



А. Ю. Телков,
кандидат физико-
математических наук,
доцент



О. Ю. Данилова,
кандидат физико-
математических наук,
доцент



С. А. Телкова,
кандидат педагогических
наук, доцент

ОБНАРУЖЕНИЕ СЕТЕВЫХ АНОМАЛИЙ ОБЪЕМА ТРАФИКА МЕТОДОМ КОНТРОЛЬНЫХ КАРТ УНИВЕРСАЛЬНОЙ СИСТЕМОЙ МОНИТОРИНГА ZABBIX

DETECTION OF NETWORK ANOMALIES OF VOLUME OF TRAFFIC BY THE METHOD OF CONTROL CARDS BY THE ZABBIX UNIVERSAL MONITORING SYSTEM

Рассмотрен вариант применения универсальной системы мониторинга ZABBIX для обнаружения сетевых аномалий объема трафика в соответствии с методом контрольных карт. Показана возможность обнаружения аномалий объема трафика, вызванная проведением многопользовательского сеанса телеконференцсвязи по данным простого протокола управления сетью SNMP, передающего информацию о транзитном трафике с граничного маршрутизатора сети с сервером телеконференцсвязи. Приведена методика получения требующихся для принятия решения о тревоге алгоритму EWMA параметров и характеристик с помощью средств и инструментов системы ZABBIX.

The application of the ZABBIX universal monitoring system for detecting network anomalies in the traffic volume in accordance with the control card method is considered. The possibility of detecting traffic volume anomalies caused by a multi-user teleconferencing session using the data of the simple SNMP network management protocol that transmits information about transit traffic from the network edge router to the teleconferencing server is shown. The technique of obtaining the parameters and characteristics required for making a decision about alarming the EWMA algorithm is presented using the tools and tools of the ZABBIX system.

Введение. Повсеместное введение карантинных мер и перевод предприятий различных форм собственности в режим удаленной работы (там, где это возможно) весной

2020 г. привели к достаточно резкому росту нагрузки на каналы связи и сервисы, предоставляющие возможности удаленной совместной работы через сеть Интернет. Так, например, согласно статистике концентратора Интернет первого слоя в Амстердаме AMS-IX, средняя нагрузка по трафику выросла примерно на 50%, с 4,0 до 6,0 TB/s в период с января по апрель 2020 г. [1]. Это произошло несмотря на то, что в середине марта представители видеохостинга YouTube заявили, что сервис снижает качество видео для пользователей Великобритании и Швейцарии, а затем и по всему ЕС и миру. Те же меры стали предпринимать и другие видеохостинги и стриминговые сервисы, в первую очередь Netflix и Twitch. В свою очередь отделы связи организаций, предоставляющих возможность совместной работы, в том числе видеоконференции, своим сотрудникам на мощностях своих внутрикорпоративных интранет-площадок, оказались перед вызовами обеспечения высокой доступности необходимых для удаленной работы сервисов, как в части корректной работы каналов связи, так и в части производительности информационных систем. Несмотря на то, что внутрикорпоративные системы видеоконференцсвязи не генерируют трафик, соизмеримый, например, с видео в формате 4к четкости, при большом количестве участников видеосвязи остро стоит задача оценки объема такого трафика и принятие своевременных мер по обеспечению необходимых ширины и качества корпоративных каналов связи для решения указанных выше задач.

Целью данной работы является разработка методики настройки универсальной системы мониторинга ZABBIX с целью обнаружения сетевых аномалий объема трафика. По данным авторов, несмотря на то, что в различных работах приводятся отдельные результаты по применению, например, статистических алгоритмов для обнаружения аномалий объема, возможности и пути реализации этих алгоритмов в продукционных системах мониторинга до сих пор в известной литературе не рассмотрены. Вместе с тем, решение этой задачи позволит в короткие сроки обеспечить обнаружение сетевых аномалий объема с использованием существующих программных средств мониторинга без кардинальной перестройки состава этих средств. Основаниями поиска подобных решений являются наличие у некоторых систем мониторинга подсистем управления и получения данных через API (Application Program Interface — программный интерфейс приложения), механизмов сбора данных через так называемые U.P. (User Parameters — пользовательские параметры, позволяющие решить широчайший спектр задач), а также механизмов запуска пользовательских скриптов и механизмов оповещений, работающих в реальном масштабе времени.

Статистические методы обнаружения сетевых аномалий. Рассмотрим статистические методы обнаружения сетевых аномалий объема для определения путей алгоритмизации получения требуемых зависимостей и характеристик в универсальных системах мониторинга. Практическое решение для статистического обнаружения изменений дает метод контрольных карт [2]. В контрольных картах среднее значение и изменение переменной характеризуются центральным, верхним и нижним контрольными пределами (CL — central line, UCL — upper control limit, LCL — lower control limit). Изменение обнаруживается, если значение решающей характеристики превышает один из контрольных пределов.

Решение может быть найдено путем сравнения гипотез — H_0 , когда нет изменений, и H_1 , когда изменения есть. Статистические свойства контрольных карт могут быть выведены из последовательного критерия отношения вероятностей тестов (SPRT — sequential probability ratio tests). Если данные до и после изменения известны, то решающая статистика описывается логарифмом отношения правдоподобия

$$s(y) = \log \frac{p_{\Theta_1}(y)}{p_{\Theta_0}(y)}, \quad (1)$$

где $p_{\Theta}(y)$ — функция плотности вероятности Y с параметрами Θ , Θ_0 и Θ_1 — параметры до и после изменения.

Если отношение $s(y)$ положительно, наблюдаемая случайная величина чаще соответствует распределению до изменения, чем после. Таким образом, можно определить порог h для $s(y)$, отклоняющий нулевую гипотезу $H_0: \Theta = \Theta_0$ и подтверждающий альтернативную гипотезу $H_1: \Theta = \Theta_1$ при заданном уровне значимости. Уровень значимости соответствует уровню ложной тревоги.

Если Y имеет нормальное распределение с постоянной дисперсией σ^2 и средним значениями μ_0 и μ_1 до и после изменения, то $s(y)$ принимает вид

$$s(y) = \frac{\mu_1 - \mu_0}{\sigma^2} \left(y - \frac{\mu_1 + \mu_0}{2} \right), \quad (2)$$

если $\mu_0 < \mu_1$, то $s(y) > h$ эквивалентно функции

$$y > \mu_0 + L\sigma, \quad (3)$$

где

$$L = \frac{h\sigma}{\mu_1 - \mu_0} + \frac{\mu_1 - \mu_0}{2\sigma}. \quad (4)$$

В этом уравнении очевидным является признак контрольных карт: μ_0 — центральная линия, $\mu_1 + L\sigma$ — верхний предел.

Контрольные карты Шухарта. Контрольные карты Шухарта определяют уровни UCL, CL, LCL для статистики, вычисленной из N наблюдений $Y_{(t-1)N+1}, \dots, Y_{tN}$.

Например, статистика имеет среднее значение $\bar{y}_I$, которое подходит для определения изменений в виде

$$\bar{y}_I = \frac{1}{N} \sum_{t=(I-1)N+1}^{IN} y_t, \quad (5)$$

если наблюдения независимы и имеют одинаковое распределение со средним значением μ_0 и дисперсией σ^2 , то $\bar{y}_I$ является оценкой μ_0 с дисперсией μ_0 / N . Верхний UCL и нижний LCL пределы могут быть определены в форме

$$\mu_0 \pm \frac{L_{\sigma}}{\sqrt{N}} \quad (6)$$

с настраиваемым параметром L_{σ} .

Тревога возникает, если $\bar{y}_I$ пересекает один из пределов. Для больших значений N в силу центральной предельной теоремы $\bar{y}_I$ имеет нормальное распределение. В этом случае контрольные пределы (в случае для больших значений N , в отсутствии серийной корреляции) для данной вероятности ложных обнаружений α будут

$$\mu_0 \pm \Phi\left(1 - \frac{\alpha}{2}\right) \frac{\sigma}{\sqrt{N}}, \quad (7)$$

Особым случаем будет $N=1$, соответствующий контрольным картам Шухарта. Эти карты сравнивают отдельные наблюдения в отношении контрольных лимитов. Поскольку в этом случае невозможно применить центральную предельную теорему, распределение Y должно быть известно, чтобы определить точные границы для заданной вероятности ложной тревоги.

Контрольные карты CUSUM. Контрольные карты CUSUM (также называемые алгоритмами cumulative sum — кумулятивных сумм) основаны на том, что $S_1 = s(y_1, \dots, y_t)$ имеет отрицательное значение в нормальных условиях и положительное при изменении. Решение в алгоритме кумулятивных сумм принимается путем сравнения функции $g_t = S_t - \min_{1 \leq i \leq t} S_i = \max(0, s(y_t) + g_{t-1}) = [g_{t-1} + s(y_t)]^+ \geq h$; $g_0 = 0$.

Тревога возникает, если g_t пересекает порог h .

Контрольные карты EWMA. Контрольные карты EWMA (Exponentially Weighted Moving Average) базируются на экспоненциальном сглаживании наблюдений. С учетом постоянной сглаживания $\lambda (0 < \lambda < 1)$ выходной эффект

$$z_t = \lambda y_t + (1 - \lambda) z_{t-1} = \lambda \sum_{i=0}^{t-1} (1 - \lambda)^i y_{t-i} + (1 - \lambda)^t z_0 \quad (8)$$

представляет собой взвешенное среднее всех наблюдений до времени t . Начальное значение наблюдаемого среднего гипотезы $H_0: \mu_0 = z_0$. Если наблюдения независимы и имеют одинаковое распределение с дисперсией σ^2 , это позволяет определить контрольные пределы для Z_t :

$$\mu_0 \pm L\sigma \sqrt{\frac{\lambda}{2 - \lambda}}, \quad (9)$$

где λ и L — основные методы EWMA контрольных карт, значения которых удовлетворяют отношениям $2,6 \leq L \leq 3$ и $0,05 \leq \lambda \leq 0,25$.

Расчетные операции на примере метода контрольных карт EWMA. Рассмотрим подробно операции, необходимые в процессе применения метода контрольных карт для определения преобразований в ходе решения задачи обнаружения согласно формулам (1), (8) и (9). Известно, что метод контрольных карт EWMA успешно работает в задачах обнаружения сетевых аномалий различного рода [3—6]. Характер и сложность математической обработки при использовании других (не статистических) методов или статистических методов в расширенном виде [7] могут потребовать разработки самостоятельных систем обнаружения в виде пакета программ. Однако несложный вид соотношений (8), (9) позволяет рассчитывать на относительно простую алгоритмизацию при использовании метода в существующих универсальных производственных системах мониторинга реального времени.

Итак, имеем исходный вектор Y измерений объемов трафика (предполагаем, что исходящего, но все рассуждения и формулы справедливы и для входящего направления) на транзитном маршрутизаторе

$$Y = [y_{t_0}, y_{t_1}, y_{t_2}, \dots, y_{t_{\text{тек}}}]^T. \quad (10)$$

Поскольку аномалии объема, которые мы рассматриваем, имеют протяженность во времени, в отличие от исходной зависимости трафика, имеющей явно выраженный пульсирующий характер, до применения метода контрольных карт целесообразно провести усреднение соседних отсчетов на временном интервале, соответствующем минимальному периоду времени ожидания аномалии. Это позволит усилить максимумы зависимости трафика от времени в протяженных периодах превышений объема и сгладить кратковременные выбросы, связанные с особенностями сетевых протоколов. Именно, поскольку сеансы телеконференцсвязи проходят обычно в течение десятков минут, будем рассматривать аномалии объема, длящиеся единицы минут. Данные с сетевого оборудования поступают обычно гораздо чаще, поэтому исходные замеры заменим на результат усреднения с соседними значениями исходной функциональной зависимости трафика. В дальнейшем будем работать с вектором Y^* :

$$Y^* = [y_{t_0}^*, y_{t_1}^*, y_{t_2}^*, \dots, y_{t_{\text{тек}}}^*]^T, \quad (11)$$

где

$$y_{t_i}^* = \begin{cases} \frac{1}{2J+1} \sum_{k=i-J}^{i+1+J} y_{t_k}, & \text{если } J \leq k \leq N-J \\ \frac{1}{2J+1} \sum_{k=0}^{2J} y_{t_k}, & \text{если } k < J \\ \frac{1}{2J+1} \sum_{k=N-(2J+1)}^N y_{t_k}, & \text{если } k > N-J \end{cases}, \quad (12)$$

где N — количество отсчетов измерений трафика, соответствующее временным меткам $t_0, t_1, \dots, t_{\text{тек}}$. Интервал усреднения содержит $2J+1$ исходных отсчетов трафика, $(J+1)$ — центральная точка в интервале усреднения). Значение J нетрудно найти — если соседние отсчеты исходной зависимости объема трафика от времени расположены через интервалы Δt , а минимальный интересующий интервал аномалии объема T_A , то из условия

$$T_A = \Delta t (2J+1) \quad (13)$$

следует, что

$$J = \left\lceil \frac{T_A - \Delta t}{2\Delta t} \right\rceil. \quad (14)$$

Условия в выражении (12) интерпретируются следующим образом: если считаем среднее значение для точки, которая находится на расстоянии больше либо равном половине T_A , то считаем по обычной формуле среднего. Если же еще не подошли к половине интервала T_A и данных для усреднения еще не набрали, то установим для всех этих точек первое значение, которое можно посчитать по формуле среднего. Аналогично для завершающих временных отсчетов: если остались точки, от которых до последней точки

массива меньше половины T_A , то для таких точек устанавливаем значение, которое удалось посчитать последним по формуле среднего.

Далее используем первую часть равенства (7), с учетом (11):

$$z_t = \lambda y_t^* + (1 - \lambda) z_{t-1}. \quad (15)$$

Левая часть выражения (15) представляет собой отсчеты зависимости, сравнение значений которых с порогами, определяемыми выражением (9) позволит говорить о наличии либо отсутствии аномалии объема.

Способ получения данных об аномалиях объема в универсальной системе мониторинга ZABBIX. В настоящее время существует достаточное число систем мониторинга, которые могут применяться в промышленных масштабах — на сотнях, тысячах и более узлов мониторинга, в общей сложности с узлов мониторинга при этом могут собираться до миллиона метрик и более. Мы не делаем акцент на выборе системы мониторинга, задача выбора достаточно сложна и зависит от многих факторов. В данной работе мы исходили из того, что система мониторинга должна свободно распространяться по лицензии GPL и, кроме этого, ориентировались на результаты обзора некоторых систем, приведенного в [8]. Результаты сравнения систем мониторинга, полученные в работе [8] можно кратко проиллюстрировать с помощью таблицы.

Некоторые характеристики систем мониторинга с лицензией GPL

Система	Автоматическое обнаружение	Поддержка SNMP	Плагины	Система оповещений	Способ хранения данных	Лицензия
Cacti	Через плагин	Да	Да	Через плагин	RRDTool	GPL
Nagios	Через плагин	Через плагин	Да	Да	RRDTool, MySQL через плагин	GPL
Zabbix	Да	Да	Да	Да	Oracle, MySQL, PostgreSQL, IBM DB2, SQLite	GPL

Zabbix позволяет изменять конфигурацию системы несколькими способами: через веб-интерфейс и посредством API (Application Program Interface). Конфигурация хранится в базе данных, это позволяет применять её «на лету», в отличие от Nagios. За счет распределенной архитектуры и использования прокси легко масштабируется, поскольку база данных может храниться на одном сервере, сервер приложения — на втором, а интерфейс конечного пользователя — на третьем. Также есть возможность распределять нагрузку по нескольким прокси-серверам, которые делят очереди опросов объектов мониторинга между собой, тем самым высвобождая ресурсы основного сервера приложения. Мощная система оповещений ZABBIX позволяет использовать оповещения и автоматические действия на основе заготовленных сценариев при достижении пороговых значений наблюдаемых метрик.

С учетом принципов работы выбранной системы мониторинга методика настройки получения в системе значений отсчетов согласно формуле (15) и принятия решения на основании сравнения получаемых значений согласно формуле (9) будет выглядеть следующим образом.

Во-первых, в системе мониторинга настраивается сбор данных с граничного маршрутизатора, за которым расположен сервер видеоконференцсвязи, по протоколу

SNMP. Существует достаточное число готовых шаблонов сетевого оборудования для решения этой задачи, например, для устройств Mikrotik и CISCO рабочие шаблоны можно взять из источников, указанных в [9]. В известных шаблонах сетевых устройств всегда присутствуют механизмы Auto Discovery (автоматического обнаружения) интерфейсов, в этой связи интересующая нас метрика, соответствующая исходящему транзитному трафику, и данные по ней появятся автоматически через некоторое время после начала сбора данных.

Во-вторых, с использованием механизма User Parameters настраивается расчет и сбор данных согласно формулам (11) и (12). При этом нужная нам метрика, назовем ее `IDSEWMA.getIntXminAvg`, создается вручную, сбор ее значений настраивается через те же временные интервалы, что и сбор значений на этапе 1. Получение данных для усреднения обеспечивается с помощью метода программного интерфейса `API history.get` [9], который вызывается с указанием временного интервала, ограниченного отметкой текущего времени сверху и отметкой текущего времени минус интервал ожидания аномалии T_A из формулы (13) снизу. После получения данных в формате JSON данные преобразуются в ассоциативный массив, подсчитывается число попавших в него элементов, рассчитывается среднее и результат выдается в качестве результата метрики при обращении к ней.

В-третьих, с использованием механизма User Parameters настраивается расчет и сбор данных согласно формуле (15). При этом нужная метрика, назовем ее `IDSEWMA.getEWMAVal`, создается вручную, сбор ее значений настраивается через те же временные интервалы, что и сбор значений на этапах 1 и 2, возможность работы с элементами Z_t и Y_t^* , Z_{t-1} обеспечивается так: с помощью метода программного интерфейса `API history.get` выбираются значения из созданных метрик `IDSEWMA.getEWMAVal`, `IDSEWMA.getIntXminAvg`. В последних случаях метод `history.get` вызывается с указанием временного интервала, ограниченного отметкой текущего времени сверху и отметкой текущего времени минус два интервала Δt из формулы (12) снизу. После получения данных в формате JSON и преобразования их в ассоциативные массивы выбираем последний элемент из массива данных метрики `IDSEWMA.getEWMAVal` (на практике этот массив после указанной выборки получался с содержанием всего одного элемента), он соответствует значению Z_{t-1} , и последний элемент из массива данных `IDSEWMA.getIntXminAvg` (на практике этот массив после указанной выборки получался с содержанием всего двух элементов — последнего и предпоследнего) — он содержит Y_t^* . Далее рассчитывается значение Z_t согласно формуле (14) и результат выдается в качестве результата метрики при обращении к ней.

В-четвертых, по значениям Z_t выносятся решение о наличии либо отсутствии аномалии объема. Обеспечить решение этой задачи, а также оперативное информирование о ситуации целесообразно с помощью встроенного механизма триггеров ZABBIX и встроенного механизма оповещений. Триггер настраивается вручную, данные для него рассчитываются заранее.

При апробации методики, приведенной в данной работе, обёрточные скрипты, обеспечивающие получение данных для ZABBIX на этапах два и три были написаны на shell, в них, в свою очередь, содержался вызов процедур, написанных на консольном php, при создании функций на php была использована библиотека `ZabbixApi.php` [10]. Стенд мониторинга работал на виртуальной машине с операционной системой Linux CentOS7 64x. Данные для триггера, инициирующего отправку оповещений о тревоге по

e-mail, рассчитывались заранее в среде MathCad в соответствии с формулой (9), для подготовки исходных данных для MathCad был написан отдельный php скрипт, который выгружал данные по трафику транзитного маршрутизатора за выбранные сутки в текстовый файл с помощью уже упоминавшегося метода `history.get`. Изначально шаблон сбора данных с граничного маршрутизатора обеспечивал при отправке по SNMP интервал между соседними отсчетами трафика, равный 2 секундам, но, поскольку такой механизм сам по себе приводил к появлению кратковременных интервалов с провалами данных, интервал между соседними отсчетами был увеличен до 5 секунд. Так в нашем случае проблему с провалами данных удалось решить.

Для более полной автоматизации процедуру регулярного поиска данных для триггера можно было бы выполнять, например, делая расчеты по планировщику заданий с некоторой периодичностью и меняя значение триггера автоматически, например, с помощью метода `API trigger.update`, но по ряду причин решение этой задачи не производилось.

Примеры результатов работы алгоритма контрольных карт в системе мониторинга ZABBIX. Приведенные ниже данные и рисунки соответствуют проведению сеанса телеконференцсвязи 30.04.2020 в период времени 09:45...11:30 с числом участников около 10 с помощью системы Web-конференций Open Meetings с участием докладчика с Web камерой с разрешением 360x240 и микрофоном, а также с графической презентацией и остальных участников без камеры и микрофона в режиме чата и просмотра видео.

На рис. 1 приведена зависимость исходящего транзитного трафика, на рис. 2 — та же зависимость, усредненная на интервале 2 минуты. Вид кривых на рис. 1 и 2, а также на рис. 3 и 4 позволяет представить, как с помощью усреднения на временном интервале высокочастотные изменения значений функции трафика от времени сглаживаются и остаются протяженные во времени изменения.

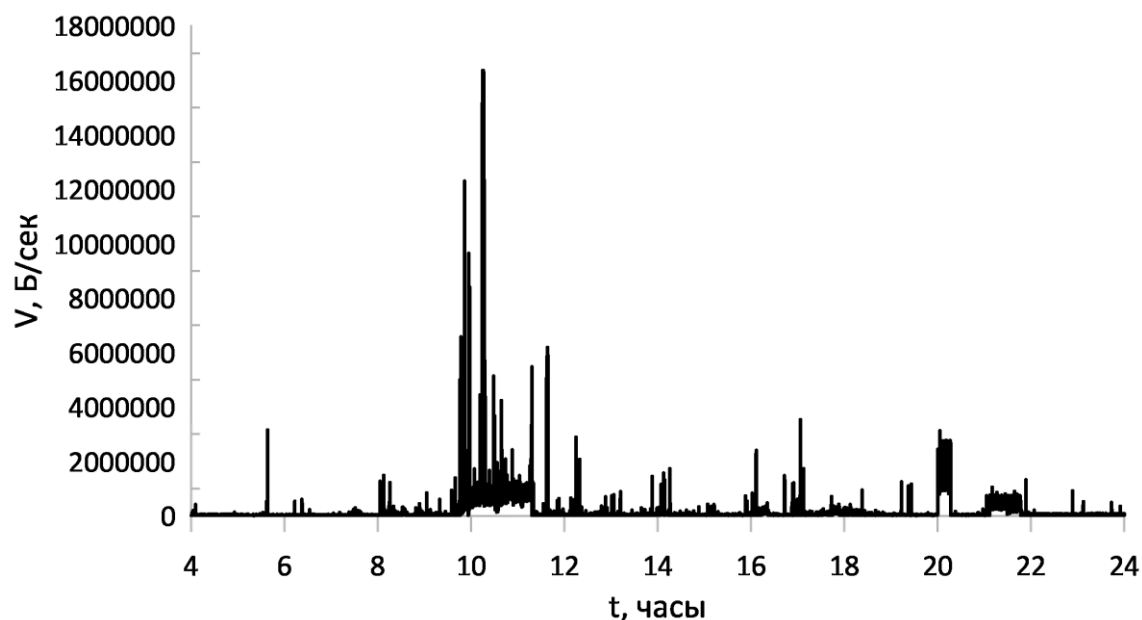


Рис. 1. Исходная зависимость

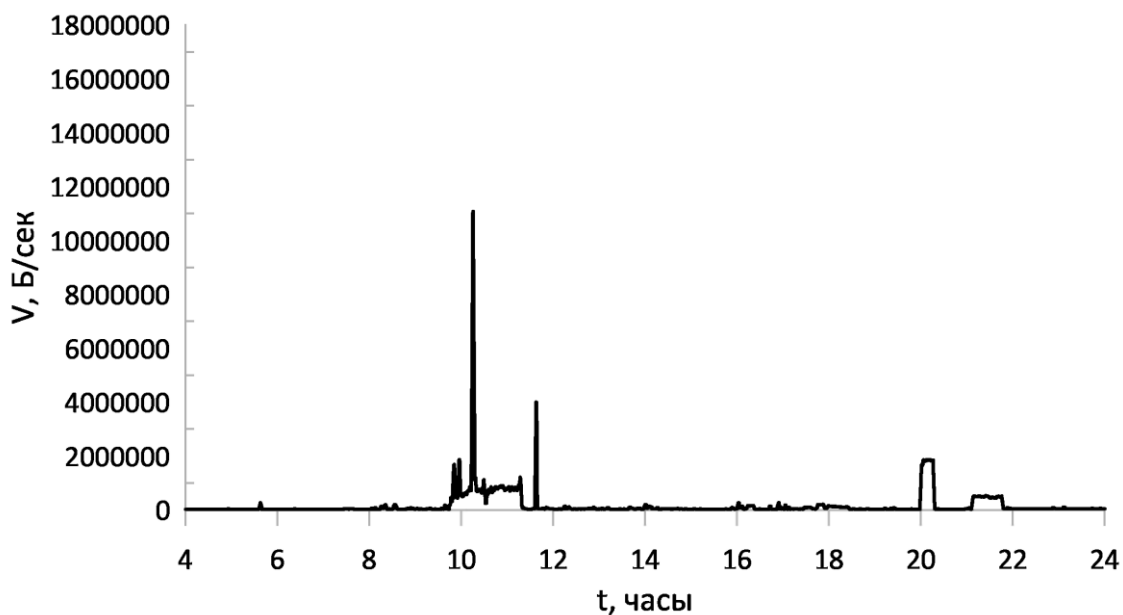


Рис. 2. Зависимость, значения которой усреднены в скользящем окне на интервале две минуты

Расчеты по формуле (15) были выполнены для разных значений и приведены на рис. 5 для трех значений λ , равных 0,1, 0,01, 0,001.

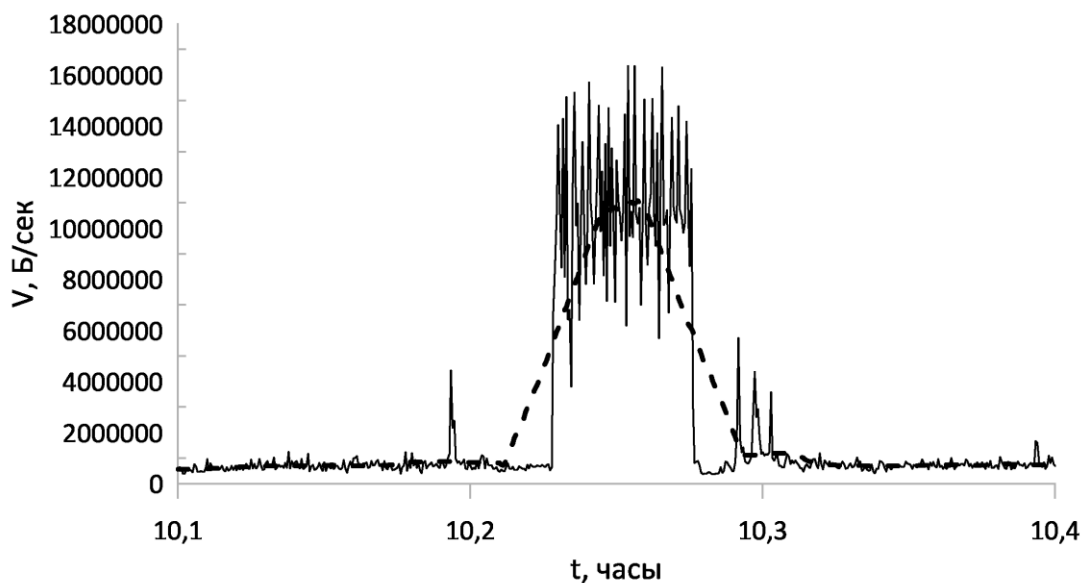


Рис. 3. Исходная зависимость (сплошная линия) и усредненная в скользящем окне на интервале две минуты (пунктир) на крупном масштабе в окрестности времени 10:15

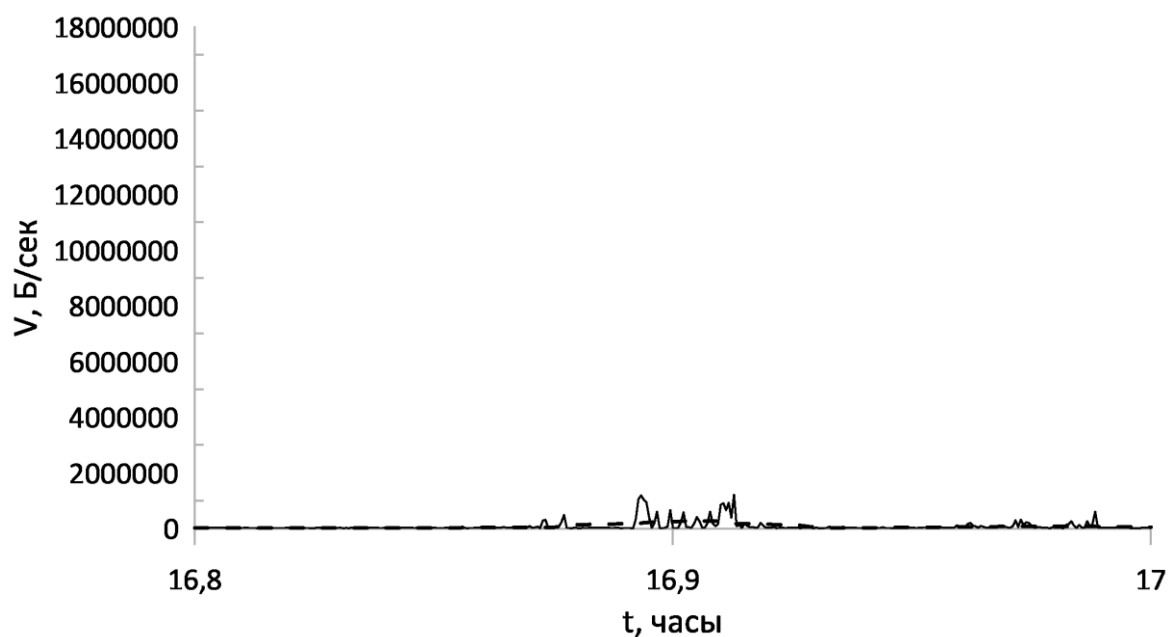


Рис. 4. Исходная зависимость (сплошная линия) и усредненная в скользящем окне на интервале две минуты (пунктир) на крупном масштабе в окрестности времени 16:55

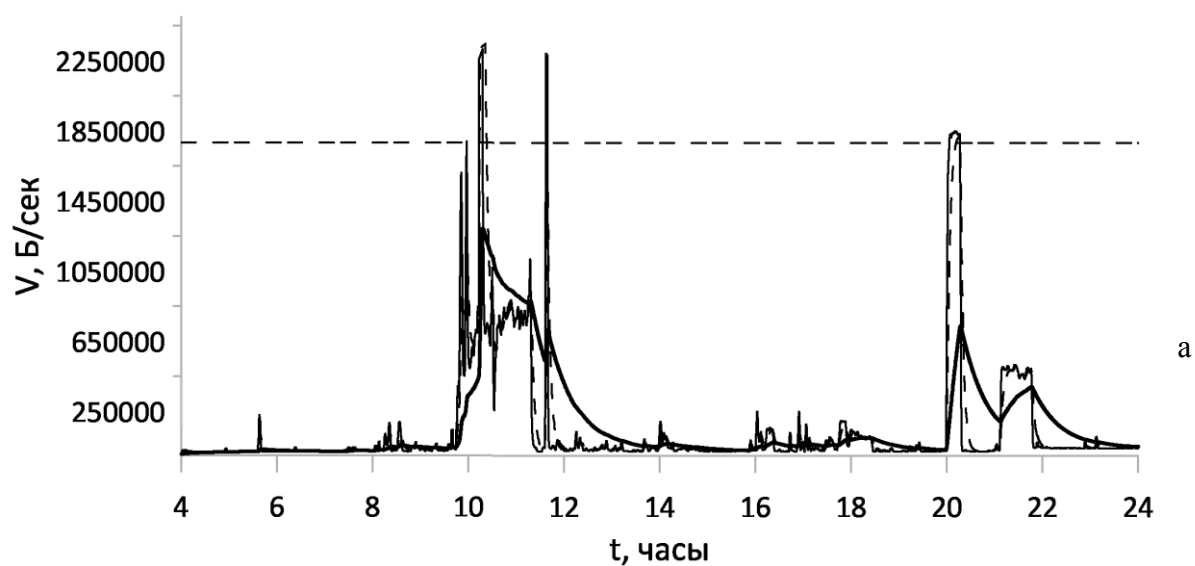


Рис. 5. Результаты вычисления значений z_t согласно формуле (15). Тонкая линия соответствует $\lambda = 0,1$, пунктирная линия — $\lambda = 0,01$, толстая линия — $\lambda = 0,001$, двойной пунктирной линией показана верхняя граница UPL

На рис. 6 приведен пример окна Web-интерфейса настроенной в соответствии с рассматриваемой задачей системы мониторинга ZABBIX в условиях минимального исходящего транзитного трафика.

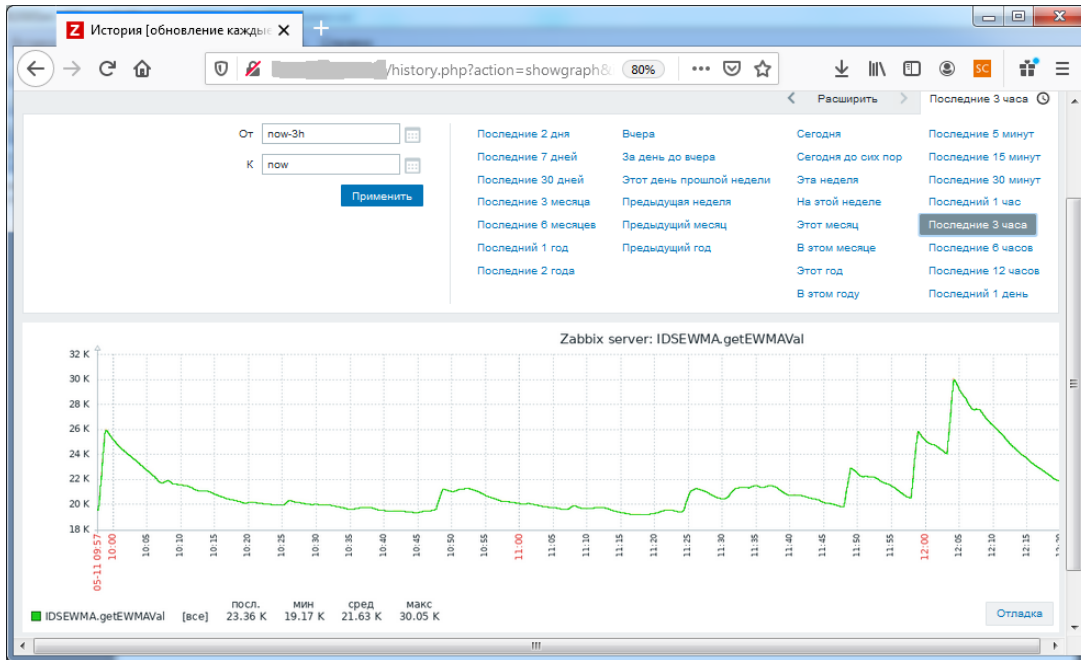


Рис. 6. Пример окна системы мониторинга ZABBIX с отсчетами Z_t в условиях минимального транзитного трафика

Обсуждение результатов. В условиях полученных данных за сутки, в которых проводился съем информации, имели значения $\mu_0 = 159.946 \cdot 10^3$ байт/с (примерно 160 Кбайт/с), $\sqrt{\sigma^2} = 541,035 \cdot 10^3$ байт/с (примерно 540 Кбайт/с). Кривая экспоненциально сглаженного среднего (15) пересекала UPL — верхний порог тревоги в моменты времени 10:30, 11:30, 20:10, сам верхний порог $\mu_0 + 3\sqrt{\sigma^2} = 1783,051 \cdot 10^3$ байт/с (примерно 1,8 Мбайт/с или 14,4 Мбит/с), нижний порог не рассматриваем, т.к. уменьшение трафика нас не интересует. Приведенные на рис. 5 кривые позволяют говорить, что алгоритм обнаружения устойчиво сработал не только для рекомендованного для формулы (9) диапазоном значения $\lambda = 0,1$, но и для выходящего за рекомендованный диапазон значения $\lambda = 0,01$. Этот факт можно объяснить предложенным нами дополнительным сглаживанием зависимости (10) с помощью окна скользящего среднего с длительностью, соответствующей минимальной временной протяженности ожидаемой аномалии по формулам (11) — (14). В некотором смысле такое сглаживание можно рассматривать как одновременный учет не только данных по текущей точке, но и данных по соседним замерам, и альтернативным вариантом сглаживанию с помощью скользящего среднего как раз является рассмотрение идущих подряд нескольких превышений порога тревоги для вынесения окончательного решения об аномалии в альтернативных подходах других исследователей. Однако при еще меньшем значении $\lambda = 0,001$ кривая Z_t опустилась значительно ниже и ни одного момента тревоги зафиксировано не было.

В качестве дополнительной задачи оценим долю трафика системы видеоконференцсвязи в общем исходящем транзитном трафике, зафиксированном на граничном маршрутизаторе. Для этого проведем сравнение данных о трафике, полученных с граничного маршрутизатора и данных, полученных с интерфейса сервера видеоконференцсвязи, а также вспомним графики 1, 2. Совместный анализ кривых позволяет заключить, что зависимость полного исходящего транзитного трафика через маршрутизатор в нашем случае практически полностью повторяет зависимость исходящего трафика системы видеоконференцсвязи.

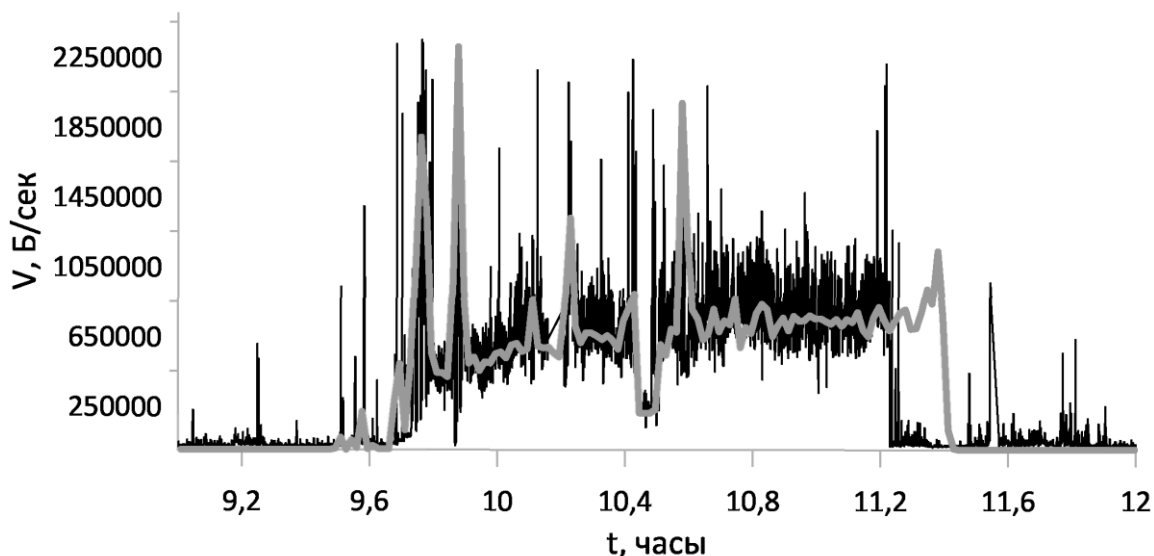


Рис. 7. Зависимости исходящего транзитного трафика с граничного маршрутизатора (сплошная тонкая линия) и с сервера видеоконференцсвязи (толстая полупрозрачная линия)

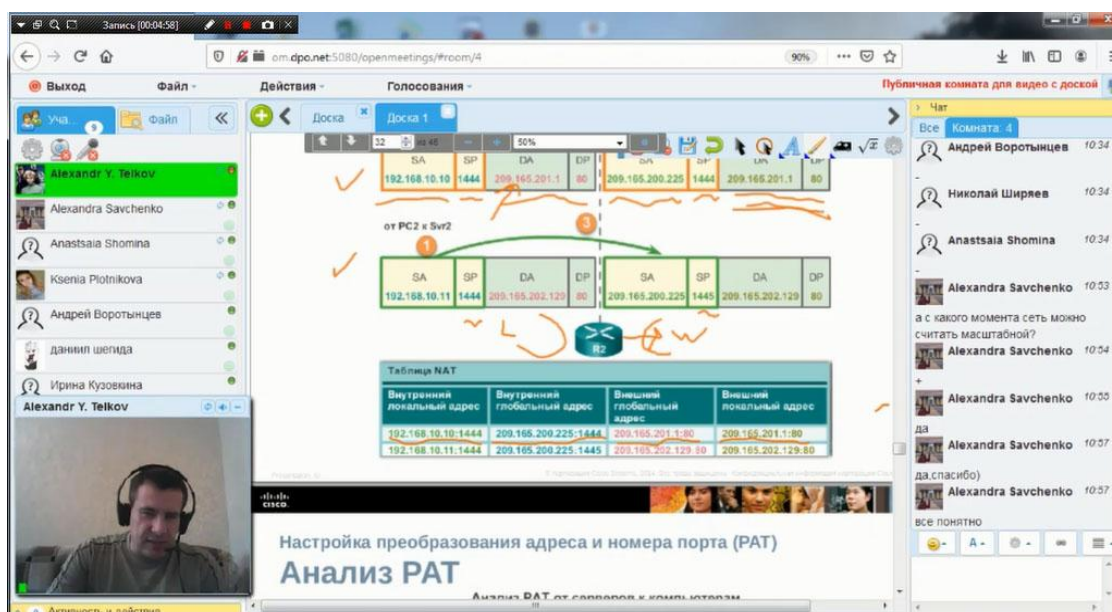


Рис. 8. Снимок экрана системы Web-видеоконференцсвязи Open Meetings в один из моментов трансляции контента участникам телеконференции

Для полноты картины приведем еще данные, соответствующие характеристикам загрузки одиночных каналов участников телеконференции. Меньшая изрезанность одной из зависимостей на рис. 7 объясняется тем, что в шаблоне маршрутизатора съем данных производился с интервалом 1 раз в 2 секунды, а на сервере конференцсвязи с частотой 2 раза в минуту (в соответствии с ZABBIX шаблонами маршрутизатора Mikrotik и OS Linux). Зависимости на рис. 7 имеют совпадающие зоны максимумов, которые соответствуют моментам подключения пользователей.

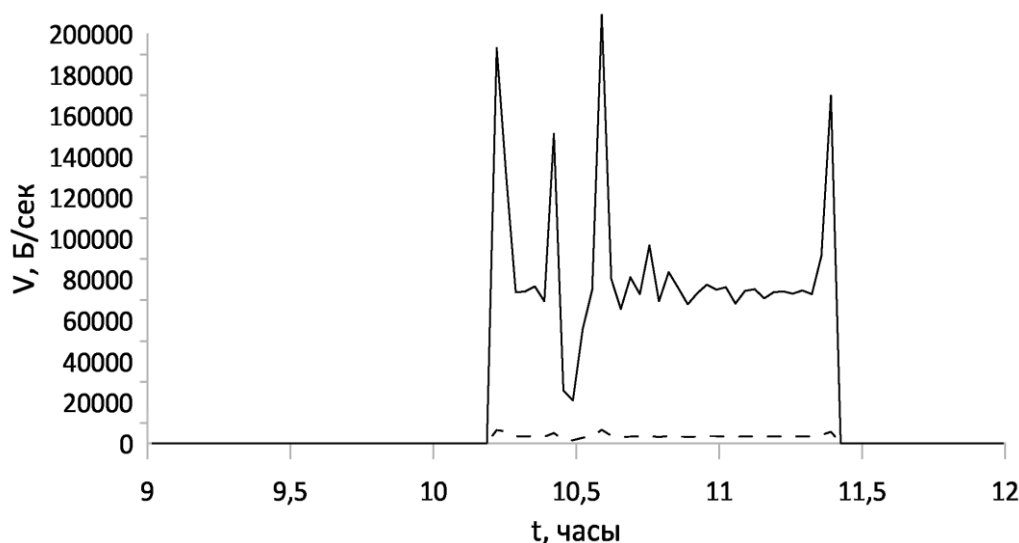


Рис. 9. Зависимости трафика типового участника телеконференции (прием видео и аудио, активное участие в конференции — в режиме чата): сплошная линия — входящий трафик, пунктирная — исходящий.

Кроме того, перерыв в середине сеанса видеосвязи нашел отражение в виде пяти-минутной площадки минимума на графиках. Отличия кривых на рис. 7 в конечной части периода видеосвязи обусловлены потерями данных SNMP от маршрутизатора, о которых упоминалось в начале практической части работы. В период телеконференции ширина канала, требующегося серверу телеконференцсвязи для передачи информации всем участникам, составила в среднем 6,5 Мбит/сек. При этом транслировались Web-камера и звук одного участника, общая доска с презентацией, а также групповой чат между всеми участниками конференции. Рядовому участнику телеконференции, принимающему аудио- и видеопоток и активно участвующему в телеконференции в режиме чата, необходим канал в нисходящем направлении шириной минимум 80 Кбит/сек и в восходящем направлении шириной минимум 5 Кбит/сек. Организатору телеконференции, демонстрирующему презентацию, передающему и принимающему аудио- и видеопоток и активно участвующему в телеконференции в режиме чата, необходим канал в нисходящем направлении шириной минимум 80 Кбит/сек и в восходящем направлении шириной минимум 80 Кбит/сек. Еще раз отметим, что оценки получены для конкретного программного обеспечения и конкретных настроек технических средств участников и не являются общими для всех возможных случаев организации телеконференций.

Заключение. В работе предложена методика настройки продукционной системы мониторинга ZABBIX, обеспечивающая практическое решение задач обнаружения протяженных аномалий объема сетевого трафика методом контрольных карт. Возможность

получения исходных данных в рамках данной методики обеспечивается применением типовых шаблонов сетевых устройств. Возможность извлечения данных для первичного и последующих рекурсивных расчетов обеспечивается с помощью механизма ZABBIX User Parameters. Рекурсивное использование данных на конечных этапах расчета обеспечивается использованием функций ZABBIX API совместно с ZABBIX User Parameters, причем в качестве определенных пользователем параметров выступают результаты некоторых действий над данными, попавшими в базу данных системы мониторинга в более ранние периоды времени. Принятие решений о тревоге и инициирование оповещений о соответствующих событиях обеспечивается встроенными в ZABBIX механизмами триггеров и оповещений. Предложенный подход позволяет в короткие сроки реализовать обнаружение сетевых аномалий объема с использованием существующих программных средств мониторинга без кардинальной перестройки состава этих средств и без перепределения способов сбора исходных данных. В сложившихся условиях целесообразно рекомендовать данное решение для контроля транзитных каналов систем внутрикорпоративной телеконференцсвязи и своевременного планирования и принятия решений, касающихся использования ресурсов.

Другой возможной областью применения предложенного решения может стать задача контроля времени просмотра потокового видео с систем видеонаблюдения удаленных объектов. Например, регламент работ центров мониторинга может предполагать периодическое подключение к удаленным серверам видеонаблюдения для визуального контроля обстановки в течение нескольких минут. Если удаленный объект подключен через сети сотовой связи по технологии пакетной передачи данных, то при забытом подключении программы-видеоклиента трафик между рабочим местом оператора видеонаблюдения и сервером видеонаблюдения может составить десятки гигабайт. Такие значения могут превысить месячный лимит объема трафика, предоставляемого типовым оператором сотовой связи за период от нескольких часов до несколько десятков часов, и связь будет отключена, что недопустимо.

ЛИТЕРАТУРА

1. Интернет-трафик в Европе вырос в полтора раза. Магистральные провайдеры фиксируют рекорды нагрузки // Блог компании «Дата-центр Миран»: Сетевые технологии, исследования и прогнозы в IT, статистика в IT, сетевое оборудование [Электронный ресурс]. — URL: <https://habr.com/ru/company/dcmiran/blog/496542/>
2. Шелухин О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. — М. : Горячая линия — Телеком, 2019. — 448 с.
3. Tang D., Chen K., Chen X., Liu H., Li X. Adaptive EWMA Method Based on Abnormal Network Traffic for LDoS Attacks // Mathematical Problems in Engineering. — Vol. 2014. — Article ID 496376, 11 pages [Электронный ресурс]. — URL: <http://dx.doi.org/10.1155/2014/496376>
4. Cisar P., Bosnjak S., Cisar S. EWMA Algorithm in Network Practice // Int. J. of Computers, Communications & Control. — 2010. — Vol. V. — No. 2. — P. 160—170 [Электронный ресурс]. — URL: <https://www.semanticscholar.org/paper>
5. Семенов Н. А., Телков А. Ю. Применение статистических методов обнаружения DoS атак в локальной сети // Вестник ВГУ. Серия: Системный анализ и информационные технологии. — 2012. — № 1. — С. 82—87.

6. Ye N., Borror C., Zhang Y. EWMA techniques for computer intrusion detection through anomalous changes in event intensity // *Quality and reliability engineering international*. — 2002. — V. 18. — P. 443—451 [Электронный ресурс]. — URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/qre.493>
7. Шелухин О. И., Филинова А. С., Васина А. В. Обнаружение аномальных вторжений в компьютерные сети статистическими методами // *T-Comm: Телекоммуникации и транспорт*. — 2015. — Т. 9. — № 10. — С. 42—49.
8. Шардаков К. С. Сравнительный анализ популярных систем мониторинга сетевого оборудования, распространяемых по лицензии GPL // *Интеллектуальные технологии на транспорте*. — 2018. — № 1. — С. 44—48.
9. ZABBIX. Документация [Электронный ресурс]. — URL: <https://www.zabbix.com/ru/manuals>
10. Zabbix API client for PHP with session cache and SSL management [Электронный ресурс]. — URL: <https://github.com/intellitrend/zabbixapi-php>

REFERENCES

1. Internet-trafik v Evrope vyiros v poltora raza. Magistralnyie provayderyi fiksiruyut rekordyi nagruzki // *Blog kompanii «Data-tsentr Miran»: Setevyie tehnologii, issledovaniya i prognozyi v IT, statistika v IT, setevoe oborudovanie* [Elektronnyiy resurs]. — URL: <https://habr.com/ru/company/dcmiran/blog/496542/>
2. Sheluhin O. I. Setevyie anomalii. Obnaruzhenie, lokalizatsiya, prognozirovanie. — M. : Goryachaya liniya — Telekom, 2019. — 448 s.
3. Tang D., Chen K., Chen X., Liu H., Li X. Adaptive EWMA Method Based on Abnormal Network Traffic for LDoS Attacks // *Mathematical Problems in Engineering*. — Vol. 2014. — Article ID 496376, 11 pages [Elektronnyiy resurs]. — URL: <http://dx.doi.org/10.1155/2014/496376>
4. Cisar P., Bosnjak S., Cisar S. EWMA Algorithm in Network Practice // *Int. J. of Computers, Communications & Control*. — 2010. — Vol. V. — No. 2. — P. 160—170 [Elektronnyiy resurs]. — URL: <https://www.semanticscholar.org/paper>
5. Semenov N. A., Telkov A. Yu. Primenenie statisticheskikh metodov obnaruzheniya DoS atak v lokalnoy seti // *Vestnik VGU. Seriya: Sistemnyiy analiz i informatsionnyie tehnologii*. — 2012. — # 1. — S. 82—87.
6. Ye N., Borror C., Zhang Y. EWMA techniques for computer intrusion detection through anomalous changes in event intensity // *Quality and reliability engineering international*. — 2002. — V. 18. — P. 443—451 [Elektronnyiy resurs]. — URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/qre.493>
7. Sheluhin O. I., Filinova A. S., Vasina A. V. Obnaruzhenie anomalnyih vtorzheniy v kompyuternyie seti statisticheskimi metodami // *T-Comm: Telekommunikatsii i transport*. — 2015. — Т. 9. — # 10. — С. 42—49.
8. Shardakov K. S. Sravnitelnyiy analiz populyarnyih sistem monitoringa setevogo oborudovaniya, rasprostranyaemyih po litsenzii GPL // *Intellectualnyie tehnologii na transporte*. — 2018. — # 1. — С. 44—48.
9. ZABBIX. Dokumentatsiya [Elektronnyiy resurs]. — URL: <https://www.zabbix.com/ru/manuals>
10. Zabbix API client for PHP with session cache and SSL management [Elektronnyiy resurs]. — URL: <https://github.com/intellitrend/zabbixapi-php>

СВЕДЕНИЯ ОБ АВТОРАХ

Телков Александр Юрьевич. Доцент кафедры информационной безопасности. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: telkov@dpo-it.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 200-52-43.

Данилова Ольга Юрьевна. Доцент кафедры математики и моделирования систем. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: danilova_olga@hotmail.com

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 200-52-13.

Телкова Светлана Анатольевна. Доцент кафедры математики и моделирования систем. Кандидат педагогических наук, доцент.

Воронежский институт МВД России.

E-mail: tsa76@inbox.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 200-52-13.

Telkov Aleksandr Yurievich. The Assistant Professor of the chair of Information Security. Candidate of Physical and Mathematical Sciences, Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: telkov@dpo-it.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-43.

Danilova Olga Yur'evna. Assistant Professor of the chair of Mathematics and Modeling Systems. Candidate of Physical and Mathematical Sciences, Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: danilova_olga@hotmail.com

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-13

Telkova Svetlana Anatolievna. Assistant Professor of the chair of Mathematics and Modeling Systems. Candidate of Pedagogical Sciences, Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: tsa76@inbox.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-13.

Ключевые слова: обнаружение сетевых аномалий объема; алгоритм обнаружения EWMA; контрольные карты.

Key words: network volume anomaly detection; EWMA detection algorithm; control cards.

УДК 621.391.01