Сравнительный анализ платформ для цифровизации государственных услуг

В.В. Бритвина, А.К. Агоштинью, Г.П. Конюхова

***Аннотация*—Приведен сравнительный анализ используемых технологий государственных услуг. По результатам обзора представлены выводы о применимости данного опыта в Республике Анголы. Также внимание уделяется изучению одного из основных видов угроз для веб-сервисов и порталов, особенно носящих государственный характер. По исследованию распределенного отказа в обслуживании приходит понимание, что разработчики инструментов DDoS-атак имеют гибкие возможности инициализации и своих методов проектирования. Это придает DDoS-атакам характеристики неопределенности и непредсказуемости. В результате этих причин акцент падает на изучение данной угрозы для сбора требуемых знаний, которые позволят выявить некоторые закономерности в сценариях и найти универсальное решение по предотвращению или прогнозированию. Обладая этими знаниями, можно повысить эффективность защиты от DDoS-атак. Часть исследовательской работы посвящена имитации DDoS-атаки с использованием математической модели M/M/k/n для систем массового обслуживания с целью определения количественной меры ее воздействия на жертву. Эксперименты, проведенные в этом исследовании, показывают, что сервер практически не используется в своих обычных условиях, таким образом, имеет высокую доступность и низкую среднюю загрузку. Однако, в момент создания большого объема ложных запросов от злоумышленника его загрузка резко возрастает и, таким образом, приводит к снижению доступности. Показан пример использования метода Т. Саати для выбора приоритетного объекта из выбранных альтернатив. Результаты эксперимента позволяют спрогнозировать ущерб от DDoS-атаки с разной степенью интенсивности и на основе полученных значений применить меры защиты в процесс разработки веб-портала.**

***Ключевые слова*— портал Госуслуг, распределенный отказ в обслуживании, метод анализа иерархий, отказоустойчивость.**

I. Введение

Правительства по всему миру сосредоточили внимание на удовлетворении потребностей граждан, стремясь создать среду цифрового правительства с хорошей организацией и большими возможности для установления сотрудничества и участия среди всех заинтересованных.

Использование технологий в государственных услугах стало мировым трендом. С развитием и освоением цифровых технологий связываются возможности достижения ключевых целей социально-экономического развития Анголы. Для их реализации принципиальное значение имеет адекватная цифровизация госуправления.

Изучение аналогичных порталов государственных услуг в разных по менталитету и климату странах поможет рассмотреть их характеристики, а также позволит провести сравнительный анализ функционала и статистики использования этих сайтов с аналогичными в России и Анголе, на что и будет создан упор данного исследования. Основной целью этой работы является проведение самого анализа, выявление различий между сайтами разных стран и сайтом госуслуг России, а также выявление их преимуществ и недостатков действующих сервисов с предложением возможных средств по обеспечению качественной и бесперебойной работы.

Когда встает вопрос о качественной работе различных сервисов, в частности касающихся государственных структур, прежде предложения рекомендаций по повышению привлекательности и гибких возможностей заказа услуг с эргономичным интерфейсом, важным всегда остается вопрос обеспечения надежности и доверия этого сервиса.

Существует разнообразие технологий для защиты информационных активов, но ни одна из них не обеспечивает идеальный уровень отказоустойчивости для предприятий, особенно сетевых сервисов. Поэтому кампании сталкиваются с различными видами информационных атак, такими как распределенный отказ в обслуживании (далее – DDoS-атаки), которые нацелены на подвергание техническим и клиентским системам организации сбоев, а также на отвлечение внимания от кражи корпоративной информации.

Кампания Radware (DDoS Threats & Security Attacks // Radware URL: https://www.radware.com/security/threat-advisories-attack-reports/) также предупреждает об угрозе развития DDoS-атак с использованием устройств IoT, особенно учитывая последние тенденции со стороны государств внести регламентирующие правила и законы, касающиеся искусственного интеллекта и интернета вещей.

Системы защиты, призванные служить опорной стеной для противодействия DDoS, усовершенствуются и продолжают поддерживаться, но с появлением новых технологий гонка средств защиты и средств совершения атак продолжается до сих пор, и поскольку злоумышленники существуют в сетевом пространстве постоянно,

Статья получена 09 марта 2024 г.

В. В. Бритвина, к.п.н, доцент кафедры управления и информатики в технических системах, МГТУ СТАНКИН, доцент кафедры Инфокогнитивные технологии Московского политехнического университета, Москва, Россия (e-mail: saaturn2015@mail.ru).

А. К. Агоштинью, аспирнат, кафедра управления и информатики в технических системах, МГТУ СТАНКИН, Москва, Россия (e-mail: adcaculo@gmail.com).

Г.П. Конюхова, к.п.н, доцент, доцент кафедры управления и информатики в технических системах, МГТУ СТАНКИН, доцент кафедры Высшей математики МИРЭА, Москва, Россия (e-mail: maurico@yandex.ru)

то победной точки одной из этих сторон в ближайшее время ожидать не стоит.

II. Сравнительный анализ используемых технологий в мировом секторе государственных услуг

Госуслуги являются удобным решением для предоставления государственных услуг гражданам в таких сферах, как здравоохранение, для более удобного взаимодействия с государственными органами в уплате налогов или штрафов, для оформления загранпаспорта, регистрации автомобиля и подачи заявления на получение гос-пособий и выплат. Для исследования были отобраны порталы следующих стран: Австралии, США, Австрии, Южной Кореи, Великобритании, Канада, Россия и Ангола.

Сайты, предоставляющие государственные услуги в рассматриваемых странах, имеют разнообразные функциональные возможности. Эти уникальные характеристики государственных услуг рассмотрены в табл.I [1].

Таблица I. Сравнения функций в рассмотренных странах.

Функции\ Страны	Австралия	США	Канада	Великобритания	Южная Корея	Ангола	Россия
Справка об отсутствии судимости	+	-	-	-	+	-	+
Записаться на прием к врачу	-	+	+	-	+	-	+
Перевыпуск удостоверения личности	+	+	+	+	+	-	+
Заявление в ЗАГС	+	+	+	+	+	+	+
Информирование о предоставлении социальной помощи	+	+	+	+	+	+	+
Легализация компаний	+	+	+	+	-	+	+
Подача на патент	+	+	+	+	+	-	+
Поддержка семейного фермерства	-	+	+	+	+	+	-
Страхование людей	+	+	+	+	+	+	+

После анализа и сравнения сайтов государственных услуг Австралии, США, Австрии, Великобритании, Южной Кореи, Канады с госуслугами России и Анголы, можно заключить, что государственные услуги в России выделяются своим удобным интерфейсом и наиболее широким набором предоставляемых услуг. Пример соотношения пользователей госуслугами в Анголе и России показан на рис. 1, 2.

К сожалению, Ангола пока не может претендовать на звание самой удобной и мультифункциональной реализации такого сайта как “Госуслуги”. Сайт Правительства Анголы[1] имеет более простой и менее эстетически привлекательный дизайн.

Сравнение патентных заявок показало, что Россия занимает пятое место среди стран, подвергнутых анализу, по числу поданных заявок, и находится на 14 месте в мировом рейтинге. Кроме того, одной из ведущих технических областей, в которой оформляются патенты, является область “Двигатели, насосы, турбины”, что свидетельствует о высоком уровне промышленно-технических разработок в стране.

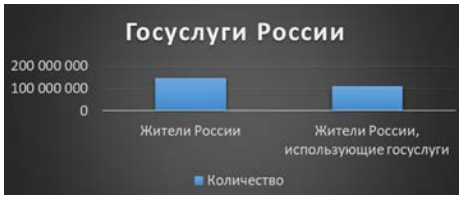

Рис. 1. Соотношение населения России к жителям, пользующимися госуслугами.

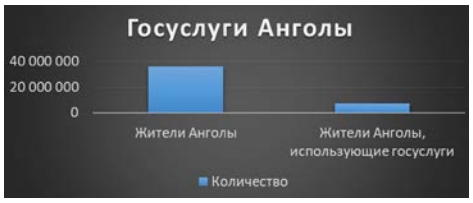

Рис. 2. Количество жителей Анголы и жителей, использующих госуслуги в Анголе.

III. Методология использования DDoS-атак

Увеличение значимости DDoS-атак происходит по ряду причин, включая использование новых методов атак и распространение IoT устройств, повышение скорости передачи данных или развитие телекоммуникационного оборудования. Динамика увеличения DDoS-атак с 2021 года стала активно расти согласно отчету Sophos State of Ransomware за 2021 год. Рис. 3 демонстрирует процент пользователей, кто стал жертвой вымогательства при совершении DDoS-атаки[2].

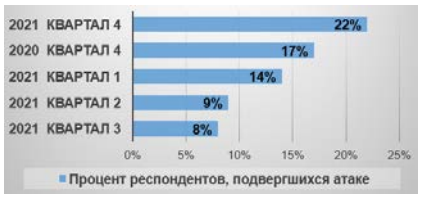

Рис. 3. Количество подвергшихся DDoS-атаке пользователей

Для осуществления DDoS-атаки злоумышленнику (или группе злоумышленников) необходим доступ к центру управления ботнетом, который состоит из зараженных компьютеров и используется для проведения атаки [2]. Ботнет представляет собой сеть компьютеров с доступом к Интернету, которые злоумышленники используют для атаки в форме множества фальшивых запросов.

IV. Имитационное моделирование

Поскольку каждая DDoS-атака уникальна, разработанные методики с установленными параметрами не могут быть проверены на практике. Принятие управленческих решений обычно происходит после DDoS-атаки, что может привести к негативным экономическим последствиям и потере репутации. В связи с этим возникает необходимость в имитационной модели, которая может

[1] sepe.gov.ao // URL: https://www.sepe.gov.ao/en/.

[2] Тенденции DDoS-атак в 4-м квартале 2021 года // habr.com URL: https://habr.com/ru/company/skillfactory/blog/646347/.

описать условия и задачи, максимально приближенные к реальной ситуации. С помощью этой алгоритмической модели можно проводить анализ объектов и проверять изменение параметров, при этом не опасаясь спровоцировать сбой системы, потерять персонал или довести до утечки технологий злоумышленникам.

Прежде построения имитационной модели всегда нужно выявить входные данные, цели и определить достаточный уровень детализации предстоящих моделируемых процессов, предстоящих смоделировать. Чтобы описать систему моделирования, для этого используются различные параметры, такие как критерии эффективности и альтернативные решения. Оценка альтернативных решений проводится итерационно, то есть достигаются приближенные значения, когда каждое завершенное действие одной итерации является начальным значением для следующего. Как только оценка эффективности всех входов будет завершена, полученные значения становятся основанием (критериями) для построения модели. Далее находится приоритетное решение из возможных альтернатив, а также условия реализации. Процесс построения модели в общем виде можно увидеть на рис. 4. [3].

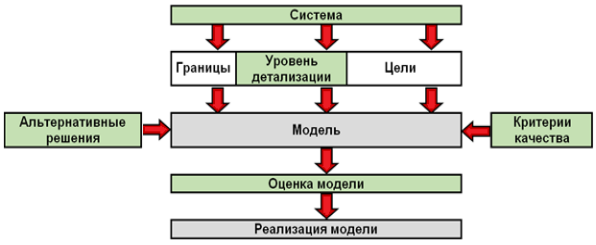

Рис. 4. Процесс построения имитационной модели.

С увеличением масштабов DDoS-атак становится крайне важным для предприятий иметь исчерпывающие знания о множестве рисков, связанных с устройствами (включая IoT-устройства) и работать над снижением их коэффициента, пока они не стали объектом незаконных действий [4].

V. Теория массового обслуживания

В разработке системы или сети всегда используется стандартный подход, который применим только к большим масштабам. Это приводит к нелинейному воздействию на время и созданию задержек, которые замедляют потоки. Теория очередей, также известная как модель очередей, является математическим анализом, который разработан для предсказания времени ожидания, понимания и улучшения пропускной способности в системах или сетях с высокой изменчивостью и случайностью [5].

Система массового обслуживания (СМО) связана с понятием эрланга, которое обозначает интенсивность трафика. Его назначением является расчет показателей нагрузки и эффективности в объекте (системе или сети). Чтобы определить необходимое количество эрлангов для того или иного случая, следует воспользоваться формулой:

$$E = \lambda \cdot h\,, \tag{1}$$

где E – трафик (единицы измерения – эрланги); λ – средняя скорость поступления новых запросов/вызовов (количество запросов в единицу времени); h – средняя продолжительность запроса/вызова (время ожидания в сек.).

С использованием этой простой функции Эрланга можно рассчитать трафик без особых затруднений.
Структурная схема СМО представлена на рис.5.

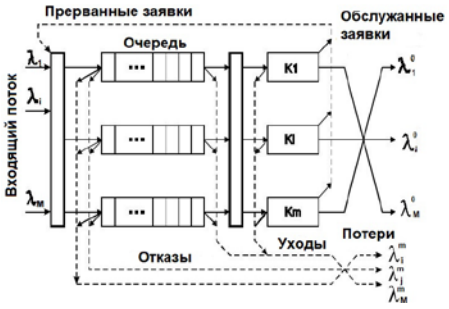

Рис. 5. Схема типовой модели СМО.

Для изучения потоков вредоносных запросов и предсказания момента времени DDoS-атаки в качестве инструмента для практического исследования применялась теория массового обслуживания, которая представляет собой динамическую систему, где объекты перемещаются по каналам ограниченной пропускной способности [5]. Аналитическое моделирование СМО часто используется для оценки характеристик исследуемой системы или узла, как количественных, так и качественных. Для данного случая был выбран класс нерегулярных потоков, так как он характеризуется случайностью в поступлении и количестве требований на обслуживание. В регулярных потоках требования заранее известны, и время обслуживания остается неизменным (занятие канала).

Входные данные: для имитационной модели DDoS-атаки использовалась многолинейная модель M/M/k/n в соответствии с параметрами:

- k– каналы обработки запросов;
- n – емкость буфера;
- μ – производительность обработки запросов;
- λ – интенсивность входного потока).

Для расчета коэффициента загрузки СМО p_s и показателя простоя p_0 использовались формулы:

$$p_s = p/k\,, \tag{2}$$

где

$$p = \lambda/\mu\,, \tag{3}$$

$$p_0 = \left[\sum_{j=0}^{k-1}\frac{p^i}{j!} + \frac{p^k(1-p_s^{N+1})}{k!(1-p_s)}\right]^{-1}. \tag{4}$$

Для оценки вероятности успеха DDoS-атаки учитывались параметры занятых каналов k_{ch} и запросов в очереди p_{den}.

$$p_{\text{den}} = p_{(k+n)} = \frac{p^{k+n}p_0}{k!\ k^n}, \tag{5}$$

$$k_{\text{ch}} = p(1-p_{\text{den}})\,. \tag{6}$$

Для определения среднего времени ожидания запросов в очереди (T_{req}) через средний показатель запросов в очереди (W_{req}) и среднего количества запросов в СМО (W_s) использовались соответствующие формулы, учитывая интенсивность полученных запросов. Также было вычислено среднее время, в течение которого запросы находятся в СМО (T_s).

$$W_{req} = \frac{p^{k+1} p_0}{k!k}\left[\frac{1 - p_s^n(n+1-np_s)}{(1-p_s)^2}\right] \quad (7)$$

$$T\,req = \frac{W\,req}{\lambda}, \quad (8)$$

$$W_s = k_{ch} + W_{req}, \quad (9)$$

$$T_s = T_{req} + \frac{(1-p_{den})}{\mu} \quad (10)$$

Проведение практического эксперимента с DDoS-атакой использовалось с помощью тестового ботнета, а значения начальных переменных устанавливались вручную с учетом параметров тестовой атаки на виртуальный сервер. Разработка модели и проведение экспериментов выполнялись на языке программирования Python для обеспечения кроссплатформенности, гибких возможностей модификации кода и использования множества библиотек, включая работу с сетью.

Инструментами для реализации тестовой атаки проводилось на OS Kali Linux с помощью ботнета ufonet (https://ufonet.03c8.net/), открытой программы с открытым исходным кодом.

VI. Полученные результаты эксперимента

DDoS-атака проводилась с сильной, средней и слабой степенью интенсивности с целью получить более разноплановые значения, чтобы определить устойчивость сервера и проверить (провести сравнительный анализ) средства защиты с вынесением рекомендаций. Рис. 6 показывает реализацию атаки на сервер с высокой интенсивностью, в результате чего вероятность сбоя значительно возрастает, а время расчета до полного отказа оказывается в границах 4-5 минут после начала DDoS-атаки.

```
Коэффициент загрузки ρ = 13.3333
Коэффициент загрузки СМО ps = 3.3333
Вероятность простоя p0 = 0.0000
Вероятность отказа в обслуживании pden = 0.7007
Среднее число занятых каналов kch = 3.9911
Среднее число запросов в очереди Wreq = 2.5855
Среднее время ожидания запроса в очереди Treq = 0.0129
Среднее число запросов в СМО Ws = 6.5766
Определяем среднее время пребывания запроса в СМО Ts = 0.0329
```

Рис. 6. Значения СМО при сильной интенсивности атаки.

Учитывая полученные результаты и возможность проверки состояния сервера, время принятия решений значительно сокращается, а эффективность принятых решений увеличивается. Исходя из значений интенсивности, зафиксированных на рис. 6, проводится аналогичная атака на тот же сервер с предварительно подготовленными мерами безопасности.

В момент обнаружения DDoS-атаки активизируется файл подкачки на 1 Тб, и сотрудник принимает решение о противодействии (блокировка входящих IP-адресов, переконфигурирование настроек сервера, переключение на резервный сервер, в крайнем случае, отключение физического сервера и т. д.). Сценарий проведения атаки на сервер представлен на рис. 7-8.

```
Коэффициент загрузки ρ = 7.5000
Коэффициент загрузки СМО ps = 1.0714
Вероятность простоя p0 = 0.0005
Вероятность отказа в обслуживании pden = 0.1749
Среднее число занятых каналов kch = 6.1880
Среднее число запросов в очереди Wreq = 1.0037
Среднее время ожидания запроса в очереди Treq = 0.0067
Среднее число запросов в СМО Ws = 7.1917
Определяем среднее время пребывания запроса в СМО Ts = 0.0479
```

Рис. 7. Значения СМО при сильной интенсивности атаки в случае осведомленности специалиста.

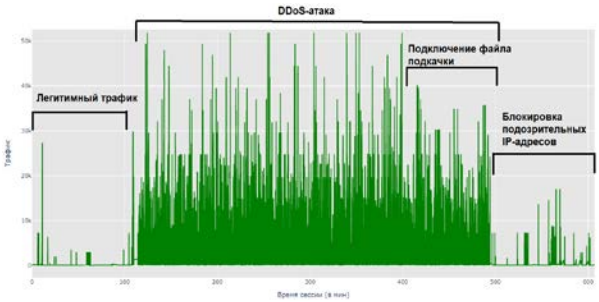

Рис. 8. Показатели сетевого трафика с реализацией метода защиты.

Результаты проведенного эксперимента позволяют выделить дополнительные средства защиты, которые помогут предотвратить или уменьшить риск успешной DDoS-атаки на сетевые ресурсы предприятия/организации.

Наиболее выгодным средством для выбора приоритетного средства защиты для конкретной задачи или определенной цели предприятия/организации является метод анализа иерархий (Т. Саати), который подразумевает выбор цели (приоритета) из списка альтернатив на основе расставления экспертных оценок лица, принимающего решение (в данном случае автор исследования).

VII. Применение метода анализа иерархий

Приведем пример использования данного метода, чтобы определить выгодное средство защиты для его внедрения в систему защиты предприятия/организации.

В качестве объекта подойдет система мониторинга сети, которая бесперебойно контролирует проходящий трафик во всей сетевой инфраструктуре предприятия/организации и, как следствие, может помочь выявить наступление атаки распределенного отказа в обслуживании. Основные характеристики подобной системы сведены в таблице II-VII [6].

Описание систем происходит по выбранным характеристикам. Для проведения эксперимента были отобраны следующие системы мониторинга: WireShark[3], Nagios[4] Zabbix[5] PRTG[6] и Network Olympus[7].

[3] WireShark. URL: https://www.wireshark.org
[4] Nagios. URL: https://www.nagios.com
[5] Zabbix. URL: https://www.zabbix.com/ru/.
[6] PRTG Network Monitor URL: https://www.paessler.com/prtg
[7] Network Olympus. URL: https://www.network-olympus.ru/network-scanner/

Таблица II. Функциональные характеристики системы мониторинга.

№	Характеристика	Значение
1.	**Платформа**	Важно
2.	**Стоимость**	Важно
3.	**Автоматическое обнаружение**	Важно
4.	**Web-интерфейс**	Важно
5.	**Распределенный мониторинг**	Важно
6.	Метод хранения данных	Не важно
7.	Лицензия	Не важно
8.	Настройка	Не важно

Таблица III. Функциональные характеристики WireShark.

№	Характеристика	Значение
1.	**Платформа**	UNIX, Windows
2.	**Стоимость**	Бесплатно
3.	**Автоматическое обнаружение**	Да
4.	**Web-интерфейс**	Нет
5.	**Распределенный мониторинг**	Нет
6.	Метод хранения данных	Временные/постоянные файлы (*.cap)
7.	Лицензия	GNU GPL
8.	Настройка	Гибкая настройка, нет диаграмм

Таблица IV. Функциональные характеристики Nagios.

№	Характеристика	Значение
1.	**Платформа**	UNIX
2.	**Стоимость**	От $1995
3.	**Автоматическое обнаружение**	Да
4.	**Web-интерфейс**	Управление, просмотр
5.	**Распределенный мониторинг**	Да
6.	Метод хранения данных	БД SQL
7.	Лицензия	Коммерческая, бесплатная
8.	Настройка	Диаграммы, SNMP, триггеры

Таблица V. Функциональные характеристики Zabbix.

№	Характеристика	Значение
1.	**Платформа**	UNIX, Windows
2.	**Стоимость**	От $1500 (есть бесплатная версия)
3.	**Автоматическое обнаружение**	Да
4.	**Web-интерфейс**	Полный доступ
5.	**Распределенный мониторинг**	Да
6.	Метод хранения данных	Oracle, MySQL, PostgreSQL, IBM DB2
7.	Лицензия	GNU GPL
8.	Настройка	Диаграммы, SNMP, триггеры

Таблица VI. Функциональные характеристики PRTG.

№	Характеристика	Значение
1.	**Платформа**	Windows
2.	**Стоимость**	От $1600
3.	**Автоматическое обнаружение**	Да
4.	**Web-интерфейс**	Полный доступ
5.	**Распределенный мониторинг**	Да
6.	Метод хранения данных	Проприетарный формат хранилища
7.	Лицензия	Коммерческая, бесплатная
8.	Настройка	Диаграммы, SNMP, триггеры

Таблица VII. Функциональные характеристики Network Olympus.

№	Характеристика	Значение
1.	**Платформа**	Windows
2.	**Стоимость**	От $500 (есть бесплатная версия)
3.	**Автоматическое обнаружение**	Да
4.	**Web-интерфейс**	Полный доступ
5.	**Распределенный мониторинг**	Да
6.	Метод хранения данных	PostgreSQL
7.	Лицензия	Коммерческая, бесплатно
8.	Настройка	Гибкая настройка, диаграммы, триггеры, скорость

Основные характеристики систем: платформа, стоимость, автоматическое обнаружение аномалий, наличие веб-интерфейса, распределенный мониторинг (для кластера серверов).

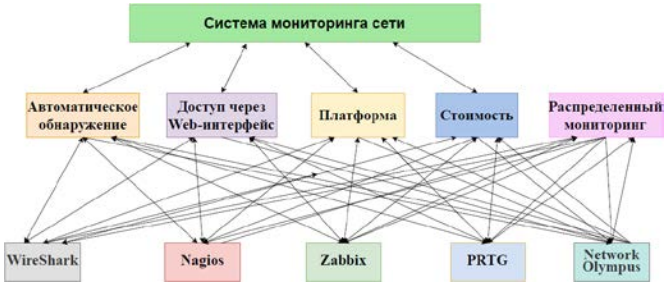

Рис. 9. Построение дерева альтернатив.

Следующим шагом необходимо попарно сравнить каждый критерий, то есть оценить методом расставления экспертных оценок (см. табл. VIII-XI) [7]. После проделанных вычислений можно будет сделать промежуточный вывод – наиболее значимым весом оказался критерий “Платформа”, а критерий “Распределенный мониторинг” имеет наименьший коэффициент. Далее следует проделать подобные шаги с оценкой каждого отдельного критерия для всех альтернатив (см. табл. XII-XXI)

Таблица VIII. Матрица попарных сравнений критериев.

Критерии	Платформа	Стоимость	Автоматическое обнаружение	Web-интерфейс	Распределенный мониторинг
Платформа	1,00	5,00	6,00	6,00	7,00
Стоимость	0,20	1,00	5,00	6,00	7,00
Автоматическое обнаружение	0,17	0,20	1,00	0,50	4,00
Web-интерфейс	0,17	0,17	2,00	1,00	6,00
Распределенный мониторинг	0,14	0,14	0,25	0,17	1,00
Сумма	1,68	6,51	14,25	13,67	25,00

Таблица XI. Среднее арифметическое значение показателей.

A_{ij}	Платформа	Стоимость	Автоматическое обнаружение	Web-интерфейс	Распределенный мониторинг	Среднее значение
Платформа	0,60	0,77	0,42	0,44	0,28	2,51
Стоимость	0,12	0,15	0,35	0,44	0,28	1,34

Автоматическое обнаружение	0,10	0,03	0,07	0,04	0,16	0,4
Web-интерфейс	0,10	0,03	0,14	0,07	0,24	0,58
Распределенный мониторинг	0,09	0,02	0,02	0,01	0,04	0,18

Таблица X. Геометрическое среднее значений показателей.

A_{ij}	**Произведение**	**$\sqrt[4]{}$ из произведения**
Платформа	1260,00	5,958
Стоимость	42,00	2,546
Автоматическое обнаружение	0,0667	0,508
Web-интерфейс	0,3333	0,759
Распределенный мониторинг	0,0009	0,171
Сумма		9,942

Таблица XI. Нахождение локальных векторов приоритетов.

A_{ij}	**Платформа**	**Стоимость**	**Автоматическое обнару-**	**Web-интерфейс**	**Распределенный монито-ринг**	**Локальный вектор**
Платформа	1,00	5,00	6,00	6,00	7,00	**0,59**
Стоимость	0,20	1,00	5,00	6,00	7,00	0,26
Автоматическое обнаружение	0,17	0,20	1,00	0,50	4,00	0,05
Web-интерфейс	0,17	0,17	2,00	1,00	6,00	0,08
Распределенный мониторинг	0,14	0,14	0,25	0,17	1,00	0,02
Сумма	1,68	6,51	14,25	13,67	25,00	

Таблица XII. Матрица попарных сравнений критерия “Платформа”.

Платформа	**WireShark**	**Nagios**	**Zabbix**	**PRTG**	**Network Olympus**
WireShark	1,00	6,00	1,00	3,00	3,00
Nagios	0,17	1,00	0,17	0,33	3,00
Zabbix	1,00	6,00	1,00	3,00	3,00
PRTG	0,33	3,00	0,33	1,00	1,00
Network Olympus	0,33	0,33	0,33	1,00	1,00

Таблица XIII. Сумма элементов и среднее арифметическое критерия “Платформа”.

Платформа	**Сумма**	**Среднее значение**
WireShark	2,83	1,71
Nagios	16,33	0,49
Zabbix	2,83	1,71
PRTG	8,33	0,63
Network Olympus	11,00	0,47

Таблица XIV. Матрица попарных сравнений критерия “Стоимость”.

Стоимость	**WireShark**	**Nagios**	**Zabbix**	**PRTG**	**Network Olympus**
WireShark	1,00	9,00	6,00	8,00	5,00
Nagios	0,11	1,00	0,25	0,33	0,17
Zabbix	0,17	4,00	1,00	2,00	0,25
PRTG	0,13	3,00	0,50	1,00	0,20
Network Olympus	0,20	6,00	4,00	5,00	1,00

Таблица XV. Сумма элементов и среднее арифметическое критерия “Стоимость”.

Стоимость	**Сумма**	**Среднее значение**
WireShark	1,60	2,77
Nagios	23,00	0,18
Zabbix	11,75	0,52
PRTG	16,33	0,34
Network Olympus	6,62	1,18

Таблица XVI
Матрица попарных сравнений критерия “Автоматическое обнаружение”.

Автоматическое обнаружение	**WireShark**	**Nagios**	**Zabbix**	**PRTG**	**Network Olympus**
WireShark	1,00	0,20	0,20	0,20	0,20
Nagios	5,00	1,00	1,00	1,00	1,00
Zabbix	5,00	1,00	1,00	1,00	1,00
PRTG	5,00	1,00	1,00	1,00	1,00
Network Olympus	5,00	1,00	1,00	1,00	1,00

Таблица XVII. Сумма элементов и среднее арифметическое критерия “Автоматическое обнаружение”.

Автоматическое обнаружение	**Сумма**	**Среднее значение**
WireShark	21,00	0,24
Nagios	4,20	1,19
Zabbix	4,20	1,19
PRTG	4,20	1,19
Network Olympus	4,20	1,19

Таблица XVIII. Матрица попарных сравнений критерия “Web-интерфейс”.

Web-интерфейс	**WireShark**	**Nagios**	**Zabbix**	**PRTG**	**Network Olympus**
WireShark	1,00	0,13	0,11	0,11	0,11
Nagios	8,00	1,00	0,17	0,17	0,17
Zabbix	9,00	6,00	1,00	1,00	1,00
PRTG	9,00	6,00	1,00	1,00	1,00
Network Olympus	9,00	6,00	1,00	1,00	1,00

Таблица XIX. Сумма элементов и среднее арифметическое для критерия “Web-интерфейс”.

Web-интерфейс	**Сумма**	**Среднее значение**
WireShark	36,00	0,14
Nagios	19,13	0,43
Zabbix	3,28	1,48
PRTG	3,28	1,48
Network Olympus	3,28	1,48

Таблица XX. Матрица попарных сравнений критерия “Распределенный мониторинг”.

Web-интерфейс	**WireShark**	**Nagios**	**Zabbix**	**PRTG**	**Network Olympus**
WireShark	1,00	0,13	0,13	0,13	0,11
Nagios	8,00	1,00	1,00	1,00	0,50
Zabbix	8,00	1,00	1,00	1,00	0,50
PRTG	8,00	1,00	1,00	1,00	0,50
Network Olympus	9,00	2,00	2,00	2,00	1,00

Таблица XXI. Сумма элементов и среднее арифметическое для критерия “Распределенный мониторинг”.

Web-интерфейс	Сумма	Среднее значение
WireShark	34,00	0,15
Nagios	5,13	1,01
Zabbix	5,13	1,01
PRTG	5,13	1,01
Network Olympus	2,61	1,82

Таблица XXII. Вектор весов *b*.

Критерий	Значение
Платформа	2,47
Стоимость	1,46
Автоматическое обнаружение	0,6
Web-интерфейс	0,29
Распределенный мониторинг	0,18

Таблица XXIII. Матрица весов альтернатив по каждому критерию *A*.

Критерии	Платформа	Стоимость	Автоматическое обнаружение	Web-интерфейс	Распределенный мониторинг
WireShark	1,71	2,77	0,24	0,14	0,15
Nagios	0,49	0,18	1,19	0,43	1,01
Zabbix	1,71	0,52	1,19	1,48	1,01
PRTG	0,63	0,34	1,19	1,48	1,01
Network Olympus	0,47	1,18	1,19	1,48	1,82

Далее нужно найти вектор весов альтернатив, для чего значение ***A*** перемножается с *b*.

$$Ab = c \text{ , иначе}$$

$$\begin{pmatrix} 1,71 & 2,77 & 0,24 & 0,14 & 0,15 \\ 0,49 & 0,18 & 1,19 & 0,43 & 1,01 \\ 1,71 & 0,52 & 1,19 & 1,48 & 1,01 \\ 0,63 & 0,34 & 1,19 & 1,48 & 1,01 \\ 0,47 & 1,18 & 1,19 & 1,48 & 1,82 \end{pmatrix} * \begin{pmatrix} 2,50 \\ 1,34 \\ 0,40 \\ 0,58 \\ 0,18 \end{pmatrix} = \begin{pmatrix} 8,06 \\ 2,36 \\ 6,42 \\ 3,52 \\ 4,67 \end{pmatrix}$$

По итогам всех проведенных вычислений, и нахождению результирующего вектора *c* определяется приоритетный объект (цель) с наибольшим набранным показателем. В данном случае им стала система мониторинга WireShark, но, также стоит обратить внимание, преимущество этой системы по большей части выступает за счет бесплатной ее версии и кроссплатформенности, однако если рассматривать приобретение системы для коммерческих целей, то более гибкие настройки и сравнительно небольшая стоимость за полный доступ показывает система Zabbix. У системы мониторинга Zabbix тоже есть бесплатная версия, средства визуализации и высокая скорость отработки задач.

Теперь следует определить, насколько мнение эксперта соответствует показателю адекватности. Для нахождения индекса согласованности (ИО) и итогового отношения согласованности (0<ОС≤1) нужно воспользоваться формулой [7]:

ОС=ИС/СС, где

$$ИС = \frac{|\lambda_{\max} - n|}{(n-1)} \quad (11)$$

n - порядок матрицы (количество критериев “важно”);

СС – случайная согласованность (зависит от размерности матрицы, см. табл. XXII).

Таблица XXIV. Случайная согласованность.

Размерность матрицы	2	3	4	5	6	7
СС	0	0,58	0,9	1,12	1,24	1,32

Найдем λ_{max} (см. табл. IX).

λ_{max}=(1,68·0,599)+(6,51·0,256)+(14,25·0,05)+
+(13,67·0,08)+(25,00·0.02)=**4,873**

N =5 (из табл. XXII)

$$ИС = \frac{|\lambda_{max} - n)|}{(n-1)} = \frac{|4,873-5)|}{(5-1)} = 0,03 \quad (12)$$

Поскольку n = 5, тогда СС=1,12

$$ОС = \frac{ИС}{СС} = \frac{0,03}{1,12} = \mathbf{0,028} \le 0,1 \quad (13)$$

Значение ОС удовлетворяет требованию, что указывает на адекватность и приемлемость экспертных оценок в практическом смысле.

Для быстрого реагирования на инициализацию DDoS-атаки и принятия решений по противодействию рекомендуется создавать рекомендации для специалистов портала (администраторов, уполномоченных лиц). Также следует учитывать различные негативные воздействия, связанные с климатическими условиями (перегрев, нашествие насекомых и т.д.) [8], которые могут повлиять на техническое обеспечение и базовые требования безопасности информации.

VIII. Заключение

Существующий уровень качества госуслуг в различных странах мира продолжает оставаться актуальной задачей для обеспечения комфортных условий использования услуг, но анализ показал наличие проблем, с которыми необходимо вести борьбу на соответствующем уровне, применяя инновационные технологии и средства. Существует разнообразие имитационных моделей с различным функционалом. Для обеспечения многофакторной системы защиты можно использовать несколько моделей, дополняющих друг друга. Например, иерархическая модель может указывать на вероятность и влияние потенциальной атаки, а сетевая модель может анализировать трафик и настраивать ограничения или запреты.

С развитием техносферы возможности мощностей атак и методы их реализации все растут. Проведенное исследование показало, что система моделирования работает верно и позволяет изучать зависимость состояния сервера от DDoS-атак, а также тестировать методы защиты и их эффективность. А примененный метод анализа иерархий выявил приоритетный продукт для увеличения эффективности защиты портала, что в совокупности

можно использовать при создании рекомендаций для организаций/предприятий различного масштаба.

Библиография

[1] Agostinho A.C., Britvina V.V., Konyukhovaa G.P., Gavrilyuk A.V., Nurgazina G.E. Development of a management model for public services on digital platforms in the Republic of Angola // Proc. SPIE, 2023, p. 12564.

[2] Diaz J.E.M. Internet of Things and Distributed Denial of Service as Risk Factors in Information Security. IntechOpen, 2020. p. 368, DOI: 10.5772/intechopen.94516.

[3] Пителинский К.В., Федоров Н.В., Чайчиц А.И., Широкова О.А. Управление информационным контуром вуза и его защита с помощью биометрической идентификации: некоторые методы и средства // Вопросы защиты информации. 2020. №1 (128). С. 19-29.

[4] Bala A., Osais Y. Modelling and simulation of DDOS Attack using SimEvents // International Journal of Scientific Research in Network Security and Communication. 2020. No. 1. P. 2321-2321.

[5] Клейнрок Л. Теория массового обслуживания. М.: Машиностроение. 1979.

[6] Локотченко В.В. Сравнение систем мониторинга сети // Исследования молодых ученых: материалы VIII Междунар. науч. конф., Казань: Молодой ученый, 2020. С. 4-7.

[7] Пителинский К.В., Федоров Н.В., Маковей С.О., Сигида М.П. О кластеризации бионических роботов по их функционалу методами машинного обучения // Оборонный комплекс научно-техническому прогрессу России. 2021. №4. С. 39-49.

[8] Lubua E.W., Semlambo A.A., Mkude C.G. Factors Affecting the Security of Information Systems in Africa: A Literature Review // University of Dar es Salaam Library Journal. 2023. Vol. 17, No. 2. P. 94-114.

Comparative analysis of platforms for digitalization of public services

V.V. Britvina, A.C. Agostinho, G.P. Konyukhova

Abstract—A comparative analysis of the technologies used in public services is presented. Based on the results of the review, conclusions are presented on the applicability of this experience in the Republic of Angola. Attention is also paid to the study of one of the main types of threats to web services and portals, especially those of a state nature. Based on the study of distributed denial of service, it is understood that developers of DDoS attack tools have flexible initialization capabilities and their design methods. This gives DDoS attacks the characteristics of uncertainty and unpredictability. As a result of these reasons, the focus falls on studying this threat in order to collect the required knowledge that will allow us to identify some patterns in scenarios and find a universal solution for prevention or forecasting. With this knowledge, you can increase the effectiveness of protection against DDoS attacks. Part of the research work is devoted to simulating a DDoS attack using the mathematical model M/M/k/n for queuing systems in order to determine the quantitative measure of its impact on the victim. The experiments conducted in this study show that the server is practically not used in its usual conditions, thus it has high availability and low average load. However, at the time of creating a large volume of false requests from an attacker, its load increases dramatically and, thus, leads to a decrease in availability. An example of using T. Saati's method to select a priority object from the selected alternatives is shown. The results of the experiment make it possible to predict the damage from a DDoS attack with varying degrees of intensity and, based on the values obtained, apply protective measures in the process of developing a web portal.

Keywords— public Services portal, distributed denial of service, hierarchy analysis method, fault tolerance.

REFERENCES

[1] A.C. Agostinho, V.V. Britvina, G.P. Konyukhovaa, A. V. Gavrilyuk, and G. E. Nurgazina “Development of a management model for public services on digital platforms in the Republic of Angola”, Proc. SPIE, p. 12564, 2023.

[2] J. E. M. Diaz, “Internet of Things and Distributed Denial of Service as Risk Factors in Information Security,” IntechOpen, p. 368, 2020.

[3] K. V. Pitelinsky, N. V. Fedorov, A. I. Chaichits and O. A. Shirokova. “Management of the information circuit of a university and its protection using biometric identification: some methods and means,” Issues of information security, No. 1 (128), p. 19-29, 2020. [rus]

[4] A. Bala, Y. Osais, “Modelling and simulation of DDOS Attack using SimEvents”, International Journal of Scientific Research in Network Security and Communication, no. 1, p. 2321-2321, 2020.

[5] L. Kleinrock, “The Theory of Queuing”, Moscow, Mechanical Engineering. 1979. [rus]

[6] V.V. Lokotchenko, “Comparison of network monitoring systems” In Research of young scientists: materials of the VIII International. scientific conf., Kazan: Young scientist, p. 4-7, 2020. [rus]

[7] K.V. Pitelinsky, N.V. Fedorov, S.O. Makovey, M.P. Sigida. “On the clustering of bionic robots by their functionality using machine learning methods,” Defense Complex for Scientific and Technical Progress of Russia, No. 4, p. 39-49, 2021. [rus]

[8] E. W. Lubua, A. A. Semlambo and C. G Mkude. “Factors Affecting the Security of Information Systems in Africa: A Literature Review” University of Dar es Salaam Library Journal, vol. 17, no. 2, p. 94-114, 2023.

V.V. Britvina, Ph.D., Associate Professor, Department of Management and Informatics in Technical Systems, Moscow State Technological University Stankin, Polytechnic University, 38, st. Bolshaya Semyonovskaya, Moscow, 107023, Russia Moscow, Russia (e-mail: saaturn2015@mail.ru).

A.C. Agostinho, Department of Management and Informatics in Technical Systems, Moscow State Technological University Stankin, Moscow, Russia (e-mail: adcaculo@gmail.com)

G.P. Konyukhova, PhD, Associate Professor, Associate Professor of the Department of Management and Informatics in Technical Systems, Moscow State Technological University Stankin, Associate Professor of the Department of Higher Mathematics of MIREA, Moscow, Russia (e-mail: maurico@yandex.ru)