершинное покрытие данного произвольного графа.

На последнем шаге для нахождения минимального покрытия удаляются все вершины, которым инцидентно наибольшее количество ребер.

Таким образом, как видно из рис. 1, после проделанной работы фильтры Блума необходимо будет расположить только на роутерах B, E, D. При этом очевидно, что эффективность обнаружения угроз не будет снижена, поскольку любая попытка распространения сетевого червя не сможет просочиться сквозь сеть, минуя установленные фильтры.

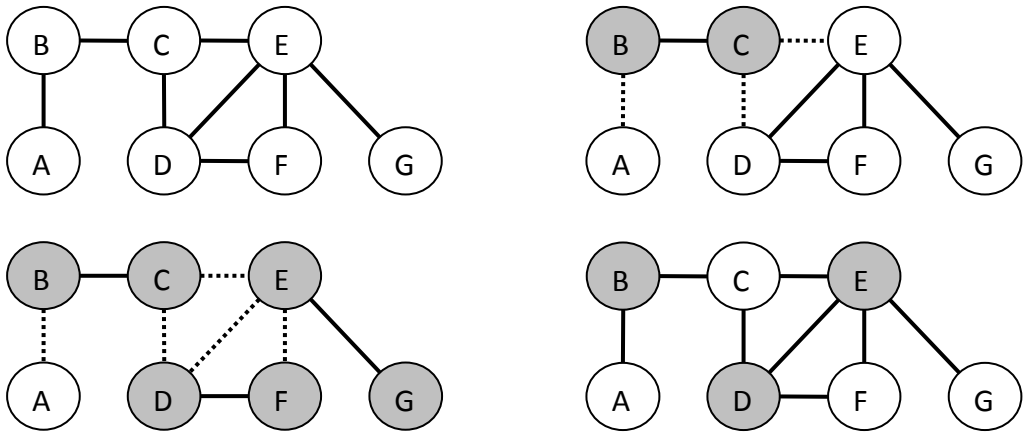


Рис. 1. Нахождение минимального вершинного покрытия произвольного графа

Как можно заметить, в данном случае вместо изначально планируемых семи фильтров Блума можно обойтись только тремя и при этом в сети обеспечивается полная защита всех узлов от распространения сетевых червей, спам-атак и других угроз и вторжений. Несложно посчитать, что стоимость установки фильтров Блума в данной сети будет меньше в 2,3 раза.

**Заключение**

При проектировании безмасштабных сетей, в которых обеспечивается защита на основе использования фильтров Блума, целесообразно оптимизировать стоимость и сложность проектирования сети за счет решения задачи о наименьшем вершинном покрытии, что позволяет снизить число фильтров Блума, необходимых для устранения угроз. Данный подход является актуальным и перспективным, поскольку он предусматривает уменьшение стоимости и сложности при расширении масштаба сети.

**Литература**

1. The AS Number Report, G. Huston, (updated on a daily basis). URL: http://www.potaroo.net/tools/asns
2. BGP Support for Four-octet AS Number Space, E. Chen, Q, Vohra, work in progress, November 2005.
3. Слядников Е. Е. Моделирование распределенных информационно -телекоммуникационных систем с пакетной передачей данных // известия тпу, 2008. №5.
4. Albert R., Barabasi A, Statistical mechanics of complex networks//Reviews of Modern Physics 74: 47-97, 2002. URL: barabasilab.com/pubs-clpxnets.php
5. Lunt, T. A survey of intrusion detection techniques. In Computers and Security 12, 4 (June 1993). 405–418.
6. Anderson James P., Computer Security Threat Monitoring and Surveillance, Washing, PA, James P. Anderson Co., 1980.
7. Ивонин А. Д. Идентификация и аутентификация, управление доступом. URL: http://www.intuit.ru/department/security/secbasics/10/3.html
8. W. Chang and T. Marr. Approximate string matching and local similarity. In Proc. 5th Combinatorial Pattern

Matching (CPM'94), LNCS 807, pages 259–273, 1994.
9. Dharmapurikar S., Krishnamurthy P., Sproull T. and Lockwood J., 2003. Deep packet inspection using parallel bloom filters. In IEEE Hot Interconnects. Vol. 12.
10. Putze, F.; Sanders, P.; Singler, J. (2007) "Cache-, Hash- and Space-Efficient Bloom Filters».
11. Барабаши А.-Л., Бонабо Э. Безмасштабные сети// В мире науки. – М.: РосНоу, 2003.–С. 55-63.
12. Milgram. The small world problem // Psychology Today. 1967. No2. Pp. 60-67.
13. Евин И. А. Введение в теорию сложных сетей // Компьютерные исследования и моделирование. — 2010. — Т.2, No2. — С. 121–141.
14. Zhao K., Halu A., Severini S. and Bianconi G. Entropy rate of nonequilibrium growing networks. Physical Review E 84, 066113 (2011).
15. Nickerson D.W. Is Voting Contagious? Evidence from Two Field Experiments. American Political Science Review. 102 (2008):49-5.
16. A. H. M. Rezaul Karim,R, M. A. P.Rajatheva, Kazi M. Ahmed, 2006. An Efficient Collaborative Intrusion Detection System for MANET Using Bayesian Approach, pp.187-190.
17. Tsong Song Hwang, Tsung-Ju Lee,Yuh-Jye Lee, 2007. A Threetier IDS via Data Mining Approach, MineNet'07.
18. H. Günes Kayacık, A. Nur Zincir-Heywood, 2006, Using Self- Organizing Maps to Build an AttackMap for Forensic Analysis, PST, Oct 30-Nov 1, Markham, Ontario, Canada, ACM 1-59593- 604-1/06/00010.

**Лістровий С.В., Моцний С.В. ПІДХОДИ ДО ЗАПОБІГАННЯ ЗАГРОЗ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ РІШЕННЯ ЗАДАЧІ ПРО НАЙМЕНШЕ ПОКРИТТЯ.** У статті розглядається модель запобігання загроз у комп'ютерних мережах на основі рішення задачі про найменше верхове покриття, яка дозволяє знизити вартість побудови комп'ютерних мереж й складність планування, не знижуючи при цьому ефективність функціонування систем виявлення та запобігання вторгнень. У результаті проведеного аналізу показана актуальність та необхідність використання оптимізованих алгоритмів знаходження мінімального верхового покриття у зв'язку з високим темпом розширення комп'ютерних мереж.
**Ключові слова:** комп'ютерні мережі, фільтри Блума, вершинні покриття, системи виявлення вторгнень, системи запобігання вторгнень, часова складність, степеневий розподіл.

---

**Listrovoy S.V., Motsnyi S.V. THREAT PREVENTION TECHNIQUES USED IN COMPUTER NETWORKS BASED ON THE SOLUTION OF A MINIMUM COVER PROBLEM.**
The article considers a threat prevention model used in computer networks based on the solution of the minimum vertex cover problem, which reduces the cost of computer networks construction and the complexity of planning without reducing the efficiency of the detection systems and intrusion prevention. The analysis shows the topicality and necessity of the optimized algorithm usage for finding the minimum vertex cover taking into account high rate of computer network expansion.
**Key words:** computer networks, Bloom filters, vertex covers, intrusion detection systems, intrusion prevention systems, time complexity, power-series distribution.

Рецензент професор кафедри «СКС» Коновалов В.С. (УкрГАЖТ)

*Поступила 12.12.2013г.*