УДК 004.94

Никулин И. А.
Студент кафедры прикладной информатики
и информационных технологий
НИУ «БелГУ», 4 курс (Белгород, Россия)
Научный руководитель: Гахова Н.Н.
К.т.н., доцент
кафедры прикладной информатики
и информационных технологий
НИУ «БелГУ», (Белгород, Россия)
Nikulin I.A.
Student of the Department of Applied Informatics
and Information Technology
NRU "BelSU", 4rd year (Belgorod, Russia)
Scientific supervisor: Gahova N.N.
Associate Professor of the Department of Applied Informatics
and Information Technology
NRU "BelSU", (Belgorod, Russia)

ОПРЕДЕЛЕНИЕ СТАТИСТИЧЕСКИХ ПОКАЗАТЕЛЕЙ ПРОЦЕССА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СРЕДСТВАМИ GPSS

DETERMINATION OF STATISTICAL INDICATORS OF THE USER AUTHENTICATION PROCESS BY MEANS OF GPSS

Аннотация: В статье рассматривается процесс имитационного моделирования системы аутентификации пользователей с использованием платформы GPSS. Моделирование включает обработку запросов на аутентификацию двумя методами: Private State Token (PST) и традиционным способом. Определены статистические показатели эффективности системы, предложены способы оптимизации для повышения производительности.

Abstract: The article discusses the process of simulation modeling of a user authentication system using the GPSS platform. The simulation includes processing authentication requests using two methods: Private State Token (PST) and the traditional method. Statistical indicators of system efficiency are determined, and optimization methods are proposed to improve performance.

Ключевые слова: имитационное моделирование, GPSS, аутентификация, Private State Token, традиционный метод.

Keywords: simulation modeling, GPSS, authentication, Private State Token, traditional method.

Современные системы аутентификации пользователей требуют высокой производительности и надежности. В данной статье рассматривается моделирование системы аутентификации, которая обрабатывает запросы пользователей с использованием двух методов: Private State Token (PST) и традиционного метода. Моделирование выполнено в среде GPSS [1], что позволяет оценить эффективность системы и предложить пути ее оптимизации [2].

В системе аутентификации пользователей сервер с потоками обрабатывает запросы на аутентификацию двумя методами: Private State Token (PST) и традиционным способом, как это реализовано во ВКонтакте (VK). Пользователи поступают в систему каждые 1,5 секунды и с вероятностью 70% выбирают метод PST, а с вероятностью 30% — традиционный метод. Каждый пользователь может сделать до трёх попыток аутентификации. Если запрос успешен, пользователь завершает процесс, в противном случае он переходит к следующей попытке или выходит из системы после трёх неудачных попыток. Время обработки одного запроса для метода PST составляет 3 секунды с отклонением ±1 секунда, а вероятность успешной аутентификации равна 95%. Для традиционного метода время обработки составляет 7 секунд с отклонением ±2 секунды, а вероятность успеха равна 90%. Система работает в течение 24 часов.

Для моделирования процесса аутентификации пользователей была разработана имитационная модель, основанная на описанных данных. Моделирование включало генерацию запросов на аутентификацию, последовательное прохождение ими всех этапов обработки (выбор метода аутентификации, попытки аутентификации и завершение процесса) и учет времени на каждом этапе. В модели также учитывались вероятности успешной и неудачной аутентификации для каждого метода, а также ограничение на количество попыток. На рисунке 1 представлена имитационная модель, реализованная в среде GPSS.

```
* Определение ресурсов
SERVER_STORAGE STORAGE 2 ; Сервер с 2 потоками для обработки запросов
* Генерация пользователей (средний интервал 3 секунды)
GENERATE 0.05 ; Интервал поступления запросов на аутентификацию
* Выбор метода аутентификации
TRANSFER .7,PST_AUTH1,TRADITIONAL_AUTH1 ; 70% используют Private State Token, 30% традиционный метод
* Первая попытка аутентификации с использованием Private State Token API
PST_AUTH1 QUEUE QUEUE_PST_AUTH ; Очередь на сервер для Private State Token
                    ENTER SERVER_STORAGE,1 ; Запрос занимает один поток
                    DEPART QUEUE_PST_AUTH ; Уход из очереди на сервер
                    ADVANCE 0.05,0.0167 ; Обработка запроса: 3 ± 1 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1 ; Освобождение потока сервера
                    TRANSFER .95,EXIT_SUCCESS,PST_AUTH2 ; 95% успешных, 5% ошибка
* Вторая попытка через Private State Token
PST_AUTH2 QUEUE QUEUE_PST_AUTH ; Очередь на сервер для Private State Token
                    ENTER SERVER_STORAGE,1
                    DEPART QUEUE_PST_AUTH
                    ADVANCE 0.05,0.0167 ; 3 ± 1 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1
                    TRANSFER .95,EXIT_SUCCESS,PST_AUTH3 ; 95% успешных, 5% ошибка
* Третья попытка через Private State Token
PST_AUTH3 QUEUE QUEUE_PST_AUTH ; Очередь на сервер для Private State Token
                    ENTER SERVER_STORAGE,1
                    DEPART QUEUE_PST_AUTH
                    ADVANCE 0.05,0.0167 ; 3 ± 1 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1
                    TRANSFER .95,EXIT_SUCCESS,EXIT_FAIL ; 95% успешных, 5% ошибка
* Первая попытка традиционной аутентификации
TRADITIONAL_AUTH1    QUEUE QUEUE_TRAD_AUTH ; Очередь на сервер для традиционного метода
                    ENTER SERVER_STORAGE,1
                    DEPART QUEUE_TRAD_AUTH
                    ADVANCE 0.1167,0.0333 ; Обработка запроса: 7 ± 2 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1
                    TRANSFER .9,EXIT_SUCCESS,TRADITIONAL_AUTH2 ; 90% успешных, 10% ошибка
* Вторая попытка через традиционную аутентификацию
TRADITIONAL_AUTH2    QUEUE QUEUE_TRAD_AUTH
                    ENTER SERVER_STORAGE,1
                    DEPART QUEUE_TRAD_AUTH
                    ADVANCE 0.1167,0.0333 ; 7 ± 2 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1
                    TRANSFER .9,EXIT_SUCCESS,TRADITIONAL_AUTH3 ; 90% успешных, 10% ошибка
* Третья попытка через традиционную аутентификацию
TRADITIONAL_AUTH3    QUEUE QUEUE_TRAD_AUTH
                    ENTER SERVER_STORAGE,1
                    DEPART QUEUE_TRAD_AUTH
                    ADVANCE 0.1167,0.0333 ; 7 ± 2 секунды (в минутах)
                    LEAVE SERVER_STORAGE,1
                    TRANSFER .9,EXIT_SUCCESS,EXIT_FAIL ; 90% успешных, 10% ошибка
* Успешная аутентификация
EXIT_SUCCESS TERMINATE
* Провал аутентификации после 3 попыток
EXIT_FAIL TERMINATE
* Завершение работы системы
GENERATE 1440 ; Система работает 24 часа (1440 минут)
TERMINATE 1 ; Завершение моделирования
```

Рисунок 1 – Имитационная модель

На рисунке 2 представлены полученные статистические данные отражающие статистику работы очередей двух вариантов обработки запросов аутентификации.

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
QUEUE_PST_AUTH	6812	6810	16077	1	3402.444	304.753	304.772	0
QUEUE_TRAD_AUTH	15172	15171	35868	1	7592.208	304.806	304.814	0
QUEUE_WAIT	0	0	0	0	0.000	0.000	0.000	0

Рисунок 2 – Статистические данные модели

Таким образом, максимальная длина очереди (MAX) равна 6812 для PST-аутентификации и 15172 для традиционного метода, среднее время ожидания (AVE.TIME) составляет 304.753 и 304.806 секунд соответственно, а общее количество запросов (ENTRY) – 16077 и 35868. Распределение запросов по очередям (QUEUE) показывает, что PST-вариант обрабатывает их быстрее, несмотря на меньшую нагрузку.

Рисунок 3 содержит статистические данные о распределении временных интервалов для событий аутентификации.

TABLE	MEAN	STD.DEV.	RANGE			RETRY	FREQUENCY	CUM.%
TIME_TO_PST_AUTH	304.181	175.028				0		
			_	-	20.000		329	3.55
			20.000	-	40.000		298	6.77
			40.000	-	60.000		263	9.60
			60.000	-	80.000		299	12.83
			80.000	-	100.000		295	16.01
			100.000	-	120.000		301	19.26
			120.000	-	140.000		331	22.83
			140.000	-	160.000		318	26.27
			160.000	-	180.000		277	29.25
			180.000	-	_		6556	100.00
TIME_TO_TRADITIONAL_AUTH	304.310	176.350				0		
			_	-	20.000		695	3.36
			20.000	-	40.000		690	6.69
			40.000	-	60.000		676	9.96
			60.000	-	80.000		664	13.17
			80.000	-	100.000		684	16.47
			100.000	-	120.000		670	19.71
			120.000	-	140.000		701	23.10
			140.000	-	160.000		680	26.38
			160.000	-	180.000		677	29.65
			180.000	-	_		14560	100.00
TIME_IN_QUEUE	0.000	0.000				0		

Рисунок 3 – Статистические данные очередей

Колонки показывают следующие параметры: среднее значение времени (MEAN), стандартное отклонение (STD.DEV.), которые составляют для TIME_TO_PST_AUTH - 304.181±175.028 сек, TIME_TO_TRADITIONAL_AUTH - 304.310±176.350 сек и TIME_IN_QUEUE -0 сек, диапазоны обработки (RANGE) составили 20-180 сек, частоту запросов в каждом интервале (RETRY FREQUENCY), примерно 263-701 случаев, и кумулятивный процент выполнения на каждый диапазон обработки (CUM.%). Анализ показывает схожую временную эффективность методов при незначительном преимуществе PST-аутентификации. Отсутствие времени в очереди (TIME_IN_QUEUE) свидетельствует о оптимальной нагрузке системы.

Варианты аутентификации с использованием метода PST и традиционного метода характеризуются высокой загруженностью и длительным временем ожидания. Эти показатели позволяют выделить ключевые узкие места системы, требующие улучшения для повышения общей эффективности процесса.

Для повышения эффективности работы системы было проведено увеличение количества потоков обработки запросов с двух до шести (рисунок 4).

QUEUE	MAX CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
QUEUE_PST_AUTH	4	0	24597	17708	0.095	0.006	0.020	0
QUEUE_TRAD_AUTH	6	0	54735	37617	0.245	0.006	0.021	0
QUEUE_WAIT	0	0	0	0	0.000	0.000	0.000	0

TABLE	MEAN	STD.DEV.	RANGE	RETRY	FREQUENCY	CUM.%
TIME_TO_PST_AUTH	0.006	0.013		0		
			_ - 2.000		24597	100.00
TIME_TO_TRADITIONAL_AUTH	0.006	0.014			0	
			_ - 2.000		54735	100.00
TIME_IN_QUEUE	0.000	0.000		0		

Рисунок 4 – Динамика работы модели с добавлением потоков

Такое перераспределение ресурсов позволило сбалансировать нагрузку между этапами и уменьшить время ожидания в очередях, что положительно

сказалось на общей производительности системы. Результаты моделирования с обновленным распределением ресурсов показали значительное сокращение времени ожидания с 0.020 до 0.006 секунд для PST-аутентификации и с 0.021 до 0.006 секунд для традиционного метода, а также увеличение пропускной способности системы с 17,708 до 24,597 обработанных запросов для PST и с 37,617 до 54,735 запросов для традиционной аутентификации, что обеспечивает более оперативную обработку запросов на аутентификацию (рисунок 4).

В результате проведенного исследования с использованием имитационного моделирования была проанализирована работа системы аутентификации пользователей. Моделирование показало, что текущая конфигурация системы с двумя потоками обработки запросов не обеспечивает достаточной производительности, что приводит к длительным временам ожидания в очередях. Основные проблемы заключаются в высокой загруженности на этапах обработки запросов с использованием методов PST и традиционной аутентификации. Оптимизация системы за счет увеличения количества потоков до шести позволила значительно сократить время ожидания и повысить общую эффективность обработки запросов. Результаты моделирования продемонстрировали улучшение производительности системы, что способствует более оперативной и надежной аутентификации пользователей.

Использованные источники:

1. Моделирование систем. Инструментальные средства GPSS WORLD [Электронный ресурс] – Режим доступа. – URL: https://djvu.online/file/0WCWHpdclwfNA (дата обращения: 10.01.2025)
2. Официальный сайт GPSS [Электронный ресурс] – Режим доступа. – URL: http://www.webgpss.com/ (дата обращения: 10.01.2025)

   Ссылка на статью: https://www.modern-j.ru/_files/ugd/b06fdc_6a3adbe6a6314244a6814a89badcfd41.pdf?index=true