УДК 004.056.53 Вестник УрФО № 1(31) / 2019, с. 17–22

Карташевский В. Г., Поздняк И. С.

DOI: 10.14529/secur190103

ФИЛЬТРАЦИЯ НАБЛЮДАЕМОГО ТРАФИКА КАК СПОСОБ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

В работе предлагается вариант обнаружения аномальной составляющей наблюдаемого трафика на основе его обработки линейным фильтром с известной импульсной характеристикой. На основе сравнения текущего значения среднеквадратической ошибки фильтрации с «эталонным» значением, полученным при фильтрации трафика без аномалий, возможно обнаружение атак, изменяющих статистические свойства трафика. При фильтрации трафика без аномалий «эталонное» значение среднеквадратической погрешности фильтрации определяется взаимной корреляционной функцией наблюдаемого трафика без вторжений и трафика на выходе линейного фильтра с некоторой импульсной характеристикой. Последняя определяется корреляционными свойствами «эталонного» трафика. Наличие вторжения в наблюдаемый трафик изменяет его корреляционные свойства, что приводит к заметному увеличению среднеквадратической погрешности фильтрации. Такой анализ позволит определить вредоносную составляющую трафика.

Ключевые слова: *среднеквадратическая ошибка фильтрации, трафик, как случайный процесс с заданными вероятностно-временными характеристиками, взаимно-корреляционная функция.*

Kartashevskiy V. G., Pozdnyak I. S.

FILTERING OBSERVED TRAFFIC AS A METHOD OF INTRUSION DETECTION

The paper proposes a detection option of the anomalous component of the observed traffic based on traffic processing by a linear filter with a known impulse response. Based on a comparison of the current value of the mean-square filter error with the "reference" value obtained by filtering traffic without anomalies, it is possible to detect attacks that change the statistical properties of the traffic. When filtering traffic without anomalies, the mean square filter error is determined by the cross correlation function of the observed traffic without intrusions and traffic at the output of the linear filter. The impulse response of such traffic is determined by the correlation properties of the "reference" traffic. The presence of an intrusion into the observed traffic changes its correlation properties. This leads to a noticeable increase in the mean-square filter error. Such an analysis will determine the anomalous component of traffic.

Keywords: *mean-square filter error, traffic as a random process with given probability-time characteristics, cross correlation function, network traffic.*

На сегодняшний день актуальной задачей является создание наиболее эффективных способов обнаружения аномальных событий в мультисервисной сети, которые могут являться следствием несанкционированных воздействий, как внутренних, так и внешних. Для этого в корпоративных сетях используются современные системы обнаружения вторжений (СОВ), которые представляют собой самостоятельный продукт или могут являться дополнением к имеющемуся комплексу средств защиты. Такие системы работают наиболее эффективно, если заранее известны характеристики атаки (вторжения). Однако, реализовать это не всегда удается, потому что злоумышленник постоянно меняет способы проникновения.

В настоящее время существует множество методов обнаружения вторжений в компьютерные сети, которые направлены на выявление как известных, так и неизвестных атак и вторжений. В современных системах выделяют несколько принципов обнаружения вторжений:

- Статистические методы обнаружения аномалий;
- Методы, основанные на использовании нейронных сетей;
- Сигнатурный анализ трафика.

Множество работ посвящено описанию, обнаружению и классификации вторжений с применением различных методов. К таким относятся работы следующих авторов: О.И. Шелухина, А. А. Браницкого, И. В. Котенко, Г.А. Максименко, Н.А. Соловьева, M. Panda, Е. В. Зубкова, В. М. Белова, S. Zhao и др. [1 – 7].

При создании новых СОВ, которые бы позволили фиксировать новые и видоизмененные атаки, необходима разработка и исследование комбинированных методов обнаружения атак, сочетающих различные традиционные методы и способы обнаружения модифицированных атак.

Применение методов статистического анализа является наиболее распространенным видом реализации технологии обнаружения аномального поведения. Универсальность данного способа заключается в том, что для проведения анализа сетевого трафика не требуется знание сигнатур (некого шаблона с набором правил и признаков) возможных атак и используемых ими уязвимостей. Анализируются лишь аномалии (отклонения от нормального вида) в сетевом трафике. Поэтому становится возможным выявление ранее неизвестных видов атак. Примером аномального поведения может являться, например, большое число соединений в единицу времени, что характерно для DDoS-атаки. Обнаружение аномалий на основе статистических методов может осуществляться в режиме реального времени.

Для применения статистических методов анализа трафика TCP/IP следует определить основные показатели, которые характеризуют полноценное функционирование сетевой инфраструктуры, и осуществлять постоянный контроль за их состоянием [1]. В качестве таких показателей должны использоваться информация, по которой можно отследить сетевое взаимодействие внутри системы. К данным, которые могут быть проанализированы при захвате трафика относятся, например, поля заголовков IP, TCP, UDP, ICMP и содержимое поля данных.

Предполагается, что причинами аномального поведения трафика является значительное изменение некоторых параметров трафика. Качество результатов обнаружения зависит не только от выбранного способа обнаружения аномалий. Также важным является выбор характеристик предлагаемого трафика, которые наиболее чувствительны к событиям, связанным с администрированием сети (сетевые сбои) и вызванным полезным трафиком. Это необходимо для того, чтобы не получать большое число ложных срабатываний.

Кроме того, в работе [8] показан еще один способ, доказывающий, что при любых условиях о наличие подозрительного трафика можно судить по форме фазового аттрактора системы. При этом показатель Херста не указывает однозначно на наличие атаки в сети.

Использование структуры фазового портрета телекоммуникационного трафика позволит дать достоверную оценку его состояния. В работе [8] определен вид фазового аттрактора мультисервисного трафика при трех различных состояниях сети: нормальном (полезный трафик), подозрительный трафик во всем интервале исследования (длительная атака), подозрительный трафик на небольшом временном интервале опреде-

ленной длины (непродолжительная атака). Также приводятся виды фазового портрета трафика мультисервисной сети в перечисленных выше состояниях, по которым можно судить о наличие или отсутствии атаки.

Оценка линейного преобразования

При статистическом методе обнаружения аномалий могут применяться различные подходы. В данном случае предлагается анализ среднеквадратической ошибки фильтрации трафика на заданном интервале времени для принятия решения о фиксации аномалий в сетевом трафике.

Будем рассматривать задачу оценки (фильтрации) линейного преобразования наблюдаемого случайного процесса x(t), который является суммой полезного трафика $\xi(t)$ и процесса $\eta(t)$, характеризующего вторжение, атаку или аномальный трафик, т.е.

$x(t)=\xi(t)+\eta(t)$.

Линейное преобразование случайного процесса $\xi(t)$ представим в виде

$$\chi(t)=\int_{-\infty}^{\infty} g(t,\tau)\xi(\tau)d\tau. \qquad (1)$$

где $g(t,\tau)$– некоторая заданная функция.

Если предположить, что $\chi(t)$ реализуется некоторым фильтром на конечном интервале *(t–T ,t)* с импульсной характеристикой $g(t,\tau)$, то выражение (1) перепишется в виде:

$$\chi(t)=\int_{0}^{T} g(t,t-\tau)\xi(t-\tau)d\tau, \qquad (2)$$

Выбор $g(t,\tau)$ определяется требуемыми свойствами линейного преобразования *x(t)*, позволяющими по его реализации дать ответ о характере фильтруемого трафика.

Обозначим оценку линейного преобразования *x(t)* через $\hat{\chi}(t)$, схема формирования которой представлена на рисунке 1.

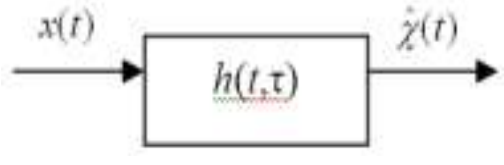

Рис. 1. Формирование оценки наблюдаемого трафика

Выражение для оценки $\hat{\chi}(t)$ имеет вид

$$\hat{\chi}(t)=\int_{0}^{T} h(t,t-u)x(t-u)dt,$$

где *h(t)* – импульсная переходная функция линейного фильтра.

В работе [9] показано, что среднее значение квадрата ошибки при использовании такой оценки равно

$$\varepsilon_{\chi}^{2}(t)=E\left\{\left[\chi(t)-\int_{0}^{T} h(t,t-u)x(t-u)du\right]^{2}\right\}=$$

$$=B_{\chi}(t,t)-2\int_{0}^{T} h(t,t-\tau)B_{x\chi}(t-\tau,t)d\tau+\int_{0}^{T}\int_{0}^{T}$$

$$h(t,t-u)h(t,t-\nu)B_{x\chi}(t-u,t-\nu)dud\nu,$$

где

$B_{x\chi}(t_1,t_2)=E\{x(t_1)\chi(t_2)\}=B_{\xi\chi}(t_1,t_2)+B_{\eta\chi}(t_1,t_2)$.

При минимизации $\varepsilon_{\chi}^{2}(t)$оценка $\hat{\chi}(t)$ получается фильтром с импульсной функцией $h^{*}(t,\tau)$, удовлетворяющей интегральному уравнению [9]

$$B_{x\chi}(t-\tau,t)=\int_{0}^{T} h^{*}(t,t-y)dy,\quad 0\le\tau\le T. \qquad (3)$$

При этом минимальное значение среднего квадрата ошибки имеет вид

$$\varepsilon_{\chi min}^{2}=B_{\chi}(t,t)-\int_{0}^{T} h^{*}(t,t-u)B_{x\chi}(t-u,t)du.$$

Если предположить локальную стационарность трафика, то

$$B_{x\chi}(\tau)=\int_{0}^{T} h^{*}(y)B_{x}(t-y)dy,\quad 0\le\tau\le T,$$

$$\varepsilon_{\chi min}^{2}=B_{\chi}(0)-\int_{0}^{T} h*(u)B_{x\chi}(u)du..$$

Различные виды линейного преобразования $\xi(t)$ отражаются только на выражениях корреляционной функции $B_{\chi}(t_1,t_2)$ и взаимной корреляционной функции $B_{x\chi}(t_1,t_2)$.

Для *x(t)* вида (1)

$$B_{\chi}(t,t)=\iint_{-\infty}^{\infty} g(t,\nu_1)g(t,\nu_2)B_{\xi}(\nu_1,\nu_2)d\nu_1 d\nu_2 \qquad (4)$$

и

$$B_{x\chi}(t_1,t_2)=\int_{-\infty}^{\infty} g(t_2,\nu)\left[B_{\xi}(t_1,\nu)+B_{\eta\xi}(t_1,\nu)\right]d\nu\ .$$

При этом оценку $\hat{\chi}(t)$ по реализации суммарного процесса *x(t)*, наблюдаемой на конечном интервале времени, можно трактовать как оценку, оптимальную по критерию минимума квадрата ошибки, процесса на выходе линейной системы с импульсной переходной характеристикой $g(t,\tau)$, если на входе действует $\xi(t)$.

Если на некотором интервале локальной стационарности предполагать известными статистические свойства полезного трафика $\xi(t)$, то можно попытаться выбрать импульсную характеристику $g(t,\tau)$ так, чтобы стати-

стические характеристики *x(t)* были предсказуемы.

Тогда из (4) для локально-стационарного процесса $\xi(t)$ в предположении, что параметры фильтра $g(t,\tau)$ постоянны, можно записать:

$$B_{\chi_\xi}(\tau) = \int_{-\infty}^{\infty} b_g(\theta) B_\xi(\tau-\theta)du, \quad (5)$$

где

$$b_g(\theta) = \int_{-\infty}^{\infty} g(u)g(u+\theta)du.$$

Выберем *g(u)* в виде $g(u) = B_\xi(u)$ и получим

$$b_g(\theta) = \int_{-\infty}^{\infty} B_\xi(u)B_\xi(u+\theta)du. \quad (6)$$

Пусть для примера

$$B_\xi(\tau) = \sigma_0^2(\tau_0 - |\tau|),\ -\tau_0 < \theta < \tau_0.$$

где σ_0^2 – мощность случайного процесса (рисунок 2).

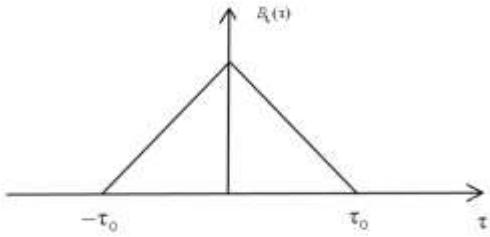

Рис. 2. Корреляционная функция $B_\xi(u)$

Такую корреляционную функцию может иметь последовательность пакетов случайной длительности и со случайным значением интервалов времени между пакетами.

Тогда (6) принимает вид:

$$b_g(\theta) = \int_{-\infty}^{\infty} \sigma_0^2(\tau_0 - |u|)\sigma_0^2(\tau_0 - |u| + \theta)du = \sigma_0^4\left(\frac{2\tau_0^3}{3} + \theta\tau_0^2\right).$$

График функции $b_g(\theta)$ представлен на рисунке 3.

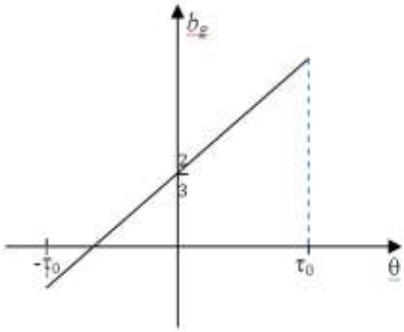

Рис. 3. Функция $b_g(\theta)$

Учитывая поведение функции $B_\xi(\tau)$ в дальнейшем будем заменять интервал интегрирования $(-\infty,\infty)$ интервалом $(-\tau_0,\tau_0)$.

Теперь для $B_{\chi_\xi}(\tau)$ из (5) можно получить:

$$B_{\chi_\xi}(\tau) = \sigma_0^6\left(\frac{2}{3}\tau_0^5 - \frac{4}{3}\tau_0^4\cdot|\tau|\right) \quad (7)$$

Вид $B_{\chi_\xi}(\tau)$ представлен на рисунке 4.

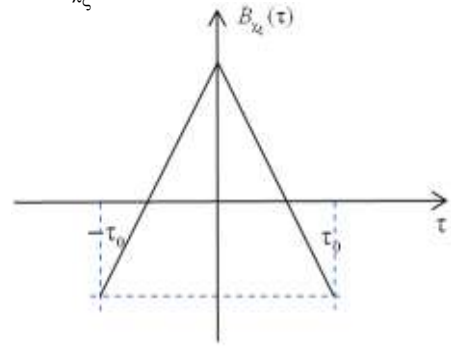

Рис. 4. Взаимная корреляционная функция $B_{\chi_\xi}(\tau)$

Рассмотрим функцию *x(t)*, формируемую согласно (2). Если $x(t) = \xi(t) + \eta(t)$, то

$$\chi(t) = \int_0^T g(t,\tau)\left[\xi(\tau) + \eta(\tau)\right]d\tau.$$

Рассмотрим компоненту $\chi(t)$, обусловленную процессом $\eta(t)$ при выборе

ре $g(t,\tau) = B_\xi(t,\tau)$.

$$\chi_\eta(t) = \int_0^T g(t,\tau)\eta(\tau)d\tau.$$

Теперь

$$B_{\chi_\eta}(\tau) = \int_{-\infty}^{\infty} b_g(\theta)B_\eta(\tau-\theta)d\theta. \quad (8)$$

Будем предполагать, что атака $\eta(t)$ обладает самоподобными свойствами. Тогда можно предположить, что $B_\eta(t)$ имеет вид [1] (см. рисунок 5):

$$B_\eta(\tau) = \sigma_\eta^2 e^{-\sqrt{\frac{\tau}{\tau_0}}}.$$

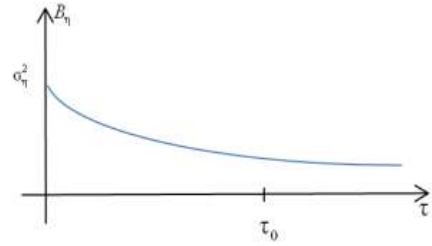

Рис. 5. Функция корреляции трафика вторжения

Используя разложение экспоненты в ряд с удержанием для простоты интегрирования двух членов разложения, а также стандартный интеграл

$$\int xX^{1/2}dx = \frac{2}{b^2}\left(\frac{X^{5/2}}{5} - \frac{aX^{3/2}}{3}\right),$$

где $X = a + bx$.

Теперь для $B_{\chi_\eta}(\tau)$ можно записать:

$$B_{X_\eta}(\tau)=\sigma_0^4\sigma_\eta^2\cdot\left\{\begin{array}{l}\frac{4}{3}\tau_0^4-\frac{4}{9}\tau_0^{\frac{5}{2}}\left[(\tau+\tau_0)^{\frac{3}{2}}-(\tau-\tau_0)^{\frac{3}{2}}\right]+\\ +2\tau_0^{\frac{3}{2}}\left(\frac{1}{5}\left[(\tau+\tau_0)^{\frac{5}{2}}-(\tau-\tau_0)^{\frac{5}{2}}\right]+\right.\\ \left.\frac{1}{3}\tau\left[(\tau-\tau_0)^{\frac{3}{2}}-(\tau+\tau_0)^{\frac{3}{2}}\right]\right)\end{array}\right\}. \quad (9)$$

Результат (9) получен в предположении, что интегрирование в (8) осуществлялось на интервале $(0,\tau_0)$, что обусловлено интервалом существования функции $b_g(\theta)$.

Сравним значения $B_{\chi_\xi}(\tau)$ и $B_{\chi_\eta}(\tau)$ в двух точках $\tau=0$ и $\tau=\tau_0$.

Для $B_{\chi_\xi}(\tau)$ из (7) следует:
при $\tau=0$, $B_{\chi_\xi}(\tau)=\sigma_0^6\cdot 0,67\tau_0^5$;
при $\tau=\tau_0$,

$$B_{\chi_\xi}(\tau)=\sigma_0^6\left(0,67\tau_0^5-1,33\tau_0^5\right)=-0,67\tau_0^5\cdot\sigma_0^6. \quad (10)$$

Для $B_{\chi\eta}(\tau)$ из (9) следует:
при $\tau=0$, $B_{\chi_\eta}(\tau)=1,29\sigma_0^4\sigma_\eta^2\tau_0^4$,
при $\tau=\tau_0$,

$$B_{\chi_\eta}(\tau)=\sigma_0^4\sigma_\eta^2\left(2,33\tau_0^4-0,94\tau_0^{\frac{5}{2}}\right). \quad (11)$$

Заключение

Итак, возможны две ситуации: $x(t)=\xi(t)$ и $x(t)=\xi(t)+\eta(t)$. Первый случай – трафик $\xi(t)$ является «типичным» для выбранного времени наблюдения и его статистические характеристики известны, т.е. известны корреляционные функции B_x и $B_{x\chi}$ при импульсной характеристике $h^*(\cdot)$, выбранной из решения интегрального уравнения (3). Тогда оценку $\hat{\chi}_1(t)$ можно считать известной, а также известным «эталонное» значение среднеквадратической ошибки $\varepsilon_\chi^2(t)$.

Во втором случае в составе *x(t)* присутствует $\eta(t)$ (вторжение, атака или аномальный трафик), и оценки $\hat{\chi}_2(t)$ будут существенно отличаться от оценок $\hat{\chi}_1(t)$ по значению $\varepsilon_\chi^2(t)$, что может служить основанием для дальнейшего анализа аномалии на предмет вторжения или изменений в полезном трафике, чтобы не допустить фиксации ложной тревоги.

В общем случае для вычисления значения $\varepsilon_\chi^2(t)$ требуется знание значений корреляционной функции $B_{x\chi}$, вычисляемой по формуле (3).

Упростить анализ рассматриваемой ситуации можно, ограничившись сравнением взаимных корреляционных функций $B_{\chi_\xi}(\tau)$ и $B_{\chi\eta}(\tau)$ в точке $\tau=\tau_0$.

Как следует из сравнения выражений (10) и (11) наличие в точке $\tau=\tau_0$ у корреляционной функции фильтруемого процесса явного положительного выброса говорит о том, что в наблюдаемом «нормальном» трафике $x(t)=\xi(t)$ на интервале времени $(t-T,t)$ появилась аномальная составляющая $\eta(t)$, обладающая самоподобными свойствами.

Представляет интерес развить представленные результаты на случай, когда не только трафик вторжений обладает самоподобными свойствами, но и типичный трафик тоже является самоподобным [10]. Целесообразно рассмотреть влияние вида распределений временных характеристик типичного и аномального трафика на результаты линейной фильтрации.

Литература

1. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. профессора О.И. Шелухина – М.: Горячая линия-Телеком. 2016. – 220 с.

2. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН, 2016. – № 45. – С. 207–244.

3. Максименко Г. А. Метод обнаружения аномалий потоков данных в сетях // Системи обробки інформації. 2009. – № 7. – С. 33-37.

4. Соловьев Н.А., Тишина Н.А., Цыганков А.С., Юркевская Л.А., Чернопрудова Е.Н. Методы спектрального анализа в задаче обнаружения аномалий информационных процессов телекоммуникационных сетей: монография // Оренбург: ОГУ, 2013. – 171 с.

5. M. Panda, A. Abraham and M. Patra, Hybrid intelligent systems for detecting network intrusions // Security Comm. Networks, 2012. – vol.8. – issue 16. – pp. 2471-2749.

6. Зубков Е. В., Белов В. М. Методы интеллектуального анализа данных и обнаружение вторжений // Вестник СибГУТИ, 2016. – № 1. – С. 118-133.

7. S. Zhao, M. Chandrashekar, Y. Lee and D. Medhi. Real-time network anomaly detection system using machine learning // 11th International Conference on the Design of Reliable Communication Networks (DRCN), Kansas City, MO, 2015. – pp. 267-270.

8. Губарева, О.Ю. Иерархическая вероятностная модель мониторинга угрозы информационной безопасности информационной системы / О.Ю. Губарева. О.В. Осипов, В.В. Пугин // Инфокоммуникационные технологии. 2016. – Т.14. – №4. – С. 429 – 435.

9. Левин Б.Р. Теоретические основы статистической радиотехники. М. Изд-во «Советское радио». 1968. – Т.2. – 504 с.

10. V. Kartashevskiy, I. Pozdnyak, M. Buranova. Intrusion Detection in Multiservice Network on the Basis of Registered Traffic Filtration // International Scientific and Practical Conference «Problems of Infocommunications. Scence and Technology» (PICS&T-2018), Ukraine, Kharkiv (unpublished).

References

1. Obnaruzheniye vtorzheniy v komp'yuternyye seti (setevyye anomalii). Uchebnoye posobiye dlya vuzov / Pod red. professora O.I. Shelukhina – M.: Goryachaya liniya-Telekom. 2016. – 220 s.

2. Branitskiy A. A., Kotenko I. V. Analiz i klassifikatsiya metodov ob-naruzheniya setevykh atak // Tr. SPIIRAN, 2016. – № 45. – S. 207–244.

3. Maksimenko G. A. Metod obnaruzheniya anomaliy potokov dannykh v setyakh // Sistemi obrobki ínformatsíí˙ . 2009. – № 7. – S. 33-37.

4. Solov'yev N.A., Tishina N.A., Tsygankov A.S., Yurkevskaya L.A., Chernoprudova Ye.N. Metody spektral'nogo analiza v zadache obnaruzheniya anomaliy informatsionnykh protsessov telekommunikatsionnykh setey: monografiya // Orenburg: OGU, 2013. – 171 s.

5. M. Panda, A. Abraham and M. Patra, Hybrid intelligent systems for detecting network intrusions // Security Comm. Networks, 2012. – vol.8. – issue 16. – pp. 2471-2749.

6. Zubkov Ye. V., Belov V. M. Metody intellektual'nogo analiza dannykh i obnaruzheniye vtorzheniy // Vestnik SibGUTI, 2016. – № 1. – S. 118-133.

7. S. Zhao, M. Chandrashekar, Y. Lee and D. Medhi. Real-time network anomaly detection system using machine learning // 11th International Conference on the Design of Reliable Communication Networks (DRCN), Kansas City, MO, 2015. – pp. 267-270.

8. Gubareva, O.YU. Iyerarkhicheskaya veroyatnostnaya model' monitoringa ugrozy informatsionnoy bezopasnosti informatsionnoy sistemy / O.YU. Gubareva. O.V. Osipov, V.V. Pugin // Infokommunikatsionnyye tekhnologii. 2016. – T.14. – №4. – S. 429 – 435.

9. Levin B.R. Teoreticheskiye osnovy statisticheskoy radiotekhniki. M. Izd-vo «Sovetskoye radio». 1968. – T.2. – 504 s.

10. V. Kartashevskiy, I. Pozdnyak, M. Buranova. Intrusion Detection in Multiservice Network on the Basis of Registered Traffic Filtration // International Scientific and Practical Conference «Problems of Infocommunications. Scence and Technology» (PICS&T-2018), Ukraine, Kharkiv (unpublished).

КАРТАШЕВСКИЙ Вячеслав Григорьевич, профессор, доктор технических наук, заведующий кафедрой Информационной безопасности, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» (ПГУТИ). 443010, г. Самара, ул, Л.Толстого, д. 23, каб.322. E-mail: kartash@psati.ru.

ПОЗДНЯК Ирина Сергеевна, кандидат технических наук, доцент кафедры Информационной безопасности, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» (ПГУТИ). 443010, г. Самара, ул, Л.Толстого, д. 23, каб.428. E-mail: i.pozdnyak@psuti.ru.

KARTASHEVSKIY Vyacheslav, Chief of Information Security Department Povolzhskiy State University of Telecommunications and Informatics, Samara, L.Tolstogo st, 23. E-mail: kartash@psati.ru

POZDNYAK Irina, Associate Professor of Information Security Department.Povolzhskiy State University of Telecommunications and Informatics, Samara, L.Tolstogo st, 23. E-mail: i.pozdnyak@psuti.ru