Научная статья
УДК 004.056
ББК 16.8
О-93
DOI: 10.53598/2410-3225-2024-1-336-36-42

Оценка функционирования SIEM-систем на основе комплекса критериев эффективности

(*Рецензирована*)

Михаил Михайлович Путято[1], Александр Самвелович Макарян[2], Александр Николаевич Черкасов[3], Виктор Алексеевич Кучер[4]

[1–4] *Кубанский государственный технологический университет, Краснодар, Россия*
[1] *putyato.m@gmail.com*
[2] *msanya@yandex.ru*
[3] *cherk@mail.ru*
[4] *vakucher@bk.ru*

Аннотация. *Оценка функционирования систем информационной безопасности всегда представлялась достаточно сложным процессом, который требует тщательной проработки. В результате этого процесса можно получить важные данные и рекомендации по улучшению системы защиты информации и уменьшению рисков. В данной статье рассматривается критериальная система оценки систем мониторинга инцидентов информационной безопасности. На основе показателей был произведен сравнительный анализ SIEM-систем отечественного производства. Кроме того, показана эффективность внедрения системы информационной безопасности на основе сформированных показателей. Результаты данного исследования могут быть применены для повышения уровня защищенности информационных систем организаций и эффективного управления угрозами информационной безопасности.*

Ключевые слова: *система управления информационной безопасностью и событиями, система критериев, оценка эффективности*

Для цитирования: *Оценка функционирования SIEM-систем на основе комплекса критериев эффективности / М. М. Путято, А. С. Макарян, А. Н. Черкасов, В. А. Кучер // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2024. Вып. 1 (336). С. 36–42. DOI: 10.53598/2410-3225-2024-1-336-36-42*

Original Research Paper

Estimation of SIEM-systems functioning on the basis of set of effectiveness criteria

Mikhail M. Putyato[1], Aleksandr S. Makaryan[2], Aleksandr N. Cherkasov[3], Viktor A. Kucher[4]

[1–4] *Kuban State Technological University, Krasnodar, Russia*
[1] *putyato.m@gmail.com*
[2] *msanya@yandex.ru*
[3] *cherk@mail.ru*
[4] *vakucher@bk.ru*

Abstract. *Estimation of functioning of information security systems has always been a rather complex process that requires careful study. This process can provide important data and recommendations for improving information security and reducing risks. This article discusses a criteria-based system for assessment information security incident monitoring systems. Based on the indicators, a comparative analysis of domestic production SIEM systems is carried out. In addition, the effectiveness of implementing an information security system based on the generated indicators is shown. The results of this study can be used to increase the level of security of organizations' information systems*

and effective management of information security threats.

Keywords: *information security and event management system, criteria system, efficiency estimation*

For citation: *Estimation of functioning of SIEM systems based on a developed set of effectiveness criteria / M. M. Putyato, A. S. Makaryan, A. N. Cherkasov, V. A. Kucher // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2024. Iss. 1 (336). P. 36–42. DOI: 10.53598/2410-3225-2024-1-336-36-42*

Введение. Рост сектора информационных технологий и телекоммуникаций стимулирует развитие рынка систем обеспечения информационной безопасности (ИБ). Средства SIEM (система управления информационной безопасностью и событиями безопасности) помогают специалистам по информационной безопасности оперативно выявлять и реагировать на возникающие в организациях инциденты. Организации используют эти средства для централизованного сбора данных, контроля, мониторинга, обнаружения и реагирования на инциденты в сфере безопасности инфраструктуры [1].

Одним из основных преимуществ систем SIEM является централизованный сбор данных. Благодаря этому специалисты по информационной безопасности могут не тратить время на обход всех помещений организации для отслеживания состояния рабочих мест – все необходимые данные система собирает и передает автоматически, что значительно ускоряет процесс выявления и реагирования на инциденты [2].

В настоящее время, после ухода иностранных вендеров (производителей программного обеспечения), разрешено использование отечественных SIEM-систем, внесенных в реестр отечественного программного обеспечения. Поэтому одним из главных факторов выбора системы мониторинга событий и инцидентов безопасности становится стоимость. Также немаловажное значение имеют факторы, которые бы влияли на результативность, масштабируемость, интеграцию с другими системами и т. д.

На современном этапе различают следующие типы взаимодействия между SIEM и оборудованием организации:

1. Схема на основе агентов. Взаимодействие между SIEM и устройствами на основе агентов заключается в установке агента SIEM на все рабочие станции и серверы.

2. Прямая отправка событий по подписке. Основная цель состоит в позиционировании службы сбора событий на устройствах, которые в автоматическом режиме отправляют события в SIEM.

3. Метод с выделением хоста. Комбинированный метод предполагает выделение или добавление хоста в организации, который функционирует как промежуточный буфер между устройством и SIEM [1].

На рисунке 1 приведены все 3 схемы функционирования SIEM с оборудованием в организации.

Кроме того, стоит отметить, в настоящий момент при внедрении SIEM-систем рассматриваются две модели внедрения:

– CAPEX – внедрение системы управления информационной безопасностью SIEM локально, обеспечивая самостоятельный контроль над процессами ИБ;

– OPEX – внедрение системы управления информационной безопасностью SIEM на основе сторонних ресурсов, обеспечивая аутсорсинг контроля над процессами ИБ [1].

На рисунке 2 приведены схемы, отражающие вложения в систему управления информационной безопасностью на основе SIEM (1 – CAPEX, 2 – OPEX).

С целью анализа рынка систем мониторинга анализа инцидентов на основе следующих источников [3–5] сформирована развернутая система критериальной оценки для полномасштабного сравнения существующих SIEM-систем, приведенная в таблице 1.

Этот набор стандартов обеспечивает наибольший охват продуктов, позволяя объективно анализировать SIEM-системы и выбирать наиболее подходящую систему для конкретной организации.

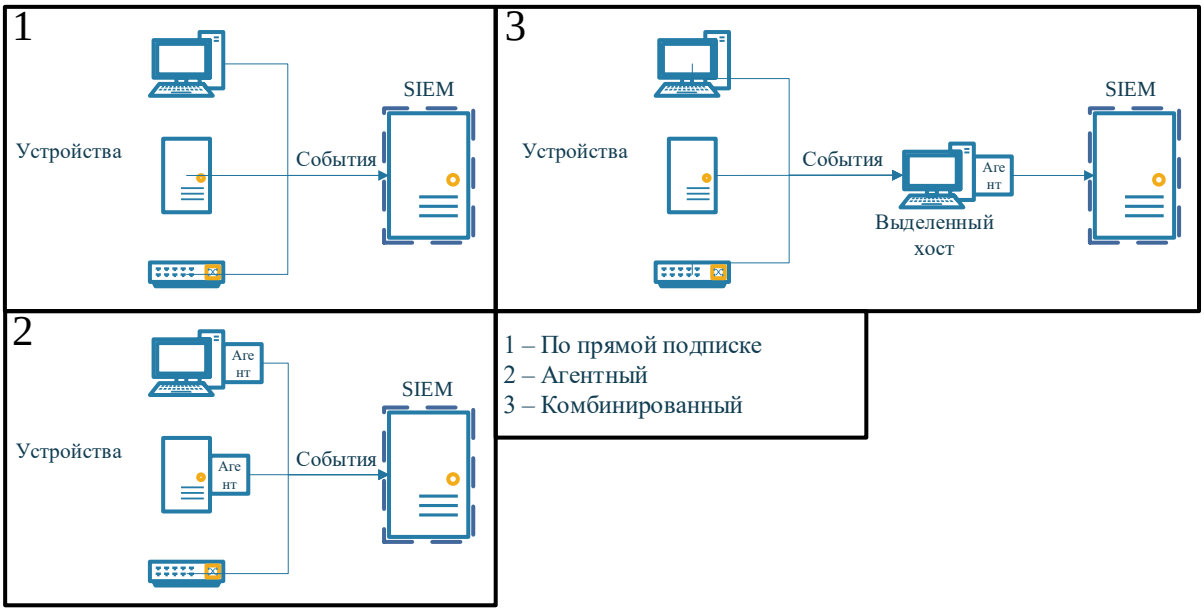

Рис. 1. Схемы взаимодействия SIEM с оборудованием
(1 – прямая подписка, 2 – агентный метод, 3 – метод выделения хоста)

Fig. 1. Schemes of SIEM interaction with equipment
(1 – direct subscription, 2 – agent method, 3 – host allocation method)

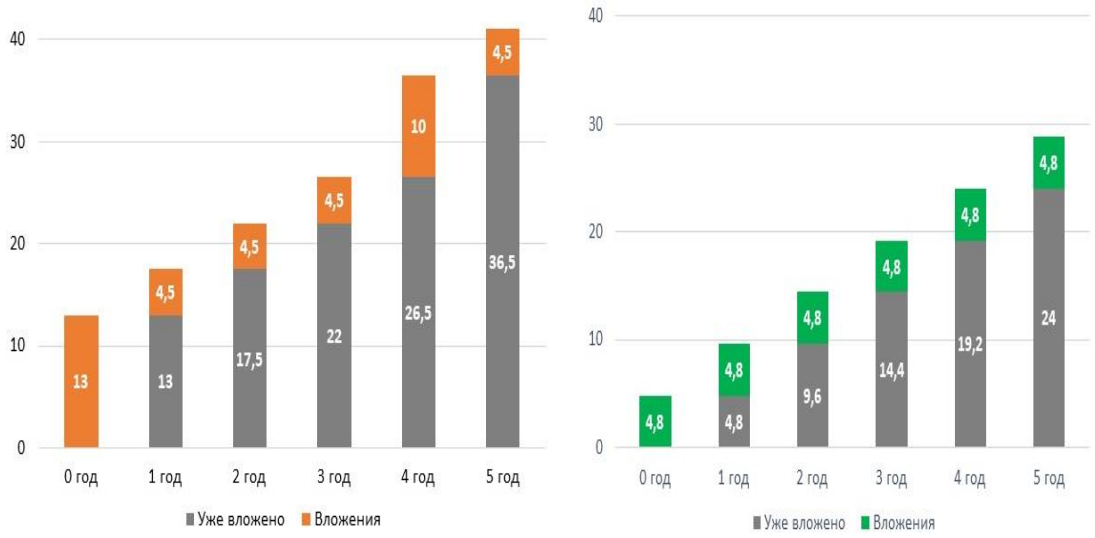

Рис. 2. Модели внедрения SIEM-систем в организации

Fig. 2. Models for implementing SIEM systems in an organization

Таблица 1

Критериальная система оценки SIEM-систем [1]

Table 1. Criteria-based evaluation system for SIEM systems [1]

№ п/п	Наименование критерия	Описание
I. *Архитектура системы*		
1	Ядро решения на базе операционной системы	Тип используемой операционной системы
2	Система управления базами данных	Тип используемой СУБД
3	Возможность виртуализации на платформе	Тип возможной виртуализации
4	Распределенное развертывание компонентов	Возможность создания распределенного развертывания компонентов системы

Таблицы 1 (Продолжение)

№ п/п	Наименование критерия	Описание
5	Возможность использования NAS/SAN	Типы хранилищ
6	Ограничение потребления канала при передаче событий от сборщиков до центра системы (для распределенных систем)	Настройка частоты опроса, количества событий, утилизации полосы и времени передачи данных
7	Средняя степень сжатия при передаче сырых событий	Коэффициент сжатия событий
8	Средняя степень сжатия при хранении нормализованных событий	Коэффициент сжатия событий
9	Ограничения по количеству обрабатываемых событий в секунду	Ограничение обрабатываемых событий в системе
10	Минимальное количество серверов для разворачивания системы	Количество физических серверов для развертывания
11	Консоль администратора	Тип консоли администратора
II. *Резервирование и отказоустойчивость*		
1	Схема резервирования ядра системы	Возможности по резервированию ядра системы
2	Резервирование конфигурации системы, возможность автоматического восстановления	Тип резервного копирования
3	Возможности по резервированию компонентов сбора событий	Количество компонентов резервирования
III. *Защищенность системы*		
1	Журналирование изменений	Изменения объектов – инициированных пользователями или системными компонентами
2	Протоколы передачи данных между компонентами системы	Тип протокола передачи данных
IV. *Подключение источников событий*		
1	Количество поддерживаемых источников событий	Количество
2	Возможность подключения нестандартных источников	Виды и количество подключения нестандартных источников
V. *Лицензирование*		
1	Метрики лицензирования	Модульность, минимальная поставка, возможности расширения
2	Варианты поставки	Тип варианта поставки
VI. *Предустановленный функционал*		
1	Наличие предустановленных правил корреляции	Количество правил корреляции
2	Наличие предустановленных графических панелей	Количество граф. панелей
3	Наличие предустановленных отчетов	Количество отчетов
VII. *Управление активами, инцидентами, уязвимостями*		
1	Поля в карточке инцидента	Количество полей
2	Пути эскалации инцидента	Тип управления инцидентом
3	Оповещение об инциденте	Тип оповещения об инциденте
4	Возможность выделения ложных срабатываний	Тип определения ложных срабатываний
5	Принятие решений в рамках процесса обработки инцидентов	Тип принятия решений
VIII. *Визуализация и аналитика*		
1	Работа с фильтрами	Типы фильтров
2	Формирование и рассылка отчетов по расписанию/по критерию	Возможность формирования и рассылки отчета
3	Возможность формирования отчетов в виде документов	Форматы экспорта отчетов в виде документов
IX. *Управление событиями и данными*		
1	Метод сбора событий с источников	Агентный или безагентный
2	Поддерживаемые форматы сбора событий	Типы формата событий
3	Корреляция по историческим данным	Наличие
X. *Возможности интеграции и обогащения из других систем*		
1	Встроенная или подключаемая поведенческая аналитика	Тип UBA&UEBA
2	Интеграция со службами каталогов	Тип интеграции
3	Наличие и вид API	Наличие и вид API

На базе представленной критериальной системы проведена оценка следующих систем мониторинга инцидентов: MaxPatrol SIEM – от компании Positive Technologies, СерчИнформ SIEM – фирмы SearchInform, Kaspersky UMA – от компании Kaspersky. В результате сравнения наиболее эффективная система была определена как Kaspersky UMA для внедрения по модели OPEX.

Сравнительный анализ и оценка эффективности представляют собой ключевые аспекты управления деятельностью любой организации. Эти процессы позволяют измерить влияние управленческих решений на результаты деятельности, выявить тенденции в этих результатах и разработать соответствующие меры по их улучшению. Для оценки эффективности внедрения системы мониторинга инцидентов в организации определены количественные и качественные показатели внедрения [6] SIEM-системы [7], представленной на рисунке 3.

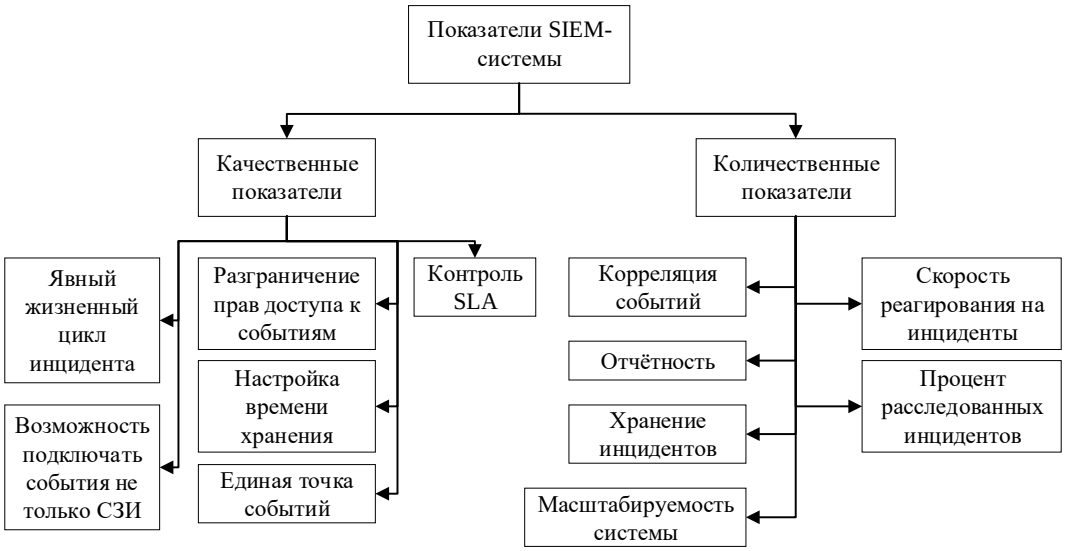

Рис. 3. Показатели внедрения SIEM-системы

Fig. 3. Indicators of the implementation of the SIEM system

Для анализа технической эффективности внедренной системы будем использовать следующие количественные показатели: корреляция событий; скорость реагирования на инциденты; хранение инцидентов; процент расследованных инцидентов; отчетность; масштабируемость системы [8].

В таблице 2 представлены данные, взятые из внутреннего отчета организации по согласованию с начальником отдела ИБ.

Таблица 2

Показатели эффективности до внедрения SIEM-системы

Table 2. Effectiveness indicators before the implementation of the SIEM system

Критерий	Корреляция событий	Скорость реагирования на инциденты	Хранение инцидентов	Процент расследованных инцидентов	Отчетность	Масштабируемость системы
Значение	0,15	0,2	0,31	0,13	0,22	0,4

После внедрения SIEM-системы были проведены повторный аудит и пентест организации. Данные представлены в таблице 3.

Таблица 3

Показатели эффективности после внедрения SIEM-системы

Table 3. Effectiveness indicators after the implementation of the SIEM system

Критерий	Корреляция событий	Скорость реагирования на инциденты	Хранение инцидентов	Процент расследованных инцидентов	Отчетность	Масштабируемость системы
Значение	0,9	1	0,98	0,94	0,88	0,5

Как видно на диаграмме, внедренная система значительно улучшила все показатели технической эффективности. Таким образом, внедренная система SIEM является более эффективным инструментом для управления событиями ИБ в организации клиента, чем ручная обработка событий, представленная на рисунке 4 [1].

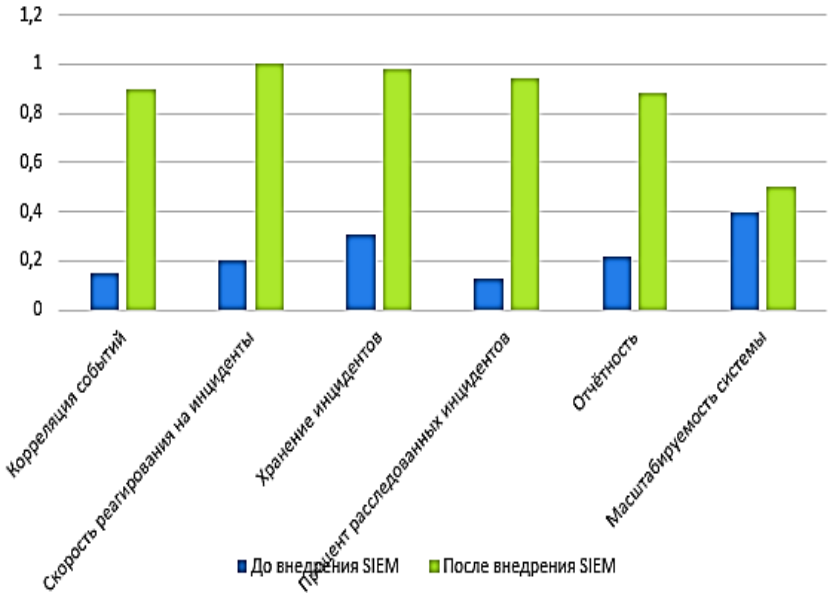

Рис. 4. Технические показатели эффективности

Fig. 4. Technical efficiency indicators

Управление инцидентами, которое обеспечивается системой SIEM, эффективно сокращает затраты на реагирование на инциденты информационной безопасности и играет важную роль в смягчении последствий утечек информации. Это позволит сократить финансовые затраты, связанные со штрафами за приостановку деятельности и несоблюдение нормативных требований.

Заключение. Таким образом, в данной работе:

1. Определены типы взаимодействия между SIEM-системами и оборудованием организации, представленные в виде схемы. Исследованы модели внедрения системы управления инцидентами информационной безопасности.

2. На основе литературных источников сформирована развернутая система критериальной оценки для полномасштабного сравнения существующих SIEM-систем. Проведена оценка современных российских SIEM-систем, внесенных в реестр отечественного программного обеспечения.

3. Проведена оценка эффективности внедрения Kaspersky UMA на основе сформированных показателей, отражающей перспективность использования систем мониторинга инцидентов информационной безопасности в отличие от ручной обработки событий.

Примечания

1. Шинджикашвили А. С. Мониторинг инцидентов информационной безопасности организации на основе SIEM-системы : дипломная работа по специальности 10.05.01 «Компьютерная безопасность» / Кубанский государственный технологический университет. Краснодар, 2023. 82 с.

2. Методический документ. Методика оценки угроз безопасности информации : утв. ФСТЭК России 05.02.2021. URL: https://www.consultant.ru/document/cons_doc_LAW_378330, свободный.

3. Хлестова Д. Р., Попов К. Г. Анализ актуальности использования SIEM-систем на предприятиях // Символ науки. 2016. № 7-1. С. 89–91.

4. Gustavo Gonzalez Granadillo, Susana González Zarzosa. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures // Cybersecurity Unit,

Atos Research & Innovation. 2021.Vol. 21, Iss. 14. DOI: 10.3390/s21144759

5. Быков Андрей Андреевич. Siem-система – универсальный инструмент службы информационной безопасности // Современные инновации. 2017. № 6. С. 46–48.

6. Черкасов А. Н. Разработка математического и алгоритмического обеспечения адаптивных систем поддержки принятия решений в ситуационных центрах : специальность 05.13.01 «Системный анализ, управление и обработка информации (по отраслям)» : автореферат диссертации на соискание ученой степени кандидата технических наук. Краснодар, 2011. 23 с.

7. Стукалин А. А., Назарова О. Б. Системы мониторинга информационных инцидентов (SIEM-системы): обзор и сравнительный анализ // Управленческие механизмы противодействия идеологии экстремизма и терроризма : материалы научно-практической конференции, Магнитогорск, 20–21 декабря 2018 года / под общ. ред. Н. Р. Балынской. Магнитогорск : Магнитогорский государственный технический университет им. Г. И. Носова, 2018. С. 116–121.

8. Белоусова И. Д. Анализ и обоснование выбора методов и средств разработки системы мониторинга и управления сетевыми инцидентами // Актуальные проблемы современной науки, техники и образования : тезисы докладов 77-й Международной научно-технической конференции, Магнитогорск, 22–26 апреля 2019 года. Том 1. Магнитогорск : Магнитогорский государственный технический университет им. Г. И. Носова, 2019. С. 431.

References

1. Shindzhikashvili A. S. Monitoring of information security incidents of an organization based on a SIEM system : thesis on specialty 05/10/2011 “Computer security” / Kuban State Technological University. Krasnodar, 2023. 82 p.

2. Methodological document. Methodology for assessing threats to information security : approved by FSTEC of Russia on 02/05/2021. URL:
https://www.consultant.ru/document/cons_doc_LAW_378330, free.

3. Khlestova D. R., Popov K. G. Analysis of the relevance of using siem systems in enterprises // Symbol of Science. 2016. No. 7-1. P. 89–91.

4. Gustavo Gonzalez Granadillo, Susana González Zarzosa. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures // Cybersecurity Unit, Atos Research & Innovation. 2021.Vol. 21, Iss. 14. DOI: 10.3390/s21144759

5. Bykov Andrey Andreevich. Siem system – a universal tool for information security services // Modern Innovations. 2017. No. 6. P. 46–48.

6. Cherkasov A. N. Development of mathematical and algorithmic support for adaptive decision support systems in situational centers : specialty 05.13.01 “System analysis, management and information processing (by industry)” : abstract of the dissertation for the degree of candidate of technical sciences. Krasnodar, 2011. 23 p.

7. Stukalin A. A., Nazarova O. B. Information incident monitoring systems (SIEM systems): review and comparative analysis // Management mechanisms for countering the ideology of extremism and terrorism : materials of a scientific and practical conference, Magnitogorsk, December 20–21, 2018 / edited by N. R. Balynskaya. Magnitogorsk : Magnitogorsk State Technical University named after G. I. Nosova, 2018. P. 116–121.

8. Belousova I. D. Analysis and justification for the choice of methods and means for developing a system for monitoring and managing network incidents // Current problems of modern science, technology and education : abstracts of the 77th International scientific and technical conference, Magnitogorsk, April 22–26, 2019. Vol. 1. Magnitogorsk : Magnitogorsk State Technical University named after G. I. Nosov, 2019. P. 431.

Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 05.02.2024; *одобрена после рецензирования 25.02.2024*; *принята к публикации 26.02.2024.*

The authors declare no conflicts of interests.

The article was submitted 05.02.2024; *approved after reviewing 25.02.2024*; *accepted for publication 26.02.2024.*