УДК 004.738.2

# МЕТОД МОНИТОРИНГА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ДАННЫХ СЕТЕВОГО ТРАФИКА

**Зайчиков Илья Дмитриевич,** студент, направление подготовки 10.03.01 Информационная безопасность, Оренбургский государственный университет, Оренбург
e-mail: ilya.zaychikov@list.ru

**Абрамова Таисия Вячеславовна,** старший преподаватель кафедры вычислительной техники и защиты информации, Оренбургский государственный университет, Оренбург
e-mail: taya357@gmail.com

***Аннотация.*** *Актуальность работы обусловлена возрастающим числом инцидентов информационной безопасности в промышленных автоматизированных системах управления (АСУ), связанных с ошибками, либо умышленными вредоносными действиями персонала системы. Целью работы является повышение оперативности распознавания нерегламентированных действий пользователей промышленной сети на основе ассоциативного подхода к поиску данных в сетевом трафике АСУ ТП. В статье предложена математическая модель ассоциативного поиска данных о поведении пользователя в трафике промышленной сети, разработаны алгоритм и программное средство для мониторинга поведения пользователя, позволяющее контролировать управляющие воздействия на АСУ в режиме реального времени. В работе использованы методы теории информационной безопасности, теории распознавания образов, методы математического и имитационного моделирования. Научную новизну работы составляют математическая модель и алгоритм мониторинга поведения пользователя на основе ассоциативного подхода, позволяющие повысить оперативность поиска сведений о командах управления в сетевом трафике АСУ. Практическая значимость результатов работы заключается в разработке метода и программного средства мониторинга, позволяющих снизить риски от принятия несанкционированных управляющих решений. В рамках дальнейших исследований планируется рассмотреть возможности ситуационного анализа действий пользователя.*

***Ключевые слова:*** *сетевой трафик, АСУ ТП, протокол Modbus TCP, нерегламентированные действия, ассоциативный поиск данных.*

***Благодарности***: статья подготовлена в рамках исследования, проводимого в ходе реализации стратегического проекта «Технологии и кадры для ОПК», выполняемого по программе стратегического академического лидерства «Приоритет-2030».

***Для цитирования:*** Зайчиков И. Д., Абрамова Т. В. Метод мониторинга поведения пользователя на основе данных сетевого трафика // Шаг в науку. – 2023. – № 1. – С. 35–40.

# A METHOD FOR MONITORING USER BEHAVIOR BASED ON NETWORK TRAFFIC DATA

**Zaichikov Ilya Dmitrievich**, student, training program 10.03.01 Information security, Orenburg State University, Orenburg
e-mail: ilya.zaychikov@list.ru

**Abramova Taisiya Vyacheslavovna,** Senior Lecturer of the Department of Computer Engineering and Information Security, Orenburg State University, Orenburg
e-mail: taya357@gmail.com

***Abstract.*** *The relevance of the work is due to the increasing number of information security incidents in industrial automated control systems (ACS) associated with errors or intentional malicious actions of the system personnel. The aim of the work is to increase the efficiency of recognizing unregulated actions of users of the industrial network, through the use of an associative approach to searching for data in the network traffic of the automated control system. The article proposes a mathematical model of associative search for data on user behavior in industrial network traffic, an algorithm and a software tool for monitoring user behavior are developed that allows controlling the control actions on the automated control system in real time. Methods of information*

*security theory, pattern recognition theory, methods of mathematical and simulation modeling are used in the work. The scientific novelty of the work consists of a mathematical model and an algorithm for monitoring user behavior based on an associative approach, which make it possible to increase the efficiency of searching for information about control commands in the automated control system network traffic. The practical significance of the results of the work lies in the development of a method and software monitoring tool that reduce the risks from making unauthorized management decisions. As part of further research, it is planned to consider the possibilities of situational analysis of user actions.*

***Key words:*** *network traffic, automated control system, Modbus TCP protocol, unregulated actions, associative data search.*

**Acknowledgements:** This article was prepared as part of research conducted during the implementation of the strategic project «Technologies and personnel for the defense industry», carried out under the program of strategic academic leadership «Priority 2030».

***Cite as***: Zaichikov, I. D., Abramova T. V. (2023) [A method for monitoring user behavior based on network traffic data]. *Shag v nauku* [Step into science]. Vol. 1, pp. 35–40.

В настоящее время возросло число инцидентов информационной безопасности (ИБ) в промышленных автоматизированных системах управления. Согласно статистике Kaspersky ICS CERT[1] прирост атак, совершённых на автоматизированные системы управления технологическими процессами (АСУ ТП) Российской Федерации, в 2021 году составил 1,2%. Ошибки персонала, непреднамеренные или целенаправленные нерегламентированные действия пользователей АСУ ТП являются одними из самых распространенных инцидентов ИБ в промышленных системах[2].

Целью настоящей работы является повышение оперативности распознавания нерегламентированных действий пользователей промышленной сети на основе ассоциативного подхода к поиску данных в сетевом трафике АСУ ТП. Для достижения цели были построены типовая структурная схема АСУ ТП и классификация нерегламентированных действий пользователя в промышленной сети. Разработана математическая модель ассоциативного поиска данных, адаптированная для распознавания нерегламентированных действий пользователя в сетевом трафике. На основе математической модели разработаны алгоритм и программное средство для мониторинга поведения пользователя, проведено экспериментальное исследование работы программы.

Типовая структурная схема АСУ ТП [8] представлена на рисунке 1.

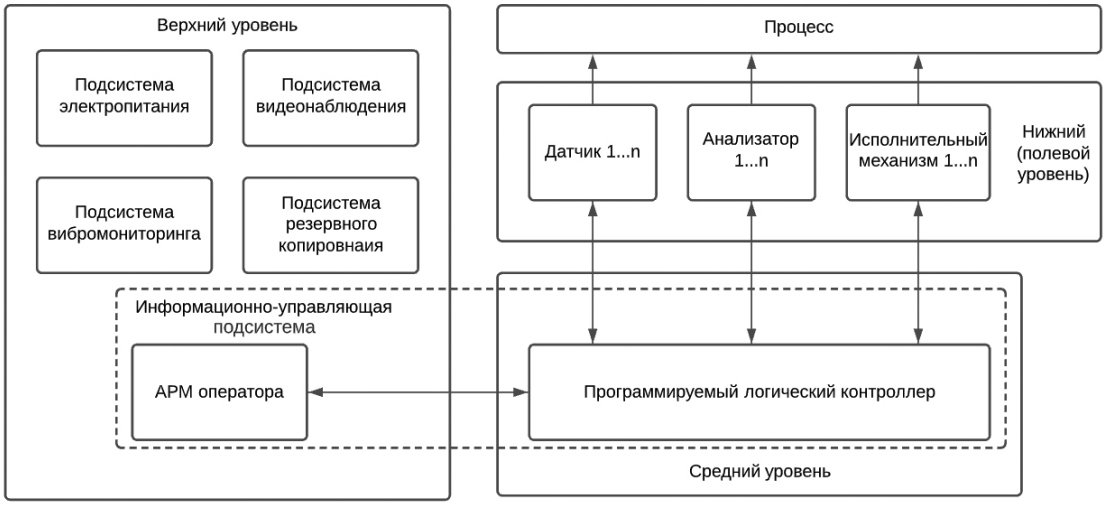



Рисунок 1. Типовая структурная схема автоматизированной системы управления технологическим процессом

*Источник: разработано автором Зайчиковым И. Д. на основе [8]*

[1] Ландшафт угроз для систем промышленной автоматизации [Электронный ресурс]. – Режим доступа: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-statistics-for-H1-2021-Ru.pdf (дата обращения: 16.04.2022).

[2] Атаки на АСУ ТП [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/threats/APCS-attacks (дата обращения: 16.04.2022).

Анализ структурной схемы показал, что основные сведения о действиях пользователя отражаются в сетевых потоках информационно-управляющей подсистемы АСУ, что предопределяет необходимость выбора сетевого трафика в качестве основного источника данных о поведении пользователя.

Классификация нерегламентированных действий пользователей сети АСУ ТП представлена на рисунке 2.

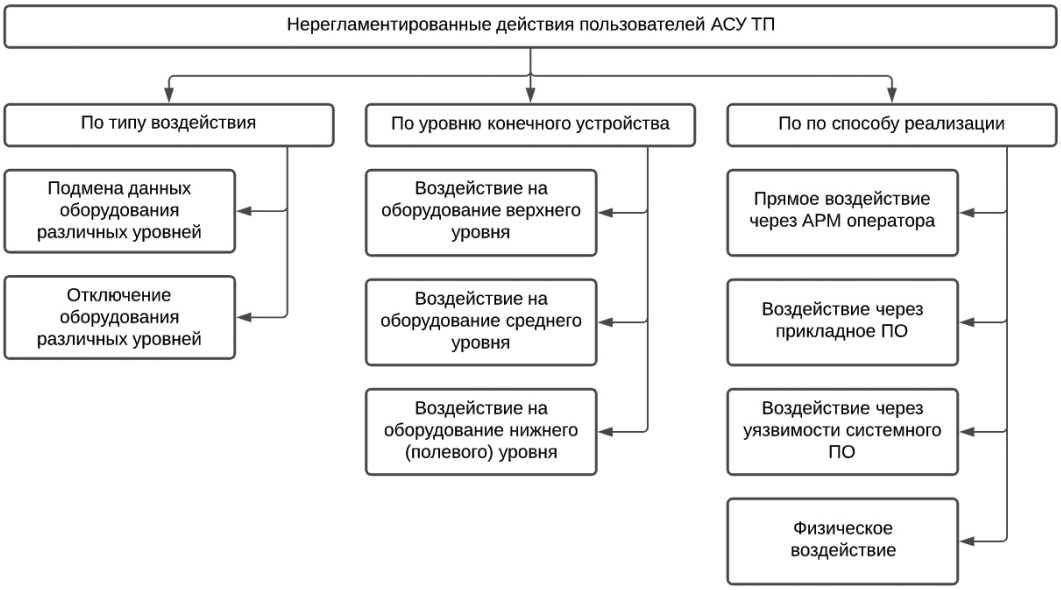



Рисунок 2. Классификация нерегламентированных действий пользователей АСУ ТП
*Источник: разработано автором Зайчиковым И. Д.*

В настоящей работе рассматриваются нерегламентированные действия, характеризующиеся подменой данных конечных узлов или их полном отключении. В частности, анализируется прямое воздействие на программируемый логический контроллер (ПЛК) АСУ ТП, посредством передачи управляющих команд с автоматизированного рабочего места (АРМ) оператора.

Особенностью задачи мониторинга поведения пользователя в промышленных АСУ является необходимость поиска сведений в больших объемах сетевого трафика. В результате анализа основных моделей поиска, представленного в работе [1], была выбрана ассоциативная модель [2–4]. Для формализации описания модели использованы следующие условные обозначения [7]:

$Q = \{Q_1, Q_2, ..., Q_N\}$ – множество классов образов распознаваемых нерегламентированных действий;

$q^x$ – неизвестное действие пользователя АСУ ТП, подлежащее распознаванию;

$Q^*$ – класс образов к которому отнесено $q^x$;

$P = \{p_1, p_2, ..., p_M\}$ – множество признаков распознавания нерегламентированных действий;

$D = \{D_1, D_2, ..., D_N\}$ – множество диапазонов изменения признаков для каждого распознаваемого действия пользователя;

$B\{q^x, Q_j\}$ – мера близости между неизвестным образом $q^x$ и $j$-ым образом из множества $Q$, $j=1, N$;

$b_{ij}\{<s_i>, Q_j\}$ – коэффициент ассоциативности зарегистрированного значения признака $s_i$ из множества зарегистрированных значений признаков $q^x$ для множества $Q_j$;

$K\{<S^x>, Q\}$ – матрица коэффициентов ассоциативности значений признаков распознаваемых действий из множества $Q$.

Модель распознавания неизвестного образа $q^x$ имеет следующий вид [7]:

$$B\{q^x, Q_j\} = \sum_{i=1}^{M} b_{ij}\{< s_i >, Q_j\},\ i=1, M, \tag{1}$$

$$b_{ij}\{<s_i>, Q_j\} = \begin{cases} 1, \text{если } < s_i^x > \in D_{ij} \\ 0, \text{если } < s_i^x > \notin Q_j \end{cases}, \tag{2}$$

$$K\{<S^x>, Q\} = \begin{pmatrix} v_{11} & v_{12} \cdots v_{1j} \cdots v_{1n} \\ v_{21} & v_{22} \cdots v_{2j} \cdots v_{2n} \\ \cdots & \cdots \cdots v_{ij} \cdots \cdots \\ v_{m1} & v_{m2} \cdots v_{mj} \cdots v_{mn} \end{pmatrix}, \quad (3)$$

$$q^x \in Q^* \in Q : B\{q^x, Q^*\} \geq B\{q^x, Q_j\}_{порог}, Q_j \in Q. \quad (4)$$

Каждое значение в матрице (3) соответствует мере близости признаков распознаваемого действия с признаками образа, к которому оно отнесено. Неизвестное действие пользователя относится к какому-либо множеству образов при превышении порогового значения совпадающих признаков (4).

Достоинством предложенной модели является значительное повышение оперативности поиска информации в большом объёме трафика по сравнению с методами, основанными на полном переборе данных [1].

Структурный анализ сетевого трафика, как основного источника сведений о нерегламентированных действиях пользователя, позволил разработать сигнатуру распознавания нерегламентированных действий, представленную в выражении (5):

$$Sx = \{AT, SIP, DIP, SP, DP, FC, RN, D\}. \quad (5)$$

Основными полями пакета сетевого трафика, содержащими признаки нерегламентированных действий пользователя, являются:

– Arrival Time (*AT*) – время прибытия сетевого пакета, которое позволит отследить время отправки команды на ПЛК;

– Src (*SIP*) и Dst (*DIP*) – IP-адреса АРМ и ПЛК;

– Src Port (*SP*) и Dst Port (*DP*) – порты источника и назначения, соответственно являются портами АРМ и ПЛК;

– Function Code (*FC*) – код функции, который позволяет определить какие действия выполняются командой на ПЛК;

– Reference Number (*RN*) – номер регистра, в котором должны будут измениться данные в ходе выполнения команды на ПЛК;

– Data (*D*) – непосредственно сами данные, которые находятся в регистре.

При превышении пороговых значений представленных выше признаков принимается решение об отнесении действия пользователя к классу нерегламентированных.

На основе полученной модели были разработаны алгоритм и программное средство [5] обнаружения нерегламентированных действий пользователей в сетевых пакетах протокола Modbus TCP, в соответствии с требованиями к системам мониторинга состояния оборудования опасных производств[3]. Схема алгоритма работы программы представлена на рисунке 3. На базе разработанной программы проведен эксперимент по моделированию и обнаружению нерегламентированной команды оператора АСУ ТП. В ходе эксперимента моделировались нерегламентированные команды записи запрещенных данных «2» и «5» в единичные регистры ПЛК «1» и «4» соответственно. Экранная форма обнаружения нерегламентированной команды пользователя представлена на рисунке 4.

В ходе эксперимента фиксировалось среднее время обнаружения нерегламентированного действия пользователя при использовании разработанного метода и программного средства Wireshark [6].

На рисунке 5 представлены графики значений времени обнаружения нерегламентированных действий пользователя АСУ при использовании базового и разработанного методов. Исследование графиков подтвердило повышение оперативности распознавания нерегламентированных действий более чем в 8 раз за счет применения ассоциативного подхода к поиску данных.

Использование разработанного метода позволяет повысить эффективность мониторинга несанкционированных команд управления в АСУ ТП за счёт сокращения времени их распознавания, что, в свою очередь, позволяет снизить риски от угроз, связанных с нерегламентированными действиями пользователей промышленной сети.

[3] ГОСТ Р 53564-2009 «Контроль состояния и диагностика машин. Мониторинг состояния оборудования опасных производств. Требования к системам мониторинга» [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200076745 (дата обращения: 16.04.2022).

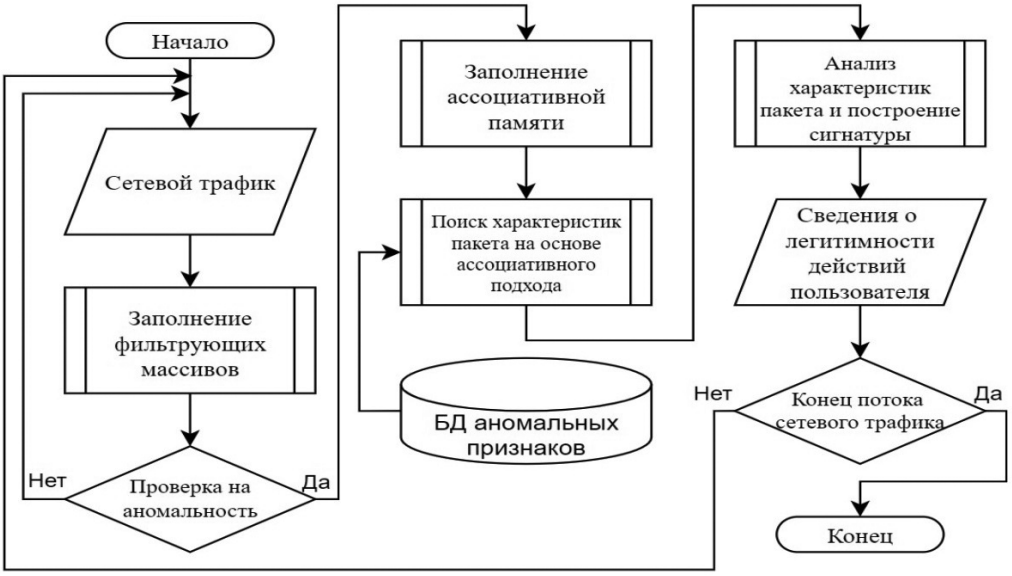
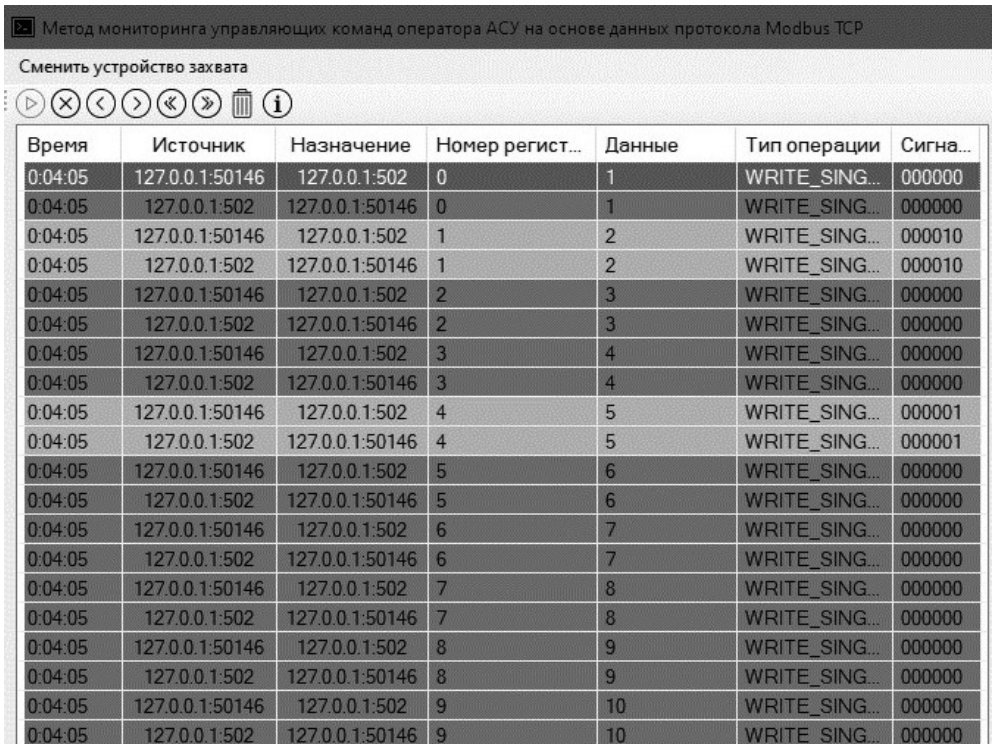



Рисунок 3. Схема обобщенного алгоритма обнаружения нерегламентированных действий пользователя в сетевом трафике АСУ

*Источник: разработано автором Зайчиковым И. Д.*




| Время | Источник | Назначение | Номер регист... | Данные | Тип операции | Сигна... |
|---|---|---|---|---|---|---|
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 0 | 1 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 0 | 1 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 1 | 2 | WRITE_SING... | 000010 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 1 | 2 | WRITE_SING... | 000010 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 2 | 3 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 2 | 3 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 3 | 4 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 3 | 4 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 4 | 5 | WRITE_SING... | 000001 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 4 | 5 | WRITE_SING... | 000001 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 5 | 6 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 5 | 6 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 6 | 7 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 6 | 7 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 7 | 8 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 7 | 8 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 8 | 9 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 8 | 9 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:50146 | 127.0.0.1:502 | 9 | 10 | WRITE_SING... | 000000 |
| 0:04:05 | 127.0.0.1:502 | 127.0.0.1:50146 | 9 | 10 | WRITE_SING... | 000000 |

Рисунок 4. Экранная форма обнаружения нерегламентированного действия пользователя

*Источник: разработано автором Зайчиковым И. Д.*

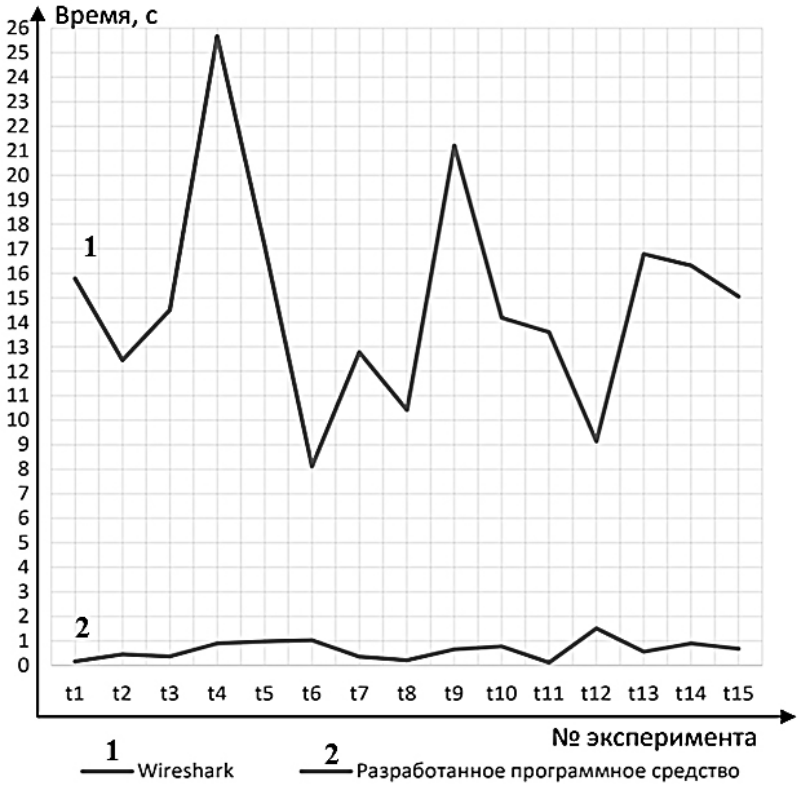



Рисунок 5. Сравнительный график значений времени обнаружения нерегламентированных действий пользователя АСУ

*Источник: разработано автором Зайчиковым И. Д.*

**Литература**

1. Аралбаев Т. З., Абрамова Т. В. Исследование эффективности метода оперативного поиска информации о сетевом трафике на основе ассоциативного принципа // Компьютерная интеграция производства и ИПИ-технологии: материалы VII Всероссийской научно-практической конференции, Оренбург, 12–13 ноября 2015 года. – Оренбург: Оренбургский государственный университет, 2015. – С. 235–239.

2. Ассоциативная память [Электронный ресурс]. – PersCom.ru, 2005–2012 – Режим доступа: http://perscom.ru/index.php/2012-01-20-09-27-13/17-kash-pamyat/33-asociativnaya-pamyat (дата обращения: 16.04.2022).

3. Ассоциативная память [Электронный ресурс]. – Языки программирования, 2002–2015 – Режим доступа: http://life-prog.ru/1_12121_assotsiativnaya-pamyat.html (дата обращения: 16.04.2022).

4. Крыжановский Б. В., Микаэлян А. Л. Ассоциативная память, способная распознавать сильно скоррелированные образы // Доклады Академии наук – 2003. – Т. 390. – № 1. – С. 27–31.

5. Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP: свидетельство о гос. регистрации программы для ЭВМ / Т. В. Абрамова, И. Д. Зайчиков; правообладатель Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – № 2022661790 заявл. 21.06.2022 опубл. 27.06.2022. – 2022. – 1 с.

6. Мешкова Е. В. Перехват и анализ сетевого трафика с помощью «Wireshark» // Контентус. – № 8(49). – С. 158–162.

7. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев и [и др.]. – Оренбург: ОГУ, 2018. – 160 с.

8. Структура АСУ ТП [Электронный ресурс]. – Режим доступа: https://ivctl.ru/o-kompanii/blog/struktura-asu-tp/ (дата обращения: 16.04.2022).

Статья поступила в редакцию: 29.05.2022; принята в печать: 03.03.2023.

Авторы прочитали и одобрили окончательный вариант рукописи.