УДК 004.056.53
DOI: 10.26102/2310-6018/2023.42.3.015

Система показателей для оценки эффективности процедур многофакторной аутентификации в Web-приложениях

Д.С. Богданов✉

«НК «Роснефть» - НТЦ, Краснодар, Российская Федерация

Резюме. Актуальность исследования обусловлена растущими темпами внедрения механизмов многофакторной аутентификации в Web-приложения, популяризацией Web-технологий, а также отсутствием в Российской Федерации конкретных стандартов, описывающих работу процедур многофакторной аутентификации и устанавливающих требования к Web-приложениям, которые используют данные процедуры. Целью проводимого исследования является разработка системы показателей для оценки эффективности процедур многофакторной аутентификации в Web-приложениях на основе ранее разработанной классификации рассматриваемых процедур. В ходе исследования был проведен анализ научных публикаций по исследуемой теме, предложены лингвистические шкалы для показателей: затрат, надежности, безопасности, эффективности, а также факторы, влияющие на соответствующие показатели, выделены допустимые значения показателей, которые в последующих публикациях по данной тематике будут уточнены с использованием метода экспертных оценок. Также в рамках исследования были предложены способы расчета значений показателей затрат, надежности, безопасности и эффективности. Полученный в ходе исследования материал в последующем может быть конкретизирован в соответствии с перечнем решаемых задач, направленных на обеспечение информационной безопасности процедур многофакторной аутентификации. Материалы работы представляют теоретическую ценность для дальнейших исследований в данной области.

Ключевые слова: многофакторная аутентификация, Web-приложение, двухфакторная аутентификация, классификация, показатели процедур аутентификации, оценка эффективности.

Для цитирования: Богданов Д.С. Система показателей для оценки эффективности процедур многофакторной аутентификации в Web-приложениях. *Моделирование, оптимизация и информационные технологии.* 2023;11(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1426 DOI: 10.26102/2310-6018/2023.42.3.015

Indicator framework for evaluating the performance of multi-factor authentication procedures in Web applications

D.S. Bogdanov✉

NK Rosneft - STC, Krasnodar, the Russian Federation

Abstract. The relevance of the study is due to the increasing use of multi-factor authentication mechanisms in Web applications, the popularization of Web technologies as well as the lack of specific standards in the Russian Federation describing the operation of multi-factor authentication procedures and establishing requirements for Web applications that use these procedures. The purpose of the research is to develop an indicator framework for assessing the performance of multi-factor authentication procedure information security in Web applications based on the previously developed classification of the procedures under consideration. An analysis of scientific publications on the issue under study was carried out; linguistic scales for indicators were proposed: costs, reliability, safety, efficiency as well as factors affecting the indicators. Acceptable indicator values were identified, which will be clarified using the method of expert assessments in subsequent publications on this issue. As part of the study, methods for calculating the values of cost, reliability, safety, and efficiency indicators were proposed. The findings of the study can later be specified in compliance with the list of the objectives

aimed at ensuring the information security of multi-factor authentication procedures. The materials of the research are of theoretical value for further research in this field.

Keywords: multi-factor authentication, Web application, two-factor authentication, classification, indicators of authentication procedures, efficiency assessment.

For citation: Bogdanov D.S. Indicator framework for evaluating the performance of multi-factor authentication procedures in Web applications. *Modeling, Optimization and Information Technology*. 2023;11(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1426 DOI: 10.26102/2310-6018/2023.42.3.015 (In Russ.).

Введение

На современном этапе развития информационных технологий большую актуальность приобрело обеспечение информационной безопасности Web-приложений. Важную роль в обеспечении конфиденциальности, целостности и доступности информации играют механизмы аутентификации, которые заложены в архитектуру функционирования Web-приложений. Анализ тенденций развития вычислительных мощностей персональных компьютеров позволяет сделать вывод об устаревании классических механизмов аутентификации, основанных на факторе знания [1]. Как показывает практика, одним из возможных вариантов решения проблемы устаревания классических процедур аутентификации является использование процедур многофакторной аутентификации (далее – МФА), приобретающих все большую популярность среди разработчиков Web-приложений и активно интегрируемых в структуру обеспечения безопасности Web-ресурсов в целях повышения качественных характеристик безопасности информации Web-приложений [2]. Как следствие, разработчиками систем безопасности Web-приложений выполняется соответствующий комплекс мер, направленный на повышение безопасности администрируемых ими ресурсов.

Для применения на практике какого-либо механизма МФА в разрабатываемой модели безопасности Web-приложения следует произвести оценку его эффективности. В качестве объекта исследования рассматриваются процедуры аутентификации в Web-приложениях.

Среди немногих публикаций в области оценки эффективности процедур МФА можно отметить работу [3], авторы которой достаточно структурированно и полно рассматривают методы оценки защищенности механизмов МФА. Однако в данной работе не учитывается специфика аутентификации в Web-приложениях, в частности, показателей оценки, играющих большую роль в построении эффективных механизмов проверки подлинности.

Целью представленной работы является формирование системы показателей для оценки эффективности создания и моделирования механизмов обеспечения информационной безопасности процедур МФА в Web-приложениях.

Материалы и методы

В работе [3] подробно исследованы механизмы МФА, однако, к аутентификации в Web-приложениях можно отнести только основу проведенного исследования из-за отсутствия соответствующих сведений. В работе достаточно подробно изложены факторы, на основе которых может быть произведена аутентификация, рассмотрены комбинации факторов МФА, приведены методы оценки защищенности ее механизмов. Отмечено, что для реализации механизмов МФА на практике необходимо провести ряд исследований и получить оценки защищенности таких механизмов от

несанкционированного доступа для конкретных моделей угроз и применяемых ключей, параметров [3].

В научном труде [4] рассмотрены способы аутентификации, применяющиеся при построении систем аутентификации в Web-приложениях, приведены примеры их реализаций, сформирована таблица комбинаций факторов МФА, проведен сравнительный анализ процедур МФА в Web-приложениях, разработана классификация механизмов МФА, положенная в основу исследования.

В публикации [5] проведен анализ применяемых систем однофакторной аутентификации, особенностей их работы и реализации. Предложена модель оценки критериев эффективности таких систем, основанная на векторном расстоянии. Однако использованные факторы для оценки эффективности не полностью удовлетворяют потребностям оценки МФА и показатели критериев оцениваются субъективно, что не обеспечивает требуемую точность оценок.

Одним из основных показателей, которым следует руководствоваться при внедрении в архитектуру обеспечения информационной безопасности Web-ресурса МФА является стоимость внедрения подобной процедуры [6]. Данный показатель определяет затраты на внедрение процедуры и ее дальнейшую поддержку в актуальном состоянии, при котором она способна функционировать и обеспечивать достаточную эффективность в общей структуре системы безопасности ресурса. Определяется как отношение текущих затрат на установку и обслуживание текущей системы к величине предотвращенного ущерба (1). Лингвистическая шкала показателя затрат представлена в Таблице 1.

$$K_{\text{зт}} = \frac{N_{\text{зт}}}{\Delta W} \in [0; \infty] \quad (1)$$

$K_{\text{зт}}$ – показатель затрат на внедрение и обслуживание;
$N_{\text{зт}}$ – затраты на внедрение и обслуживание текущей системы;
ΔW– величина предотвращенного ущерба.

Величина предотвращенного ущерба при условии реализации угрозы определяется соотношением:

$$\Delta W = W_0 - W_1 \quad (2)$$

W_0 – ущерб до принятия мер защиты;
W_1 – ущерб после принятия мер защиты.

Таблица 1 – Лингвистическая шкала показателя затрат
Table 1 – Linguistic scale of the cost indicator

Диапазон значений показателя $K_{\text{зт}}$	**Оценка затрат**
$K_{\text{зт}} \in [0; 0.79]$	Низкие
$K_{\text{зт}} \in [0.8; 0.99]$	Средние
$K_{\text{зт}} \geq 1$	Высокие

Данный показатель коррелирует с приведенной в работе [4] классификацией и может быть выражен, исходя из требований следующих классов процедур МФА в Web-приложениях:

1. Двусторонние процедуры аутентификации. Данные механизмы аутентификации имеют более высокие требования к аппаратному обеспечению серверов. Двусторонние механизмы аутентификации предполагают проверку не только клиентской составляющей, но и проверку аутентичности сервера (со стороны клиента).

Если учесть практически удвоенную сложность программной реализации двусторонних процедур аутентификации, можно сделать вывод о повышенных минимальных аппаратных требованиях к подобным алгоритмам, которые предполагают дополнительные финансовые вложения.

2. Процедуры аутентификации, реализованные с использованием сервера аутентификации на стороне сервера-обработчика запросов. Подобные механизмы наиболее просты в реализации, с точки зрения аппаратных требований, а с учетом выполнения всех вычислительных операций на одном оборудовании, не требуют дополнительных финансовых ресурсов.

3. Процедуры аутентификации с обособленным сервером аутентификации. Использование обособленного сервера аутентификации повышает надежность процедуры в целом за счет децентрализации критически важных компонентов в общей архитектуре системы безопасности, в частности, оборудование, которое производит обработку аутентификационных запросов размещается отдельно от основного оборудования, на котором физически размещен Web-ресурс. Подобное разделение серверов требует дополнительных финансовых затрат.

4. Процедуры аутентификации с независимым сервером аутентификации. Под независимым сервером аутентификации понимается сервер-обработчик запросов аутентификации, который физически размещен за пределами владельца Web-ресурса и не является его собственностью. Реализация данного механизма аутентификации может быть вызвана требованием к использованию обособленного сервера аутентификации в условиях недостаточного финансового обеспечения, что вынуждает организацию временно арендовать выделенный сервер для обработки аутентификационных запросов. В данном контексте следует учитывать затраты, связанные с арендой за использование вычислительных мощностей стороннего сервера.

5. Комбинированные процедуры аутентификации [7]. Таковыми, как правило, являются многофакторные механизмы аутентификации, реализуемые последовательными и (или) параллельными схемами. Их применение требует дополнительных вычислительных мощностей, что в свою очередь приводит к дополнительным финансовым вложениям.

Рассмотренные классы процедур аутентификации в аспекте их эффективности характеризуются повышением финансовых затрат не только при разработке и внедрении, но и обслуживании.

Результаты

Не менее важным показателем эффективности процедур МФА следует понимать их надежность. Данный показатель характеризуется вероятностью бесперебойного выполнения процедуры МФА своих функций в заданном режиме в условиях жизненного цикла и может сильно варьироваться в зависимости от используемой процедуры аутентификации.

В соответствии с ГОСТ 27.002-2015 «Надежность в технике (ССНТ). Термины и определения», надежность – это свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования. Например, при интеграции в систему безопасности Web-ресурса сложной комбинированной процедуры МФА с применением последовательных и параллельных схем вероятность возникновения ошибки первого рода может возрасти из-за повышенной сложности механизма аутентификации в целом. Однако упрощение схемы аутентификации приводит к снижению безопасности за счет увеличения вероятности ошибок второго рода. Исходя

из этого разработчикам систем безопасности Web-приложений требуется найти наиболее рациональный подход к построению процедур аутентификации, на основе оптимизации соотношения ошибок первого и второго рода безопасности и надежности разрабатываемых систем [8].

В системе МФА с последовательной структурой отказ любого компонента аутентификации приводит к отказу системы в целом. Расчет надежности для последовательной процедуры МФА производится следующим образом:

$$K_{\text{н}} = \prod_{i=1}^{N} p_i \in [0; 1] \quad (3)$$

$K_{\text{н}}$ – показатель надежности процедуры МФА;
p_i – вероятность безотказной работы компонента аутентификации;
N – количество компонентов аутентификации.

В системе аутентификации с параллельной структурой отказ системы в целом происходит только при отказе всех компонентов аутентификации. Расчет надежности процедуры МФА с параллельной структурой производится следующим образом:

$$K_{\text{н}} = \prod_{i=1}^{N} (1 - p_i) \in [0; 1]. \quad (4)$$

Вероятностная оценка надежности компонента процедуры МФА определяется методом экспертных оценок. Лингвистическая шкала показателя надежности представлена в Таблице 2.

Таблица 2 – Лингвистическая шкала показателя надежности
Table 2 – Linguistic scale of the reliability indicator

Диапазон значений показателя $K_{\text{н}}$	**Оценка надежности**
$K_{\text{н}} \in [0; 0.49]$	Низкая
$K_{\text{н}} \in [0.5; 0.79]$	Средняя
$K_{\text{н}} \in [0.8; 1]$	Высокая

Безопасность процедуры МФА была также выделена отдельным показателем оценки эффективности. Показатель безопасности зависит от множества факторов, например, таких как:

1) трудозатраты, выделяемые для реализации атаки на процедуру МФА. В данном случае форма данного фактора может быть выражена временными ресурсами, финансовыми затратами, эффективностью алгоритмов перебора аутентификаторов и иными требованиями, которые могут варьироваться в зависимости от условий атаки на процедуру МФА и требованиями к ее реализации;

2) уровень квалификации злоумышленника, который производит попытку атаки на процедуру МФА. При определении данного фактора стоит учитывать, что проводить подготовительные мероприятия к атаке могут несколько человек, каждый из которых может иметь соответствующие знания в различных областях, при этом, знания конкретного специалиста могут быть эффективны только лишь на конкретном этапе атаки;

3) сложность подбора злоумышленником требуемого аутентификатора. Чем выше сложность аутентификатора в рассматриваемом механизме МФА, тем выше показатель безопасности.

В Таблице 3 представлены факторы, оказывающие влияние на показатели надежности, безопасности и эффективности процедуры МФА. Основой для предложенной таблицы послужили результаты ранее проведенного исследования,

описанные в работе [4]. Данный перечень не является исчерпывающим и требует проведения экспертных оценок для определения степени влияния факторов на итоговые показатели. Результаты проведения экспертных оценок будут опубликованы в дальнейших исследованиях.

Таблица 3 – Факторы, влияющие на показатели процедур МФА
Table 3 – Factors affecting the performance of multi-factor authentication procedures

Показатель	Фактор	Описание
Затраты на внедрение и обслуживание	Затраты на реализацию двусторонней аутентификации	Отношение текущих затрат к средним затратам на разработку системы аутентификации подобного класса
	Затраты на обособленный сервер аутентификации	
	Затраты на независимый сервер аутентификации	
	Затраты на комбинацию механизмов аутентификации	
Надежность	Наличие комбинированных механизмов аутентификации	Показатель, который может принимать два значения
	Наличие двусторонней аутентификации в составе системы	
	Глубина комбинаций механизма аутентификации	Количество этапов аутентификации, которые должен успешно завершить клиент
	Наличие обособленного или независимого сервера аутентификации в составе системы	Показатель, принимающий три значения, в зависимости от типа сервера аутентификации и его наличия
Безопасность	Оценка временных ресурсов на реализацию атаки	Временные затраты на реализацию атаки на процедуру аутентификации
	Оценка финансовых вложений на реализацию атаки	Количество денежных средств, затраченных на реализацию атаки на процедуру аутентификации
	Оценка уровня квалификации злоумышленника	Числовой показатель, основанный на типовой модели нарушителя
	Сложность аутентификатора	Числовой показатель, основанный на типовой модели аутентификатора

Таблица 3 (продолжение)
Table 3 (extended)

Показатель	Фактор	Описание
Эффективность	Безопасность	Обобщенный числовой показатель, определяющий эффективность процедуры аутентификации
	Надежность	
	Затраты на внедрение и обслуживание	

Риск для каждой отдельной уязвимости процедуры аутентификации рассчитывается как произведение вероятности угрозы реализации уязвимости процедуры МФА и ущерба, получаемого в случае наступления негативных последствий:

$$p_r = p_d w \in [0; 1]. \quad (5)$$

Показатель безопасности для всей процедуры аутентификации рассчитывается следующим образом:

$$K_б = \sum_{i=1}^{N}(1 - p_d w) \in [0; 1] \quad (6)$$

$K_б$ – показатель безопасности процедуры МФА;
p_d – вероятность угрозы реализации уязвимости процедуры МФА;
w – ущерб от реализации уязвимости.

Для w принимается шкала, исходя из возможностей субъекта и его риск-аппетита. При этом, следует учесть, что ущерб от реализации уязвимости должен удовлетворять условию $w \in [0; 1]$. Лингвистическая шкала показателя безопасности представлена в Таблице 4.

С перечнем типовых уязвимостей для Web-приложений можно ознакомиться на официальном сайте Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК) в разделе «Типовые уязвимости веб-приложений», базовой моделью угроз безопасности ФСТЭК и методикой оценки угроз безопасности информации [9, 10].

Таблица 4 – Лингвистическая шкала показателя безопасности
Table 4 – Linguistic scale of the safety indicator

Диапазон значений показателя $K_б$	Оценка надежности
$K_б \in [0; 0.49]$	Низкая
$K_б \in [0.5; 0.79]$	Средняя
$K_б \in [0.8; 1]$	Высокая

В соответствии с ГОСТ Р ИСО 9000-2015 «Системы менеджмента качества. Основные положения и словарь», эффективность – соотношение между достигнутым результатом и использованными ресурсами. Показатель эффективности имеет прямую зависимость от ранее рассмотренных показателей надежности и безопасности и дает понимание целесообразности использования процедуры МФА (7). Лингвистическая шкала показателя эффективности представлена в Таблице 5.

$$K_{эф} = \frac{K_н K_б}{K_{эт}} \in [0; \infty] \quad (7)$$

$K_{эф}$ – показатель эффективности;
$K_н$ – показатель надежности;

$K_б$ – показатель безопасности;
$K_{зт}$ – показатель затрат.

Таблица 5 – Лингвистическая шкала показателя эффективности
Table 5 – Linguistic scale of the performance indicator

Диапазон значений показателя	Класс эффективности системы МФА
$K_{эф} \in [0; 0.49]$	III класс
$K_{эф} \in [0.5; 0.79]$	II класс
$K_{эф} \in [0.8; 1]$	I класс

Для диапазонов значений показателей были установлены соответствующие классы эффективности систем МФА. В дальнейших исследованиях на основе данных, полученных методом экспертных оценок, классификация будет раскрыта подробнее.

Исходя из результатов проведенных исследований, можно сделать вывод о том, что показатели, за исключением показателя затрат, выражается совокупностью вероятностных оценок влияния различных факторов. В данном случае основой показателей послужили результаты ранее проведенных исследований, представленные классификацией процедур МФА в работе [4]. Для каждого из предложенных показателей были установлены лингвистические шкалы.

Обсуждение

В результатах исследования были отражены факторы и показатели для оценки эффективности процедур МФА в Web-приложениях. За их основу были взяты результаты ранее проведенного исследования [4]. Был произведен анализ научных трудов в исследуемой области и отобран материал для последующей его адаптации к оценке эффективности процедур МФА.

В результате исследования эффективности процедур МФА были сделаны выводы о необходимости введения факторов, влияющих на расчет показателей (Таблица 3). Были предложены лингвистические шкалы для показателей, часть из которых требует дополнительной конкретизации и разработки моделей нарушителя и аутентификатора, что будет отражено в дальнейших исследованиях.

Заключение

В работе были предложены факторы и показатели оценки эффективности процедур МФА Web-приложений. К показателям были отнесены:

1) затраты на внедрение и обслуживание процедур МФА;
2) надежность процедуры МФА;
3) безопасность процедуры МФА;
4) эффективность процедуры МФА.

Для каждого из показателей были выделены факторы, влияющие на них (Таблица 3).

Стоит отметить, что некоторые из полученных значений показателей требуют дополнительного обоснования путем разработки моделей: угроз, злоумышленника и аутентификатора. Также требуется провести дополнительные исследования, направленные на получение экспертных оценок, которые в дальнейшем будут использованы в целях получения вероятностных оценок для рассматриваемых

показателей и последующей разработки формальных моделей, описывающих функционирование механизмов МФА в Web-приложениях.

СПИСОК ИСТОЧНИКОВ

1. Бирюков А. Сравнение систем двухфакторной аутентификации. *Системный Администратор*. 2011;102(5):60–65.
2. Антипов А. Важность многофакторной аутентификации. URL: https://www.securitylab.ru/analytics/425166.php [дата обращения: 12.05.2023].
3. Горбенко Ю.И., Олешко И.В. Модели и методы оценки защищенности механизмов многофакторной аутентификации. *Восточно-Европейский журнал передовых технологий.* 2013;6(2):4–10.
4. Богданов Д.С., Клюев С.Г. Классификация и сравнительный анализ технологий многофакторной аутентификации в Веб-приложениях. *Моделирование, оптимизация и информационные технологии.* 2020;8(1). URL: https://moit.vivt.ru/wpcontent/uploads/2020/02/BogdanovKluev_1_20_1.pdf. DOI: 10.26102/2310-6018/2020.28.1.033 (дата обращения: 12.05.2023).
5. Сухаревская Е.В. Исследование систем аутентификации. *Международный студенческий научный вестник*. 2018;1(1):71.
6. Малков А. Оценка эффективности и защищённости механизмов аутентификации. URL: https://habr.com/ru/post/179179 [дата обращения: 10.04.2023].
7. Макуха М.Ю., Клюев С.Г. Анализ и критерии эффективности современных методов и способов выявления инкапсулированных пакетов TCP/IP-трафика. *Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки.* 2020;6:110–115.
8. Горюн К.Н., Клюев С.Г. Особенности проведения аудита и мониторинга информационной безопасности в распределенных информационных системах. *Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки.* 2020;7:58–61.
9. Банк данных угроз – типовые уязвимости Web-приложений. ФСТЭК: 2023. URL: https://bdu.fstec.ru/webvulns [дата обращения: 20.06.2023].
10. Методика оценки угроз безопасности информации. ФСТЭК: 2021. URL: http://www.garant.ru/products/ipo/prime/doc/400325044 [дата обращения: 20.06.2023].

REFERENCES

1. Biryukov A. Comparison of two-factor authentication systems. *Sistemnyi Administrator*. 2011;102(5):60–65. (In Russ.).
2. Antipov A. The importance of multi-factor authentication. URL: https://www.securitylab.ru/analytics/425166.php [accessed on 12.05.2023]. (In Russ.).
3. Gorbenko Yu.I., Oleshko I.V. Models and methods for assessing the security of multi-factor authentication mechanisms. *Vostochno-Evropeiskii zhurnal peredovykh tekhnologii = Eastern-European Journal of Enterprise Technologies.* 2013;6(2):4–10. (accessed on 12.05.2023) (In Russ.).
4. Bogdanov D.S., Klyuev S.G. Classification and comparative analysis of technologies of multifactor authentication in Web applications. *Modeling, Optimization and Information Technology.* 2020;8(1). URL: https://moit.vivt.ru/wpcontent/uploads/2020/02/BogdanovKluev_1_20_1.pdf. DOI: 10.26102/2310-6018/2020.28.1.033 (In Russ).
5. Sukharevskaya E.V. Research of authentication systems. *Mezhdunarodnyi studencheskii nauchnyi vestnik*. 2018;1(1):71. (In Russ.).

6. Malkov A. Evaluation of the effectiveness and security of authentication mechanisms. URL: https://habr.com/ru/post/179179 [accessed on 10.04.2023]. (In Russ.).
7. Makukha M.Yu., Klyuev S.G. Analysis and criteria for the effectiveness of modern methods and methods for detecting encapsulated TCP/IP traffic packets. *Sovremennaya nauka: Aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki = Modern Science: actual problems of theory and practice. Series "Natural & Technical Sciences"*. 2020;6:110–115. (In Russ.).
8. Goryun K.N., Klyuev S.G. Features of information security audit and monitoring in distributed information systems. *Sovremennaya nauka: Aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki = Modern Science: actual problems of theory and practice. Series "Natural & Technical Sciences"*. 2020;7:58–61. (In Russ.).
9. Threat Data Bank – typical vulnerabilities of Web applications. FSTEK: 2023. URL: https://bdu.fstec.ru/webvulns [accessed on 20.06.2023]. (In Russ.).
10. Methodology for assessing information security threats. FSTEC: 2021. URL: http://www.garant.ru/products/ipo/prime/doc/400325044 [accessed on 20.06.2023]. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Богданов Дмитрий Сергеевич, ведущий инженер отдела интегрированного и концептуального проектирования, ООО «НК «Роснефть» - НТЦ, Краснодар, Российская Федерация.
e-mail: ds_bogdanov@ntc.rosneft.ru
ORCID: 0000-0002-6523-7725

Dmitriy Sergeevich Bogdanov, Chief Engineer at the Integrated and Conceptual Design Department, OOO NK Rosneft - STC, Krasnodar, the Russian Federation.

Статья поступила в редакцию 14.07.2023; одобрена после рецензирования 11.08.2023; принята к публикации 07.09.2023.

The article was submitted 14.07.2023; approved after reviewing 11.08.2023; accepted for publication 07.09.2023.