Инфокоммуникационные технологии и системы

УДК 62-51 **DOI: 10.14529/ctcr190405**

МОДЕЛИРОВАНИЕ ИДЕНТИФИКАЦИИ ПРОФИЛЯ КИБЕРАТАК НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ УСТРОЙСТВ В СЕТИ ПРОВАЙДЕРА ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ

И.П. Болодурина[1, 2], Д.И. Парфёнов[1, 2], Л.С. Забродина[1], А.Ю. Жигалов[1], В.А. Торчин[1]

[1] Оренбургский государственный университет, г. Оренбург, Россия,
[2] Федеральный научный центр биологических систем и агротехнологий РАН, г. Оренбург, Россия

В настоящее время существует множество угроз сетевой безопасности. Это особенно актуально для операторов связи и провайдеров телекоммуникационных услуг, являющихся ключевым звеном инфраструктуры передачи данных для любой компании. Для обеспечения защиты собственной инфраструктуры и облачных сервисов, предоставляемых конечным пользователям, операторам связи приходится применять нетривиальные решения. При этом не последнее место занимает точность определения атак системами безопасности. В рамках настоящего исследования разработан подход и проведено моделирование обнаружения атак на основе анализа цепочек состояний сетевых узлов. Предложенный подход позволяет осуществлять сопоставление событий, происходящих в сети, с событиями, фиксируемыми системами обнаружения вторжений. В нашем исследовании мы решаем проблему формализации типичного профиля атаки в сети провайдеров телекоммуникационных услуг путем построения последовательности переходов состояний узлов сети и времени изменения состояния отдельных исследуемых устройств. Исследование затрагивает наиболее популярные типы атак. Для формализации правил классификации состояний в исследовании используется алгоритм дерева решений для построения цепочки событий безопасности. В экспериментальной части исследования проведена оценка точности классификации известных типов атак, зафиксированных в журналах событий безопасности с использованием ROC-анализа. Полученные результаты позволили оценить эффективность разработанной модели для распознавания сетевых атак в инфраструктуре провайдеров телекоммуникационных услуг. Экспериментальные результаты показывают достаточно высокую точность определения популярного типа атаки. Это позволит в будущем также сократить время реагирования на инциденты безопасности в большой сети за счет более раннего обнаружения нелегитимного поведения.

Ключевые слова: обнаружения вторжений, сети провайдеров телекоммуникационных услуг, мониторинг сети, ROC-анализ, профиль кибератаки.

Введение

Широкое применение компьютерных сетей в различных сферах деятельности и высокие требования по обеспечению надежности их работы обусловливают актуальность задачи мониторинга сетей. Задача инверсивного выявления подозрительной активности при заведомо известном нелегитимном событии на данный момент является в достаточной степени изученной.

С другой стороны, решение проблемы обнаружения атак в реальном времени является нетривиальной задачей. Это обусловлено несколькими факторами. В первую очередь, ввиду разнородности представленных данных серверами и сетевыми устройствами. Вторым, но при этом не менее важным, фактором является сложность разделения нетипового поведения сети на легитимное и нелегитимное [1]. В связи с этим разработка современных методов выявления вторжений и атак на сети провайдеров телекоммуникационных услуг в настоящее время направлена на фор-

мирование нового класса алгоритмических решений. Основой для разрабатываемых решений являются методы интеллектуального анализа данных. Одним из ключевых источников таких данных являются журналы сетевых событий. Существующие Security Information and Event Management (SIEM) системы позволяют работать с потоками данных в режиме реального времени [2]. Как правило, большая часть таких систем основана на построении типового профиля пользователя и поиске в его действиях подозрительной активности. При этом точность и эффективность выявления атак при использовании данного подхода напрямую зависит от набора признаков, выбранных для идентификации нелегитимного поведения. В рамках настоящего исследования разработана методика построения типового профиля наиболее распространенных типов атак, основанная на мониторинге изменений состояния узлов сети.

1. Обзор исследований

Подход определения подозрительной сетевой активности, предложенный в данной работе, основан на анализе изменений состояний узлов сети провайдеров телекоммуникационных услуг и формировании на их базе профилей различных типов нелегитимного поведения. Анализ событий безопасности и выявление сетевых атак исследовался в ряде научных работ.

В работе исследователей из Санкт-Петербургского политехнического университета Петра Великого решается задача обнаружения атак на магистральных сетях передачи данных. Авторы предлагают прототип модуля анализа сетевого трафика, позволяющий объединять данные, получаемые из потока трафика во временные ряды и проводить дальнейший математический анализ. В основе предложенного модуля положен иерархический принцип агрегации данных, что существенно сокращает время на анализ данных [3].

В работе L. Olejnik и C. Castelluccia предложен потенциально новый подход к системе идентификации активности пользователей внутри сети. Этот метод может использоваться для обнаружения аномалий в анализе трафика и выявления подозрительной активности при доступе к облачным информационным ресурсам, расположенным на сайте поставщика телекоммуникационных услуг [4].

В рамках исследования, проведенного T. Ishitaki и др., разработан подход, основанный на использовании нейронной сети для идентификации сетевых соединений, организованных с использованием Tor. Авторы отмечают, что основными метриками выступали: число сетевых пакетов, время отклика, джиттер и число потерянных сетевых пакетов. Данная работа подтверждает возможность формирования типового профиля пользователя для идентификации его активности в сети [5].

Подход, основанный на анализе системных журналов, которые содержат данные сетевых подключений, предлагается в исследовании B.S. Borkar и A.S. Patil [6]. Для обработки данных авторы использовали метод Sequitur, который позволил уменьшить размер журнала событий. В качестве классификатора в рамках исследования авторы использовали алгоритм *k*-средних. Это позволило идентифицировать аномальное поведение пользователей.

В исследовании A. Ambre и N. Shekokar разработали вероятностный подход анализа журнала событий, иллюстрирующий частоту возникновения события, при одновременном учете частоты ложных тревог на приемлемом уровне [7]. Однако авторы указывают на необходимость создания превентивного подхода.

В работе V. Eliseev и Yu. Shabalin исследована проблема обнаружения аномалий в сетевой телекоммуникационной среде. Авторами предложен метод обнаружения аномалий, основанный на анализе динамического отклика сетевых устройств. При анализе характеристик проводится корреляция времени отклика системы и показателей ее производительности. При этом для выявления аномального поведения системы построен классификатор, основанный на нейронной сети [8].

В рамках реализации проекта SHIELD H2020 авторами предложен проект системы обеспечения сетевой безопасности. Основу системы безопасности составляет интеллектуальная система адаптивного мониторинга, позволяющая проводить обнаружение атак в режиме реального времени. Предложенное решение использует функциональные возможности NFV и SDN для перенастройки инфраструктуры, что позволяет эффективно реагировать на сетевые атаки [9].

Исследование эффективности метода обнаружения низкоинтенсивных атак проводилось Е.С. Абрамовым и Я.В. Тарасовым [10]. Авторы рассмотрели модель низкоинтенсивных атак в сети, содержащей аномальный трафик. Реализованный метод обнаружения при выделении одно-

родных групп на основе моделей распознавания образов и построения прогноза для обнаружения сценария атаки показал высокий процент обнаружения атак и низкий уровень ложных срабатываний.

В работе Ю.Г. Емельянова, А.А.Талалаева и др. предложен нейросетевой подход идентификации атак с использованием IDS Snort, который показал высокую скорость обработки сетевого трафика за счет сжатия признаков [11]. Технология может быть использована в комбинации с другими системами мониторинга для повышения уровня сетевой безопасности.

В работе I. Kotenko и др. предложен подход, основанный на применении интеллектуальных агентов для анализа сетевого трафика. В качестве базового алгоритма в рамках исследования используется псевдоградиентное адаптивное обнаружение аномалий. В качестве регулятора параметров работы алгоритма используется система нечеткого логического вывода [12].

В работе V. Dagar и др. проведено исследование различных алгоритмов сопоставления с образцом, применяемых в системах обнаружения вторжений [13]. В качестве входного набора данных авторы использовали файлы Pcap для определения эффективности алгоритмов с учетом их времени выполнения. Основной проблемой перечисленных наборов данных является то, что они не в полной мере соответствуют текущему конвергентному трафику современных сетей передачи данных и не позволяют провести верификацию построенных алгоритмических решений, направленных на их защиту. В представленных наборах данных отсутствует информация о влиянии атак на объекты инфраструктуры.

Таким образом, проведенный анализ исследований показал, что в настоящее время существует множество методов выявления атак на сетевую инфраструктуру. Однако не все рассмотренные методы могут с достаточной точностью определять атакующие воздействия, в том числе в реальном времени.

2. Постановка задачи

Рассмотрим сеть провайдеров телекоммуникационных услуг. Как правило, она представляет собой иерархию устройств, связанных между собой с использованием топологии «дерево». Подключение оборудования клиента к сети провайдера при помощи коммутаторов или базовых станций происходит на уровне доступа. На уровне агрегации потоки трафика сети объединяются на магистральном сетевом узле и предаются выше в ядро сети, которое в свою очередь соединится с вышестоящими провайдерами. Типовая схема сети провайдеров телекоммуникационных услуг представлена на рис. 1.

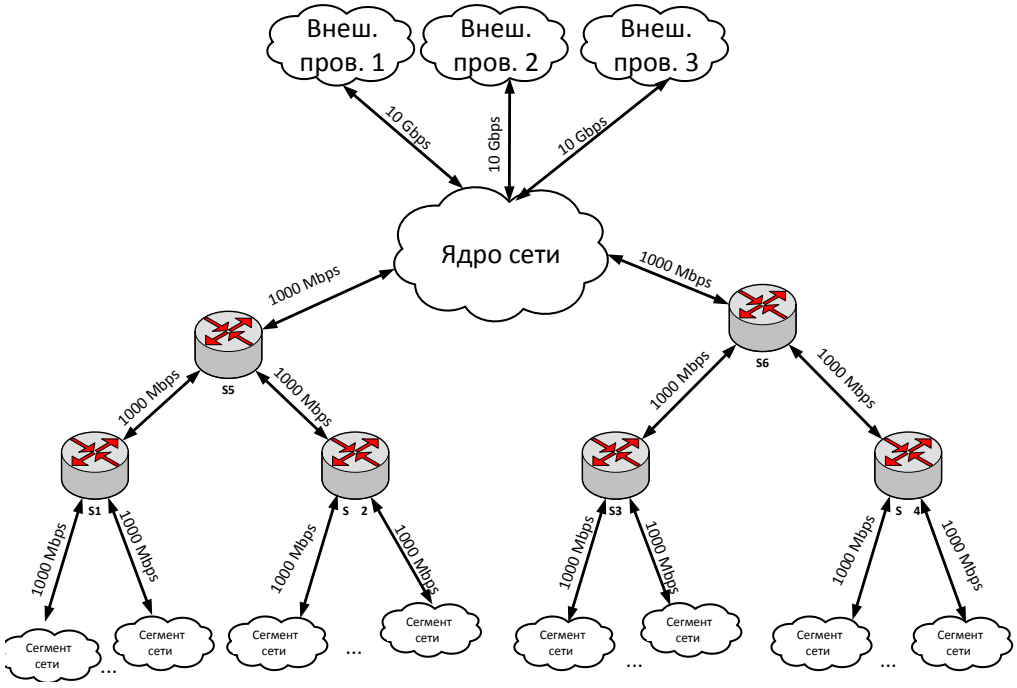

Рис. 1. Схема сети провайдеров телекоммуникационных услуг

В целом задачу мониторинга сети можно описать следующим образом. Поскольку события, происходящие в сети провайдеров телекоммуникационных услуг, носят случайный характер, то для их анализа наиболее подходящими являются вероятностные математически модели. Кроме того, отметим, что переход каждого узла сети из одного состояния в другое проходит при определенных условиях, а значит, сопровождается соответствующими характеристиками.

Зафиксируем основные возможные состояния узлов сети провайдеров телекоммуникационных услуг в процессе мониторинга параметров сетевого оборудования:

S_0 – отсутствие неисправностей;

S_1 – перегрузка узла;

S_2 – снижение пропускной способности;

S_3 – недоступность порта;

S_4 – физическая недоступность устройства;

S_5 – фрагментация пакета;

S_6 – полный отказ.

Цепь событий, имеющих некоторую вероятность происхождения, в ходе мониторинга сети можно представить в виде графа состояний (рис. 2).

Вероятность того, что узел находится в *i*-м состоянии, определяется в данном случае как вероятность нахождения в состоянии, то есть вероятность обнаружения системой мониторинга изменений в отслеживаемом параметре в сети. В каждый момент времени t_i вероятность перехода из состояния S_i в состояние S_j зависит от изменения параметров сети. В рамках настоящего исследования основными параметрами, влияющими на переход из одного состояния в другое, являются:

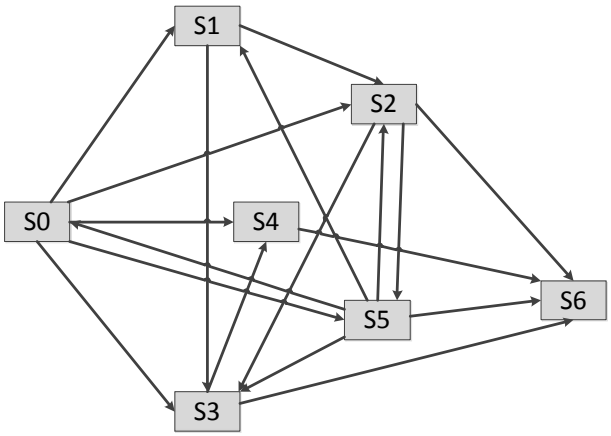

Рис. 2. Граф перехода состояний узла в сети провайдера телекоммуникационных услуг

1) количество трафика K_0, проходящего через узел в момент времени t_i;

2) показатель CPU K_1, %;

3) время отклика узла K_2, мс;

4) количество потерянных пакетов K_3, %;

5) состояние оперативной памяти RAM K_4, %;

6) пропускная способность K_5, %;

7) статистика нарушений входов K_6, %.

Для того чтобы исследовать влияние каждого фактора на переход из состояния S_i в состояние S_j ($i, j = \overline{0,6},\ i \neq j$), проведем анализ, который позволит выявить зависимость состояния узла от параметров, фиксируемых системой мониторинга. В исследовании для оценки зависимости состояний узла от его параметров будет использоваться набор данных, аппроксимированных на основе CICIDS2017, разработанный в University of New Brunswick [14].

3. Моделирование идентификации кибератак

Для выявления наличия зависимости между различными факторами внутри определенного класса (каждое состояние узла является классом, которому соответствуют свои характеристики) используем решающие деревья, которые относятся к группе логических методов поддержки принятия решений, активно использующихся в машинном обучении, а также в анализе данных. Основная идея построения решающих деревьев состоит в объединении конечного количества простых решающих правил, вследствие чего конечный алгоритм становится легко интерпретируемым.

Решающее дерево представляет собой бинарное дерево, где каждой вершине сопоставляется некоторое правило вида « j – признак имеет значение меньше b», а листья содержат значения

предсказаний. Важность каждого признака можно оценить на основании того, насколько существенно улучшился критерий качества благодаря использованию этого признака в вершинах деревьев.

Алгоритм LearnID3 построения решающего дерева:

1) **ПРОЦЕДУРА** LearnID3 ($U \subseteq X^l$);

2) **если** все объекты из U лежат в одном классе $c \in Y$, **то** вернуть новый лист $v, c_v := c$;

3) найти предикат с максимальной информативностью:

$\beta := \arg \max_{\beta \in B} I(\beta, U)$;

$I(\beta, X^l) = \#\{(x_i; x_j) : y_i = y_j \ \beta(x_i) = \beta(x_j)\}$ – критерий Джини;

4) разбить выборку $U = U_0 \bigcup U_1$ по предикату β:

$U_0 = \{u \in U : \beta(x) = 0\}$;

$U_1 = \{u \in U : \beta(x) = 1\}$;

5) **если** $U_0 = \varnothing$ или $U_1 = \varnothing$, **то**

6) **вернуть** новый лист $v, c_v :=$ Мажоритарный класс (U);

7) создать новую внутреннюю вершину $v, \beta_v := \beta$;

построить левое поддерево: $L_v := LearnID3(U_0)$;

построить правое поддерево: $R_v := LearnID3(U_1)$;

8) **вернуть** v.

На основе рассмотренного алгоритма LearnID3 построения решающего дерева проанализированы данные о состоянии узла и его параметрах, фиксируемые системой мониторинга, и получены результаты, представленные на рис. 3. Каждая вершина решающего дерева содержит информацию о количестве объектов каждого класса, попавших в рассматриваемый узел.

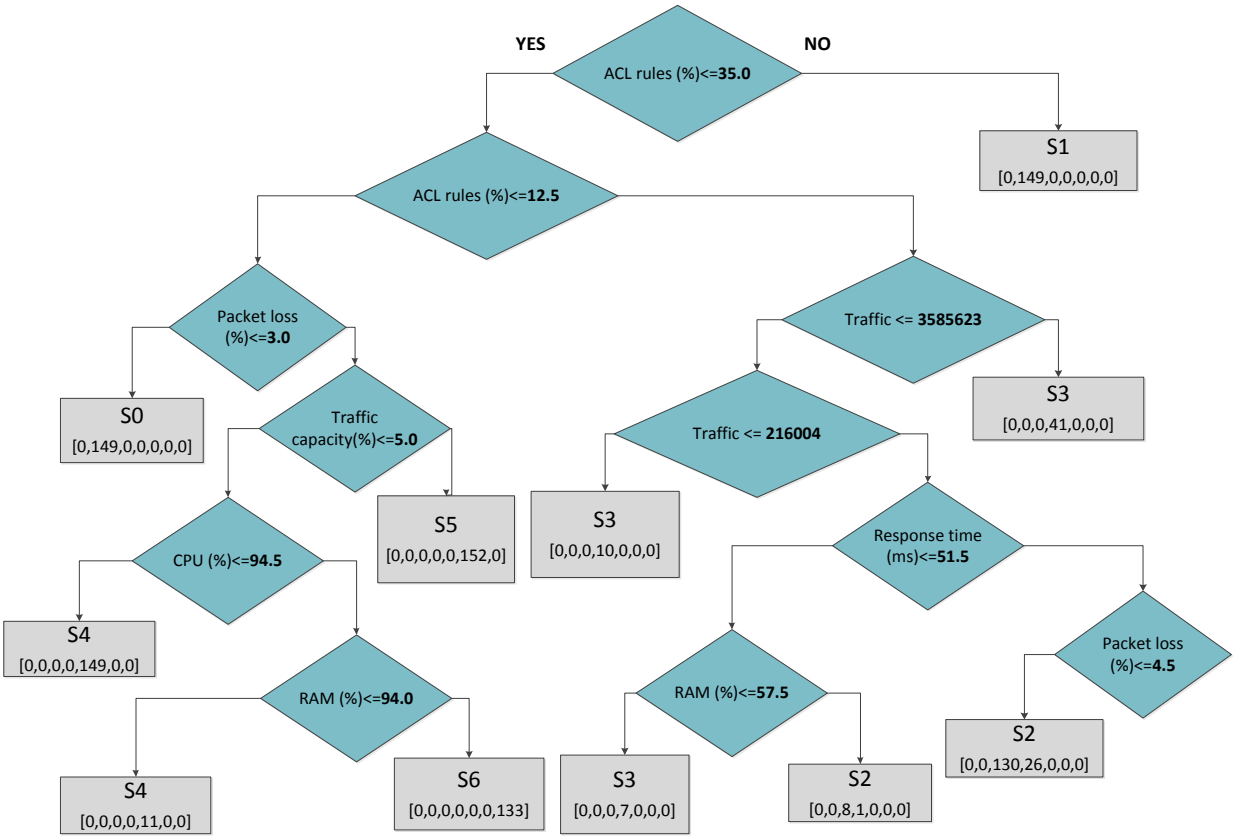

Рис. 3. Дерево решений зависимости состояния узла от параметров

Согласно построенному дереву решений (см. рис. 3) можно выделить для каждого состояния S_i узла сети наиболее важные параметры K_j, влияющие на изменение данного состояния. Результаты оценки зависимостей состояний узла от его параметров представлены в табл. 1.

Таблица 1

Значимые характеристики состояний узла сети

Состояние	Параметры
S_0 – отсутствие неисправностей	$\{K_0;\ K_1;\ K_2;\ K_3;\ K_4; K_5;\ K_6\}$
S_1 – перегрузка узла	$\{K_6\}$
S_2 – снижение пропускной способности	$\{K_0;\ K_2;\ K_3;\ K_4;\ K_6\}$
S_3 – недоступность порта	$\{K_0;\ K_2;\ K_3;\ K_6\}$
S_4 – физическая недоступность устройства	$\{K_1;\ K_3;\ K_5\}$
S_5 – фрагментация пакета	$\{K_1;\ K_3\}$
S_6 – полный отказ	$\{K_1;\ K_3; K_4; K_5\}$

По графу (см. рис. 2) составим математическую модель процесса изменения состояний узла в виде системы уравнений с учётом вероятностей $p_i(t)$ нахождения в момент времени t в состоянии i. Заметим, что каждое состояние в соответствии с решающим деревом (см. рис. 3) зависит от определенного набора характеристик. Однако переход в это состояние возможен лишь из состояний, связанных с ним (см. рис. 2). В связи с этим распределим набор влияющих характеристик между состояниями, из которых возможен переход в соответствии с техническими возможностями узла:

$$\begin{cases} \frac{dp_0(t)}{dt} = -p_0(t)(k_0 + k_1 + k_2 + k_3 + k_4 + \frac{1}{k_5} + k_6); \\ \frac{dp_1(t)}{dt} = p_0(t)k_6 + p_5(t)k_6 - p_1(t)k_6; \\ \frac{dp_2(t)}{dt} = p_0(t)(k_0 + k_6) + p_1(t)(k_2 + k_3 + k_4) + p_5(t)(k_0 + k_4) - p_2(t)(k_0 + k_2 + k_3 + k_4 + k_6); \\ \frac{dp_3(t)}{dt} = p_0(t)(k_0 + k_2) + p_1(t)(k_3 + k_6) + p_2(t)k_3 + p_5(t)(k_0 + k_2) - p_3(t)(k_0 + k_2 + k_3 + k_6); \\ \frac{dp_4(t)}{dt} = p_0(t)(k_1 + k_3 + \frac{1}{k_5}) + p_3(t)k_3 - p_4(t)(k_1 + k_3 + \frac{1}{k_5}); \\ \frac{dp_5(t)}{dt} = p_0(t)(k_1 + k_3) + p_1(t)k_3 + p_2(t)(k_1 + k_3) - p_5(t)(k_1 + k_3); \\ \frac{dp_6(t)}{dt} = p_2(t)(k_1 + k_3 + k_4 + \frac{1}{k_5}) + p_3(t)(k_3 + k_4) + p_5(t)(k_1 + k_3) + p_4(t)(k_1 + k_3 + k_4 + \frac{1}{k_5}), \end{cases} \quad (1)$$

где k_i – соответствующие безразмерные характеристики параметров K_i.

Математическая модель процесса изменения состояний узла (1) описывает скорости изменения вероятностей нахождения узла в каждом из состояний. Зафиксируем момент времени t^i, характеризующий последнюю запись основных характеристик узла в системе мониторинга. Тогда вероятности нахождения узла в каждом из состояний в следующий момент времени t^{i+1}, согласно методу Эйлера, описываются следующей системой уравнений:

$$p_j(t^{i+1}) = p_j(t^i) + \frac{dp_j(t^i)}{dt} \cdot (t^{i+1} - t^i), \quad j = 0,...,6. \quad (2)$$

Таким образом, построенная модель (1)–(2) определения вероятностей нахождения узла в состоянии i позволяет с помощью наиболее вероятного из состояний сделать прогноз для узла на

следующий момент времени и, следовательно, отследить для каждого узла полную цепочку событий.

Построим типовой профиль каждой атаки на основе отслеживания и прогноза состояний всех узлов в сети. В данном исследовании рассмотрены следующие наиболее распространенные типы атак: Brute-force; Heartbleed; Ботнет; DoS -атака; DDoS-атака; SQL-инъекция; Атака на проникновение; Fuzzers; Worms; Analysis (табл. 2).

Типовой профиль каждой атаки определен цепочкой переходов состояний и скоростью перехода между ними, которую определим интервалами, статистически определенными как зафиксированные минимальные и максимальные скорости переходов.

Таблица 2

Типовые профили атак

Тип атаки	Профиль атаки
Brute-force	$S_0 \xrightarrow{T^1_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_1} S_2 \xrightarrow{T^1_{2,5}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_1} S_5 \xrightarrow{T^1_{5,1}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_1}$ $S_1 \xrightarrow{T^1_{1,2}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_1} S_2 \xrightarrow{T^1_{2,5}\in[\Delta t^5_{\min};\Delta t^5_{\max}]_1} S_5$
Heartbleed	$S_0 \xrightarrow{T^2_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_2} S_2 \xrightarrow{T^2_{2,5}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_2}$ $S_5 \xrightarrow{T^2_{5,2}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_2} S_2 \xrightarrow{T^2_{2,5}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_2} S_5$
Ботнет	$S_0 \xrightarrow{T^3_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_3} S_2 \xrightarrow{T^3_{2,5}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_3}$ $S_5 \xrightarrow{T^3_{5,3}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_3} S_3 \xrightarrow{T^3_{3,6}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_3} S_6$
DoS-атака	$S_0 \xrightarrow{T^4_{0,1}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_4} S_1 \xrightarrow{T^4_{1,2}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_4} S_2 \xrightarrow{T^4_{2,3}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_4}$ $S_3 \xrightarrow{T^4_{3,4}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_4} S_4 \xrightarrow{T^4_{4,6}\in[\Delta t^5_{\min};\Delta t^5_{\max}]_4} S_6$
DDoS-атака	$S_0 \xrightarrow{T^5_{0,1}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_5} S_1 \xrightarrow{T^5_{1,2}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_5} S_2 \xrightarrow{T^5_{2,5}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_5}$ $S_5 \xrightarrow{T^5_{5,3}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_5} S_3 \xrightarrow{T^5_{3,4}\in[\Delta t^5_{\min};\Delta t^5_{\max}]_5} S_4 \xrightarrow{T^5_{4,6}\in[\Delta t^6_{\min};\Delta t^6_{\max}]_5} S_6$
SQL-инъекция	$S_0 \xrightarrow{T^6_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_6} S_2 \xrightarrow{T^6_{2,3}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_6}$ $S_5 \xrightarrow{T^6_{5,1}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_6} S_1 \xrightarrow{T^6_{1,5}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_6} S_5$
Атака на проникновение	$S_0 \xrightarrow{T^7_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_7} S_2 \xrightarrow{T^7_{2,5}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_7} S_5 \xrightarrow{T^7_{5,3}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_7} S_3$
Fuzzers	$S_0 \xrightarrow{T^8_{0,1}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_8} S_1 \xrightarrow{T^8_{1,2}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_8} S_2 \xrightarrow{T^8_{2,5}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_8}$ $S_5 \xrightarrow{T^8_{5,3}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_8} S_3 \xrightarrow{T^8_{3,4}\in[\Delta t^5_{\min};\Delta t^5_{\max}]_8} S_4 \xrightarrow{T^8_{4,8}\in[\Delta t^6_{\min};\Delta t^6_{\max}]_8} S_6$
Worms	$S_0 \xrightarrow{T^9_{0,1}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_9} S_1 \xrightarrow{T^9_{1,5}\in[\Delta t^2_{\min};\Delta t^2_{\max}]_9} S_5 \xrightarrow{T^9_{5,2}\in[\Delta t^3_{\min};\Delta t^3_{\max}]_9}$ $S_2 \xrightarrow{T^9_{2,3}\in[\Delta t^4_{\min};\Delta t^4_{\max}]_9} S_3 \xrightarrow{T^9_{3,4}\in[\Delta t^5_{\min};\Delta t^5_{\max}]_9} S_4$
Analysis	$S_0 \xrightarrow{T^{10}_{0,2}\in[\Delta t^1_{\min};\Delta t^1_{\max}]_{10}} S_2$

Запись вида $S_i \xrightarrow{T_{i,j}^k \in [\Delta t_{\min}^l ; \Delta t_{\max}^l]_k} S_j$ означает, что переход из состояния S_i в состояние S_j для определенного типа атаки происходит за минимальное время $\Delta t_{\min}^l$ и максимальное время $\Delta t_{\max}^l$, где l – порядковый номер перехода в цепочке, k – идентификатор атаки в базе данных SIEM.

4. Экспериментальные исследования

Для оценки эффективности использования типовых профилей атак при выявлении подозрительной сетевой активности в сети провайдеров телекоммуникационных услуг проведем ROC-анализ, используемый для анализа результатов бинарной классификации. Процесс классификации действий на атаки различного типа представляет собой бинарную классификацию атака/неатака. При этом выделяют класс с положительными исходами (верно классифицированные события), а также с отрицательными исходами (неверно классифицированные события). ROC-кривая показывает зависимость истинно положительных примеров от ложно отрицательных примеров.

Введем следующие обозначения:

TP (True Positives) – истинно положительные случаи;

TN (True Negatives) – истинно отрицательные случаи;

FN (False Negatives) – положительные примеры, классифицированные как отрицательные (ошибка I рода, ложно отрицательные случаи);

FP (False Positives) – отрицательные примеры, классифицированные как положительные (ошибка II рода, ложно положительные случаи).

При анализе чаще оперируют относительными показателями (долями):

доля истинно положительных примеров (True Positives Rate):

$$TP \cdot 100\,\% / (TP + FN); \tag{3}$$

доля ложно положительных примеров (False Positives Rate):

$$FPR = FP \cdot 100\,\% / \left(TN + FP\right). \tag{4}$$

Важно отметить, что объективная ценность бинарного классификатора отражается в его чувствительности и специфичности.

Чувствительность (Sensitivity) – доля истинно положительных случаев:

$$Se = TPR = TP \cdot 100\,\% / \left(TP + FN\right). \tag{5}$$

Специфичность (Specificity) – доля истинно отрицательных случаев, которые были верно идентифицированы моделью:

$$Sp = TN \cdot 100\,\% / \left(TN + FP\right). \tag{6}$$

Выделим для прогностической модели идентификации атак ложно положительные (False Positive) и истинно положительные (True Positive) случаи (табл. 3).

Таблица 3

Типовые профили атак

Результаты классификации	fp	tp	fpf	tpf
	4264	39643	0	0
Brute-force	543	5462	0,01643	0,100635
Heartbleed	254	7342	0,101641	0,236837
Ботнет	763	2039	0,365854	0,374417
DoS-атака	1209	4454	0,64939	0,486769
DDoS-атака	439	5955	0,752345	0,636985
SQL-инъекция	76	2953	0,770169	0,711475
Атака на проникновение	142	2806	0,803471	0,782257
Fuzzers	309	2778	0,846096	0,813162
Worms	378	3227	0,867943	0,934106
Analysis	151	2627	1	1

Построим на их основе ROC-кривую, позволяющую провести анализ результатов точности и прогностической силы модели распознавания атак с помощью разработанных типовых профилей

(рис. 4). Для подтверждения эффективности предложенного решения (Классификатор 1) проведено сравнение на наборе данных CICIDS2017 с использованием аналогичного классификатора (Классификатор 2), предложенного авторами I. Sharafaldin и A.H. Lashkari [15].

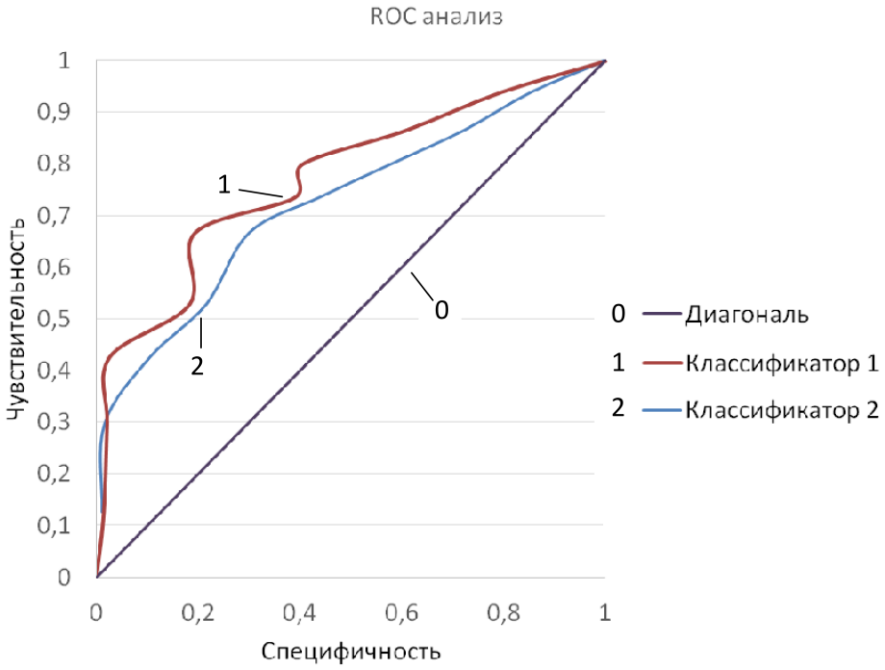

Рис. 4. ROC-кривые моделей распознавания атак в сети

Баланс между чувствительностью и специфичностью модели распознавания атак в сети провайдеров телекоммуникационных услуг на основе типовых профилей (Классификатор 1) определяет значение показателя AUC (Area Under Curve) = 0,77141905, что, согласно экспертной шкале, соответствует хорошей прогностической силе модели и достаточно высокой точности определения класса подозрительной активности. Классификатор 2, построенный на основе алгоритма машинного обучения, указания наилучшего набора функций для обнаружения определенных категорий атак, соответствует значению AUC = 0,722304611. Таким образом, можно сделать вывод о том, что разработанная модель идентификации подозрительной сетевой активности работает более эффективно и построенные типовые профили атак позволяют оптимально проводить классификацию.

Заключение

В ходе исследования представлена модель вычисления вероятностей нахождения узла телекоммуникационной сети провайдера в некотором состоянии. Предложенная модель позволяет спрогнозировать изменение состояния для каждого узла сети в следующий момент времени. На основе выявленных закономерностей изменения состояний сетевых и вычислительных узлов определены цепочки событий, формирующие типовой профиль для исследуемых типов кибератак. В рамках экспериментального исследования проведена оценка эффективности разработанной модели распознавания атак в сети провайдеров телекоммуникационных услуг, которая показывает достаточно высокую точность определения класса подозрительной активности. Полученные результаты в дальнейшем планируется использовать для управления механизмами обеспечения безопасности в сетях провайдеров телекоммуникационных услуг.

Работа выполнена при финансовой поддержке РФФИ проект № 18-07-01446, гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук (МК-860.2019.9), а также Министерства образования Оренбургской области (Соглашение № 12 от 14.08.2019). Исследования выполнены в соответствии с планом НИР на 2019–2020 гг. ФГБНУ «Федеральный научный центр биологических систем и агротехнологий РАН» (№ 0761-2019-0004).

Литература

1. Near-miss situation based visual analysis of SIEM rules for real time network security monitoring / A. Majeed, R. Ur Rasool, F. Ahmad et al. // Journal of Ambient Intelligence and Humanized Computing. – 2019. – Vol. 10 (4). – P. 1509–1526. DOI: 10.1007/s12652-018-0936-7

2. Парфёнов, Д.И. Разработка и исследование алгоритмов формирования правил для узлов сетевой безопасности в мультиоблачной платформе / Д.И. Парфёнов, И.П. Болодурина, В.А. Торчин // Моделирование и анализ информационных систем. – 2019. – Т. 26, № 1 (79). – С. 90–100.

3. Poltavtseva, M.A. The hierarchial data aggregation method in backbone traffic streaming analyzing to ensure digital systems information security / M.A. Poltavtseva, P.D. Zegzhda, Il.D. Pankov // Eleventh International Conference "Management of large-scale system development" (MLSD). – 2018. – Paper number 8551916. DOI: 10.1109/MLSD.2018.8551916

4. Olejnik, L. Towards web-based biometric systems using personal browsing interests / L. Olejnik, C. Castelluccia // The 8th International Conference on Availability, Reliability and Security (ARES). – 2013. – Paper number 6657252. DOI: 10.1109/ARES.2013.36

5. Ishitaki, T. A neural network based user identification for tor networks: data analysis using friedman test / T. Ishitaki, T. Oda, L. Barolli // 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA). – 2016. – Paper number 7471164. DOI: 10.1109/WAINA.2016.143

6. Borkar, B.S. Post-attack detection using log files analysis / B.S. Borkar, A.S. Patil // International Journal of Innovative Research in Science, Engineering and Technology. – 2013. – Vol. 2 (1). – P. 1195–1199.

7. Ambre, A. Insider threat detection using log analysis and event correlation / A. Ambre, N. Shekokar // Procedia Computer Science. – 2015. – Vol. 45. – P. 436–445. DOI: 10.1016/j.procs.2015.03.175

8. Eliseev, V. Dynamic response recognition by neural network to detect network host anomaly activity / V. Eliseev, Y. Shabalin // Proceeding SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks. – 2015. – P. 246–249. DOI: 10.1145/2799979.2799991

9. Nandi, A.K. Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender-attacker model / A.K. Nandi, H.R. Medal, S. Vadlamani // Computers & Operations Research. – 2016. – Vol. 75. – P. 118–131. DOI: 10.1016/j.cor.2016.05.005

10. Абрамов, Е.С. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы / Е.С. Абрамов, Я.В. Тарасов // Инженерный вестник Дона. – 2017. – Т. 46, № 3 (46). – С. 59.

11. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю.Г. Емельянова, А.А. Допира, И.П. Тищенко, В.П. Фраленко // Программные системы: теория и приложения. – 2011. – Т. 2, № 3. – С. 3–15.

12. Kotenko, I. Intelligent agents for network traffic and security risk analysis in cyber-physical systems / I. Kotenko, S. Ageev, I. Saenko // 11th International Conference on Security of Information and Networks. – 2018. – Paper number 3264487. DOI: 10.1145/3264437.3264487

13. Dagar, V. Analysis of pattern matching algorithms in network intrusion detection systems / V. Dagar, V. Prakash, T. Bhatia // 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA). – 2016. – Paper number 7748969. DOI: 10.1109/ICACCAF.2016.7748969

14. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB // Canadian Institute for Cybersecurity. – https://www.unb.ca/cic/datasets/ids-2017.html (дата обращения: 01.08.2019).

15. Sharafaldin, I. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization / I. Sharafaldin, A.H. Lashkari // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018). – 2018. – P. 108–116. DOI: 10.5220/0006639801080116

Болодурина Ирина Павловна, д-р техн. наук, профессор, заведующий кафедрой прикладной математики, Оренбургский государственный университет; Федеральный научный центр биологических систем и агротехнологий РАН, г. Оренбург; prmat@mail.osu.ru.

Парфёнов Денис Игоревич, канд. техн. наук, заведующий сектором программно-технической поддержки дистанционного обучения, Оренбургский государственный университет; Федеральный научный центр биологических систем и агротехнологий РАН, г. Оренбург; parfenovdi@ mail.ru.

Забродина Любовь Сергеевна, ассистент кафедры прикладной математики, Оренбургский государственный университет, г. Оренбург; zabrodina97@inbox.ru.

Жигалов Артур Юрьевич, ведущий программист, Оренбургский государственный университет, г. Оренбург; leroy137.artur@gmail.com.

Торчин Вадим Александрович, студент, Оренбургский государственный университет, г. Оренбург; vadim.torchin@gmail.com.

Поступила в редакцию 1 сентября 2019 г.

DOI: 10.14529/ctcr190405

MODELING THE IDENTIFICATION OF THE PROFILE OF CYBER ATTACKS BASED ON ANALYSIS OF THE DEVICE BEHAVIOR IN THE TELECOMMUNICATION SERVICES PROVIDER NETWORK

I.P. Bolodurina*[1, 2]*, prmat@mail.osu.ru,
D.I. Parfenov*[1, 2]*, parfenovdi@mail.ru,
L.S. Zabrodina*[1]*, zabrodina97@inbox.ru,
A.Ju. Zhigalov*[1]*, leroy137.artur@gmail.com,
V.A. Torchin*[1]*, vadim.torchin@gmail.com

[1] Orenburg State University, Orenburg, Russian Federation,
[2] Federal Research Centre of Biological Systems and Agrotechnologies RAS, Orenburg, Russian Federation

There are currently many threats to network security. This is especially true for telecom operators and telecommunication service providers, which are a key link in the data transmission infrastructure for any company. To ensure the protection of their infrastructure and cloud services provided to end-users, telecom operators have to use non-trivial solutions. At the same time, the accuracy of defining attacks by security systems is not the least. In the framework of this study, an approach was developed and attack detection was modeled based on the analysis of state chains of network nodes. The proposed approach allows the comparison of events occurring in the network with events recorded by intrusion detection systems. In our study, we solve the problem of formalizing a typical attack profile in a network of telecommunication service providers by constructing a sequence of transitions of states of network nodes and the time of the state change of individual devices under study. The study covers the most popular types of attacks. To formalize the rules for classifying states, the study uses a decision tree algorithm to build a chain of security events. In the experimental part of the study, the accuracy of the classification of known types of attacks recorded in security event logs using ROC analysis was assessed. The results obtained made it possible to evaluate the effectiveness of the developed model for recognizing network attacks in the infrastructure of telecommunication service providers. The experimental results show fairly high accuracy in determining the popular type of attack. This will also help in the future to reduce the response time to security incidents in a large network, due to earlier detection of illegitimate behavior.

Keywords: intrusion detection; network of telecommunication service providers; network monitoring; ROC-analysis; cyberattack profile.

References

1. Majeed A., Rasool R. Ur, Ahmad F., Alam M., Javaid N. Near-miss Situation Based Visual Analysis of SIEM Rules for Real Time Network Security Monitoring. *Journal of Ambient Intelligence and Humanized Computing*, 2019, vol. 10 (4), pp. 1509–1526. DOI: 10.1007/s12652-018-0936-7

2. Parfyonov D.I., Bolodurina I.P., Torchin V.A. Development and Research of Algorithms of Rule Formation for Network Safety Nodes in Multi-Layer Platform. *Modeling and Analysis of Information Systems*, 2019, vol. 26, no. 1 (79), pp. 90–100. (in Russ.)

3. Poltavtseva M.A., Zegzhda P.D., Pankov Il.D. The Hierarchial Data Aggregation Method in Backbone Traffic Streaming Analyzing to Ensure Digital Systems Information Security. *Eleventh International Conference "Management of Large-scale System Development" (MLSD)*, 2018, Paper Number 8551916. DOI: 10.1109/MLSD.2018.8551916

4. Olejnik L., Castelluccia C. Towards Web-Based Biometric Systems Using Personal Browsing Interests. *The 8th International Conference on Availability, Reliability and Security (ARES)*, 2013, Paper Number 6657252. DOI: 10.1109/ARES.2013.36

5. Ishitaki T., Oda T., Barolli L. A Neural Network Based User Identification for Tor Networks: Data Analysis Using Friedman Test. *30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2016, Paper Number 7471164. DOI: 10.1109/WAINA.2016.143

6. Borkar B.S., Patil A.S. Post-Attack Detection Using Log Files Analysis. *International Journal of Innovative Research in Science, Engineering and Technology*, 2013, vol. 2 (1), pp. 1195–1199.

7. Ambre A., Shekokar N. Insider Threat Detection Using Log Analysis and Event Correlation. *Procedia Computer Science*, 2015, vol. 45, pp. 436–445. DOI: 10.1016/j.procs.2015.03.175

8. Eliseev V., Shabalin Y. Dynamic Response Recognition by Neural Network to Detect Network Host Anomaly Activity. *Proceeding SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks*, 2015, pp. 246–249. DOI: 10.1145/2799979.2799991

9. Nandi A.K., Medal H.R., Vadlamani S. Interdicting Attack Graphs to Protect Organizations from Cyber Attacks: A Bi-Level Defender-Attacker Model. *Computers & Operations Research*, 2016, vol. 75, pp. 118–131. DOI: 10.1016/j.cor.2016.05.005

10. Abramov E.S., Tarasov Y.V. Application of Combined Neural Network Method for Detection of Low-Intensity DDoS-Atak on Web-Services. *Don 's Engineering Bulletin*, 2017, vol. 46, no. 3 (46), pp. 59. (in Russ.)

11. Emel'yanova Y.G., Dopira A.A., Tishchenko I.P., Fralenko V.P. Neural Network Technology for Detection of Network Attacks on Information Resources. *Software Systems: Theory and Applications*, 2011, vol. 2, no. 3, pp. 3–15. (in Russ.)

12. Kotenko I., Ageev S., Saenko I. Intelligent Agents for Network Traffic and Security Risk Analysis in Cyber-Physical Systems. *11th International Conference on Security of Information and Networks*, 2018, Paper Number 3264487. DOI: 10.1145/3264437.3264487

13. Dagar V., Prakash V., Bhatia T. Analysis of Pattern Matching Algorithms in Network Intrusion Detection Systems. *2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)*, 2016, Paper Number 7748969. DOI: 10.1109/ICACCAF.2016.7748969

14. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. *Canadian Institute for Cybersecurity*. Available at: https://www.unb.ca/cic/datasets/ids-2017.html (accessed 01.08.2019).

15. Sharafaldin I., Lashkari A.H. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 2018, pp.108-116. DOI: 10.5220/0006639801080116

Received 1 September 2019

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Моделирование идентификации профиля кибератак на основе анализа поведения устройств в сети провайдера телекоммуникационных услуг / И.П. Болодурина, Д.И. Парфёнов, Л.С. Забродина и др. // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2019. – Т. 19, № 4. – С. 48–59. DOI: 10.14529/ctcr190405

FOR CITATION

Bolodurina I.P., Parfenov D.I., Zabrodina L.S., Zhigalov A.Ju., Torchin V.A. Modeling the Identification of the Profile of Cyber Attacks Based on Analysis of the Device Behavior in the Telecommunication Services Provider Network. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2019, vol. 19, no. 4, pp. 48–59. (in Russ.) DOI: 10.14529/ctcr190405