# Интеллектуальные технологии и информационная безопасность

УДК 004.056.5
DOI:10.38028/ESI.2023.29.1.013

## Подход к защите интерфейсов управления киберфизической системой от угроз нарушения доступности

**Исхаков Андрей Юнусович, Жарко Елена Филипповна**
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, Москва, *iay@ipu.ru*

**Аннотация.** Необходимость развития существующих подходов и научно-технических решений в области обеспечения информационной безопасности вызвана стремительным развитием киберфизических систем, требующих адаптации механизмов защиты под новые архитектуры, технические ограничения и особенности функционирования. Одним из важных, но слабо рассмотренных в мировой литературе направлений защиты киберфизических систем, остаются вопросы построения эффективных протекторов, нивелирующих угрозы нарушения доступности интерфейсов взаимодействия на прикладном уровне. Нарушение доступности подсистем управления для рассматриваемых объектов может привести к трагическим последствиям, в связи с чем требуется уже сейчас проводить комплексный анализ и модернизацию подходов к их защите от атак типа DDoS. В данном исследовании предлагается подход к обеспечению защиты интерфейсов управления киберфизической системой от внешних воздействий, направленных на нарушение доступности за счет отсутствия технических возможностей эшелонирования защиты прикладного программного обеспечения. В качестве объекта киберфизической системы был использован виртуальный полигон беспилотных транспортных средств. Приводится анализ применимости существующих подходов к защите от атак прикладного уровня для выбранного класса объектов, предлагается адаптированный подход к защите объекта и проводится исследование его эффективности.

**Ключевые слова:** киберфизические системы, нарушение доступности, информационная безопасность, атаки, беспилотные транспортные средства

**Цитирование:** Исхаков А.Ю. Подход к защите интерфейсов управления киберфизической системой от угроз нарушения доступности / А.Ю. Исхаков, Е.Ф. Жарко // Информационные и математические технологии в науке и управлении. – 2023. – № 1(29). – С. 149-157. – DOI:10.38028/ESI.2023.29.1.013.

**Введение.** В течение последнего года с распределенными атаками типа «отказ в обслуживании» сталкивались практически все объекты критически важной информационной инфраструктуры, предоставляющие сервисы, доступные из внешней сети Интернет. Так, согласно [1], статистика направленных DDoS-атак на отечественные ресурсы стала не просто рекордной, а беспрецедентной не только по количеству и интенсивности атак, но и по уровню подготовки злоумышленников. Безусловно, существуют регуляторные требования [2], которые обязывают владельцев значимых объектов критической информационной инфраструктуры запрещать удаленный доступ, а также исключить возможности бесконтрольного доступа к управлению лицами, не являющимися работниками предприятия.

Наряду с этим, следует отметить тренд современного общества на развитие технологий умного города, беспилотного транспорта и других концепций, невозможных без предоставления массового внешнего (но не бесконтрольного) доступа, в том числе, к беспилотным транспортным средствам – средствам повышенной опасности. В связи с этим, необходимо уже сейчас, на заре интеграции таких систем в массовый сектор, разрабатывать и апробировать научно-технические решения для противодействия вредоносным воздействиям и различным атакам информационной безопасности.

В данной статье рассматривается подход к обеспечению защиты от внешних воздействий беспилотных транспортных средств от Flood-атак на интерфейсы управления прикладного уровня.

**1. Необходимость защиты интерфейсов управления.** Целью создания умного города является улучшение качества жизни жителей с помощью технологии городской цифровизации для повышения эффективности обслуживания и удовлетворения нужд резидентов. Развитие беспилотных транспортных средств является одной из составляющих данного процесса. Создание эффективной системы мониторинга и управления таким транспортом, обеспечивающей, в условиях их массового использования (в различных средах – земля/воздух), безопасное функционирование и максимальную пропускную способность транспортной системы, является одним из условий реализации планов создания умных городов.

На рисунке 1 представлено место исследуемых атак в разрезе различных классификаций вредоносных воздействий, направленных на беспилотные транспортные средства (БТС).

| **Расстояние от злоумышленника до БТС** | **Цели воздействия** | **Уровень воздействия в соответствии с моделью OSI** |
|---|---|---|
| физический доступ к автомобилю: например, через интерфейс OBD (бортовая диагностика) | Нарушение конфиденциальности (получить доступа к информационно-развлекательной системе для записи голоса или для получения информации о маршруте через навигатор) | L1 - физический. Работа с сигналами и двоичными данными |
| | | L2 - канальный. Установка соединения и физическая адресация. |
| | | L3 - сетевой. Взаимодействие устройств друг с другом |
| ближнее расстояние: сюда входят пассивная сигнализация (10 см), система считывания давления в шинах (1 м), бесключевые системы открытия и запуска двигателя (5–20 м) и все системы, подключённые через Bluetooth (10 м); | Нарушение целостности (изменить скорость БТС, воздействуя на электронные блоки, управляющие акселератором, или воздействуя непосредственно на тормоз) | L4 - транспортный. Транспортировка данных между конечными пунктами |
| | | L5 - сеансовый. Управление соединениями |
| **большие расстояния: системы связи Wi-Fi или 4/5G, системы управления дорожной инфраструктурой, мобильные приложения, предназначенные для управления БТС.** | **Нарушение доступности (блокировать доступ легитимного оператора / вывести из строя систему поддержки и принятия решений)** | L6 – представления. Кодирование и декодирование данными |
| | | **L7 - прикладной. Доступ к сетевым ресурсам** |

**Рис. 1.** Характеристики рассматриваемых воздействий на киберфизические системы

Угрозы нарушения доступности направлены на снижение работоспособности системы обработки данных, либо на реализацию полной блокировки доступа субъектов к некоторым ее ресурсам [3-14]. При этом для нарушения доступности основной функциональности не всегда необходимо достигать внутренних отказов информационной системы (основных модулей), зачастую злоумышленникам достаточно добиться отказа поддерживающей инфраструктуры или интерфейсов управления. Когда речь идет о беспилотных транспортных средствах и умной дорожной инфраструктуре, достаточным является блокировка интерфейсов управления, как для операторов машин, так и операторов облачных центров мониторинга транспортной инфраструктуры (например, V2X технологий). На рисунке 2 представлены выдержки из исследования актуальных угроз информационной безопасности современного автотранспорта [15].

Ранее проведенный авторами настоящего исследования анализ уязвимостей и точек отказа беспилотных транспортных средств [16] свидетельствует о необходимости защиты высокоуровневых интерфейсов управления беспилотных транспортных средств от атак на прикладном уровне.


**Рис. 2.** Актуальные угрозы информационной безопасности автотранспорта
RSU (Roadside Unit) – придорожные блоки (модули)

**2. Особенность защиты в условиях ограничений.** Классические подходы с выстраиванием нескольких эшелонов защиты, которые используются для обеспечения безопасности современных IT-инфраструктур, не могут быть применены в защите интерфейсов управления беспилотными транспортными средствами. Это связано с архитектурой и особенностями текущей реализации подобных решений, в частности:

- ограниченными вычислительными ресурсами оборудования, установленного непосредственно на беспилотном транспортном средстве, которые можно использовать в реализации задач механизмов защиты;
- невозможностью повсеместного применения облачных средств защиты информации (СЗИ), поскольку зачастую требуется предоставление доступа операторов в локализованных сетевых сегментах без доступа в глобальную сеть;
- необходимость обеспечения возможности децентрализованных схем взаимодействия, не предусматривающих возможность установки единого инструмента для глубокой инспекции трафика;
- невозможностью передачи ключей шифрования трафика для сторонних систем.

Разрабатываемый подход заключается в разработке такого алгоритмического обеспечения, которое, с учетом вышеперечисленных особенностей, может быть локально интегрировано в подсистему защиты информации беспилотного транспортного средства и осуществлять блокировку атак «Отказ в обслуживании», направленных на интерфейсы взаимодействия с точки зрения инспектирования прикладного уровня.

**3. Предлагаемый подход.** В основе предлагаемого подхода лежит ранее разработанное авторским коллективом алгоритмическое обеспечение детектирования источников вредоносных запросов в киберфизических системах [17]. При этом была учтена необходимость обеспечения имплементации защитных механизмов локально, опираясь на вычислительные мощности вычислителя и без связи с централизованной системой защиты информации.

На протяжении 2022 года в сети Интернет была размещена HoneyPot система, эмулирующая сегмент киберполигона с беспилотными транспортными средствами посредством специально подготовленных Linux контейнеров. Для защиты от L3-L4 атак был развернут

межсетевой экран, а также система предотвращения вторжений (IPS) с существенными исключениями по сервисам. Посредством проброса наиболее популярных TCP-портов для веб-сервисов был открыт массовый доступ по нескольким выделенным IP-адресам в виртуализованную инфраструктуру без необходимости прохождения процесса авторизации. Часть контейнеров были открыты для любого пользователя без необходимости ввода каких-либо учетных данных. Подобные сервисы демонстрировали по заранее заданным сценариям случайные значения параметров беспилотного транспортного средства (мониторинга двигателей, приводов и различных датчиков, установленных на борту). Другая часть веб-сервисов представляла собой эмулятор системы управления транспортным полигоном. С целью создания эффекта интерактивности, веб-интерфейс отображал нагрузку на системные ресурсы, включая загрузку центрального процессора, оперативной памяти, среднее время ответа front-сервером клиентам. Злоумышленнику требовалось подобрать данные для формы HTTP-аутентификации, при этом были реализованы несколько учетных записей с уровнем доступа ReadOnly со словарными паролями, которые в автоматизированном режиме перебиралось большинством brute-force сканеров. Для сегмента с «защищенной» системой управления транспортным полигоном был установлен межсетевой экран уровня приложений одного из известных отечественных вендоров. В результате проведенного анализа сценариев, которые применялись злоумышленниками в разрезе атаки «Отказ в обслуживании», были сформированы основные векторы атак злоумышленников – GET и POST flood на основные формы, эмулирующие команды управления (конфигурирования) беспилотного транспортного средства, а также атаки малого объема (“Low and Slow”).

Учитывая проведенный этап, был выработан следующий подход к защите от атак типа «Отказ в обслуживании» на интерфейсы прикладного уровня. На рисунке 3 представлена скорректированная структура подсистемы защиты, внедряемая непосредственно в беспилотное транспортное средство.

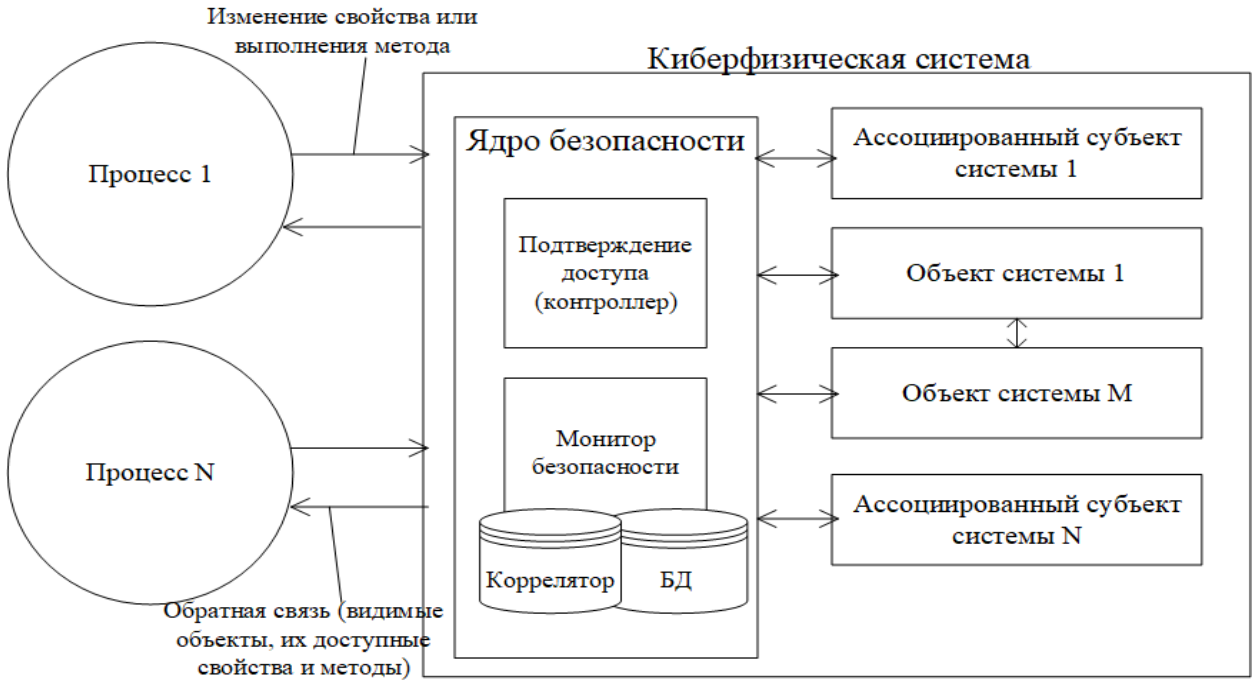


**Рис. 3.** Структура подсистемы защиты от DDoS атак на интерфейсы управления с учетом особенностей имплементации в инфраструктуру беспилотных транспортных средств

Опыт использования межсетевого экрана прикладного уровня в HoneyPot эксперименте продемонстрировал необходимость внедрения коррелятора, который бы учитывал основные метрики в HTTP-запросах на веб-интерфейс управления. Поскольку атаки проводились в

большей степени на бизнес-логику интерфейсов таким образом, чтобы не зафиксировать превышение пороговых значений в трафике, необходимо реализовывать систему защиты, основанную не на количественных показателях общего среза трафика, а на основании инспектирования кодов запросов от операторов.

В случае имплементации на беспилотное транспортное средство с низкой вычислительной способностью предлагается ограничить функциональность монитора безопасности исключительно оценкой доли возвращаемых интерфейсом ошибок (4xx, 5xx) с группировкой по сессии субъекта, а также оценкой стандартного отклонения времени между запросами и количеством уникальных запрашиваемых субъектом ресурсов. В отличие от применения ранее представленного подхода по обеспечению безопасности информационных/киберфизических систем, в случае защиты интерфейса управления беспилотного транспортного средства следует осуществлять быструю реакцию и передачу управляющего воздействия на межсетевые экраны уровня L3-L4 с блокировкой источников вредоносных воздействий не только по IP-адресам, но и автономным системам. Это связано с ограниченным количеством числа операторов, а также риском быстрого вывода сервиса из строя по причине ограниченных аппаратных ресурсов.

**4. Результаты.** Эксперимент по оценке эффективности предложенного подхода проводился на представленной ранее HoneyPot системе, эмулирующей наличие систем. Реализация коррелятора была выполнена на языке Python. Для наглядности, был использован наименьший инструментарий, включающий оценку кодов ошибок, среднее время ответа и стандартные пороги по количеству запросов в рамках одной сессии. В ходе эксперимента внешний доступ к системам был закрыт. В качестве генераторов паразитного трафика, в том числе, использовались виртуальные машины с установленными утилитами: HULK, Slowloris, LOIC, Xoic, DDOSIM, Rudy. Были реализованы 5 сценариев (различных техник) управляемой DDoS-атаки на заранее определенные endpoint всех интерфейсов управления. Используемый подход показал свою эффективность и возможность применения для беспилотных транспортных средств в децентрализованной схеме управления.

Так, на рисунке 4 представлен пример успешного детектирования целенаправленной атаки на форму аутентификации при условии стабильного тренда подключений (отсутствие взрывного эффекта).


**Рис. 4.** Пример успешного детектирования вредоносной активности на сервис аутентификации

В таблице 1 представлена консолидация оценки эффективности определения DDoS атак на интерфейсы управления прикладного уровня. Критерий $D$ – «Деградация сервиса» – соответствует появлению 500, 502 и 503 ошибок от веб-сервиса интерфейса в течение более 30 секунд тестирования. Критерий $t$ – среднее время детектирования атаки и начала блокирующих действий.

**Таблица 1.** Оценка эффективности определения DDoS атак прикладного уровня на интерфейсы управления

| Тип атаки | Методы защиты интерфейса | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Встроенные средства защиты интерфейса | | Интегрированный WAF с стандартной политикой безопасности | | Интегрированный WAF + HMM-модель защиты от DDoS | | Предложенный подход + интегрированный WAF + HMM-модель защиты от DDoS | |
| | *D* | *t*, сек | *D* | *t*, сек | *D* | *t*, сек | *D* | *t*, сек |
| GET FLOOD | + | 180 | + | 180 | - | 60 | - | 30 |
| POST FLOOD | + | 180 | + | 60 | + | 60 | - | 30 |
| Slowloris | + | 0 | - | 60 | - | 60 | - | 30 |
| POST-атака с большой полезной нагрузкой | + | 30 | - | 60 | - | 60 | - | 15 |

Встроенные средства защиты веб-сервисов со статичными порогами показали свою несостоятельность. Применение предложенного подхода и более строгих правил блокировки источников запросов позволили добиться отсутствия эффекта деградации сервиса. При этом стоит отметить, что данный подход ориентирован на конкретный класс систем и, учитывая вышеописанные ограничения, предлагается с целью оптимизации инспекционных механизмов и ускорения реакции систем защиты интерфейсов управления беспилотных транспортных средств.

**Заключение.** Учитывая возможные масштабы DDoS-атак с использованием ботнетов и степень критичности стремительно растущих киберфизических систем, действительно важной задачей является разработка научно-технических решений противодействия угрозам «Отказ в обслуживании», несущим опасность не только отдельным компонентам киберфизических систем, но и жизни и здоровью окружающих.

Защита от атак «Отказ в обслуживании» на уровне приложений требуе адаптивной стратегии, включая возможность ограничения трафика на основе определенных наборов правил, которые могут регулярно меняться. Между тем, особенности функционирования беспилотных транспортных средств не всегда позволяют обеспечить общедоступные интерфейсы взаимодействия полноценным набором межсетевого экранирования и глубокой инспекции трафика. В данном исследовании была предпринята попытка разработки подхода к обеспечению защиты интерфейсов управления киберфизической системой от внешних воздействий, направленных на нарушение доступности за счет отсутствия технических возможностей эшелонирования защиты прикладного программного обеспечения.

**Благодарности.** Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-06044.

## Список источников

1. Amiri I.S., Soltanian M.R.K. Theoretical and experimental methods for defending against DDoS attacks. Waltham: Syngress is an imprint of Elsevier, 2016, 62 p.
2. Кульмамиров С. А.Современное состояние обнаружения DDOS-атак и противодействие к ним / С. А. Кульмамиров, А. А. Баймаманова, 2020. – № 4-2(60). – С. 50-57.
3. Власенко А.В. Идентификация DDOS-атак на web-серверы / А.В. Власенко, П.И. Дзьобан // Прикаспийский журнал: управление и высокие технологии, 2019. – № 1(45). – С. 181-187.

4. Титов Ф.М. Исследование методов защиты от атаки DDOS / Ф.М. Титов // Научные междисциплинарные исследования, 2021. – №5. – С. 36-41.
5. Bhattacharyya D.K., Kalita J.K. DDoS Attacks: Evolution, Prevention, Reaction and Tolerance. Chapman and Hall/CRC, 2016, 312 p.
6. Кусаинова У.Б. Методы противодействия угрозам нарушения информационной безопасности при ddos-атаках / У.Б. Кусаинова, Ж. Сарсенбаева, Д.В. Плескачев // Наука и реальность, 2020. – №4. – С. 35-43.
7. Rahal B.M., Santos A., Nogueira M. A Distributed Architecture for DDoS Prediction and Bot Detection. IEEE Access, 2020, vol. 8, pp. 159756-159772.
8. Rao Varre D.N.M., Bayana J. A secured botnet prevention mechanism for HTTP flooding based DDoS attack. 3rd International Conference for Emerging Technology (INCET), Belgaum, India, 2022, pp. 1-5.
9. Dhanapal A., Nithyanandam P. An effective mechanism to regenerate HTTP flooding DDoS attack using real time data set. International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India, 2017, pp. 570-575.
10. Nashat D., Khairy S., Hassan M.M. Detection of application layer DDoS attack based on SIS epidemic model. IEEE Access, 2021, vol. 9, pp. 159827-159832.
11. Beckett D., Sezer S. HTTP/2 Cannon: Experimental analysis on HTTP/1 and HTTP/2 request flood DDoS attacks. Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 2017, pp. 108-113.
12. Yang S.J., Huang H.L. Design a hybrid flooding attack defense scheme under the Cloud Computing Environment. IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS), Beijing, China, 2019, pp. 41-46.
13. Vanitha K.S., Uma S.V., Mahidhar S.K. Distributed denial of service: Attack techniques and mitigation. International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 226-231.
14. Wang J., Zhang M., Yang X., Long K., Xu J. HTTP-sCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs. China Communications, 2015, vol. 12, no. 2, pp. 118-128.
15. Правиков Д.И. Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств / Д.И. Правиков, Е.А. Пономарева, В.П. Куприяновский // International Journal of Open Information Technologies, 2020. – №6. – С. 98-103.
16. Iskhakov A.Yu., Mamchenko M.V. Vulnerabilities, Points of failure and adaptive protection methods in the context of group control of unmanned vehicles. J. Phys., Conf. Ser, vol. 1864, pp. 1-10.
17. Исхакова А.О. Алгоритм детектирования источников вредоносных запросов в киберфизических системах / А.О. Исхакова, А.Ю. Исхаков, Д.Н. Богачева, А.А. Молотов // Моделирование, оптимизация и информационные технологии, 2022. – № 10(3). – С. 1-9.

***Исхаков Андрей Юнусович.*** *Кандидат технических наук, старший научный сотрудник ИПУ РАН. Область научных интересов: информационная безопасность, идентификация и аутентификация субъектов доступа, анализ данных, интернет вещей, системы поддержки и принятия решений. AuthorID: 925433, SPIN: 3390-0291, ORCID: 0000-0002-6603-265X, iskhakovandrey@gmail.com, Россия, Москва 117997, Профсоюзная улица, д.65.*

***Жарко Елена Филипповна.*** *Кандидат технических наук, доцент, старший научный сотрудник ИПУ РАН. Область научных интересов: кибербезопасность, верификация, валидация, автоматизация, обеспечение качества программного обеспечения, объекты повышенного риска, прогностические модели, имитационные модели. AuthorID: 30748, SPIN: 6288-1776, ORCID: 0000-0002-8895-4786, elena_hot@inbox.ru, Россия, Москва 117997, Профсоюзная улица, д.65.*

UDC 004.056.5
DOI:10.38028/ESI.2023.29.1.013

# Approach to protecting cyber-physical system management interfaces from accessibility threats

**Andrey Yu. Iskhakov, Elena F. Jharko**
V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences,
Russia, Moscow, *iay@ipu.ru*

**Abstract.** The need to develop existing approaches and scientific and technical solutions in the field of information security is caused by the rapid development of cyber-physical systems that require adaptation of protection mechanisms to new architectures, technical limitations and features of operation. One of the important, but poorly considered in the world literature areas of protection of cyber-physical systems, are the issues of building effective protectors that mitigate threats to the accessibility of interfaces at the application level. Disruption of the availability of control subsystems for the objects in question can lead to tragic consequences, so a comprehensive analysis and modernization of approaches to protect them from DDoS attacks is already required. This study proposes an approach to protecting cyber-physical system control interfaces from external influences aimed at disrupting accessibility due to the lack of technical capability to echelle the protection of application software. As the object of the cyber-physical system, a virtual polygon of unmanned vehicles was used. An analysis of applicability of existing approaches to protection against application layer attacks for the selected class of objects is given, an adapted approach to object protection is proposed and its effectiveness is investigated.

**Keywords:** cyber-physical systems, availability disruption, information security, attacks, unmanned vehicles

**Acknowledgements:** The reported study was partially funded by RFBR, project number 19-29-06044.

## References

1. Amiri I.S., Soltanian M.R.K. Theoretical and experimental methods for defending against DDoS attacks. Waltham: Syngress is an imprint of Elsevier, 2016, 62 p.
2. Kulmamirov S.A., Baymanova A.A. Sovremennoe sostoyanie obnaruzheniya DDOS-atak i protivodejstvie k nim [The current state of DDOS attack detection and countermeasures]. Aktual'nyye nauchnyye issledovaniya v sovremennom mire [Current scientific research in the modern world], 2020, no. 4-2(60), p. 50-57.
3. Vlasenko A.V., Dzoban P.I. Identifikaciya DDOS-atak na web-servery [Identification of DDOS-attacks on web-servers]. Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii [The Caspian Journal: Management and High Technologies], 2019, no. 1(45), p. 181-187.
4. Titov F.M. Issledovanie metodov zashchity ot ataki DDOS [Investigation of methods of protection against DDOS attacks]. Nauchnyye mezhdistsiplinarnyye issledovaniya [Scientific Interdisciplinary Research], 2021, no.5, p. 36-41.
5. Bhattacharyya D.K., Kalita J.K. DDoS Attacks: Evolution, Prevention, Reaction and Tolerance. Chapman and Hall/CRC, 2016, 312 p.
6. Kusainova U.B., Sarsenbayeva Zh., Pleskachev D.V. Metody protivodejstviya ugrozam narusheniya informacionnoj bezopasnosti pri ddos-atakah [Methods of countering threats to information security during ddos-attacks]. Nauka i real'nost' [Science & Reality], 2020, no. 4, p. 35-43.
7. Rahal B.M., Santos A., Nogueira M. A Distributed Architecture for DDoS Prediction and Bot Detection. IEEE Access, 2020, vol. 8, pp. 159756-159772.
8. Rao Varre D.N.M., Bayana J. A Secured Botnet Prevention Mechanism for HTTP Flooding Based DDoS Attack. 3rd International Conference for Emerging Technology (INCET), Belgaum, India, 2022, pp. 1-5.
9. Dhanapal A., Nithyanandam P. An effective mechanism to regenerate HTTP flooding DDoS attack using real time data set. International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India, 2017, pp. 570-575.
10. Nashat D., Khairy S., Hassan M.M. Detection of Application Layer DDoS Attack Based on SIS Epidemic Model. IEEE Access, 2021, vol. 9, pp. 159827-159832.
11. Beckett D., Sezer S. HTTP/2 Cannon: Experimental analysis on HTTP/1 and HTTP/2 request flood DDoS attacks. Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 2017, pp. 108-113.
12. Yang S.-J., Huang H.-L. Design a hybrid flooding attack defense scheme under the Cloud Computing Environment. IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS), Beijing, China, 2019, pp. 41-46.

13. Vanitha K.S., Uma S.V., Mahidhar S.K. Distributed denial of service: Attack techniques and mitigation. International conference on circuits, controls, and communications (CCUBE), Bangalore, India, 2017, pp. 226-231.
14. Wang J., Zhang M., Yang X., Long K., Xu J. HTTP-sCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs. China Communications, 2015, vol. 12, no. 2, pp. 118-128.
15. Pravikov D.I., Ponomareva E.A., Kupriyanovsky V.P. Problemy obespecheniya informacionnoj bezopasnosti vysokoavtomatizirovannyh transportnyh sredstv [Problems of Information Security of Highly Automated Vehicles]. International Journal of Open Information Technologies, 2020, no.6, p. 98-103.
16. Iskhakov A.Yu., Mamchenko M.V. Vulnerabilities, Points of failure and adaptive protection methods in the context of group control of unmanned vehicles. J. Phys.: Conf. Ser, vol. 1864, pp. 1-10.
17. Iskhakova A.O. Iskhakov A.Y. Bogacheva D.N., Molotov A.A. Algoritm detektirovaniya istochnikov vredonosnyh zaprosov v kiberfizicheskih sistemah [Algorithm for detecting sources of malicious requests in cyber-physical systems]. Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii [Modeling, Optimization and Information Technology], 2022, 10(3), p. 1-9.

***Iskhakov Andrey Yunusovich.*** *Candidate of Technical Sciences, Senior Researcher at the V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. Main research interests: information security, identification and authentication systems, data mining, Internet of things, decision-making systems. AuthorID: 925433, SPIN: 3390-0291, ORCID: 0000-0002-6603-265X, iskhakovandrey@gmail.com, Russia, Moscow, 117997, Profsoyuznaya street, 65.*

***Jharko Elena Filippovna.*** *Candidate of Technical Sciences, Senior Researcher at the V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. Main research interests: cybersecurity, verification, validation, automation, quality assurance, high-risk facilities, predictive models, simulation models. AuthorID: 30748, SPIN: 6288-1776, ORCID: 0000-0002-8895-4786, elena_hot@inbox.ru, Russia, Moscow, 117997, Profsoyuznaya street, 65.*

*Статья поступила в редакцию 27.02.2023; одобрена после рецензирования 01.03.2023; принята к публикации 06.03.2023.*
*The article was submitted 02/27/2023; approved after reviewing 03/01/2023; accepted for publication 03/06/2023.*