DOI 10.21778/2413-9599-2018-1-68-73 УДК 04.056.5

В.А. Федорова, Т.А. Моисеева, И.А. Колягина

Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия

АНАЛИЗ ВЛИЯНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОПУСКНУЮ СПОСОБНОСТЬ СЕТИ

В работе рассматривается построение защищенных коммуникационных сетей и их элементов. Приведен анализ имитационного моделирования сегмента коммуникационной сети в условиях атаки, влияние средств защиты информации на сетевой трафик, приводятся примеры расчетов. Выполнен анализ метода оптимизации сетевого трафика с учетом применения различных средств защиты информации; предложены варианты разработки политики безопасности. Приведены результаты экспериментов при различных условиях защиты информации: при отсутствии атаки без использования средств защиты информации; при отсутствии атаки с использованием средств защиты информации; при DoS-атаке без использования средств защиты информации; при DoS-атаке с использованием средств защиты информации. Рассмотрены несколько методов по оптимизации трафика с использованием средств защиты информации, а также политика безопасности для достижения заданного уровня защищенности информации в компьютерной системе при минимуме снижения сетевого трафика и стоимости средств защиты информации.

Ключевые слова: *коммуникационная сеть, информационная безопасность, сетевая атака, WAN, WOC, DoS-атака, имитационное моделирование, политика безопасности.*

Для цитирования: Федорова В.А., Моисеева Т.А., Колягина И.А. Анализ влияния средств защиты информации на пропускную способность сети // Радиопромышленность. 2018. № 1. С. 68–73.

V.A. Fedorova, T.A. Moiseeva, I.A. Kolyagina

Bauman Moscow State Technical University, Moscow, Russia

ANALYSIS OF THE IMPACT OF INFORMATION SECURITY TOOLS ON NETWORK BANDWIDTH

The paper considers the construction of secure communication networks and their elements. The analysis of simulation modeling of the communication network segment under attack conditions, the influence of information security tools on network traffic, and examples of calculations are given. The analysis of the method of network traffic optimization is performed taking into account the use of various information security products, as well as options for developing a security policy. The results of experiments under various conditions of information security are given: in the absence of an attack without the use of information security products; in the absence of an attack using information security products; under a DoS attack without the use of information security products; under a DoS-attack with the use of information security products. Several methods for optimizing traffic using information security products are considered. A security policy is considered to achieve a given level of information security in a computer system with a minimum reduction in the network traffic and the cost of information security products.

Keywords: *communication network, information security, network attack, WAN, WOC, DoS-attack, simulation modeling, security policy.*

For citation: Fedorova V.A., Moiseeva T.A., Kolyagina I.A. Analysis of the impact of information security tools on network bandwidth. Radiopromyshlennost, 2018, no. 1, pp. 68–73 (In Russian).

DOI 10.21778/2413-9599-2018-1-68-73

Введение

В настоящее время многочисленным компаниям, центрам, сервисам приходится переходить от обычного, рутинного бумажного метода работы с документами к наиболее перспективному и современному – компьютерному. Развитие информационных технологий, а также средств вычислительной техники позволяют увеличить производительность обрабатываемой информации и обеспечить ее безопасность. Современные средства аппаратных и сетевых технологий и новые информационные технологии становятся основой развития и конкурентной борьбы в научной, производственной и других областях.

Помимо плюсов новых информационных технологий также существуют и актуальные проблемы, в том числе проблема защиты информации разной степени секретности от злоумышленников и посторонних, а также обеспечения условия для работы лицам, имеющим право к доступу к той или иной информации, при этом без значительного снижения пропускной способности и безопасности сети.

Таким образом, средства защиты информации (СЗИ) предназначены для обеспечения безопасности коммуникационной сети (КС). При решении задач информационной безопасности (ИБ) определено, что конечной целью СЗИ является безопасность всех компонентов, принимающих участие в информационных процессах, предотвращение нанесения им материального или иного ущерба в результате случайных или преднамеренных воздействий на элементы КС. В качестве возможных деструктивных воздействий на компьютерные системы рассматриваются действия злоумышленников, ошибочные действия работающего персонала и пользователей системы, а также ошибки в программном обеспечении, сбои и отказы в оборудовании, форс-мажорные ситуации, которые могут привести к разглашению, искажению, нарушению целостности, утере, разрушению или снижению степени доступности и достоверности информации.

Способность безопасной работы информационной системы зависит от многих факторов, в том числе от стабильной работы узла коммуникационной сети, от его возможности противостоять угрозам ИБ и техническим отказам оборудования. Эту способность предусматривают при проектировании различных СЗИ. Однако включение СЗИ в телекоммуникационную сеть порою значительно влияет на ее пропускную способность. Проведем анализ влияния СЗИ на пропускную способность телекоммуникационной сети, на обеспечение стабильности и удобства работы пользователей.

Влияние СЗИ и ПО на угрозы атак

Существует целый ряд событий, которые могут привести узел в нерабочее состояние. Узел связи может находиться в трех состояниях:

- Состояние готовности.
- Состояние неготовности из-за технического отказа оборудования.
- Состояние неготовности из-за реализации угрозы ИБ, направленной на нарушение целостности или доступности информации для пользователей.

Для снижения вероятности угрозы ИБ используются различные специализированные СЗИ, они включаются в состав оборудования телекоммуникационной сети. Любое техническое устройство, как и СЗИ, недостаточно совершенно и может не только оказывать положительное влияние, например защитить узел сети от угроз ИБ, но и негативно влиять на технические характеристики узлов телекоммуникационной сети и их надежность. Таким негативным влиянием на сегмент сети можно считать время отклика удаленного ресурса и пропускную способность сегмента сети. Примеры средств защиты информации приведены на рис. 1 [1].

Рассмотрим на примере имитационного моделирования сегмента КС в условиях реализации атаки

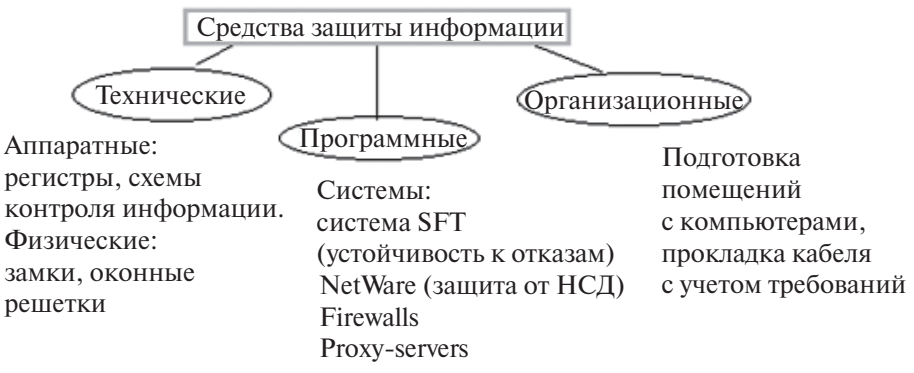

Рисунок 1. Средства защиты информации

типа DoS – «Отказ в обслуживании». Экспериментальная часть была взята из статьи [2].

В проведенном эксперименте персональные компьютеры и СЗИ ПАК «ФПСУ-IP» были объединены в телекоммуникационную сеть при помощи коммутатора. В коммутатор был включен атакующий персональный компьютер. На атакующем компьютере с помощью специального программного обеспечения pktgen (тестирование сети с помощью генератора пакетов) развернут комплекс, имитирующий атаку типа DoS. Атакующее ПО производит рассылку пакетов, направленных на полную утилизацию канала связи. После запуска ПО, имитирующего атаку, производится замер времени отклика и пиковой пропускной способности канала связи. При измерении времени отклика выполняется оценка количества потерянных пакетов. Таким образом, определяется среднее время прохождение пакета с одного компьютера на другой в направлении атакуемого компьютера и вычисляется процент потерянных пакетов. Пиковая пропускная способность определяется встроенными средствами программного обеспечения IPerfMeasurementTool (аналог TTCP). Эти показатели характеризуют способность сети выполнять свои задачи в условиях атаки типа DoS [2].

Обнаружение состояния атаки является первостепенной задачей и должно сводиться к анализу некоторого числа параметров, величина которых должна дать возможность классифицировать их по двум категориям: «нормальные» и «при атаке». Применив теорию принятия решений Байеса, получаем коэффициент подобия $l(x) = f(x|wD)/f(x|wN)$. После сравнения его с порогом T, где x является измеренным значением некоторого параметра, необходимо решить, в какую из двух категорий входит этот параметр (в нормальную категорию wN или в DDoS-категорию wD). Значение x распределяется в категорию wD, если $l(x) > T$, иначе в wN. Порог T обычно определяется эмпирически и зависит от начальных вероятностей для двух типов категорий. Неправильный выбор приведет к ложным срабатываниям и пропущенным атакам.

Возможность быстрого определения атаки является важным параметром в борьбе с DDoS-атакой, так как ускоренное обнаружение приводит к упрощению систематизации и выбору механизмов противодействия.

Параметры, позволяющие определить состояние атаки:

- Скорость потока данных.
- Скорость увеличения скорости потока данных.
- Энтропия. Энтропия нормального Интернет-трафика и трафика при DDoS-атаке существенно различается. Энтропию можно вычислить по формуле

$$E = -\sum_i f_i \log_2 f_i, \quad (1)$$

где f_i – это функция плотности вероятности, полученная из нормализованных значений гистограмм для потока.

- Параметр Херста. Другой статистический параметр, который демонстрирует различное поведение при нормальном и DDoS-трафике, – это самоподобие. Вычислить действительное значение параметра Херста для скорости потока данных можно, проанализировав результат, полученный по формуле

$$(R/S)_N = \frac{\max_{1\le n\le N}\sum_{n=1}^{N}(x-\bar{x}) - \min_{1\le n\le N}\sum_{n=1}^{N}(x-\bar{x})}{\sqrt{\sum_{n=1}^{N}(x-\bar{x})^2 / N}}, \quad (2)$$

где x – скорость потока данных входящего трафика; n – время наблюдения; N – общее количество точек наблюдения. Параметры (H) и $(R/S)_N$ сотносятся как $(R/S)_N = CN^H$, которое при c = 1 становится $H = \log_N((R/S_N)$.

- Задержка. Естественным следствием высокой скорости потока данных и нарастания перегрузки является увеличение задержки пакетов.
- Скорость изменения задержки. По аналогии со скоростью потока данных, в зависимости от типа атаки и для всей ее длительности, задержки пакетов испытывают значительные изменения.

После нахождения данных параметров определить состояние атаки можно по формуле

$$l_{final} = \frac{l_c + l_{у.с.} + l_{энтр} + l_H + l_з + l_{и.з.}}{\textit{общая сумма нормальных параметров}}, \quad (3)$$

где l_{final} величина дает представление о том, производится ли в данный момент атака на систему. Гибридная система, обученная анализировать таким образом параметры, сможет своевременно и не перегружая аппаратные ресурсы определить состояние атаки.

РНС, впервые предложенная Эролом Геленбе, – это вычислительная парадигма, основанная на случайном импульсном поведении биологических нейронов. РНС является вычислительно эффективной структурой и представляет собой более приемлемую аппроксимацию реального функционирования биофизической нейронной сети, где сигнал передается в импульсном, а не в аналоговом виде.

В РНС нейроны обмениваются положительными и отрицательными импульсными сигналами с единичной амплитудой, которые представляют возбуждение и торможение соответственно. Нейроны накапливают сигналы по мере поступления, при этом положительные сигналы могут быть

компенсированы отрицательными. Если потенциал нейрона положителен, он может передать сигнал другим нейронам или за пределы сети.

Потенциал нейрона i в момент времени t, называемый также состоянием нейрона, обозначается как $k_i(t)$. Потенциал $k_i(t)$ может уменьшаться, если нейрон испускает импульс или если получен тормозящий сигнал либо от другого нейрона сети, либо извне. Аналогично этому потенциал $k_i(t)$ возрастает, если получен внешний возбуждающий сигнал или возбуждающий сигнал от другого нейрона сети. В РНС импульс может быть передан от нейрона i к нейрону j как положительный сигнал с вероятностью $p^+(i,j)$, как отрицательный сигнал с вероятностью $p^-(i,j)$ или может покинуть сеть с вероятностью $d(i)$, где $p(i,j) = p^+(i,j) + p^-(i,j)$ и $\Sigma_j p(i,j) + d(i) = 1$. Формулы (4) и (5) показывают способ вычисления положительных и отрицательных весов:

$$w^+(j,i) = r(i)p^+(i,j) \geq 0, \quad (4)$$

$$w^-(j,i) = r(i)p^-(i,j) \geq 0, \quad (5)$$

где $r(i)$ – Пуассоновский коэффициент срабатывания, при этом интервалы между импульсами распределены экспоненциально идентичным образом независимо друг от друга:

$$r(i) = \sum_j w^+(i,j) + w^-(i,j). \quad (6)$$

Веса w могут быть интерпретированы подобно весам в искусственных нейронных сетях, но на самом деле они представляют собой интенсивности появления возбуждающих и тормозящих сигналов.

Установившееся значение вероятности того, что нейрон i возбужден, определяется следующим образом:

$$q_i = \lim_{t\to\infty} \Pr[k_i(t) > 0]. \quad (7)$$

Его можно вычислить по формуле $q_i = N(i)/D(i)$, где

$$N(i) = \sum_j q_j w^+(j,i) + \Lambda(i), \quad (8)$$

$$D(i) = r(i) + \sum_j q_j w^-(j,i) + \lambda(i). \quad (9)$$

При этом $\Lambda(i)$ и $\lambda(i)$ определяют интенсивности поступления соответственно внешних возбуждающих и тормозящих сигналов на вход нейрона i. Формулы (8) и (9) используются для нахождения потенциала нейрона, который определяется согласно формуле (7).

Проведены четыре эксперимента со следующими условиями:

1. Без атаки, без использования СЗИ (эталонное измерение).
2. Без атаки, но с использованием СЗИ (оценка влияния СЗИ на характеристики сегмента ТКС).
3. DoS-атака без использования СЗИ (контрольное измерение, демонстрирующее неспособность сегмента ТКС выполнять функции передачи данных в условиях атаки типа DoS).
4. DoS-атака с использованием СЗИ (оценка способности СЗИ противостоять атакам типа DoS).

Полученные результаты представлены в табл. 1.

Отсюда определяем, что пиковая пропускная способность моделируемого сегмента КС падает и составляет более 65% (измерение 3) по сравнению с эталонным значением (измерение 1) [2].

Время отклика увеличилось незначительно по сравнению с измерением 1, выявленный процент потери пакетов фактически приводит к невозможности выполнения сетевым сегментом функции по передаче данных. Таким образом, в рамках рассматриваемой модели атака типа DoS, направленная на моделируемый узел связи, приводит к его неработоспособности [3].

Есть несколько методов по оптимизации трафика с использованием СЗИ:

1. Оптимизация приложений. Многие приложения могут отправлять до десятков пакетов тогда, когда достаточно и одного. Это вызвано тем, что разработчики ориентируются на локальные сети, а не на работу через каналы «дальней» связи. В данном случае рекомендуется использовать оптимизатор числа проходов «туда-обратно» – это позволит существенно увеличивать пропускную способность. Оптимизатор выступает в роли клиента по отношению к серверу, а оптимизатор филиала выступает в роли сервера по отношению к клиентам. Таким образом, получается, что «болтливое» общение между приложениями остается внутри локальной сети (рис. 2).

Таблица 1. Результаты эксперимента

№ измерения	Измерение	Время отклика, мс	Потеря пакетов, %	Пропускная способность, кбит/с (%)
1	Без атаки, без СЗИ	0,160	0	928653 (100%)
2	Без атаки, с СЗИ	0,396	0	893101 (96%)
3	DoS-атака без СЗИ	0,163	29	306116 (33%)
4	DoS-атака с СЗИ	8,966	0	467688 (50%)

Рисунок 2. Пример оптимизации

2. Оптимизация WAN. Одним из самых быстрых и простых способов является оптимизация WAN, которая позволяет повысить производительность, обойтись без особых затрат и не требует изменений в архитектуре сети.

Для ускорения сетевого трафика в центре обработки данных (ЦОД) и филиалах устанавливают контроллеры оптимизации WAN Optimization Controller (WOC). Эти устройства устраняют основные причины низкой эффективности работы приложений в глобальных сетях, например: большие задержки, неэффективность транспортных протоколов, ограниченность пропускной способности канала.

Принцип работы: WOC подключается к маршрутизаторам глобальной сети со стороны локальной сети (рис. 3). Сокращаются объем данных, передаваемых приложением, распределяется пропускная способность между приложениями. Благодаря этому скорость работы через WAN значительно увеличивается.

После решения системных и инженерных задач применения СЗИ необходимо определить показатели, которые обеспечат требуемый уровень поддержания пропускной способности и безопасности функционирования объектов. Отсутствие общепринятых показателей усугубляет обеспечение требуемой эффективности управления процессом обеспечения пропускной способности. Под общим показателем эффективности функционирования сетевой системы с использованием СЗИ будем понимать минимальное среднее время доставки сообщения от пользователя-отправителя к пользователю-адресату [4].

Работка политики безопасности

Политика безопасности – это комплекс превентивных мер, основанных на совокупности руководящих принципов, правил и процедур в области безопасности, по защите конфиденциальных данных и информационных процессов на объекте информатизации [5].

Основные направления работки политики безопасности:

- Определение данных и степени их защиты.
- Определение лиц, допущенных к работе с информацией.
- Определение степени и вида возможного ущерба объекта информатизации.
- Расчет рисков ИБ.
- Разработка системы мер по снижению рисков.

Существует несколько методов анализа угроз на объекте информатизации. Рассмотрим некоторые из них.

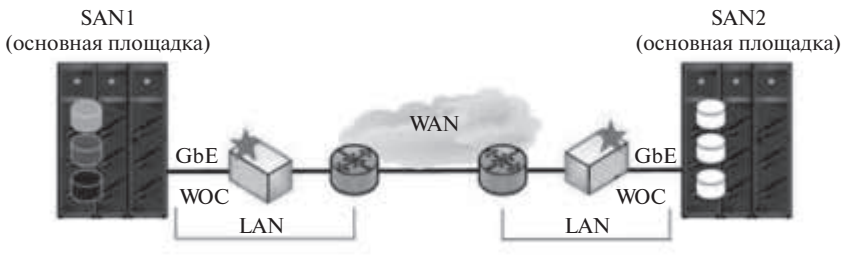

Рисунок 3. Установка контроллеров оптимизации (за маршрутизаторами)

1. Метод «исследования снизу вверх» – довольно простой метод, обладающий небольшими возможностями и требующий меньших вложений по сравнению с остальными.

Он основан на схеме «Вы – злоумышленник. Ваши действия?». То есть служба ИБ, основываясь на данных о всех известных видах атак, пытается определить их на практике с целью проверки того, возможна ли такая атака со стороны реального злоумышленника.

2. Метод «сверху вниз» представляет собой, наоборот, детальный анализ всей существующей схемы обработки информации на объекте информатизации, т.е. определение готовности объектов и потоков к защите:

- Анализ состояния системы информационной безопасности с целью исключения уже реализованных методик защиты.
- Распределение всех объектов согласно требованиям к конфиденциальности.
- Прогноз реализации угрозы и ее вероятный ущерб.

Выводы

Результаты исследования показали, что использование СЗИ позволяет обеспечить бесперебойное функционирование сегмента КС в условиях DoS-атаки и осуществление необходимых условий для работы пользователей. В случае, когда на ПК отсутствует СЗИ при моделировании атаки, атакующий узел находится в состоянии неготовности. В случае, когда установлено СЗИ, узел находится в состоянии готовности, но функционирует со сниженными характеристиками.

Требуемый уровень защищенности в КС может быть достигнут за счет увеличения числа СЗИ, но это значительно снижает производительность КС и приводит к удорожанию системы защиты. С другой стороны, существует несколько методов по оптимизации трафика с использованием СЗИ. В связи с этим для разрешения указанного противоречия разрабатываются методическое обеспечение и политика безопасности для достижения заданного уровня защищенности информации в КС при минимуме снижения сетевого трафика и стоимости СЗИ.

СПИСОК ЛИТЕРАТУРЫ

1. Белоножкин В.И., Остапенко Г.А. Средства защиты информации в компьютерных системах. Воронеж: ВГТУ. 2005. 337 с.
2. Митрохин В.Е., Рингенблюм П.Г. Математическая модель влияния средств защиты информации на характеристики узла связи телекоммуникационной сети // Вестник СибГУТИ. 2016. № 1. С. 66–73.
3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учебное пособие / под ред. Ю.Ф. Каторина. СПб.: НИУ ИТМО, 2012. 416 с.
4. Зайончковская Д.А., Федорова В.А. Методика выбора алгоритма маршрутизации, основанная на анализе исходных данных // Вопросы радиоэлектроники. 2017. № 11. С. 21–25.
5. Биячуев Т.А. Безопасность корпоративных сетей: учебное пособие. СПб.: СПбГУ ИТМО. 2004. 161 с.

REFERENCES

1. Belonozhkin V.I., Ostapenko G.A. *Sredstva zashhity informacii v komp'juternyh sistemah* [Information security products in computer networks]. Voronezh, VGTU, 2005, 337 p. (In Russian).
2. Mitrokhin V.E., Ringenblyum P.G. Mathematical model of the influence of information security products on the characteristics of a telecommunication network communication center. *Vestnik SibGUTI,* 2016, no. 1, pp. 66–73 (In Russian).
3. Katorin Yu. F., Razumovskiy A.V., Spivak A.I. *Zashhita informacii tehnicheskimi sredstvami: uchebnoe posobie* [Information security by means of technological tools: tutorial]. In: Yu.F. Katorin, ed. Saint-Petersburg, NIU ITMO, 2012, 416 p. (In Russian).
4. Zayonchkovskaya D.A., Fedorova V.A. Method of choosing a routing algorithm based on the analysis of the initial data. *Voprosy radioelektroniki,* 2017, no. 11, pp. 21–25 (In Russian)
5. Biyachuev T.A. *Bezopasnost korporativnyh setej: uchebnoe posobie* [Corporate network security: text book]. Saint-Petersburg, SPbGU ITMO, 2004, 161 p. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Федорова Вероника Анатольевна, к.т.н., доцент, Московский государственный технический университет им. Н.Э. Баумана, 105005, Москва, ул. 2-я Бауманская, д.5, стр. 1, тел.: 8 (985) 815-53-21, e-mail: bmstukf@mail.ru.
Моисеева Татьяна Александровна, аспирант, Московский государственный технический университет им. Н.Э. Баумана, 105005, Москва, ул. 2-я Бауманская, д.5, стр. 1, тел.: 8 (964) 522-70-27, e-mail: ttt-ttt-mmm@mail.ru.
Колягина Ирина Андреевна, студент, Московский государственный технический университет им. Н.Э. Баумана, 105005, Москва, ул. 2-я Бауманская, д.5, стр. 1, e-mail: airishandreevna@gmail.com.

AUTHORS

Fedorova Veronika, PhD, associate professor, Bauman Moscow State Technical University, 5/1, 2 Baumanskaya ulitsa, Moscow, 105005, Russian Federation, tel.: +7 (985) 815-53-21, e-mail: bmstukf@mail.ru.
Moiseeva Tatyana, postgraduate student, Bauman Moscow State Technical University, 5/1, 2 Baumanskaya ulitsa, Moscow, 105005, Russian Federation, tel.: +7 (964) 522-70-27, e-mail: ttt-ttt-mmm@mail.ru.
Kolyagina Irina, student, Bauman Moscow State Technical University, 5/1, 2 Baumanskaya ulitsa, Moscow, 105005, Russian Federation, e-mail: airishandreevna@gmail.com.