DOI: 10.25728/mlsd.2023.1301

ЗАЩИТА ИНТЕРФЕЙСОВ УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКОЙ СИСТЕМОЙ ОТ МНОГОВЕКТОРНЫХ АТАК ПРИКЛАДНОГО УРОВНЯ, НАПРАВЛЕННЫХ НА НАРУШЕНИЕ ДОСТУПНОСТИ[1]

Исхакова А.О.
Институт цифровых технологий Финансового университета, Москва, Россия
shumskaya.ao@gmail.com

Аннотация. Работа посвящена обнаружению запросов, направленных на нарушение доступности интерфейсов управления. Предлагается алгоритм адаптивного анализа входящих запросов. Применяется метод визуального анализа и обработки данных, основанный на представлении в виде единого нормализованного набора. Алгоритм обеспечивает снижение ошибок по сравнению с регрессионными моделями.

Ключевые слова: информационная безопасность, нарушение доступности, обнаружение вредоносных запросов, брандмауэр, DDoS-атака, наводнение, анализ данных, безопасность web, безопасность киберфизических систем, реагирование, обнаружение атак.

Введение

Необходимость развития существующих подходов и научно-технических решений в области обеспечения информационной безопасности киберфизических систем обусловлена их стремительным развитием, требующим адаптации механизмов защиты под новые архитектуры, технические ограничения и особенности функционирования. К числу важных, но слабо рассмотренных в мировой литературе направлений защиты киберфизических систем, относятся вопросы построения научно обоснованных эффективных методов защиты от многовекторных атак типа «отказ в обслуживании», направленных на прикладной уровень интерфейсов управления. Поскольку DDoS-атаки зачастую используют ботнеты, которые могут состоять из множества компьютеров, сложно отделить легитимный трафик от злонамеренного. Кроме того, характеристики и методы DDoS-атак часто изменяются, что требует постоянного обновления алгоритмов обнаружения. Особенностью таких вредоносных воздействий является то, что они слабообнаружимы, не имеют явной корреляции с объемом передаваемого трафика и в совокупности с использованием различных уязвимостей могут на длительное время нарушить доступность подсистем управления, что для рассматриваемых объектов может привести к трагическим последствиям.

Под многовекторными атаками в данной работе понимаются процедуры распараллеливания потоков и итеративной модернизации параметров генерации вредоносных запросов, включая смену тактик (HTTP-flood; медленные атаки малого объема; имитация поведения легитимного пользователя и т.д.) на компоненты внешнего интерфейса. Для подобных случаев применение статистических методов вызывает проблему определения граничных (пороговых) значений отслеживаемых характеристик. Задача усложняется, когда количество характеристик увеличивается при одновременном рассмотрении многовекторной атаки. В рамках данного подхода предлагается выполнять комбинировании статистического анализа и выявления аномалий при фильтрации поступающих запросов на разных уровнях L3/L7, что позволит обеспечить минимизацию плотности проверок различных векторов обработки трафика на основе частных показателей доступности интерфейса управления киберфизической системой. Это позволит учесть особенности проведения распределенных низкоинтенсивных атак прикладного уровня с разными векторами воздействия, тенденции к использованию злоумышленниками особенностей мультиплексирования, обеспечивая при этом приемлемую вычислительную сложность анализируемых параметров адаптивно под вычислительные возможности объекта.

1. Современное состояние исследований

При проведении анализа мировой литературы, посвященной тематике статьи, было установлено, что со стороны научного сообщества наиболее подробно проработаны и систематизированы подходы к защите от атак типа «отказ в обслуживании» для сетевого и транспортного уровней модели OSI. Тенденции последних нескольких лет способствовали активизации исследований и разработке отдельных алгоритмов для противодействия различным техникам HTTP(S) Flood, атакам Slowloris, Full

[1] *Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета*

Browser Stack-атакам и имитации поведения субъекта пользователя. При этом необходимо отметить, что проблеме активно применяемого синтеза различных L7-техник, как и особенностям имплементации защитных механизмов подобного класса для киберфизических систем, не уделяется достаточного внимания.

DDoS-атаки с использованием протокола HTTP начали приобретать известность в прошлом десятилетии [1-6], и уже в первом квартале 2018 года составили около 10% всех атак [7]. При этом динамика наблюдения показывает, что число таких атак только растет. Например, в отчете за второй квартал 2022 года [8] обозначен значительный рост атак типа «отказ в обслуживании» на прикладном уровне, а также дополнительно отмечена важная тенденция к атакам на критически важные (в том числе государственные) информационные объекты – транспортные, энергетические и др. Атаки, направленные исключительно на использование центрального процессора, называемые атаками с исчерпанием процессора, составляют большую часть DDoS-атак на уровне приложений [9-11]. Также была задокументирована более сложная версия атак, использующая дорогостоящие вычислительные HTTP-запросы, эти атаки называются атаками с асимметричной рабочей нагрузкой и могут исчерпать сервер с еще меньшим количеством ресурсов [12, 13], тем самым создавая довольно серьезную уязвимость.

Опубликовано множество исследований DoS-атак на прикладном уровне [14-19]. Например, Yi и Yu в работе [14] показали, что новые DDoS-атаки на уровне приложений могут использовать легитимные HTTP-запросы для перегрузки ресурсов жертвы, и предложили детектор аномалий для обнаружения таких атак на трафике популярных веб-ресурсов. Jazi и др. [19] представили несколько уникальных признаков, характеризующих атаки на прикладном уровне, и предложили непараметрический алгоритм обнаружения CUSUM для их выявления с использованием найденных признаков. Однако предыдущие работы по DoS-атакам прикладного уровня в основном основываются на протоколе HTTP/1.1 или HTTPS, а также на их защитных механизмах для смягчения последствий. При этом, мало исследований посвящено DoS-атакам на прикладном уровне против протокола HTTP/2 и его различных программных реализаций. Данная область является гораздо менее проработанной. В отчете компании Imperva (одного из ведущих поставщиков решений по кибербезопасности) [20] сообщается о четырех громких уязвимостях в новых реализациях HTTP/2 от основных производителей. Одна из атак – атака медленного чтения, которая использует вредоносный клиент для очень медленного чтения ответов с серверов, поддерживающих HTTP/2. Таким образом, становится понятна актуальность исследований новых возможностей DoS против HTTP/2.

Перспективными являются направления исследований на основе управления потоком для создания DoS-атаки на уровне приложений. Adi и др. [21] впервые представили, что можно запустить DoS-атаку, используя внешне легитимный, но вредоносный трафик HTTP/2 flash crowd. Вредоносные HTTP/2 пакеты были созданы путем использования значения "Window Size Increment" в кадре WINDOW UPDATE для моделирования атаки на основе флудинга на веб-сервер жертвы HTTP/2, а также провели четыре исследования для наблюдения за эффектом потребления ресурсов на веб-сервере жертвы. В данном исследовании атака была ограничена атрибутом WINDOW UPDATE, при этом использовании других атрибутов могут быть использованы для дальнейшего усиления воздействия атаки.

Выявление DDoS-атак на прикладном уровне является трудоемкой задачей, требующей постоянного контроля за системой и вовлечения многих специалистов, так как существующие системы обнаружения вторжений требуют постоянного обновления набора правил для отработки различных поступающих сценариев [22]. При этом даже методичная проработка набора правил может быть недостаточной для защиты информационной системы.

Детектирование атак типа «отказ в обслуживании» затрудняется и уже нецелесообразно лишь с применением аппаратных средств отслеживания трафика, так как пропускная способность интернет-канала в целом, и пользовательских интерфейсов в частности, растет [23-26]. При этом использование традиционных межсетевых экранов на сегодняшний день малоэффективно ввиду использования определенного набора правил, в соответствии с которым осуществляется фильтрация всех данных [27]. Чаще всего для детектирования таких атак проводится анализ аномалий сетевого трафика, то есть при штатных условиях работы сети ведется поиск отклонений от контрольных характеристик трафика [28]. Таким образом, с повышением количества и сложности сетевых распределенных атак типа «отказ в обслуживании» необходимо повышение точности и скорости детектирования сетевых атак. Современное состояние прикладных комплексов защиты информации позволяет повысить точность детектирования за счет использования алгоритмов машинного обучения и комплексного применения аппаратных и программных средств защиты от такого рода атак.

2. Предлагаемый подход

В основе предлагаемого алгоритмического обеспечения лежит процесс, объединяющий сетевую активность в рамках взаимодействия сниффера сетевого трафика и веб-ориентированных интерфейсов управления киберфизической системы в единый набор данных. При этом детектирование вредоносной активности предлагается выявлять как на прикладном, так и сетевом уровне с выполнением следующих итераций:

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

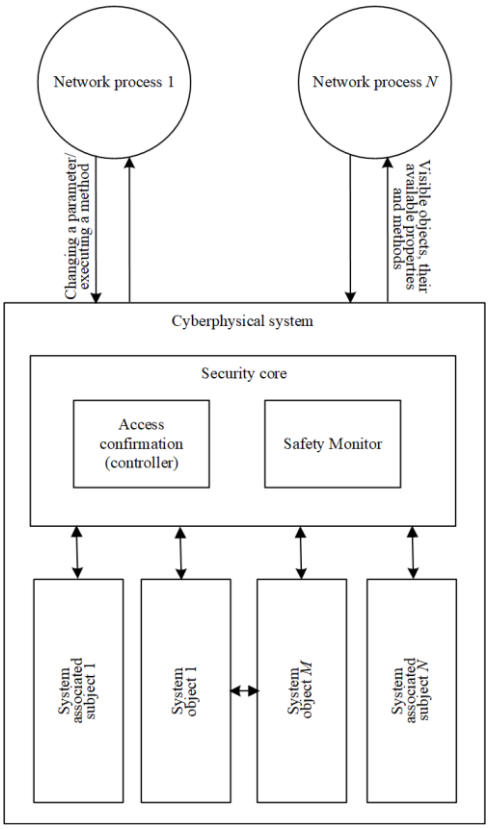

Рис. 1. Схема предлагаемого подхода

Для анализа данных предполагается подготовка среза трафика для проведения ретроспективной оценки в некотором интервале времени. 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 [6]. В основе детектирования источников вредоносных запросов проводилась дополнительная визуальная аналитика различных метрик оценки веб-сервисов интерфейса управления киберфизической системой.

3. Техники и наборы данных

К наиболее известным и опубликованным в открытых источниках наборам данных можно отнести следующие: DARPA1998, KDD Cup 1999, Kyoto 2006, NSL-KDD 2009, ISCX 2012, CTU-13, UNSW-NB15, CIDDS-001, UGR-16, CICIDS 2017, CICIDS 2018 и другие. Данные наборы используются

подавляющим большинством исследователей для апробации исследуемых алгоритмов обнаружения. Учитывая требования к актуальности данных в наборе и наличие качественного сниффера трафика был выбран один из популярных наборов датасетов CIC-IDS. Стоит отметить, что CIC-IDS это набор датасетов, включающий в себя данные собранные в период 2017-2019 годов, за это время сформировано три набора с разного рода атаками. Сами данные представлены как 80 признаков, собранных из трафика на основе сниффера CICFlowMeter, так как данный сниффер является свободно распространяемым программным обеспечением, это позволяет использовать его на реальном трафике для тестирования.

Infiltration - ботнет собирает информацию о сети, ставшую уязвимой из-за проникновения в систему вирусного файла. Сценарий атаки, следующий: вирус проникает в систему через файл, следующем этапе атаки злоумышленник использует уязвимость, созданную этим вирусом, для выполнения атак сканирования портов в сети.

Bot – ботнет Ares использует специальный инструмент атаки, написанный на языке программирования Python, для координации и выполнения своих злонамеренных действий. Этот инструмент, называемый Ares Bot, представляет собой программное обеспечение, которое устанавливается на зараженных компьютерах, превращая их в боты, которые подчиняются командам и контролируются злоумышленниками. Ares Bot осуществляет связь с удаленным командным и контрольным сервером (C&C-сервером) ботнета Ares, который управляет всей ботнет-инфраструктурой. Команды, отправленные с C&C-сервера, включают инструкции для ботов, например, запуск атак DDoS на целевые системы, распространение вредоносного программного обеспечения, сбор конфиденциальных данных или выполнение других вредоносных операций.

BENIGN - данная категория представляет нормальный и легитимный сетевой трафик без признаков злонамеренной активности.

DDOS attack-HOIC - атака типа DDoS с использованием инструмента HOIC (High Orbit Ion Cannon). HOIC является инструментом, предназначенным для координированной атаки на целевую систему путем отправки большого количества запросов или пакетов с целью перегрузить ее.

DoS attacks-Slowloris – атака типа DoS (Denial of Service) с использованием метода Slowloris. Slowloris осуществляет атаку, занимая доступные соединения на целевом сервере путем отправки неполных HTTP-запросов и задержки их завершения, что приводит к блокированию новых соединений.

DoS attacks-GoldenEye – атака типа DoS с использованием инструмента GoldenEye. GoldenEye предназначен для истощения ресурсов целевой системы путем отправки множества некорректных запросов, что приводит к ее недоступности для легитимных пользователей.

DoS attacks-Hulk - атака типа DoS с использованием инструмента Hulk. Hulk также нацелен на истощение ресурсов целевой системы, но использует метод отправки большого количества запросов с некорректными заголовками, что приводит к истощению ее ресурсов.

SSH-Bruteforce - атака на протокол SSH с использованием метода перебора паролей (bruteforce). Злоумышленник пытается получить несанкционированный доступ к системе, перебирая различные комбинации логинов и паролей.

DDOS attack-LOIC-UDP - атака типа DDoS с использованием инструмента LOIC (Low Orbit Ion Cannon) и протокола UDP. LOIC выполняет атаку путем отправки большого количества пакетов через протокол UDP, что может привести к перегрузке целевой сети или системы.

4. Результаты эксперимента

В результате анализа исследований было выявлено, что хоть и большая часть классических методов машинного обучения показывает высокие результаты по метрике F-мера, но наилучшие результаты остаются за моделями, основанными на деревьях решений. Основные критерии к выбору:

- Модель должна достаточно быстро обучаться
- Модель должна быть легко интерпретируемой
- Модель не должна требовать большого объема подготовки данных

Данные критерии подходят к дереву решений. Также, чтобы улучшить вероятность детектирования модели, было принято решение использовать не просто деревья, а их ансамбль.

Итоговая модель выглядит так:

- Дерево решений (в ансамбле);
- Случайный лес (в ансамбле);
- Логистическая регрессия – обработка предсказаний деревьев и конечный вывод результатов

По результатам построенной корреляционной матрицы, были отброшены признаки с коэффициентом более 0.9 (линейная зависимость). В итоге было выбрано всего 14 признаков, которые вносят наибольший вклад в окончательный результат:

- Fwd Seg Size Min;
- Init Fwd Win Byts;
- Flow IAT Min;
- Fwd Header Len;
- Fwd IAT Mean;
- Flow IAT Mean;
- Fwd IAT Max;
- Fwd Pkts/s;
- Flow Duration;
- Init Bwd Win Byts;
- Flow IAT Std;
- Bwd Header Len;
- Bwd IAT Min;
- Bwd Pkts/s.

На данных признаках проводилось обучение и тестирование модели (на синтетическом датасете и реальном трафике). Показатели эффектиности обучения модели приведены в табл.1.

Таблица 1. Показатели эффективности обучения модели детектирования DDoS-атак на уровне L3.

	Precision	**Recall**	**F1-score**	**Support**
BENIGN	0,90	0,97	0,93	4059
DDOS attack-HOIC	1,00	1,00	1,00	2689
DoS attacks-Slowloris	1,00	1,00	1,00	2685
Bot	1,00	1,00	1,00	1833
DoS attacks-GoldenEye	1,00	1,00	1,00	1731
DoS attacks-Hulk	1,00	1,00	1,00	1805
Infilteration	0,93	0,75	0,83	1772
SSH-Bruteforce	1,00	1,00	1,00	1843
DDOS attack-LOIC-UDP	1,00	1,00	1,00	552
accuracy			0,97	18969
macro avg	0,98	0,97	0,97	18969
weighted avg	0,97	0,97	0,97	18969

Проведенный анализ синтетического датасета показал необходимость расширения признакового пространства за счет выявления атак класса «отказ в обслуживании», воспроизведенными на уровне L7. Для этого модель была интегрирована в межсетевой экран прикладного уровня, разбирающий SSL трафик. Эксперимент проводился на виртуальном полигоне, эмулирующем работу киберфизических систем. Были реализованы 5 сценариев (различных техник) управляемой DDoS-атаки на заранее определенные endpoint всех интерфейсов управления. В табл. 2 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 типа межсетевой экран уровня приложений. 3) имплементация предложенного алгоритма в дополнение ко 2 способу.

Таблица 2. Результаты детектирования вредоносных источников запросов

Режим защиты	**Метрика**	**Сценарий атаки на нарушение доступности**				
		1	**2**	**3**	**4**	**5**
1	FAR	0,043	0,023	0,095	0,052	0,020
	FRR	0,203	0,157	0,177	0,307	0,150
2	FAR	0,031	0,050	0,102	0,043	0,031
	FRR	0,173	0,237	0,221	0,114	0,331
3	FAR	0,030	0,022	0,097	0,041	0,125
	FRR	0,092	0,112	0,201	0,082	0,104

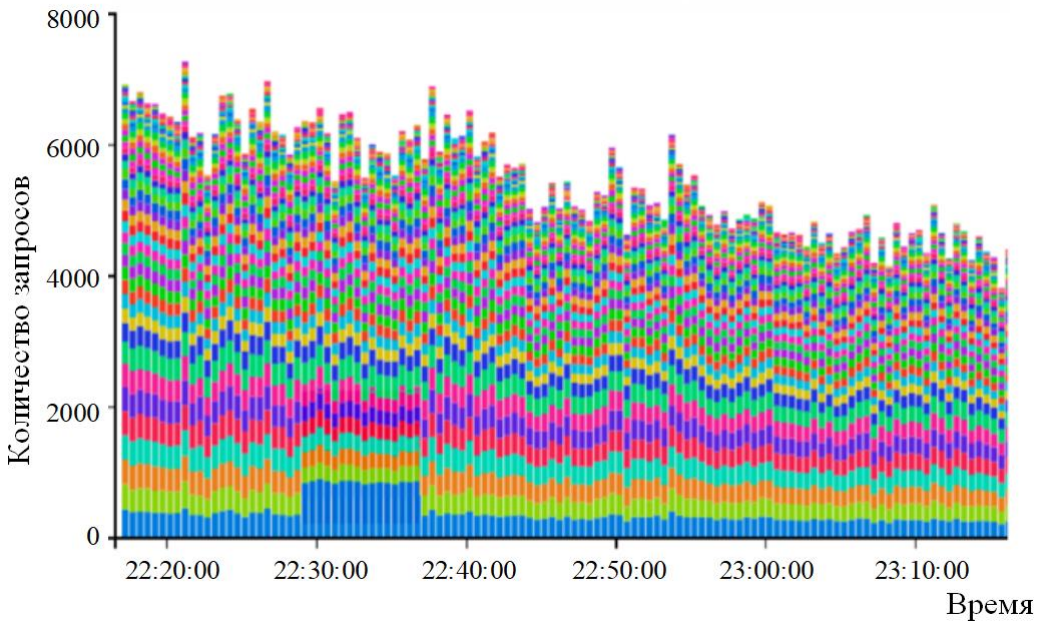

Рис. 2. Пример успешного распознавания DDoS L7 атаки на интерфейс управления

5. Заключение

Проведенное исследование подтверждает необходимость адаптации моделей, апробированных на тестовых датасетах под реальный трафик и специфику объекта защиты. Предлагаемый подход подразумевает, что построенная модель обнаружения компьютерных атак как на сетевом, так и прикладном уровне должна дообучаться по мере расширения набора данных, а также апробироваться на атаках, реализуемых из разных точек расположения сетевой инфраструктуры киберфизической системы.

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.

Литература

1. *Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Halderman J., Ma Z., Mason J., Menscher D., Seaman C., Sullivan N., Thomas K., Zhou Y., Bernhard M., Durumeric Z., Kumar D., Lever C., Kallitsis M., Invernizzi L.* Understanding the Mirai Botnet // Proceedings of the 26th USENIX Security Symposium. – Vancouver, BC, Canada, 2017. – P. 1092–1110.
2. *Praseed A., Thilagam P.S.* DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, N 1. – P. 661-685.
3. *Lin H., Cao S., Wu J., Cao Z., Wang F.* Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices // IEEE Access. – 2019. – Vol. 7. – P. 164480-164491.
4. *Black S., Kim Y.* An Overview on Detection and Prevention of Application Layer DDoS Attacks // 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). – Las Vegas, NV, USA, 2022. – P. 791-800.
5. *Najafabadi M.M., Khoshgoftaar T.M., Calvert C., Kemp C.* User Behavior Anomaly Detection for Application Layer DDoS Attacks // 2017 IEEE International Conference on Information Reuse and Integration (IRI). – San Diego, CA, USA, 2017. – P. 154-161.
6. *Bhosale K.S., Nenova M., Iliev G.* Detection of Application Layer Ddos Attacks Based on Uml Modelling // 2018 International Conference on Smart City and Emerging Technology (ICSCET). – Mumbai, India, 2018. – P. 1-6.
7. *Khalimonenko O.K.A., Badovskaya E.* DDoS Attacks in Q1 2018. // SecureList. – 2018. – URL: https://securelist.com/ddos-report-in-q1-2018/85373/ (access date: 01.07.2023).

8. *Gutnikov A., Kupreev O., Shmelev Y.* DDoS attacks in Q2 2022 // SecureList. – 2022. – URL: https://securelist.com/ddos-attacks-in-q2-2022/107025/ (access date: 01.07.2023).
9. *Meng W., Qian C., Hao S., Borgolte K., Vigna G., Kruegel C., Lee W.* Rampart: Protecting Web applications from CPUexhaustion denial-of-service attacks // Proceedings of the 27th USENIX Security Symposium. – Baltimore, MD, USA, 2018. – Vol. 18. – P. 393–410.
10. *Zhan M., Li Y., Yang H., Yu G., Li B., Wang W.* Coda: Runtime Detection of Application-Layer CPU-Exhaustion DoS Attacks in Containers // IEEE Transactions on Services Computing. – 2023. – Vol. 16, N 3. – P. 1-12.
11. *Olivo O., Dillig I., Lin C.* Detecting and exploiting second order denial-of-service vulnerabilities in Web applications // Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. – 2015. – P. 616–628.
12. *Ranjan S., Swaminathan R., Uysal M., Nucci A., Knightly E.* DDoS-shield: DDoS-resilient scheduling to counter application layer attacks // IEEE/ACM Trans. Netw. – 2009. – Vol. 17, N 1. – P. 26–39.
13. *Xie Y., Yu S.Z.* A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors // IEEE/ACM Trans. Netw. – 2009. – Vol. 17, N 1. – P. 54–65.
14. *Xie Y., Yu S.-Z.* Monitoring the application-layer DDoS attacks for popular websites // IEEE/ACM Trans. Netw. – 2009. – Vol. 17(1). – P. 5–25.
15. *Khatkar M., Kumar K., Kumar B.* An overview of distributed denial of service and internet of things in healthcare devices // 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH). – Greater Noida, India, 2020. – P. 44-48.
16. *Wehbe N., Alameddine H., Pourzandi M., Bou-Harb E., Assi C.* A Security Assessment of HTTP/2 Usage in 5G Service Based Architecture // IEEE Communications Magazine. – 2022. – Vol. 61, N 1. – P. 48-54.
17. *Praseed A., Thilagam P.S.* DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, N 1. – P. 661-685.
18. *Wang Y., Liu L., Si C., Sun B.* A novel approach for countering application layer DDoS attacks // 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). – Chongqing, China, 2017. – P. 1814-1817.
19. *Jazi H.H., Gonzalez H., Stakhanova N., Ali A.* Detecting HTTP-based application layer DoS attacks on Web servers in the presence of sampling // Comput. Netw. – 2017. – Vol. 121. – P. 25–36.
20. Imperva: HTTP/2: In-depth analysis of the top four flaws of the next generation web protocol. – *2022. – URL: https://www.imperva.com/docs/Imperva_HII_HTTP2.pdf (access date 01.07.2022).*
21. *Adi E., Baig Z.A., Hingston P., Lam C.-P. Distributed denial-of-service attacks against HTTP/2 services* // Clust. Comput. – 2016. – Vol. 19. – P. 79–86.
22. *Praseed A., Thilagam P.S.* Modelling Behavioural Dynamics for Asymmetric Application Layer DDoS Detection // IEEE Transactions on Information Forensics and Security – 2021. – Vol. 16. – P. 617-626.
23. *Beitollahi H., Sharif D.M., Fazeli M.* Application Layer DDoS Attack Detection Using Cuckoo Search Algorithm-Trained Radial Basis Function // IEEE Access. – 2022. – Vol. 10. - P. 63844-63854.
24. *Bravo S., Mauricio D.* DDoS attack detection mechanism in the application layer using user features // 2018 International Conference on Information and Computer Technologies (ICICT). – DeKalb, IL, USA, 2018. – P. 97-100.
25. *Bhosale K.S., Nenova M., Iliev G.* The distributed denial of service attacks (DDoS) prevention mechanisms on application layer // 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS). – Nis, Serbia, 2017. – P. 136-139.
26. *Mann P., Tyagi N., Gautam S., Rana A.* Classification of Various Types of Attacks in IoT Environment // 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN). – Bhimtal, India, 2020. – P. 346-350.
27. *Sreenivasarao S.* Application Layer DDOS Attack Detection and Defense Methods // Proceedings of Emerging Trends and Technologies on Intelligent Systems. ETTIS 2021. Advances in Intelligent Systems and Computing. – 2021. – Vol. 1371. – P.1-12.
28. *Zolotukhin M., Hämäläinen T., Kokkonen T., Siltanen J.* Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic // 2016 23rd International Conference on Telecommunications (ICT). – Thessaloniki, Greece, 2016. – P. 1-6.