УДК 004.056
DOI: 10.26102/2310-6018/2022.38.3.020

Алгоритм детектирования источников вредоносных запросов в киберфизических системах

А.О. Исхакова✉, А.Ю. Исхаков, Д.Н. Богачева, А.А. Молотов

Институт проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация
shumskaya.ao@gmail.com✉

Резюме. Работа посвящена решению задачи алгоритмизации процессов управления безопасностью киберфизических систем с помощью детектирования вредоносных запросов от ряда других сопряженных систем, внутренних сервисов или действий человека. Актуальность работы обусловлена высокой степенью критичности защиты от возможной деградации сервисов в рамках осуществления атак на сложные комплексы, отвечающие за интеграцию вычислительных ресурсов в физические сущности. Особое внимание уделено атакам, направленным на отказ в обслуживании киберфизических систем посредством отправки http-flood на веб-интерфейсы управления. Предлагаемый алгоритм детектирования вредоносных запросов анализирует активность всех исследуемых компонентов веб-сервисов киберфизической системы. В работе применяется метод визуального анализа и обработки данных на основе представления в виде единого нормализованного набора. Сырые данные анализируемых запросов группируются специальным образом для детектирования того или иного отклонения как подозрения на угрозу. Приведены примеры изменения данных и реакции системы безопасности. Результаты эксперимента подтверждают, что предложенное алгоритмическое обеспечение позволяет добиться снижения ошибок первого и второго рода в сравнении с широко применяемыми регрессионными моделями в современных межсетевых экранах прикладного уровня.

Ключевые слова: информационная безопасность, вредоносные запросы, источники вредоносных запросов, безопасность киберфизических систем, анализ данных, угрозы, отказ в обслуживании, DDoS, URI, HTTP, POST.

Благодарности: исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-3172.2021.1.6.

Для цитирования: Исхакова А.О., Исхаков А.Ю., Богачева Д.Н., Молотов А.А. Алгоритм детектирования источников вредоносных запросов. *Моделирование, оптимизация и информационные технологии*. 2022;10(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1238
DOI: 10.26102/2310-6018/2022.38.3.020

Algorithm for detecting sources of malicious requests in cyber-physical systems

A.O. Iskhakova✉, A.Y. Iskhakov, D.N. Bogacheva, A.A. Molotov

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation
shumskaya.ao@gmail.com✉

Abstract. The paper is devoted to solving the problem of algorithmic security management processes of cyber-physical systems by detecting malicious requests from a number of other associated systems, internal services or human actions. The relevance of the research is due to the high degree of criticality

of protection against possible degradation of services as part of the implementation of attacks on compound complex systems responsible for the integration of computing resources into physical entities. The authors focus on denial-of-service attacks on cyber-physical systems by sending http-flood to web management interfaces. The proposed algorithm for detecting malicious requests analyzes the activity of all investigated components of cyber-physical system web services. The research employs the method of visual analysis and data processing based on the representation as a single normalized set. Raw data of the analyzed queries is grouped in a specific way to detect a particular deviation as a suspected threat. Examples of data changes and security system responses are given. Experimental results confirm that the suggested algorithmic software achieves first- and second-order error reduction compared to commonly used regression models in modern application-level firewalls.

Keywords: information security, malicious requests, sources of malicious requests, cyber security, data analysis, threats, denial of service, DDoS, URI, HTTP, POST.

Acknowledgements: the reported research was supported by the grant of the President of the Russian Federation for government support of young Russian scientists – candidates of science MK-3172.2021.1.6.

For citation: Iskhakova A.O., Iskhakov A.Y., Bogacheva D.N., Molotov A.A. Algorithm for detecting sources of malicious requests in cyber-physical systems. *Modeling, Optimization and Information Technology*. 2022;10(3). Available from: https://moitvivt.ru/ru/journal/pdf?id=1238 DOI: 10.26102/2310-6018/2022.38.3.020 (In Russ.).

Введение

Разработка и внедрение инновационных киберфизических систем, в том числе сервисных и мобильных роботов, беспилотного транспорта, интернета вещей и других прикладных направлений интеграции интеллектуальных технологий в исполнительные механизмы в окружающей среде, сегодня немыслимы без аспектов обеспечения конфиденциальности, целостности и доступности. Это обусловлено высокой степенью критичности при возможной деградации сервисов в рамках осуществления киберфизических атак [1]. Данный класс атак ориентирован на существенное влияние на физическое пространство посредством эксплуатации уязвимостей в вычислительном контуре и коммуникационной инфраструктуре, предоставляющей интерфейсы для систем контроля за различными датчиками и управления отдельными исполнительными механизмами. Например, при проведении успешной атаки на систему аутентификации злоумышленник может взять под контроль и управление вычислительные или коммуникационные компоненты газопроводов, систем водо- и теплоснабжения, нанося ущерб имуществу или окружающей среде и подвергая риску жизни людей. В результате, безопасность повсеместно рассматривается как одна из важнейших задач при проектировании надежных киберфизических систем [2, 3].

Угроза отказа в обслуживании (Denial of Service, DoS) является популярной категорией сетевых атак, предназначенной для достижения эффекта недоступности того или иного веб-сервиса управления для легитимных пользователей киберфизических систем. Одной из популярных реализаций атак сегодня является метод DDoS-атаки на уровне L7 (HTTP-flood) на веб-ориентированные интерфейсы управления киберфизическими системами. Данные действия особенно разрушительны и трудны для детектирования, так как могут имитировать легитимный трафик [4, 5]. Они предназначены для перегрузки элементов инфраструктуры сервера приложений и выведении их из строя. На этом уровне киберпреступники используют ресурсозатратные вызовы и взаимосвязи приложений, провоцируя систему атаковать себя же. Ниже представлены некоторые из существующих реализаций [6-8]:

1. Slowloris-реализация нацелена на одновременное открытие множества соединений с веб-сервером и отправкой частичных запросов (в том числе добавляя

заголовки HTTP), но никогда не завершая их до момента таймаута. Данные действия значительно затрудняют работу серверов, замедляется время отклика и игнорируя запросы легитимных субъектов доступа (операторов).

2. Медленная POST-атака, в основе которой – отправка правильно заданных заголовков HTTP POST на сервер. Важным аспектом является передача заголовка с очень низкой скоростью, обрывая и инициируя новое соединение. Поскольку заголовок сообщения правильный, сервер отвечает на запрос, расходуя ресурсы на множество таких соединений.

3. Атака медленного чтения, схожая с медленной POST-атакой, но в обратном направлении. Разница в том, что в случае POST-атаки медленно отправляется тело сообщения, а в случае атаки медленного чтения – HTTP-запросы намеренно принимаются и читаются с очень низкой скоростью. Сервер должен держать такие запросы открытыми – это увеличивает нагрузку.

4. Low and slow атака основана на небольшом потоке очень медленного трафика. Этим методом киберпреступники постепенно перегружают серверы, в результате чего запросы реальных пользователей на подключение отклоняются. Для таких атак необходима небольшая полоса пропускания и их трудно предотвратить, так как генерируется трафик аналогичный трафику реальных пользователей.

5. POST-атака с большой полезной нагрузкой основана на использовании расширяемого языка разметки XML. Сервер получает измененные киберпреступниками данные в кодировке XML. Фактический размер таких данных в разы больше, и при попадании на сервер они занимают значительные ресурсы его памяти.

6. Имитация просмотра страниц. Этот тип DDoS-атак имитирует паттерны поведения реальных пользователей на страницах приложения, что приводит к резкому увеличению количества посетителей и усложняет возможность отсеивать легитимный трафик от трафика ботнета.

Материалы и методы

В основе предлагаемого алгоритмического обеспечения лежит процесс, объединяющий сетевую активность в рамках взаимодействия с веб-сервисами и веб-ориентированными интерфейсами управления киберфизической системы в единый набор данных. При этом предполагается обеспечить:

1) сбор данных и приведение их к единому нормализованному виду;

2) группирование данных по определенным признакам и атрибутам;

3) выявление инцидентов на основе обнаружения корреляций и оповещение персонала служб безопасности;

4) визуализация обрабатываемых данных как инструмент анализа и проведение расследования инцидентов;

5) создание отчетов о состоянии активов защищаемой системы.

Подход, используемый в алгоритме, подразумевает разработку монитора обращений (Рисунок 1), основной функцией которого является проведение парсинга всех входящих запросов и первичный контроль полей на содержание значений в стоп-листах.

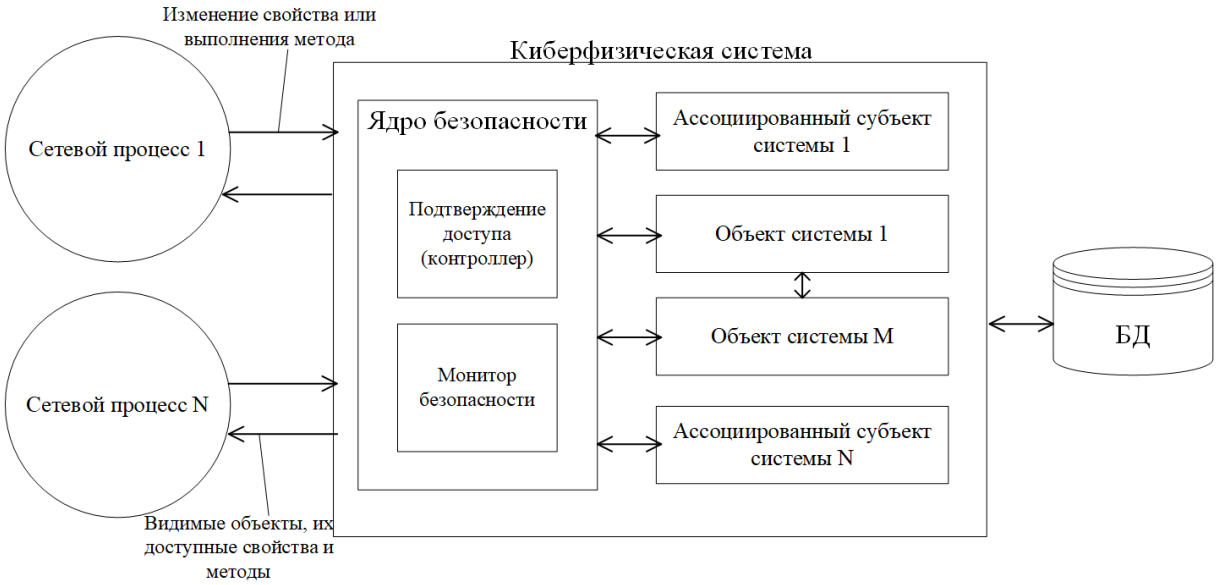

Рисунок 1 – Концептуальная схема реализации предложенного подхода
Figure 1 – Conceptual diagram for implementing the proposed approach

Для анализа данных предполагается подготовка среза трафика для проведения ретроспективной оценки в некотором интервале времени. На Рисунке 2 представлена концептуальная схема применяемого алгоритмического обеспечения.

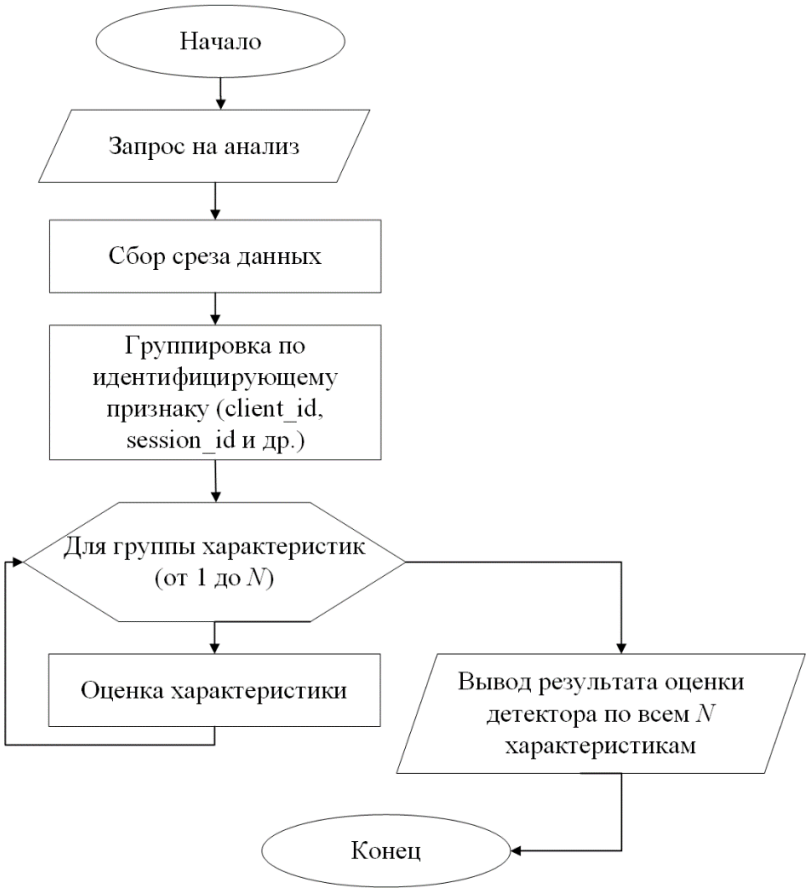

Рисунок 2 – Концептуальная схема основных шагов алгоритмического обеспечения
Figure 2 – Conceptual diagram of the basic steps of the algorithm

В качестве базовых оцениваемых признаков могут выступать такие параметры как количество запросов, среднее время между запросами, стандартное отклонение времени между запросами, доля ошибок с кодом 5XX в ответах приложения данному пользователю, доля ошибок с кодом 4XX в ответах приложения данному пользователю; уникальность запрашиваемых пользователем ресурсов [9]. В основе детектирования источников вредоносных запросов проводилась дополнительная визуальная аналитика различных метрик оценки веб-сервисов интерфейса управления киберфизической системой.

Результаты

Эксперимент проводился на виртуальном полигоне ИПУ РАН, эмулирующем работу киберфизических систем. Были реализованы 5 сценариев (различных техник) управляемой DDoS-атаки на заранее определенные endpoint всех интерфейсов управления. В Таблице 1 представлены результаты эксперимента по оценке эффективности атак на пул серверов управления киберфизической системой в режимах:

1) отработка встроенных механизмов безопасности типа RateLimit;
2) детектирование и блокировка DDoS атак с помощью средства защиты информации (СЗИ) типа межсетевой экран уровня приложений.
3) имплементация предложенного алгоритма в дополнение ко 2 способу.

Таблица 1 – Оценка эффективности детектирования и блокировки источников вредоносных HTTP-запросов
Table 1 – Evaluating the effectiveness of detecting and blocking sources of malicious HTTP requests

Типа атаки	Встроенные механизмы безопасности		Митигация DDoS с помощью регрессионной модели		DDoS-протектор на основе регрессионной модели + предложенное обеспечение	
	FAR, %	FRR, %	FAR, %	FRR, %	FAR, %	FRR, %
Сценарий 1	0,12	0,23	0,08	0,17	0,08	0,15
Сценарий 2	0,03	0,09	0,01	0,11	0,01	0,07
Сценарий 3	0,04	0,14	0,03	0,16	0,03	0,12
Сценарий 4	0,07	0,30	0,03	0,33	0,03	0,20
Сценарий 5	0,12	0,41	0,09	0,27	0,04	0,17

В качестве примера преимуществ предложенного подхода на диаграмме (Рисунок 3) представлено распределение количества запросов субъектов по времени, сгруппировано с помощью различных цветов по признаку «URI-путь обращения». Так, всплески запросов к интерфейсу киберфизической системы в период 21:20-21:40 были ошибочно детектированы программным СЗИ как атака в связи с нетипичным временным диапазоном работы субъектов доступа. При этом, используемые детекторы не зафиксировали фактов вредоносных запросов.

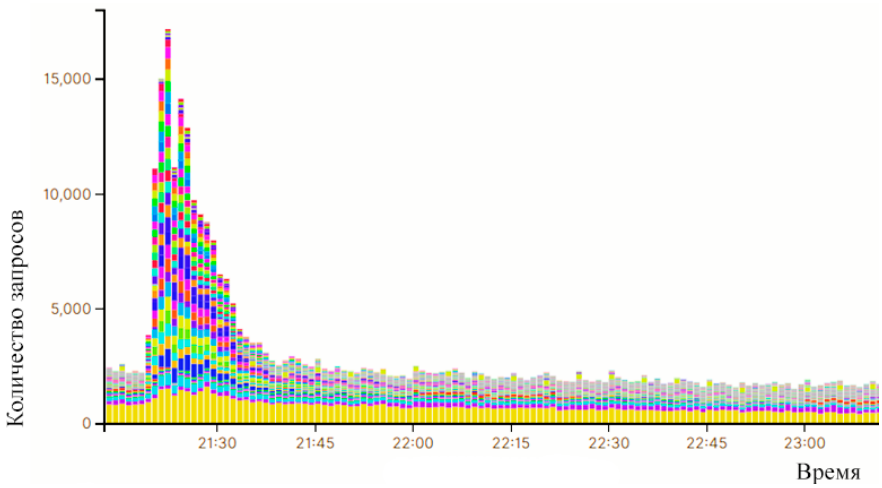

Рисунок 3 – Пример ошибочного детектирования атаки
Figure 3 – Example of an incorrect attack detection

При этом, на Рисунке 4 демонстрируется однородный объем запросов, который ошибочно не был классифицирован СЗИ как атака на сервис киберфизической системы. Детальный разбор данного среза трафика подтвердил признаки попытки реализации атаки, отказ в обслуживании на api одного из сервисов.

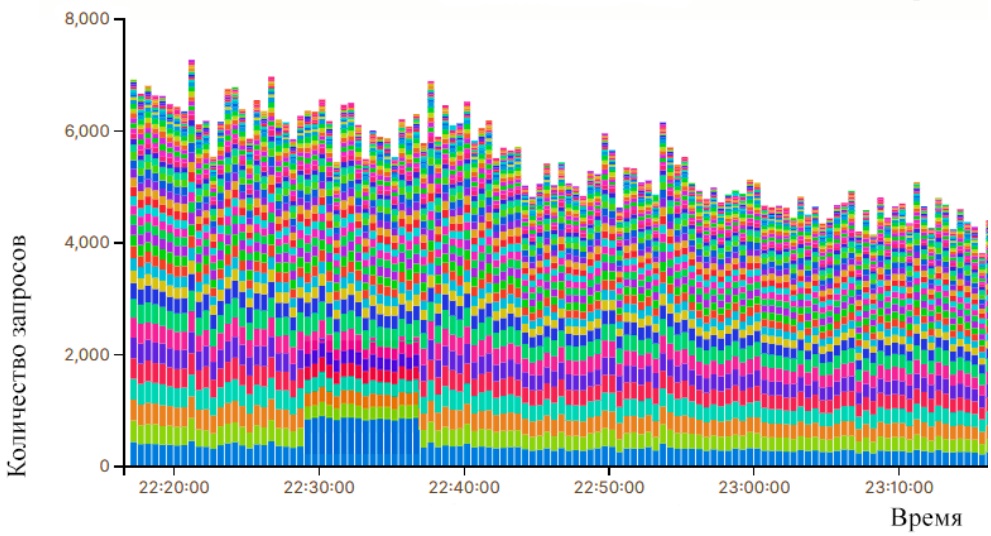

Рисунок 4 – Пример ошибочного пропуска атаки, направленной на location api
Figure 4 – Example of a missed attack targeting the location api

Обсуждение

Программная имплементация алгоритмического решения, представленного в данной статье, позволила обнаружить нехарактерные изменения в векторах запросов в 22:28-22:38 на основе одного из признаков (в данном случае в качестве второго параметра группировки среза трафика использовался запрашиваемый URI). Таким образом, применяемый подход позволяет добиться снижения ошибок первого и второго рода в сравнении с широко применяемыми регрессионными моделями в современных межсетевых экранах прикладного уровня.

Применение современных высокоэффективных интеллектуальных методов классификации с помощью машинного обучения позволит снизить вычислительные

ресурсы и затраты на проведение глубинного анализа вредоносных запросов, а также повысить степень его достоверности [10-12]. При решении частных задач будет применяться теория информационной безопасности и методы защиты информации В дальнейшем предполагается сформировать более полную методологическую базу, включающую глубокую инспекцию признаков трафика и угроз, с которыми сталкивается инфраструктура киберфизических систем.

Данные алгоритмы обеспечат возможность на основании результата постоянного мониторинга и нейросетевого анализа информационных потоков веб-компонентов киберфизической системы, генерируемых конкретным субъектом доступа, а также исходя из оценки риска угрозы при нетипичном поведении пользователя относительно его многокомпонентного профиля, подбирать набор и тип факторов, требуемых для аутентификации в режиме реального времени. Реализация многопоточного режима работы для создаваемого комплекса позволит обеспечить высокое быстродействие в условиях распределенных атак на киберфизические системы.

Заключение

Исследования по автоматизированному анализу вредоносных запросов в веб-ориентированных сервисах и оперативному детектированию их источников расширяют базу теоретических знаний о методах выявления потенциально опасных потоков информации. Детальное рассмотрение проблемы позволяет моделировать средства защиты на основе классификации поступающих запросов посредством применения методов интеллектуального анализа данных. Совокупность теоретических и методологических наработок, полученных в результате выполнения данного исследования, станет основой для формирования научно-обоснованных принципов совершенствования системы противодействия атакам на веб-ориентированные компоненты киберфизических систем. Актуальность задач обеспечения комплексной безопасности киберфизических систем за счет специализированных научно обоснованных методов организации защищенного взаимодействия их компонентов обусловлена стремительным ростом кибератак по всему миру – сложных, многошаговых и зачастую адаптированных под целевую инфраструктуру.

СПИСОК ИСТОЧНИКОВ

1. Исхаков А.Ю., Мещеряков Р.В., Исхаков С.Ю. Проблемы применения индикаторов компрометации для проактивного поиска угроз в работе робототехнических комплексов. *Управление развитием крупномасштабных систем (MLSD'2021). Труды Четырнадцатой международной конференции. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. Москва*; 2021. С. 1340–1347.
2. Черкасов А.Н., Туркин Е.А. Разработка модели обнаружения вредоносных программ на основе анализа последовательностей API-запросов. *Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки*. 2021;2(281):90–96.
3. Meshcheryakov R., Iskhakov A., Mamchenko M., Romanova M., Uvaysov S., Amirgaliyev Y., Gromaszek K. A Probabilistic Approach to Estimating Allowed SNR Values for Automotive LiDARs in «Smart Cities» under Various External Influences. *Sensors (Basel)*. 2022;22(2):609. DOI: 10.3390/s22020609
4. Salomatin A.A., Iskhakov A.Y., Meshcheryakov R.V. Comparison of the Effectiveness of Countermeasures Against Tracking User Browser Fingerprints. *IFAC-PapersOnLine*. 2022;55(9):244–249. DOI: 10.1016/j.ifacol.2022.07.043.

5. Iskhakova A., Meshcheryakov R., Iskhakov A., Kulagina I. Analysis of textual content as a mechanism for ensuring safety of the socio-cyberphysical system. *SIBCON 2021 - International Siberian Conference on Control and Communications*. 2021:9438924. DOI: 10.1109/SIBCON50419.2021.9438924.
6. Шапиро Л. Атаки DDoS. Часть 4. Военные хитрости. *БИТ. Бизнес & Информационные технологии.* 2015;8(51):22–23.
7. Янгляев И. Какие бывают DDoS-атаки и почему защищаться сложнее из года в год. [Электронный ресурс]. Доступно по: https://www.orange-business.com/ru/blogs/kakie-bivayut-ddos-ataki-i-pochemu-zaschischatsya-slozhnee-iz-goda-v-god (дата обращения 01.08.2022).
8. Tobin D., Bogomolov A., Golosovskiy M. Model of Organization of Software Testing for Cyber-Physical Systems. *Studies in Systems, Decision and Control.* 2022;418:51–60.
9. Казарян К.К., Белан В.В. Вредоносные запросы. *StudNet.* 2022;1(5):58–64.
10. Болгов А.О., Каменских А.Н. Подбор оптимальных параметров для методов машинного обучения при обнаружения вредоносных запросов к веб-приложениям. *Международная конференция по мягким вычислениям и измерениям*. 2022;1:290–294.
11. Успенский Е.Н., Стариков А.С., Ромашкиина Г.В., Норкина А.Н. Адаптивное обнаружение вредоносных запросов в веб-атаках. *Актуальные проблемы менеджмента, экономики и экономической безопасности. Сборник материалов Международной научной конференции.* 2019:308–311.
12. Feher K. Digital identity and the online-self: footprint strategies – an exploratory and comparative research study. *Journal of information science.* 2019;47(2):1–5.

REFERENCES

1. Iskhakov A.Y., Meshcheryakov R.V., Iskhakov S.Y. Problems of Application of Compromise Indicators for Proactive Threat Search in Robotics Complexes. *Management of Large-Scale Systems Development (MLSD'2021). Proceedings of the Fourteenth International Conference. Edited by S.N. Vasiliev, A.D. Tsvirkun. Moscow*; 2021. 1340–1347. (In Russ.).
2. Cherkasov A.N., Turkin E.A. Development of a malware detection model based on the analysis of API-request sequences. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-matematicheskiye i tekhnicheskiye nauki = The Bulletin of the Adyghe State University. Series 4 "Natural-Mathematical and Technical Sciences".* 2021;2(281):90–96. (In Russ.).
3. Meshcheryakov R., Iskhakov A., Mamchenko M., Romanova M., Uvaysov S., Amirgaliyev Y., Gromaszek K. A Probabilistic Approach to Estimating Allowed SNR Values for Automotive LiDARs in «Smart Cities» under Various External Influences. *Sensors (Basel).* 2022;22(2):609. DOI: 10.3390/s22020609.
4. Salomatin A.A., Iskhakov A.Y., Meshcheryakov R.V. Comparison of the Effectiveness of Countermeasures Against Tracking User Browser Fingerprints. *IFAC-PapersOnLine.* 2022;55(9):244–249. DOI: 10.1016/j.ifacol.2022.07.043.
5. Iskhakova A., Meshcheryakov R., Iskhakov A., Kulagina I. Analysis of textual content as a mechanism for ensuring safety of the socio-cyberphysical system. *SIBCON 2021 - International Siberian Conference on Control and Communications*. 2021:9438924. DOI: 10.1109/SIBCON50419.2021.9438924.
6. Shapiro L. DDoS attacks. Part 4. Military tricks. *BIT. Biznes & Informatsionnyye tekhnologii*. 2015;8(51):22–23. (In Russ.).
7. Yangliaev I. What DDoS attacks are and why it is more difficult to defend oneself from year to year. Available from: https://www.orange-business.com/ru/blogs/kakie-bivayut-

ddos-ataki-i-pochemu-zaschischatsya-slozhnee-iz-goda-v-god (accessed 01.08.2022). (In Russ.).
8. Tobin D., Bogomolov A., Golosovskiy M. Model of Organization of Software Testing for Cyber-Physical Systems. *Studies in Systems, Decision and Control*. 2022;418:51–60.
9. Kazarian K.K., Belan V.V. Malicious queries. *StudNet*. 2022;1(5):58–64. (In Russ.).
10. Bolgov A.O., Kamenskikh A.N. Selection of optimal parameters for machine learning methods for detecting malicious queries to web applications. *Mezhdunarodnaya konferentsiya po myagkim vychisleniyam i izmereniyam = International Conference on Soft Computing and Measurement*. 2022;1:290–294. (In Russ.).
11. Uspensky E.N., Starikov A.S., Romashkina G.V., Norkina A.N. Adaptive detection of malicious requests in web attacks. *Aktual'nyye problemy menedzhmenta, ekonomiki i ekonomicheskoy bezopasnosti. Sbornik materialov Mezhdunarodnoy nauchnoy konferentsii*. 2019:308–311. (In Russ.).
12. Feher K. Digital identity and the online-self: footprint strategies – an exploratory and comparative research study. *Journal of information science*. 2019;47(2):1–5.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Исхаков Андрей Юнусович, кандидат технических наук, старший научный сотрудник Института проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация.
e-mail: iskhakovandrey@gmail.com
ORCID: 0000-0002-6603-265X

Andrey Yunusovich Iskhakov, Candidate of Technical Sciences, Senior Researcher, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation.

Исхакова Анастасия Олеговна, кандидат технических наук, старший научный сотрудник Института проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация.
e-mail: shumskaya.ao@gmail.com
ORCID: 0000-0001-8358-298X

Anastasia Olegovna Iskhakova, Candidate of Technical Sciences, Senior Researcher, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation.

Богачева Дарья Николаевна, инженер-программист Института проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация.
e-mail: bogacheva@ipu.ru

Darya Nikolaevna Bogacheva, Software Engineer, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation.

Молотов Александр Анатольевич, инженер-программист Института проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация.
e-mail: alpha.sphere@ya.ru

Aleksandr Anatolyevich Molotov, Software Engineer, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation.

Статья поступила в редакцию 23.09.2022; одобрена после рецензирования 26.09.2022; принята к публикации 29.09.2022.

The article was submitted 23.09.2022; approved after reviewing 26.09.2022; accepted for publication 29.09.2022.