МЕТОД ОБНАРУЖЕНИЯ НИЗКОИНТЕНСИВНЫХ РАСПРЕДЕЛЕННЫХ АТАК ОТКАЗА В ОБСЛУЖИВАНИИ СО СЛУЧАЙНОЙ ДИНАМИКОЙ ХАРАКТЕРИСТИК ФРАГМЕНТАЦИИ И ПЕРИОДИЧНОСТИ

Слесарчик К.Ф.[1]

В статье рассматривается подход к обнаружению низкоинтенсивных распределенных атак на отказ в обслуживании, направленных на прикладной уровень инфокоммуникационной сети. Рассмотрены особенности обнаружения низкоинтенсивных DDoS–атак со случайной динамикой характеристик фрагментации и периодичности приема пакетов. Предложен показатель оценивания состояния объекта атаки. Разработан способ обнаружения низкоинтенсивной атаки со случайной динамикой её характеристик. Представлены результаты экспериментальных исследований, характеристики ошибок первого и второго рода.

Ключевые слова*: низкоинтенсивная атака; анализатор DDoS–атак; деструктивное информационное кибернетическое воздействие; сетевая безопасность; атака малой мощности; инфокоммуникационная сеть; прикладной уровень.*

DOI: 10.21681/2311-3456-2018-1-19-27

Введение.

Стремительное внедрение инфокоммуникационных технологий в различные сферы человеческой деятельности способствует развитию методов противодействия их функционированию. Для сдерживания предлагаемых ими возможностей со стороны злоумышленников. Причем такое противодействие реализуется на различных уровнях для влияния, как на частных лиц, так и государственные структуры. В результате появляется множество классов деструктивных информационных кибернетических воздействий (ДИКВ).

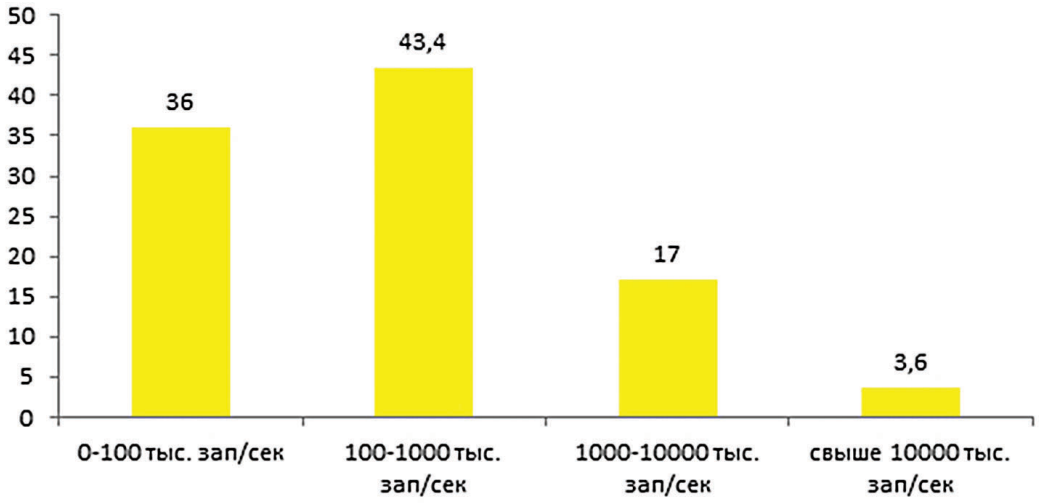
Общий анализ атак показывает, что одним из эффективных способов воздействий на инфокоммуникационную сеть с целью нарушения процессов управления ею является несанкционированное блокирование доступа к информационным ресурсам. Наиболее распространенным методом ДИКВ является распределенная атака отказа в обслуживании (DDoS-атака).

Результаты анализа ДИКВ на инфокоммуникационные сети в 3 квартале 2017 года указывают на то, что одной из основных целей ДИКВ является прикладной уровень инфокоммуникационной сети (рис. 1). Статистика атак по количеству запросов в секунду показывает, что более чем в 79,4% случаев атак мощность атаки лежит в пределах 10-1000 тыс. запросов в секунду (RPS) при средней продолжительности от 30 до 60 минут в 41,4% случаев [1]. Если сравнивать с тем же периодом 2016 года, когда мощность атаки находилась в пределах от 80 до 268 тыс. RPS, а её длительность в 52,2% случаев составляла менее 1 часа, то рассмотрение проблемы в аспекте индустрии криминальных киберуслуг, позволяет сделать вывод о том, что технология проведения низкоинтенсивных атак позволит снизить вычислительную нагрузку на средства проведения атак и увеличить их эффективность по временному критерию. Следовательно, рассматривая динамику тенденции проведения распределенных атак отказа в обслуживании прикладного уровня, можно дать прогноз увеличения в ближайшем будущем доли применения низкоинтенсивных атак, что делает необходимым совершенствование методов их обнаружения.

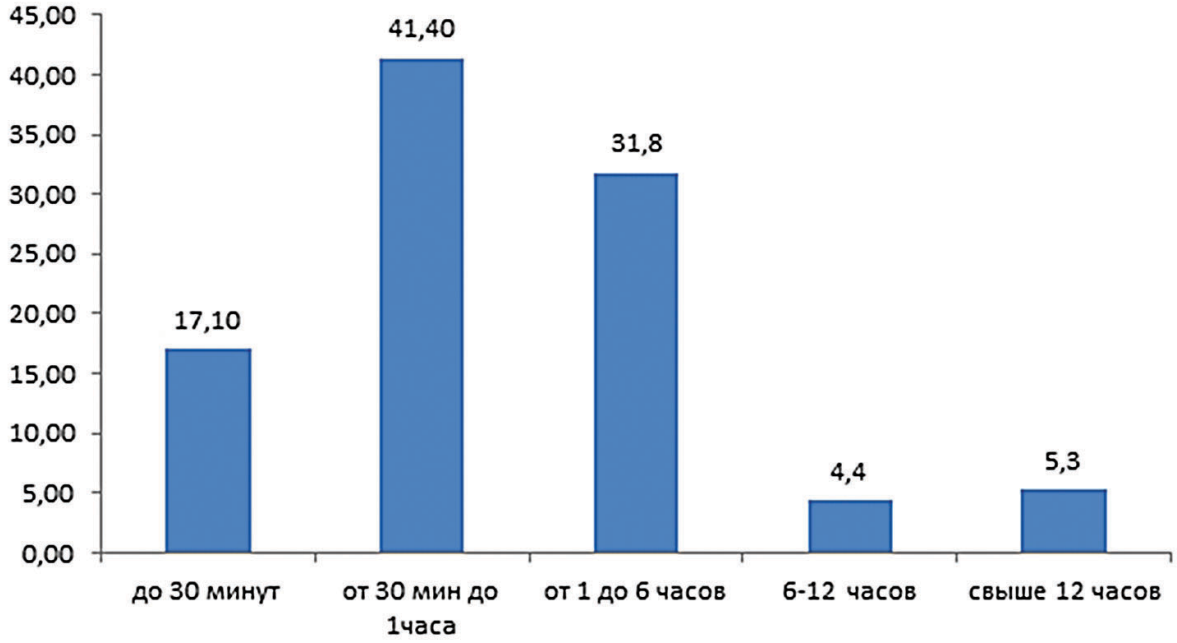
Сценарий низкоинтенсивной DDoS-атаки

Низкоинтенсивная DDoS-атака характеризуется продолжительными периодами между передачей пакетов для одной сессии и большим значением фрагментации пакетов в данной сессии для передачи контентной информации. Возможность проведения низкоинтенсивной атаки объясняется уязвимостью протокола HTTP и необходимостью обязательного ожидания сервером конца передачи POST-запроса. При реализации низкоинтенсивной DDoS-атаки злоумышленник фрагментирует POST-запрос на пакеты малой длины и отправляет их серверу с периодичностью меньше, чем значение времени ожидания окончания соединения. В результате чего сервер вынужден

1 Слесарчик Константин Федорович, Академия ФСО России, г. Орёл, interline57@mail.ru.



а) мощность DDoS-атак на прикладной уровень



б) длительность DDoS-атак на прикладной уровень

***Рис. 1**. Статистика DDoS атак на прикладной уровень в 3 квартале 2017 года*

ожидать окончание приема POST-запросов злоумышленника, в тот момент как запросы легитимных пользователей игнорируются ввиду отсутствия свободного ресурса [2].

Существующие методы обнаружения DDoS-атак (табл. 1), позволяют эффективно распознавать DDoS-атаки транспортного и сетевого уровней и малоэффективны для обнаружения низкоинтенсивных DDoS-атак прикладного уровня, так как не учитывают особенностей низкоинтенсивной атаки. Исключение составляют методы на основе мягких решений, но и они обладают рядом существенных недостатков, снижающих эффективность их применения, главный из которых – необходимость предварительного обучения. Кроме того, точность функционирования методов на основе мягких решений зависит от качества наборов характеристик атаки. Чем больше для обучения анализатора используется значений из пространства характеристик атаки, тем точнее ее определение (меньше ошибок 1 и 2 рода). Однако обучение по всему пространству значений характеристик атаки невозможно ввиду вычислительной и временной сложности реализации такого обучения. В дополнение к этому обучение анализатора атаки становится бесперспективным в случае случайного характера динамики характеристик низкоинтенсивной атаки, так как трафик атаки малой мощ-

Таблица 1.
Методы обнаружения DDoS-атак

№ п/п	Метод	Достоинства	Недостатки
1.	**Статистический**	Адаптация к поведению субъекта, не требуется знание о возможных атаках и используемых уязвимостях	1. Возможность манипуляции эталонными профилями параметров трафика. 2. Нечувствительность к порядку следования событий. 3. Объективная трудность определения граничных (пороговых) значений отслеживаемых характеристик.
2.	**Использование экспертных систем (сигнатурный метод)**	Отсутствие ложных тревог	Необходимость постоянного обновления сигнатур (актуализация)
3.	**Использование методов на основе мягких решений (нейросетевые анализаторы и генетические алгоритмы)**	Способность «изучать» характеристики атак и идентифицировать элементы, которые не похожи на те, что наблюдались ранее.	Точность обнаружения атак зависит от качества обучения нейросети
4.	**Использование методов Data Mining и машинного обучения**	Малое время обнаружения события атаки	1. Недостаточно апробирован на практике. 2. Требует достаточно больших вычислительных мощностей

ности становится непериодическим, что является нетипичным её признаком [3-5].

Способ обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности

Анализ наличия или отсутствия атаки проводится относительно состояния объекта атаки, которое описывается значением, являющимся точкой, взятой в ортогональном базисе пространства состояний, независимых функций, описывающих признаковые показатели низкоинтенсивной атаки. Точка в пространстве состояний объекта – это показатель тревоги (1), рассчитываемый на основе трех признаковых показателей атаки (2–4):

$$\overline{K_{\text{тр}}} = \left[K_{\text{фр}}, K_{\lambda}, K_{\text{д}}\right], \quad (1)$$

где $K_{\text{фр}}$ – коэффициент фрагментации пакетов определяется выражением:

$$K_{\text{фр}} = \frac{L_{\text{ср.фр.}POST}}{L_{\text{ср.фр.}}}, \quad (2)$$

где $L_{\text{ср.фр.}POST}$ – среднее значение размера данных POST запросов к серверу службы во фрагментированных пакетах; $L_{\text{ср.фр.}}$ – среднее значение размера данных для всех фрагментированных пакетов отправленных к серверу службы.

K_{λ} – коэффициент интенсивности приема фрагментированных пакетов вычисляется по формуле:

$$K_{\lambda} = \frac{t_{\text{ср.фр.}}}{t_{\text{ср.фр.}POST}}, \quad (3)$$

где $t_{\text{ср.фр.}}$ – среднее время между приемом для всех фрагментированных пакетов отправленных к серверу службы; $t_{\text{ср.фр.}POST}$ – среднее время между приемом фрагментированных пакетов с данными POST–запросов к серверу службы.

Коэффициент доступности службы определяется как:

$$K_{\text{д}} = \frac{N_{ack1}}{N_{SYN}}, \quad (4)$$

N_{ack1} – количество ответов службы сервера с согласием на установление соединения, N_{SYN} – количество запросов к службе сервера на установку соединения.

Блок–схема алгоритма расчета показателя тревоги $\overline{K_{\text{тр}}}$ представлен на рис.2.

На первом шаге производится прием пакета, на 2-м и 9-м шагах выявляются пакеты запросов на соединение с сервером и пакеты с его согласием на установку соединений. На 11-м и 12-м шагах выявляются целевые пакеты с признаками содержания фрагментированных данных HTTP–запросов к серверу. На 13-м шаге определяется принадлежность пакета к ранее зарегистрированным соединениям по признаку идентификатора соединения. На шагах 4, 10, 14 и 17–19-м определяются параметры соединения, на основе которых будет рассчитан показатель тревоги (шаги 5–7).

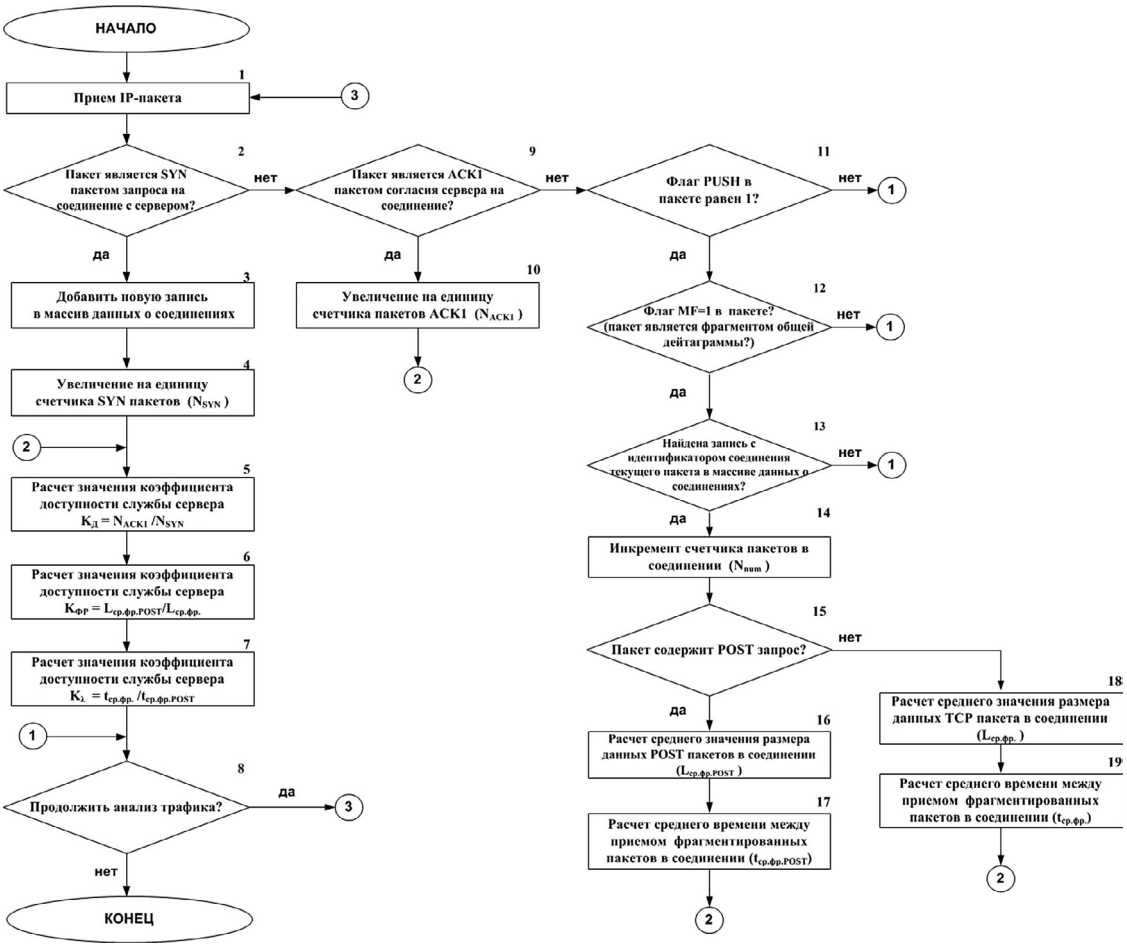


***Рис.2**. Блок–схема алгоритма расчета показателя тревоги*

В настоящее время наиболее эффективным способом реализации обнаружения низкоинтенсивной атаки по предлагаемому показателю является анализатор на основе гибридной нейронной сети, состоящей из фильтров запрета и нейронной сети с обратным распространением на основе звезды Гроссберга (рис. 3) [6].

Такая реализация позволяет сузить бесконечное множество возможных значений показателя тревоги на входе нейронной сети до трех четких состояний: «Атака», «Возможность атаки», «Отсутствие атаки» (рис. 4), однако обладает следующими недостатками:

- необходимость предварительного знания характеристик атак для предварительного обучения нейросети;

- трудность в точном определении границы областей состояний наличия и отсутствия атаки, что в совокупности определяет значение риска не обнаружения атаки.

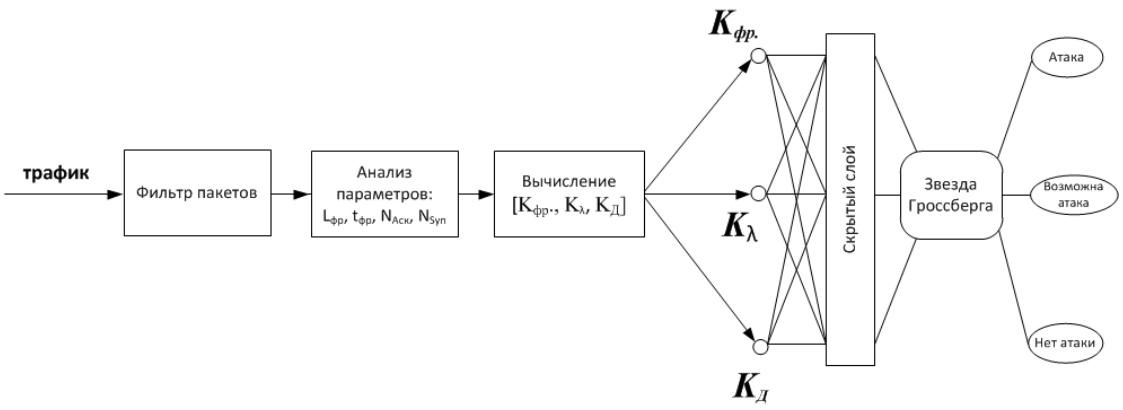


***Рис. 3**. Гибридная нейронная сеть с обратным распространением на основе звезды Гроссберга*

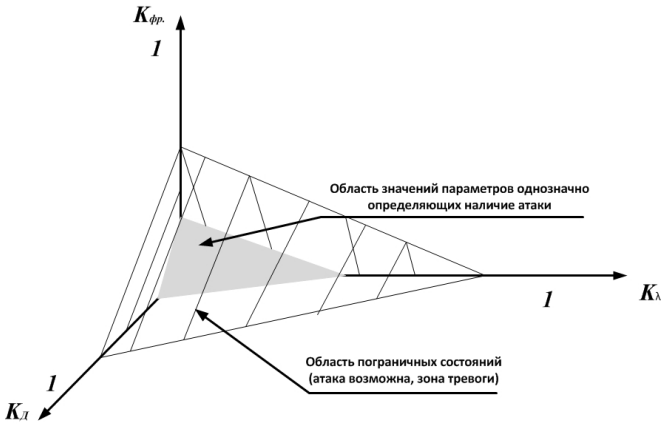


***Рис. 4**. Области возможных состояний анализатора атаки*

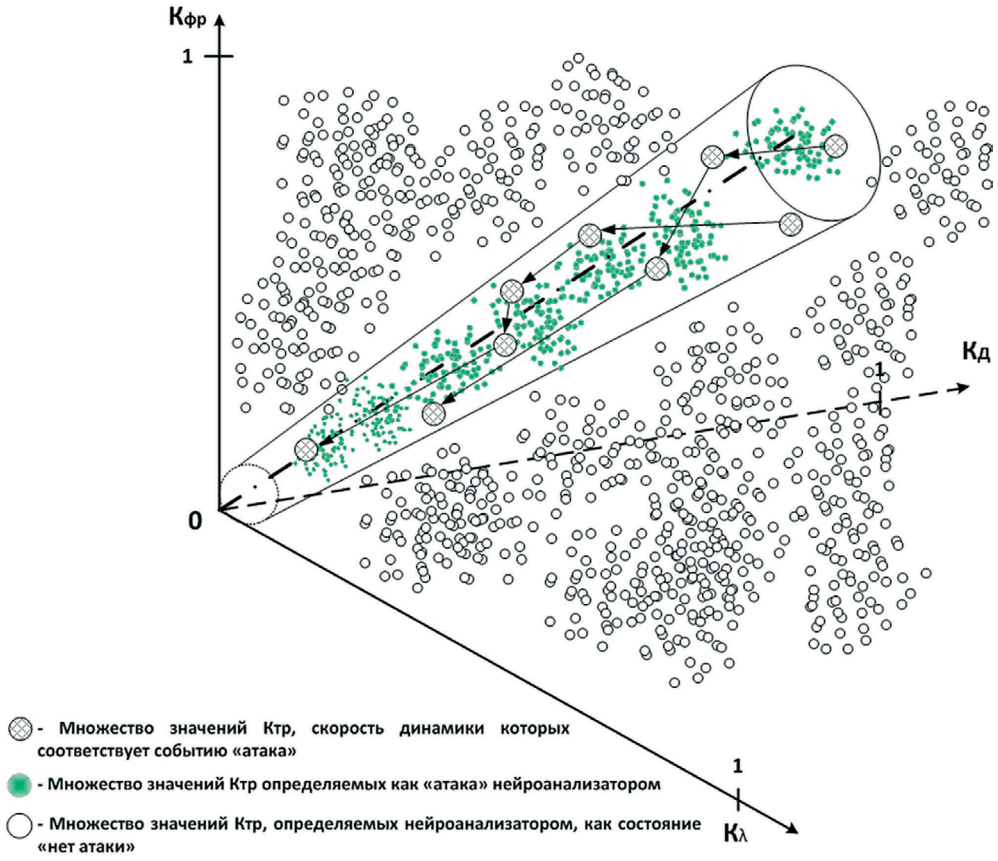


***Рис. 5**. Динамика градиентного движения показателя тревоги* $\overline{К_{тр}}$

Для устранения указанных недостатков предлагается дополнительно анализировать скорость динамики градиентного движения показателя тревоги $\overline{К_{тр}}$, (рис. 5).

Полученные расчетные значения показателя $\overline{К_{тр}}$ проверяются на предмет изменения скорости градиентного движения к нулевому вектору $[K_{фр} = 0, K_{л} = 0, K_{д} = 0]$, на основании чего делается вывод о наличии низкоинтенсивной атаки.

Однако такой анализ скорости динамики градиентного движения показателя тревоги дает положительный результат при ограничении согласно которому степень фрагментации пакетов нелегитимного трафика и значение периода получения пакетов нелегитимного трафика являются постоянными величинами. Известные примеры проведенных низкоинтенсивных атак в отношении ресурсов коммерческих и общественных организаций показали, что характеристики фрагментации и период получения пакетов атаки носят случайный характер.

В рамках проведенных исследований были выдвинуты и проверены две гипотезы.

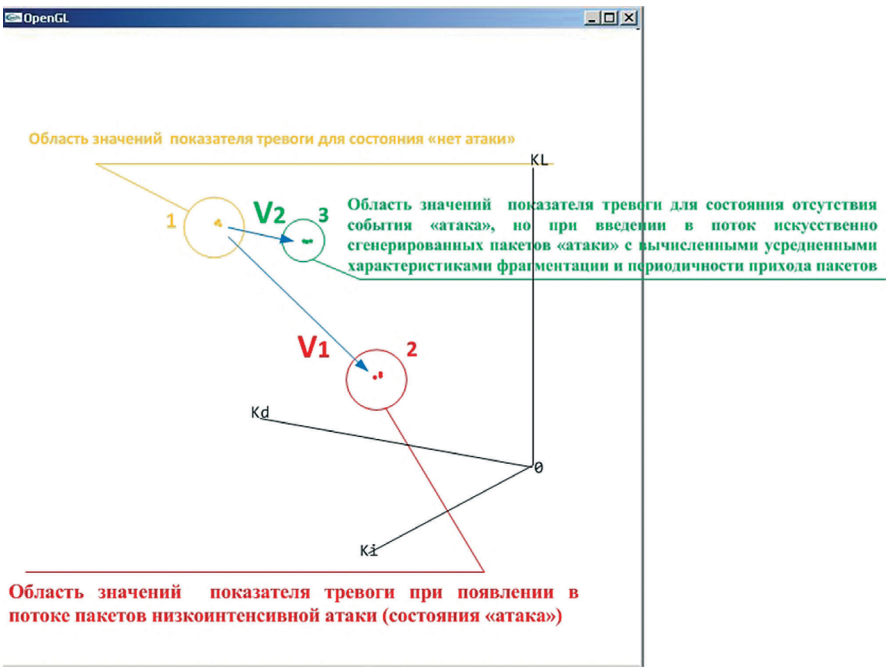


Рис. 6. *Результаты экспериментальной проверки первой гипотезы*

Гипотеза 1. Скорость динамики показателя тревоги при появлении в потоке пакетов низкоинтенсивной атаки всегда будет выше, чем при введении в поток дополнительных (искусственно сгенерированных) пакетов атаки, с усредненными характеристиками фрагментации и периодичности регистрации пакетов (рис. 6).

На рисунке 6 начальное состояние «Отсутствие атаки», показано жёлтым цветом (область «1»). При введении в поток искусственно сгенерированных пакетов атаки, с усредненными характеристиками фрагментации и периодичности регистрации пакетов для состояния «отсутствия атаки» показатель перемещается в область показанную зелёным цветом (область «3»).

При моделировании низкоинтенсивной атаки, показатель тревоги перемещается в область «атаки», помеченную красным цветом (область «2»).

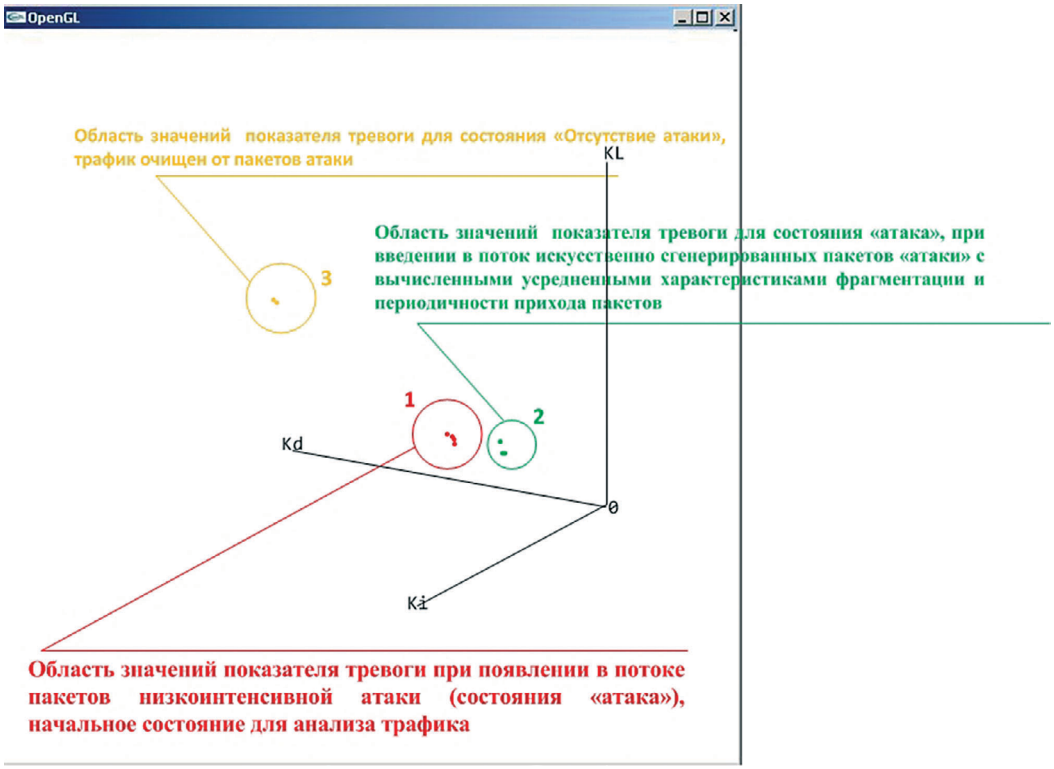


Рис. 7*. Результаты экспериментальной проверки второй гипотезы*

При этом расстояние между точками из областей «1» и «2» будет всегда больше, чем между точками из областей «1» и «3».

Гипотеза 2. Если в анализируемом потоке присутствуют пакеты низкоинтенсивной атаки, то при дополнительном введении в поток искусственно сгенерированных пакетов атаки с характеристиками фрагментации и периодичности регистрации пакетов скорость динамики показателя тревоги, будет всегда выше, чем при отсутствии в потоке таких дополнительно сгенерированных искусственных пакетов атаки (рис. 7).

На рисунке 7 при начальном состоянии «Атака присутствует» показатель тревоги находится в области «1», показана красным цветом. Если усредненные характеристики атаки не изменяются, то значения показателя тревоги концентрируются в области «1», не превышая значения, определяемого дисперсией характеристик фрагментации и периодичности атаки. При введении в поток искусственно сгенерированных пакетов атаки с характеристиками фрагментации и периодичности регистрации пакетов, вычисленных в предыдущем окне анализа, показатель тревоги перемещается в «2», обозначена зелёным цветом. При этом расстояние между точками, рассчитанными с учетом дополнительных пакетов и без них, будет всегда больше, чем флуктуация показателя тревоги в состоянии атаки. Жёлтым цветом показана область значений показателя тревоги после удаления из потока пакетов низкоинтенсивной атаки, область «3».

На основе сформулированных гипотез разработан алгоритм обнаружения низкоинтенсивных атак (рис. 8). Согласно предлагаемому алгоритму, по рассчитанному значению показателя тревоги

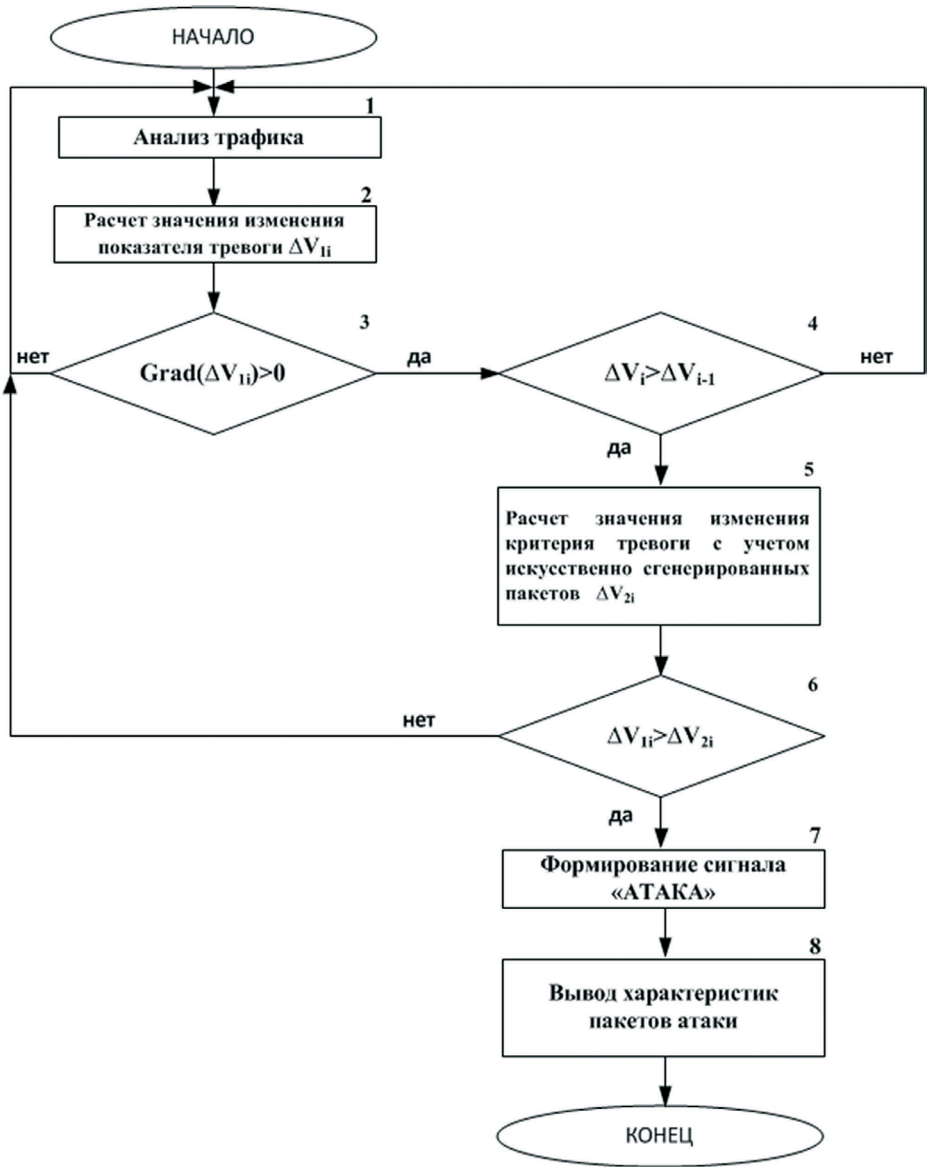


***Рис. 8**. Алгоритм работы анализатора низкоинтенсивной DDoS атаки на основе анализа динамики градиента показателя тревоги*

определяется направление градиента ΔV_{i1} (рис. 8, шаг 2–3) и в случае его положительного значения (движения к нулевой координате) сравнивается скорость изменения ΔV_{1i} с результатом анализа на предыдущем окне ΔV_{1i-1} (рис. 8, шаг 4). При увеличении скорости изменения показателя тревоги рассчитывается следующие значение показателя тревоги ΔV_{2i} с учетом характеристик фрагментации и периодичности регистрации искусственно сгенерированных пакетов атаки, определенных для предыдущего окна анализа (рис. 8, шаг 5).

Если значение изменения показателя тревоги для текущего окна анализа ΔV_{1i} больше, чем для значения вычисленного на шаге 5 (рис. 8, шаг 6), то формируется сообщение о наличии низкоинтенсивной атаки и определяются характеристики фрагментации и периодичности пакетов атаки (рис. 8, шаг 7–8). Полученные значения показателя тревоги для события «Атака» дополнительно могут быть использованы для обучения нейросетевого анализатора.

Результаты экспериментальных исследований

Целью эксперимента являлась определение значений ошибок 1 и 2 рода для предложенного алгоритма обнаружения низкоинтенсивных DDoS-атак (рис. 8) со случайной динамикой характеристик фрагментации и периодичности, при различных значениях размера окна анализа.

Проверка проводилась для трех сценариев:

1) Анализатор функционирует, когда объект не подвергается атаке и обрабатывается легитимный трафик с периодическим увеличением нагрузки (значение коэффициента нагрузки изменяется случайным образом в диапазоне от 1 до 10);

2) Анализатор функционирует, когда объект не подвергается атаке, обрабатывается легитимный трафик с периодическим увеличением нагрузки (значение коэффициента нагрузки изменяется случайным образом в диапазоне от 1 до 10). Затем через 100 окон анализа подключается генератор деструктивных информационно-кибернетических воздействий, реализующий низкоинтенсивную атаку типа «Rudy», со случайными характеристиками фрагментации и периодичности пакетов (закон распределения характеристик атакующего трафика равномерный);

3) Анализатор функционирует, когда объект уже подвергнут атаке и объект обрабатывает смесь легитимного и атакующего трафика. Причём нагрузка легитимного трафика периодически увеличивается (значение коэффициента нагрузки изменяется случайным образом в диапазоне от 1 до 10). При этом генератор атаки имитирует низкоинтенсивную атаку типа «Rudy» со случайными характеристиками фрагментации и периодичности пакетов (закон распределения характеристик атакующего трафика равномерный).

При проведении экспериментов значение окна анализа изменялось в диапазоне от 30 до 1500 пакетов. При генерации нормального трафика использовалось случайное количество запросов с случайным тайм-аутом без генерации случайных путей (только к корневой папке WEB-сервера). При генерации трафика атаки типа «Rudy» сценарий производил множество запросов к Web-серверу и в дальнейшем поддерживал их.

В ходе экспериментов значение максимальной ошибки первого рода (ложное срабатывание) при минимальном значении окна анализа (30 пакетов) не превысило 0,89%, а при максимальной значении окна анализа (1500 пакетов) не превысила 0,0896%. Ошибка второго рода в наихудшем случае (окно анализа 30 пакетов) составляет 1,73%, при окне анализа 1500 пакетов – 0,63%.

Заключение

Предлагаемый метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании позволяет решить ряд проблем, основными из которых являются следующие:

Эффективное выявление принадлежности трафика к распределённой по времени атаке, при условии перманентного изменения характеристик атаки с меньшим объемом анализируемых данных по сравнению со статистическими методами.

Реализация обнаружения низкоинтенсивных распределенных атак отказа в обслуживании непосредственно на серверах служб и/или интегрироваться в ПО маршрутизаторов.

Формирование данных для предварительного обучения нейросети с целью уменьшения объема вычислительных операций и снижения времени реакции анализатора низкоинтенсивной DDoS-атаки в случае совместного применения с нейросетевым методом.

***Рецензент**: Иванов Юрий Борисович, кандидат технических наук, доцент, сотрудник Академии ФСО России, г. Орел, Россия. E-mail: 89102697376@yandex.ru*

Литература

1. DDoS Threat Landscape Report Q3 2017. [Электронный ресурс]. – Режим доступа: https://www.incapsula.com/ (дата обращения: 14.01.2018).
2. A. Carlsson, E. Duravkin, A. Loktionova. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. method of detecting slow HTTP attacks. // Problems of the telecommunication. – 2014. – № 1 (13). – С. 96-100.
3. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. – 2017.-№5 (24).- С.23-29.
4. Абрамов Е.С., Сидоров И.Д. Метод обнаружения распределенных информационных воздействий на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 154-164.
5. Тарасов Я. В. Метод обнаружения низкоинтенсивных DDsoS-атак на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2010. – № 1 (13). – С. 47-57.
6. Слесарчик К.Ф., Шульгин Р. Н., Аристархов А.А. Обнаружение «низкоинтенсивной» DDoS атаки методами нейросетевого анализа//сборник трудов научно-практической конференции «Проблемы технического обеспечения войск в современных условиях» Военная Академия связи им. Маршала советского союза С.М. Буденного (09 февраля 2016 г.) – г.Санкт-Петербург: Военная Академия связи им. Маршала советского союза С.М. Буденного , – 2016, С. 22-26.

METHOD FOR THE DETECTION OF LOW INTENSITY ATTACKS DISTRIBUTED DENIAL OF SERVICE WITH A RANDOM DYNAMICS OF CHARACTERISTICS OF FRAGMENTATION AND FREQUENCY

Slesarchik K. [2]

The article discusses an approach to the detection of low intensity attacks distributed denial of service attacks aimed at application layer network information and communication. The features of detection of low–intensity DDoS–attacks with random dynamics of fragmentation characteristics and frequency of packet reception are considered. The indicator of estimation of the state of the object of attack is offered. A method for detecting a low–intensity attack with random dynamics of its characteristics is developed. The results of experimental studies, characteristics of errors of the first and second kind are presented.

Keywords*: low–attack; analyzer DDoS attacks; destructive information impact cyber; network security; attack of small capacity; information communication network; the application layer.*

References

1. DDoS Threat Landscape Report Q3 2017. [https://www.incapsula.com/]. (14.01.2018).
2. A. Carlsson, E. Duravkin, A. Loktionova. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. method of detecting slow HTTP attacks. // Problems of the telecommunication. – 2014. – № 1 (13). – С. 96-100.
3. Tarasov YA.V. Issledovanie primeneniya nejronnyh setej dlya obnaruzheniya nizkointensivnyh DDoS-atak prikladnogo urovnya // Voprosy kiberbezopasnosti. – 2017.-№5 (24).- S.23-29.
4. Abramov E.S., Sidorov I.D. Metod obnaruzheniya raspredelennyh informacionnyh vozdejstvij na osnove gibridnoj nejronnoj seti // Izvestiya YUFU. Tekhnicheskie nauki. – 2009. – № 11 (100). – S. 154-164.
5. Tarasov YA. V. Metod obnaruzheniya nizkointensivnyh DDsoS-atak na osnove gibridnoj nejronnoj seti // Izvestiya YUFU. Tekhnicheskie nauki. – 2010. – № 1 (13). – S. 47-57.
6. Slesarchik K.F., SHul'gin R. N., Aristarhov A.A. Obnaruzhenie «nizkointensivnoj» DDoS ataki metodami nejrosetevogo analiza// sbornik trudov nauchno-prakticheskoj konferencii «Problemy tekhnicheskogo obespecheniya vojsk v sovremennyh usloviyah» Voennaya Akademiya svyazi im. Marshala sovetskogo soyuza S.M. Budennogo (09 fevralya 2016 g.) – g.Sankt-Peterburg: Voennaya Akademiya svyazi im. Marshala sovetskogo soyuza S.M. Budennogo , – 2016, S. 22-26.

2 Konstantin Slesarchik, Academy of Federal security service of Russia, Orel, Russia. E-mail: interline57@mail.ru