Научная статья
DOI 10.66424/2071-8217-2026-2-5
УДК 004.056

ПСИХОЛОГИЧЕСКИЕ ПОСЛЕДСТВИЯ РАБОТЫ С СИСТЕМАМИ SECURITY OPERATIONS CENTER (SOC): ВЫГОРАНИЕ, КОГНИТИВНАЯ НАГРУЗКА И РОЛЬ ИИ-АССИСТЕНТОВ

Е. В. Ларионова[1], И. Л. Бунас[1], А. Ю. Гарькушев[1], А. Ф. Супрун[2*]

[1]Санкт-Петербургский государственный морской технический университет, Санкт-Петербург, Россия
[2]Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия
✉ *afs54@inbox.ru*

ДЛЯ ЦИТИРОВАНИЯ

Ларионова Е. В., Бунас И. Л., Гарькушев А. Ю., Супрун А. Ф. Психологические последствия работы с системами Security Operations Center (SOC): выгорание, когнитивная нагрузка и роль ИИ-ассистентов // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 60–69.
DOI: 10.66424/2071-8217-2026-2-5

ПОСТУПИЛА 28.01.2026
ПРИНЯТА 08.05.2026
ОПУБЛИКОВАНА 15.06.2026

АННОТАЦИЯ

Рассматриваются психологические последствия работы аналитиков в Security Operations Center (SOC): хронический стресс, профессиональное выгорание и связанные с ними ошибки в обеспечении кибербезопасности. Показано, что выгорание следует рассматривать как операционный риск, влияющий на вероятность инцидентов и снижающий эффективность решений. Анализируются современные ИИ-решения для SOC (LLM-ассистенты, агентные системы, поведенческие модели) и их ограничения. Рассматриваются принципы мониторинга функционального состояния оператора и структуры анализа инцидентов, механизмы ограничения влияния ИИ в целях сохранения управляемости и ответственности. Показана практическая применимость предложенного подхода, где надежность принятия решений оператором поддерживается ИИ-контуром.

КЛЮЧЕВЫЕ СЛОВА

SOC, профессиональное выгорание, усталость от оповещений, когнитивная нагрузка, кибербезопасность, ИИ-ассистенты, человеческий фактор

Original article
DOI 10.66424/2071-8217-2026-2-5

PSYCHOLOGICAL EFFECTS OF WORK IN SECURITY OPERATIONS CENTER (SOC) SYSTEMS: BURNOUT, COGNITIVE LOAD, AND THE ROLE OF AI-ASSISTANTS

E. V. Larionova[1], I. L. Bunas[1], A. Yu. Garkushev[1], A. F. Suprun[2*]

[1]Saint-Petersburg State Marine Technical University, St. Petersburg, Russia
[2]Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia
✉ *afs54@inbox.ru*

FOR CITATION

Larionova E. V., Bunas I. L., Garkushev A. Yu., Suprun A. F. Psychological effects of work in Security Operations Center (SOC) systems: burnout, cognitive load, and the role of AI-assistants. *Problems of information security. Computer systems*. 2026. No. 2, pp. 60–69. DOI: 10.66424/2071-8217-2026-2-5 (In Russian)

RECEIVED 28.01.2026
ACCEPTED 08.05.2026
PUBLICATION 15.06.2026

ABSTRACT

The article examines the psychological consequences of analysts' work in a Security Operations Center (SOC), including chronic stress, professional burnout, and related cybersecurity errors. Burnout is considered as an operational risk that increases the likelihood of incidents and reduces decision effectiveness. Modern AI solutions for SOCs (LLM assistants, agent-based systems, and behavioral models) and their limitations are analyzed. The paper discusses monitoring of the operator's functional state, the structure of incident analysis, and mechanisms for limiting AI influence in order to preserve manageability and responsibility. The practical applicability of the proposed approach is demonstrated, where the reliability of operator decision-making is supported by an AI-assisted loop.

KEYWORDS

SOC, professional burnout, alert fatigue, cognitive load, cybersecurity, AI-assistants, human factors

1. ВВЕДЕНИЕ

Современный SOC (центр управления безопасностью) функционирует в условиях постоянной перегрузки: рост поверхности атак, гибридная инфраструктура, дефицит кадров и десятки тысяч оповещений в сутки. Для оператора центра безопасности это означает практически непрерывный режим многозадачности, дефицит времени на глубокий анализ и постоянное давление высокой цены ошибки.

По данным отраслевых опросов 83 % специалистов по информационной безопасности связывают ошибки, приведшие к инцидентам, со стрессом и профессиональным выгоранием. Аналогичные выводы содержатся и в обзорах по кибербезопасности в целом: значимая доля утечек и инцидентов обусловлена не только техническими отказами, но и влиянием человеческого фактора на фоне хронической усталости, напрямую отражающейся на качестве принимаемых решений [1–3].

На рынке параллельно присутствуют ИИ-ассистенты для SOC: от крупных решений уровня Microsoft Security Copilot и Google Sec-PaLM до агентных систем, автоматически собирающих контекст и формирующих черновики расследований. Публикуемые бенчмарки показывают рост скорости и полноты анализа инцидентов [4], однако в открытых описаниях таких решений основной акцент делается на ускорении triage, сокращении MTTR и автоматизации типовых операций. Вопрос, как подобные инструменты влияют на устойчивость принятия решений оператором в условиях неполных данных, пиковых нагрузок и длительного стресса, остается открытым.

В российских разработках также используются ML-модули поведенческого анализа для выявления аномалий и атак, а также интеграция результатов с механизмами SIEM. В описаниях таких решений заявляется снижение объема рутинных операций и нагрузки на аналитиков [5], однако влияние подобных подходов на надежность решений человека в контуре управления, как правило, не рассматривается системно. Роль человеческого фактора и когнитивных ограничений оператора в системах информационной безопасности рассматривается и в ряде отечественных работ [6–11]. Тем не менее вопрос о проектировании ИИ-ассистента как средства стабилизации процесса анализа, а не только ускорения обработки, практически не рассматривается.

В рамках данной работы предложено понятие «функциональное состояние оператора», под которым понимаются не клинические или эмоциональные характеристики, а наблюдаемые признаки дестабилизации процесса анализа в человеко-машинном контуре. К ним относятся: зацикливание рассуждения, потеря

связности, смешение контекстов задач, рост повторных перепроверок и снижение устойчивости движения к цели расследования.

Цель исследования – очертить психологические и операционные механизмы стресса в SOC, обозначить ограничения существующих ИИ-подходов и предложить концептуальный контур ИИ-ассистента, ориентированного на поддержание когнитивной стабильности операторов в условиях стрессовой и критической нагрузки, а не только на метрики MTTR и объем обработанных инцидентов.

Дополнительно обозначаются классы признаков, по которым может фиксироваться дестабилизация анализа, и базовые направления дальнейшей оценки эффективности подобных систем.

2. СНИЖЕНИЯ СТАБИЛЬНОСТИ РЕШЕНИЙ В УСЛОВИЯХ ХРОНИЧЕСКОЙ КОГНИТИВНОЙ НАГРУЗКИ

Факторы нагрузки. Рабочая среда SOC комбинирует несколько типов давления (рис. 1). Кратко рассмотрим их.

Постоянная мультизадачность. Оператор одновременно ведет несколько рас-

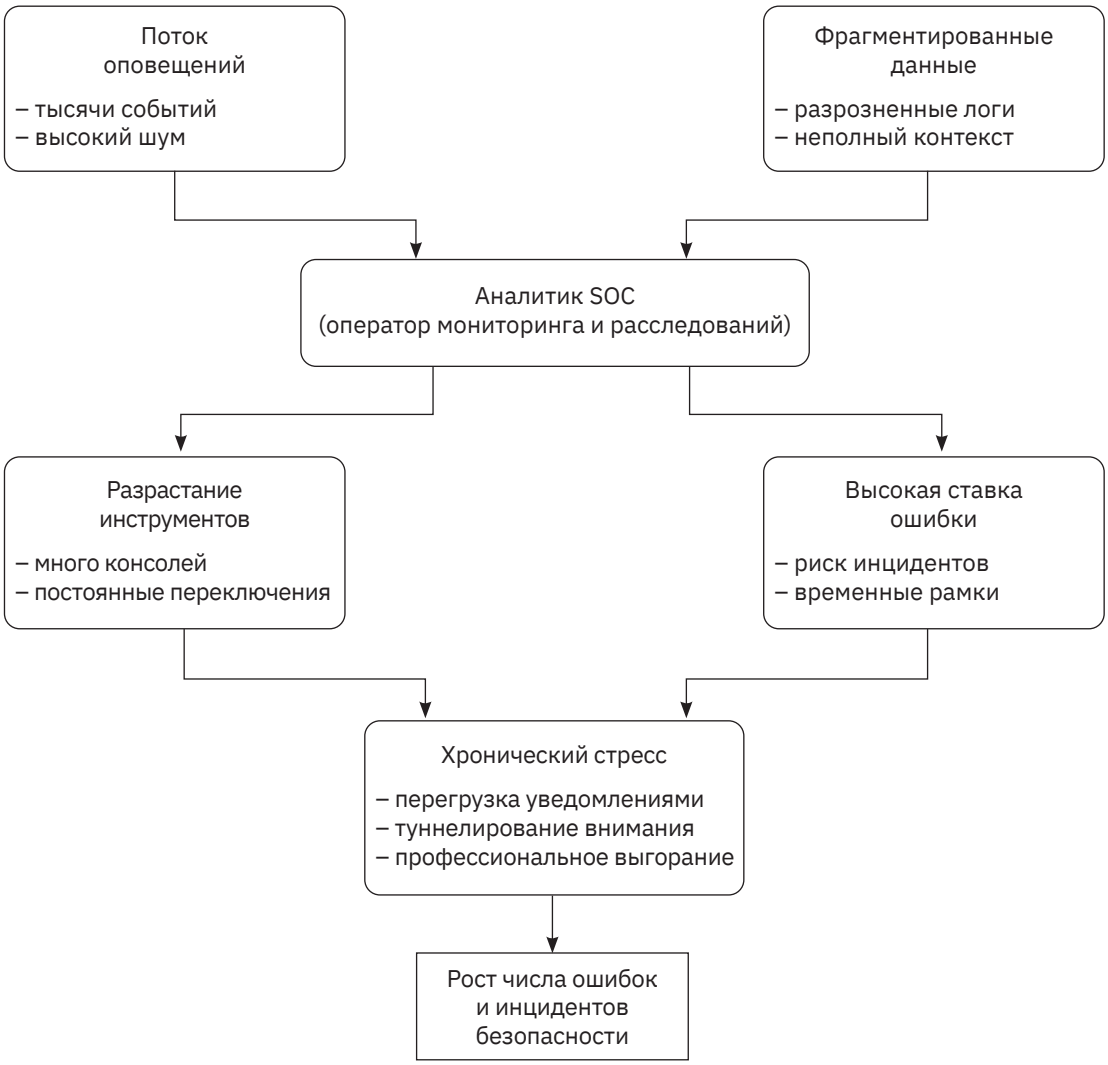

Рис. 1 | Основные источники когнитивной нагрузки в SOC

Fig. 1 | The main sources of cognitive load in SOC

следований, отслеживает очередь оповещений и дежурные каналы связи, а также вынужден регулярно переключаться между задачами. Каждое такое переключение требует концентрации внимания, расходует ресурсы рабочей памяти и снижает качество принимаемых решений.

Фрагментированные данные. Инцидент собирается из разрозненных источников отчетов, событий, внешних источников сведений об угрозах, записей обращений. Необходимость держать в голове несогласованные фрагменты усиливает нагрузку и делает анализ угрозы более уязвимым к шаблонному реагированию и риску пропустить значимые данные.

Высокая цена ошибки. Ошибочная классификация оповещения может привести к утечке, простоям и репутационным потерям, что формирует устойчивый стрессовый фон.

«Разрастание инструментов». Постоянное переключение между многочисленными консолями SIEM, EDR (обнаружение и реагирование на конечных устройствах), TI-порталами (централизованная точка доступа к сведениям о киберугрозах) и системами учета приводит к феномену контекстной усталости, требованию постоянных перепроверок и увеличению механических ошибок.

Усталость от оповещений и профессиональное выгорание. Усталость от оповещений описывается как состояние десенситизации: при тысячах оповещений в день, значительная часть которых может оказывается ложной тревогой, оператор перестает своевременно реагировать даже на действительно важные сигналы [3–5, 12]. На практике это обычно выражается в увеличении времени реакции на критические события, росте числа пропущенных инцидентов, субъективном ощущении нехватки времени у оператора.

Хроническая перегрузка приводит к профессиональному выгоранию: эмоциональному истощению, деперсонализации и снижению чувства профессиональной компетентности. Это повышает риск ошибок, усиливает текучесть кадров и разрушает накопленную экспертизу команды [1, 2, 13, 14].

Таким образом, функциональное и психологическое состояние аналитиков прямо влияет на качество принимаемых решений и устойчивость SOC как системы и рекомендуется рассматривать как отдельный класс операционных рисков.

В этом контексте задача ИИ-ассистента состоит не в диагностике психологического состояния оператора, а в выявлении признаков дестабилизации процесса анализа и поддержании надежности решений в человеко-машинном контуре.

3. СОВРЕМЕННЫЕ ИИ-РЕШЕНИЯ ДЛЯ SOC: ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

Если абстрагироваться от маркетинговых формулировок, ИИ-решения для SOC можно условно разделить на три группы [4, 15]:

1. LLM-ассистенты. Генеративные модели, встроенные в экосистемы SIEM и SOAR (оркестрация и автоматизация реагирования): резюмируют инциденты, помогают формировать запросы, предлагают шаги реагирования.

2. Агентные системы. Автоматически собирают контекст, запускают типовые проверки, формируют черновой таймлайн инцидента и рекомендации по реагированию.

3. Модули поведенческого анализа и приоритизации. Используют ML/Big Data для выявления аномалий и оценки риска активов, снижая шум и перераспределяя внимание аналитиков на более критичные события.

Эти системы хорошо решают задачи снятия рутины, ускорения триажа и улучшения документирования инцидентов. При этом в открытых описаниях практически не освещаются несколько критически важных аспектов [4, 6]:

1. Отсутствие работы с состоянием анализа. Метрики фокусируются на MTTR и количестве обработанных кейсов. При этом влияние ИИ на выгорание и когнитивную нагрузку не измеряется систематически. Более корректной постановкой

задачи представляется не прямая «диагностика состояния оператора», а фиксация признаков дестабилизации процесса анализа в человеко-машинном контуре. К таким признакам могут относиться зацикливание рассуждения, потеря связности, смешение контекстов задач и рост повторных перепроверок без прироста результата.

2. Смещение автоматизации и деквалификация. Чем «умнее» ведет себя ассистент, тем выше риск, что уставшие аналитики будут следовать его рекомендациям без критической проверки. Одновременно сокращается поле для практики глубокого анализа, что ведет к постепенному обеднению навыков. В этом смысле ИИ может ускорять обработку инцидентов без повышения надежности решений, особенно в условиях неполных и противоречивых данных.

3. Техностресс и смещение ответственности. Формально человек остается в контуре принятия решений, фактически же значительная часть логики расследования переходит к ИИ, тогда как ответственность за ошибки сохраняется за оператором. Это усиливает стресс и чувство неконтролируемости системы. В результате критичной становится не только скорость реакции, но и сохранение управляемости контура принятия решений: ИИ-ассистент должен не подменять решение оператора, а поддерживать структуру анализа, не навязывая конкретного действия при неполноте данных.

Отдельной проблемой является различение высокой сложности самого инцидента и признаков дестабилизации анализа. Сложный инцидент сам по себе может порождать длительные циклы проверки, рост числа гипотез и возвраты к ранее просмотренным данным. Поэтому корректная архитектура ассистента должна учитывать не единичные признаки, а их устойчивые сочетания и контекст задачи, не сводя любой рост сложности к «перегрузке оператора».

Также необходимо учитывать организационные и этические рамки использования таких систем, включая разграничение режима помощи оператору и уровень управленческого мониторинга. Наличие у системы доступа к признакам дестабилизации анализа не должно автоматически означать возможность их использования в целях контроля производительности без отдельного регламентирования и разграничения прав доступа.

Таким образом, ИИ, будучи мощным усилителем аналитических возможностей SOC, остается ограниченным инструментом поддержки людей, если не дополняется контуром, ориентированным на надежность процесса анализа и допустимые границы влияния на решения оператора. Важно отметить, что ИИ-ассистенты, оптимизируя темп реагирования и предлагая готовые решения, могут снижать надежность принятия решений оператором за счет сглаживания неопределенности и ослабления критической проверки.

4. КОНЦЕПЦИЯ ИИ-АССИСТЕНТА, ОРИЕНТИРОВАННОГО НА ПОДДЕРЖКУ СТАБИЛЬНОСТИ РЕШЕНИЙ

Основные принципы. Предлагаемый подход исходит из трех базовых принципов:

1. Фокус на функциональных признаках дестабилизации анализа, а не на эмоциях. Искусственный интеллект не оценивает эмоции аналитика и не решает задачу психологической диагностики. Его задача заключается в фиксации наблюдаемых признаков дестабилизации процесса анализа в человеко-машинном контуре: зацикливания рассуждения, потери связности, смешения контекстов разных задач, роста повторных перепроверок без прироста результата и дрейфа относительно цели расследования. При этом такие признаки не должны интерпретироваться изолированно от характеристик самого инцидента.

2. Стабилизация процесса анализа, а не только ускорение принятия решений. Ассистент контролирует структуру рассуждения, согласованность анализа с целью и распределение внимания между смыс-

ловыми ветками. При необходимости он не навязывает готовое решение, а переводит взаимодействие в более консервативный режим поддержки: замедляет темп, дробит задачу на последовательные шаги, фиксирует контекст, выделяет зону неопределенности и помогает различать обратимые и необратимые действия на ранних стадиях расследования.

3. Этическое ограничение влияния. Использование данных о процессе анализа должно быть ограничено явно заданными правилами допустимого воздействия. Ассистент может предлагать паузу, изменение формата работы, пересборку плана или уточнение контекста, но не должен скрыто подталкивать оператора к конкретному решению. Под этическим контуром в работе понимается не свод моральных предписаний, а слой функциональных ограничений, разграничивающий режимы помощи оператору, порядок использования данных о признаках дестабилизации анализа и границы перехода от поддержки к управленческому контролю.

Концептуальная архитектура ИИ-ассистента. На концептуальном уровне ИИ-ассистент [16] строится поверх классического LLM-ядра и интеграции с SOC-инфраструктурой, включая источники событий, в том числе данные из CMDB (базы данных управления конфигурациями) и UEBA (анализа поведения пользователей и сущностей) (рис. 2). При этом архитектура включает не только технический контур обработки инцидента, но и когнитивно-аналитический слой поддержки надежности решений оператора.

В предлагаемой постановке учитываются два взаимосвязанных, но не тождественных контура:

• контур инцидента, отражающий сложность самой задачи: объем входящих данных, число затронутых активов, противоречивость признаков, количество допустимых гипотез и цену ошибки;

• контур дестабилизации анализа, отражающий особенности протекания процесса рассуждения в человеко-машинном взаимодействии: рост повторных проверок, потерю связности, смешение контекстов, циклические возвраты к уже просмотренным данным и дрейф относительно цели расследования.

Высокая сложность инцидента сама по себе может приводить к росту числа гипотез, возвратов к данным и длительным циклам проверки. Поэтому ассистент не должен трактовать любой рост сложности как признак перегрузки оператора. Переход к более консервативному режиму поддержки должен определяться не единичным наблюдаемым параметром, а устойчивым сочетанием признаков, не объясняемых только сложностью самой задачи.

Когнитивно-аналитический слой в этой архитектуре включает три функциональных блока:

• слой наблюдения функционального состояния анализа: выполняет анализ текста и паттернов взаимодействия оператора с системой и выявляет признаки дестабилизации процесса анализа без постановки «диагноза» оператору;

• слой стабилизации совместного рассуждения: контролирует смысловую плотность, когерентность и связность анализа, управляет темпом и объемом выдачи, структурирует расследование на последовательные шаги и помогает сохранять контекст при росте нагрузки;

• этический контур: определяет допустимые типы вмешательства, разграничивает контур помощи оператору и контур управленческого мониторинга, предотвращает скрытое навязывание действий и ограничивает использование информации о признаках дестабилизации анализа вне согласованного домена.

Такая архитектура позволяет рассматривать ИИ в SOC не только как ускоритель процессов, но и как стабилизатор когнитивной функции оператора, уменьшая риск выгорания и связанных с ним. Вклад ИИ-ассистента в сокращение времени реагирования в данной постановке связан не только с ускорением поиска ответа, но и навигацией оператора по полю допустимых решений, включая различение обратимых, условно обратимых и необратимых действий на ранних этапах расследования. Тем самым повышается качество решений при скачкообразном росте пиковой нагрузки.

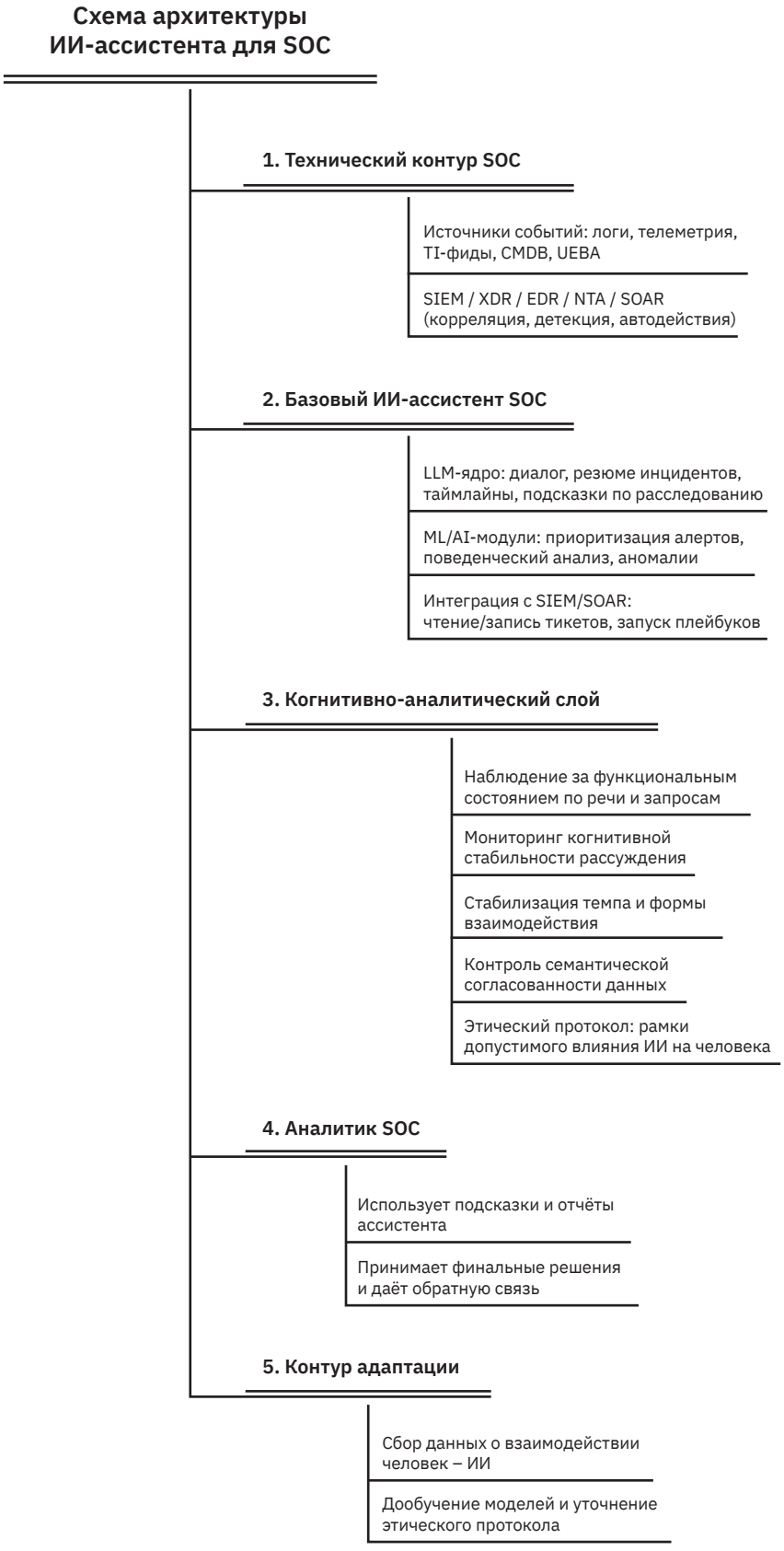

Рис. 2 | Концептуальная архитектура ИИ-ассистента для SOC

Fig. 2 | Conceptual architecture of an AI assistant for SOC

Эффективность подобного ассистента целесообразно оценивать не только по сокращению MTTR, но и по метрикам устойчивости анализа под нагрузкой. К ним могут относиться: снижение вариативности времени реакции при пиковых нагрузках; уменьшение числа пропущенных индикаторов компрометации; снижение частоты контекстных срывов и повторных перепроверок без прироста результата; сокращение доли необратимых действий, предпринятых до подтверждения рабочей гипотезы.

5. ВЫВОД

Работа в SOC характеризуется высокой когнитивной нагрузкой, утомлением от избыточных уведомлений и высоким уровнем профессионального выгорания, что напрямую влияет на частоту инцидентов и устойчивость команд. Современные ИИ-решения уже демонстрируют преимущества в скорости и полноте расследований, но в основном игнорируют психологическое состояние аналитиков, а в ряде случаев могут усиливать нагрузку за счет роста темпов работы и склонности к автоматизации.

Предложенный концептуальный контур ИИ-ассистента предполагает дополнение классического подхода функциональным слоем, ориентированным на наблюдение состояния оператора, стабилизацию совместного рассуждения и этическое ограничение влияния ИИ.

Такие системы могут рассматриваться как переход от преимущественно технологической оптимизации SOC к архитектурам, направленным на повышение надежности принятия решений ключевого элемента – человеческого мышления в условиях повышенной и нестационарной нагрузки.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. **Tines.** Voice of the SOC Analyst. 2022. URL: https://www.tines.com/reports/Tines%20Report%20-%20Voice%20of%20the%20SOC%20Analyst.pdf (дата обращения: 15.01.2026).
2. **Devo Technology.** 83 % of IT Security Professionals Say Burnout Causes Data Breaches. 2023. URL: https://www.devo.com/company/newsroom/it-security-professionals-say-burnout-causes-data-breaches (дата обращения: 15.01.2026).
3. **Карпова И. Л., Курилов А. В., Супрун А. Ф., Иванова Л. А.** Учет влияния человеческого фактора в моделях кибербезопасности // Проблемы информационной безопасности. Компьютерные системы. 2023. № 2 (54). С. 27–36.
4. **Cloud Security Alliance.** SOC Analyst Fatigue: What Our Data Says About Sustaining Investigation Speed and Quality. URL: https://cloudsecurityalliance.org/blog/2025/10/10/soc-analyst-fatigue-what-our-data-says-about-sustaining-investigation-speed-and-quality (дата обращения: 15.01.2026).
5. **ГК «Солар».** «Солар» выходит на рынок SIEM: две технологии в одном продукте и до 40 % экономии на внедрении. URL: https://rt-solar.ru/events/news/6173/ (дата обращения: 15.01.2026).
6. **Cyber Sierra.** What Is Alert Fatigue and How to Combat It in Your SOC. URL: https://cybersierra.co/blog/alert-fatigue-in-soc/ (дата обращения: 15.01.2026).
7. **Гарькушев А. Ю., Липис А. В., Карпова И. Л. и др.** Оценка компетентности интеллектуальной системы управления информационной безопасностью // Проблемы

информационной безопасности. Компьютерные системы. 2024. № 1(58). С. 18–27. DOI: 10.48612/jisp/92vv-6m6t-7tmh.

8. **Ведерников Ю. В., Гарькушев А. Ю., Липис А. В., Супрун А. Ф.** Реконфигурация модели развития системы управления информационной безопасностью: взаимодействие базовых модулей с оператором // Проблемы информационной безопасности. Компьютерные системы. 2024. № 2(59). С. 9–19. DOI: 10.48612/jisp/amv1-kdnf-zaae.
9. **Suprun A. F., Gar'kushev A. Yu., Lipis A. V. et al.** Assessment of the Competence of an Intelligent Information Security Management System // Automatic Control and Computer Sciences. 2024. Vol. 58. № 8. P. 1429–1435. DOI: 10.3103/S0146411624701220.
10. **Гарькушев А. Ю., Сазыкин А. М., Шалковская А. А.** Учет обоснованности в моделях оценки эффективности информационно-управляющих систем // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2024. № 3–4 (189–190). С. 40–44. DOI: 10.53816/23061456_2024_3-4_40.
11. **Гарькушев А. Ю., Липис А. В., Карпова И. Л., Супрун А. Ф.** Моделирование работы сотрудника службы информационной безопасности промышленного предприятия // Проблемы информационной безопасности. Компьютерные системы. 2023. № 3(56). С. 148–153. DOI: 10.48612/jisp/1vmb-73pk-5e9e.
12. **Dropzone AI.** Alert Fatigue in Cybersecurity: AI-Powered SOC Solutions Guide. URL: https://www.dropzone.ai/blog/how-to-address-cybersecurity-alert-fatigue-with-ai (дата обращения: 15.01.2026).
13. **Bria M., Spânu F., Băban A., Dumitraşcu D. L.** Maslach Burnout Inventory – General Survey: Factorial Validity and Invariance among Romanian Healthcare Professionals // Burnout Research. 2014. Vol. 1. Iss. 3. P. 103–111. DOI: 10.1016/j.burn.2014.09.001.
14. **Maslach C., Leiter M. P.** Understanding the Burnout Experience: Recent Research and Its Implications for Psychiatry // World Psychiatry. 2016. Vol. 15. № 2. P. 103–111. DOI: 10.1002/wps.20311.
15. ИИ-технологии в SIEM-системе KUMA. URL: https://www.kaspersky.ru/blog/ai-technology-in-kaspersky-siem/39252 (дата обращения: 15.01.2026).
16. **Глушко А.** Введение: современные вызовы для центров реагирования. URL: https://ptsecurity.com/research/analytics/autonomous-socs-future-of-cybersecurity-monitoring-and-incident-response/?ysclid=mp56tgtis9263489058 (дата обращения: 15.01.2026).

REFERENCES

1. **Tines.** Voice of the SOC Analyst. 2022. URL: https://www.tines.com/reports/Tines%20Report%20-%20Voice%20of%20the%20SOC%20Analyst.pdf (accessed: 15.01.2026).
2. **Devo Technology.** 83 % of IT Security Professionals Say Burnout Causes Data Breaches. 2023. URL: https://www.devo.com/company/newsroom/it-security-professionals-say-burnout-causes-data-breaches (accessed: 15.01.2026).
3. **Karpova I. L., Kurilov A. V., Suprun A. F., Ivanova L. A.** Accounting for the impact of the human factor in cyber security models. *Problems of information security. Computer systems*. 2023. No. 2 (54), pp. 27–36. (In Russian)
4. **Cloud Security Alliance.** SOC Analyst Fatigue: What Our Data Says About Sustaining Investigation Speed and Quality. URL: https://cloudsecurityalliance.org/blog/2025/10/10/soc-analyst-fatigue-what-our-data-says-about-sustaining-investigation-speed-and-quality (accessed: 15.01.2026).
5. **Solar Group.** Solar enters the SIEM market: two technologies in one product and up to 40 % cost savings. URL: https://rt-solar.ru/events/news/6173/ (accessed: 15.01.2026).
6. **Cyber Sierra.** What Is Alert Fatigue and How to Combat It in Your SOC. URL: https://cybersierra.co/blog/alert-fatigue-in-soc/ (accessed: 15.01.2026).
7. **Garkushev A. Yu., Lipis A. V., Karpova I. L. et al.** Assessment of the competence of the intelligent information security management system. *Problems of information security. Computer systems*. 2024. No. 1, pp. 18–27. DOI: 10.48612/jisp/92vv-6m6t-7tmh. (In Russian)
8. **Vedernikov Yu. V., Garkushev A. Yu., Lipis A. V., Suprun A. F.** Reconfiguration of the

system development model information security management: interaction of base modules with the operator. *Problems of information security. Computer systems*. 2024. No. 2, pp. 9–19. DOI: 10.48612/jisp/amv1-kdnf-zaae. (In Russian)
9. **Suprun A. F., Gar'kushev A. Yu., Lipis A. V. et al.** Assessment of the Competence of an Intelligent Information Security Management System. *Automatic Control and Computer Sciences*. 2024. Vol. 58. No. 8, pp. 1429–1435. DOI: 10.3103/S0146411624701220.
10. **Garkushev A. Yu., Sazykin A. M., Shalkovskaya A. A.** Accounting for justification in models for evaluating the effectiveness of information and control systems. *Defense Technology Issues. Series 16: Counter-Terrorism Technical Means*. 2024. No. 3–4(189–190), pp. 40–44. DOI: 10.53816/23061456_2024_3-4_40. (In Russian)
11. **Garkushev A. Yu., Lipis A. V., Karpova I. L., Suprun A. F.** Modeling of work of an employee of the information security service of an industrial enterprise. *Problems of information security. Computer systems*. 2023. No. 3(56), pp. 148–153. DOI: 10.48612/jisp/1vmb-73pk-5e9e. (In Russian)
12. **Dropzone AI.** Alert Fatigue in Cybersecurity: AI-Powered SOC Solutions Guide. URL: https://www.dropzone.ai/blog/how-to-address-cybersecurity-alert-fatigue-with-ai (accessed: 15.01.2026).
13. **Bria M., Spânu F., Băban A., Dumitraşcu D. L.** Maslach Burnout Inventory – General Survey: Factorial Validity and Invariance among Romanian Healthcare Professionals. *Burnout Research*. 2014. Vol. 1. Iss. 3, pp. 103–111. DOI: 10.1016/j.burn.2014.09.001.
14. **Maslach C., Leiter M. P.** Understanding the Burnout Experience: Recent Research and Its Implications for Psychiatry. *World Psychiatry*. 2016. Vol. 15. No. 2, pp. 103–111. DOI: 10.1002/wps.20311.
15. Use of artificial intelligence technologies in Kaspersky SIEM. URL: https://www.kaspersky.ru/blog/ai-technology-in-kaspersky-siem/39252 (accessed: 15.01.2026). (In Russian)
16. **Glushko A.** Introduction: modern challenges for response centers. URL: https://ptsecurity.com/research/analytics/autonomous-socs-future-of-cybersecurity-monitoring-and-incident-response/?ysclid=mp56tgtis9263489058 (accessed: 15.01.2026). (In Russian)

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

ЛАРИОНОВА Екатерина Владимировна – канд. техн. наук, преподаватель, Санкт-Петербургский государственный морской технический университет, Россия, 190121, Санкт-Петербург, ул. Лоцманская, д. 3
E-mail: cf.82@mail.ru
ORCID: 0009-0009-1677-8355

LARIONOVA Ekaterina V. – Candidate of Engineering Sciences, Lecturer, Saint-Petersburg State Marine Technical University, Russia, 190121, St. Petersburg, Lotsmanskaya str., 3

БУНАС Ирина Леонидовна – преподаватель, Санкт-Петербургский государственный морской технический университет, Россия, 190121, Санкт-Петербург, ул. Лоцманская, д. 3
E-mail: ik070889@gmail.ru

BUNAS Irina L. – Lecturer, Saint-Petersburg State Marine Technical University, Russia, 190121, St. Petersburg, Lotsmanskaya str., 3

ГАРЬКУШЕВ Александр Юрьевич – канд. техн. наук, доцент, заведующий кафедрой, Санкт-Петербургский государственный морской технический университет, Россия, 190121, Санкт-Петербург, ул. Лоцманская, д. 3
E-mail: sangark@mail.ru
ORCID: 0000-0001-6695-2328

GARKUSHEV Alexander Yu. – Candidate of Engineering Sciences, Associate Professor, Head of Department, Saint-Petersburg State Marine Technical University, Russia, 190121, St. Petersburg, Lotsmanskaya str., 3

СУПРУН Александр Федорович – канд. техн. наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: afs54@inbox.ru
ORCID: 0000-0001-9665-0128

SUPRUN Alexander F. – Candidate of Engineering Sciences, Associate Professor, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29