УДК 004.056.5:316.6

Козырев Владислав Сергеевич
независимый исследователь

Давыдов Виталий Владимирович
независимый исследователь

ПРОФЕССИОНАЛЬНЫЙ СТРЕСС И ОПЕРАЦИОННАЯ НАДЁЖНОСТЬ ИБ-КОМАНД: КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ДИСБАЛАНСА НАГРУЗКИ, РЕСУРСОВ И ЗАЩИТНОГО МОЛЧАНИЯ

Аннотация. На основе систематизации научных, отраслевых и рыночных данных разработана проверяемая концептуальная модель связи профессионального стресса и операционной надёжности ИБ-команд с учётом охлаждения широкого IT-рынка, сохраняющегося спроса на отдельные ИБ-компетенции и высокой интенсивности киберугроз. Предложено различать внешний контекст и локальную экспозицию команды: национальные числа атак и вакансий не используются как прямые показатели стресса, а их предполагаемое влияние операционализируется через поток приоритетных оповещений, инцидентов, параллельных расследований, дежурств и доступную мощность команды. В модели требований и ресурсов работы основным фактором выступает дисбаланс нагрузки и ресурсов. Небезопасность занятости и низкая психологическая безопасность рассматриваются как модераторы, повышающие риск профессионального стресса, выгорания, защитного молчания и задержки эскалации сомнений и ошибок. Разработан контур психосоциального риска ИБ-команды, использующий процессную единицу «команда-неделя» и независимые анонимные опросные срезы без продольного идентификатора сотрудника. Для полевой проверки определён 16-недельный ступенчато-кластерный дизайн с четырьмя последовательностями внедрения. В событийной симуляции с 10 000 прогонами недели без событий, требующих эскалации, исключались из расчёта Yop - среднего времени до

формальной эскалации. Статистическая мощность базового сценария при предполагаемом стандартизованном эффекте d = 0,4 составила 0,665 для 72 команд и 0,792 для 96 команд. Для 96 команд анализ чувствительности дал диапазон 0,219-0,607. Расчёт обосновывает предварительный пилот как этап проверки осуществимости и калибровки. Совокупность данных позволяет рассматривать ИБ-команды как приоритетную группу управления психосоциальными рисками внутри IT вследствие специфически высокого профиля рабочих требований.

Ключевые слова: информационная безопасность, профессиональный стресс, выгорание, операционная надёжность, рабочая нагрузка, небезопасность занятости, психологическая безопасность, защитное молчание, SOC, эскалация инцидента.

WORK-RELATED STRESS AND OPERATIONAL RELIABILITY OF INFORMATION SECURITY TEAMS: A CONCEPTUAL MODEL OF WORKLOAD-CAPACITY IMBALANCE AND DEFENSIVE SILENCE

Abstract. Based on a synthesis of scientific, industry, and labour-market evidence, this paper develops a testable conceptual model linking work-related stress to the operational reliability of information security teams against the background of a cooling broad IT labour market, continued demand for selected cybersecurity skills, and persistent cyber threats. External context is separated from team-level exposure: national attack and vacancy counts are not treated as direct stress measures, and their hypothesized influence is operationalized through priority alerts, incidents, concurrent investigations, on-call duties, and available team capacity. Within the Job Demands-Resources framework, workload-capacity imbalance is the principal factor. Job insecurity and low psychological safety are specified as moderators that increase the risk of work-related stress, burnout, defensive silence, and delayed escalation. The proposed Psychosocial Risk Loop uses a team-week process unit and independent anonymous survey waves without longitudinal employee identifiers. A 16-week stepped-wedge cluster design with four implementation sequences is specified for field testing. In 10,000 event-aware simulation runs, weeks without events requiring

escalation were excluded from the calculation of Yop, the mean time to formal escalation. Under the base planning scenario, statistical power for an assumed standardized effect magnitude of d = 0.4 was 0.665 with 72 teams and 0.792 with 96 teams. Sensitivity analyses for 96 teams ranged from 0.219 to 0.607. The calculation supports a preliminary feasibility and calibration pilot. Taken together, the evidence supports treating cybersecurity teams as a priority group for psychosocial risk management within IT because of their distinctively high profile of job demands.
Keywords: information security, work-related stress, burnout, operational reliability, workload, job insecurity, psychological safety, defensive silence, security operations center, incident escalation.

Введение

В Международной классификации болезней МКБ-11 выгорание определено как профессиональный феномен, возникающий вследствие хронического стресса на рабочем месте, с которым не удалось успешно справиться - Всемирная организация здравоохранения отдельно указывает, что оно не классифицируется как заболевание [1]. Для исследования ИБ это различие принципиально: задача организации состоит не в дистанционной диагностике личности, а в выявлении изменяемых условий труда. ГОСТ Р ИСО 45001-2020 закрепляет системный подход к управлению рисками для здоровья работников [2]. ГОСТ Р ИСО 45003-2026, утверждённый приказом Росстандарта от 16 июня 2026 г. № 668-ст и вводимый с 1 февраля 2027 г., переносит в российскую практику руководство по психосоциальным рискам [3] - его международная основа ISO 45003:2021 ориентирует организацию на устройство работы, социальные факторы и рабочую среду [4].

Работа ИБ-команды сочетает постоянную бдительность, противодействие активному нарушителю, высокую цену ошибки, непредсказуемую инцидентную нагрузку и непрерывное изменение угроз. На уровне команды это выражается в потоке приоритетных оповещений, параллельных расследований и дежурств. Когда найм и организационные ресурсы ограничены, рабочая нагрузка начинает превышать доступную компетентную рабочую ёмкость, повышая риск

хронического стресса, истощения и снижения операционной надёжности. Небезопасность занятости и низкая психологическая безопасность усиливают этот эффект, в том числе через защитное молчание и задержку эскалации значимых сомнений и ошибок. Поэтому ИБ-команды рассматриваются как приоритетная группа управления психосоциальными рисками внутри IT.

Цель работы - разработать проверяемую концептуально-методическую модель связи профессионального стресса и операционной надёжности ИБ-команд, объединяющую локальный дисбаланс нагрузки и ресурсов, небезопасность занятости, психологическую безопасность, стресс, выгорание, защитное молчание и показатели реагирования. Объектом выступает организация труда сотрудников ИБ, предметом - предполагаемые механизмы влияния рабочих требований и ресурсов на психосоциальное состояние и операционную надёжность команды. Работа основана на анализе научной литературы, вторичном анализе рыночных и отраслевых данных, концептуальном моделировании и вычислительном эксперименте по оценке мощности будущего полевого дизайна. Научная новизна состоит в формализации перехода от внешнего контекста угроз и рынка труда к локальным требованиям D и доступной рабочей ёмкости CAP, далее - к дисбалансу WCR, профессиональному стрессу STR, выгоранию BO, защитному молчанию SIL и операционному исходу Yop, а также в использовании обезличенной единицы «команда–неделя».

Рынок труда IT и ИБ в России и контекст киберугроз

По данным hh.ru за июнь 2026 г., число активных вакансий в широкой IT-категории снизилось на 31% относительно июня 2025 г., число резюме выросло на 23%, а hh.индекс достиг 22,4 резюме на вакансию при 8,3 по рынку в целом [5]. Медианное предложение составляло 92,7 тыс. руб. при ожидании 113,3 тыс. руб. Эти показатели характеризуют охлаждение и усиление конкуренции в широком IT-сегменте, но не одинаковую динамику всех специальностей.

В узкой выборке вакансий кибербезопасности их число выросло с 10,8 тыс. в 2024 г. до 12,2 тыс. в 2025 г., то есть на 13% [6]. Более широкий поиск «Солара»

и hh.ru дал иные уровни, которые нельзя объединять с узкой выборкой из-за различий критериев [7]. Медианное предложение в кибербезопасности составляло 99,9 тыс. руб. при ожидании 162,4 тыс. руб., однако у специалистов с опытом более шести лет предложение было выше ожидания. Рынок сегментирован по опыту, специализации и доступному бюджету.

Российские источники фиксируют высокий уровень распределённых атак типа «отказ в обслуживании» (DDoS), целевой активности и утечек [8, 9]. Агентство Европейского союза по кибербезопасности (ENISA) проанализировало 4875 инцидентов за год, а Национальный центр кибербезопасности Великобритании (NCSC) обработал 429 инцидентов и отнёс 204 из них к национально значимым [10, 11]. Эти показатели собраны по разным правилам и не предназначены для прямого численного сравнения, но показывают устойчивую интенсивность и сложность угроз.

Российские и западные показатели отражают разные контуры наблюдения - телеметрию поставщика, отраслевую аналитику и национальную обработку инцидентов - и интерпретируются в рамках методики каждого источника. В совокупности они характеризуют сохраняющееся давление и сложность угроз. Связь с профессиональным стрессом раскрывается через промежуточное звено: фактическое изменение локального числа приоритетных сигналов, расследований, дежурств и сверхурочной работы конкретной команды. Сводные рыночные и отраслевые показатели, а также границы их интерпретации представлены в таблице 1.

Таблица 1. Рыночные и отраслевые показатели и границы их интерпретации

Контекст и источник	**Показатель**	**Наблюдение**	**Что поддерживает**	**Граница вывода**
Россия, IT, hh.ru, июнь 2026 [5]	Вакансии, резюме, hh.индекс	−31% - +23% - 22,4	Охлаждение широкой IT-категории и рост конкуренции	Не характеризует одинаково все IT- и ИБ-роли

Контекст и источник	Показатель	Наблюдение	Что поддерживает	Граница вывода
Россия, кибербезопасность, hh.ru [6]	Публикации вакансий	10,8 тыс. → 12,2 тыс. - +13%	Спрос на узкий сегмент ИБ сохраняется	Методика уже, чем в исследовании [7]
Россия, зарплаты ИБ, «Солар»/hh.ru [7]	Медианы предложения и ожидания	99,9 и 162,4 тыс. руб. - 6+ лет: 259,2 и 190,5 тыс.	Сильная сегментация по опыту	Не измеряет стресс и не доказывает общий дефицит
Россия, Anti-DDoS [8]	События сервиса	665,3 тыс. - +11%	Высокая интенсивность наблюдаемого класса атак	Телеметрия поставщика, не национальный итог
ЕС и Великобритания [10 - 11]	Инциденты разных контуров	ENISA: 4875 - NCSC: 429 обработано	Устойчивое давление присутствует и вне РФ	Определения и охват несопоставимы с [8]

Теоретические и эмпирические основания исследования

Крупные профессиональные опросы подтверждают значимую субъективную нагрузку. В исследовании ISC2 2025 г. участвовали 16 029 практиков и руководителей: 48% сообщили об истощении из-за необходимости отслеживать новые угрозы и технологии, 47% - о перегруженности ожидаемым объёмом работы, 32% - о переработке вследствие дефицита навыков и персонала [12]. В опросе ISACA более 3800 специалистов 55% назвали команды недоукомплектованными, 65% сообщили об открытых позициях, а 66% - что роль стала более стрессовой за пять лет [13]. Эти результаты характеризуют масштаб субъективно воспринимаемой нагрузки внутри ИБ и поддерживают приоритетность управления психосоциальными рисками в ИБ-командах.

Российские исследования связывают работу аналитиков центров мониторинга информационной безопасности (Security Operations Center, SOC) с выгоранием, когнитивной нагрузкой, ошибками и операционным риском, а в IT-выборках выделяют многозадачность, неопределённость и непрерывное обучение [14-17]. Международные обзоры и исследования добавляют постоянную бдительность, нарушения сна, ролевые и культурные стрессоры, усталость от потока оповещений (alert fatigue) и кадрово-компетентностные ограничения [18-23]. Интервью с 37 руководителями информационной безопасности (Chief Information Security Officer, CISO) также показали, что внешние, ресурсные и коммуникативные стрессоры действуют совместно [22]. В совокупности эти работы связывают специфические требования ИБ с истощением, снижением качества решений и намерением уйти.

Сравнение с другими IT-ролями дополняет эту картину. В разведочном препринте с 50 участниками 66% ИБ-специалистов воспринимали свою работу как более стрессовую, а четыре исследования кибероперациий в Агентстве национальной безопасности США (NSA) зафиксировали стресс, усталость и когнитивную нагрузку в рабочих сценариях [24, 25]. Вместе с данными о бдительности и усталости от оповещений это подтверждает специфически высокий профиль требований ИБ внутри IT.

Модель требований и ресурсов работы (Job Demands-Resources, JD-R) объясняет истощение устойчивым превышением требований над доступными ресурсами, а не слабостью сотрудника [26]. Метаанализ 535 независимых выборок показывает устойчивые неблагоприятные связи небезопасности занятости [27]. Психологическая безопасность означает разделяемое убеждение, что в команде допустим межличностный риск, включая вопрос, сомнение и признание ошибки [30]. Метаанализ 136 выборок связывает её с рабочими результатами и обучающим поведением [31].

Защитное молчание - мотивированное удержание значимой информации для снижения личного риска - следует отличать от отсутствия речи и от просоциальной конфиденциальности [32]. Пятинедельное дневниковое

исследование 97 работников связало небезопасность занятости с меньшим голосом и большим молчанием в текущую и следующую неделю [33]. Метаанализ 84 исследований (N = 34 975) выявил связь молчания с выгоранием ($\rho = 0{,}43$) и голоса с меньшим выгоранием ($\rho = -0{,}28$), однако все включённые исследования были корреляционными, а ни одно не получило высокой оценки качества [34]. Следовательно, цепочка «небезопасность занятости → защитное молчание → задержка эскалации» является обоснованной, но ещё проверяемой именно для ИБ гипотезой, а не установленной причинностью. Предполагаемые связи между внешним контекстом, локальной нагрузкой и операционной надёжностью обобщены на рисунке 1.

Рисунок 1. Концептуальная модель дисбаланса нагрузки, ресурсов и операционной надёжности

Концептуальная модель и гипотезы

Модель сопоставляет объём работы с реальной способностью команды выполнять задачи того же класса. Индекс g обозначает команду, t - неделю, p - четырёхнедельный опросный период, k - класс задач. Индекс i обозначает задачу, j - сотрудника. Множество $B_k(g,t)$ включает новые и перенесённые задачи. Для каждой задачи учитываются оставшиеся плановые трудочасы r_i и заранее установленный вес сложности w_i. Исходная оценка трудозатрат определяется по калибровочному периоду или фиксируется экспертно до внедрения КПР-ИБ. Сверхурочные часы в D_k не включаются. Показатель D_k обозначает объём рабочих требований класса k в эффективных трудочасах, CAP_k - доступную рабочую ёмкость команды для этого класса, WCR - индекс положительного дисбаланса нагрузки и доступной ёмкости.

$$D_k(g,t) = \Sigma_{i \in B_k(g,t)} r_i(g,t) \cdot w_i.$$

$$CAP_k(g,t) = \Sigma_j Hplan(j,g,t) \cdot q_{jk}(g,t) \cdot s_{jk}(g,t) \cdot a(g,t).$$

$$WCR(g,t) = \Sigma_k \omega_k \cdot max\{0, ln([D_k(g,t) + c] / [CAP_k(g,t) + c])\}, \quad \Sigma_k \omega_k = 1.$$

В формуле CAP_k величина Hplan обозначает плановые продуктивные часы сотрудника, q_{jk} - долю этих часов, выделенную для класса k, s_{jk} - коэффициент соответствия навыков, a(g,t) - коэффициент доступности критичных инструментов. Величины q_{jk}, s_{jk} и a(g,t) принимают значения от 0 до 1, а сумма q_{jk} по классам задач для сотрудника не превышает 1. Коэффициент ω_k задаёт вес класса задач. Положительная константа c фиксируется до рандомизации в тех же единицах, что D_k и CAP_k, и предотвращает деление на ноль. Обозначение ln означает натуральный логарифм. Остаток трудочасов уменьшается по мере выполнения работы, поэтому перенесённая задача не получает повторно полную трудоёмкость. WCR суммирует только дефициты рабочей ёмкости. Чем он выше, тем сильнее нагрузка превышает возможности команды. При отсутствии дефицита WCR равен нулю, а резерв рабочей ёмкости показывается отдельно. Национальное число атак в формулу не подставляется.

JI обозначает количественную небезопасность занятости, STR - профессиональный стресс, BO - выгорание, SIL - защитное молчание, PS - психологическую безопасность, REC - восстановление. WCRprev(g,p) равен среднему WCR за четыре недели перед опросом. JI измеряется шкалой Job Insecurity Scale (JIS) [28], STR - валидированной русскоязычной версией третьей редакции Copenhagen Psychosocial Questionnaire (COPSOQ III) [41, 42], BO - шкалой Burnout Assessment Tool (BAT) [29], PS - командной шкалой психологической безопасности Эдмондсон [30]. Для SIL используется набор пунктов защитного молчания на основе конструкции Van Dyne et al. [32]. REC и усталость измеряются коротким командным опросом с заранее установленными вариантами ответов и правилами расчёта. Русскоязычные формулировки SIL и REC проходят прямой и обратный перевод и когнитивную проверку до пилота. Медиатор описывает промежуточное звено предполагаемой связи, модератор - изменение её силы при разных уровнях другого показателя. В анализ входят

только заранее определённые командные агрегаты. WCRprev, JI и PS центрируются, а назначенная экспозиция и календарный период учитываются в каждом шаге модели.

$$WCRprev(g,p) \rightarrow \{STR(g,p),\ BO(g,p)\} \rightarrow SIL(g,p+1) \rightarrow Yop(g,p+2).$$

STR и BO измеряются одновременно и образуют два параллельных пути к последующему SIL. Ответы одного сотрудника между волнами не связываются. Операционная надёжность не смешивается с самоотчётами. Первичным командным исходом Yop выступает ограниченное среднее время от объективно определённого события до формальной эскалации в минутах. Более высокое Yop означает меньшую операционную надёжность.

$$T\tau(e) = min\{Tобъект \rightarrow эск(e),\ \tau\},\quad Yop(g,t,\tau) = N(g,t)^{-1} \Sigma e \in E(g,t)\ T\tau(e),\quad N(g,t) \geq 1.$$

Здесь e обозначает отдельное событие, E(g,t) - множество событий, подлежащих формальной эскалации, N(g,t) - число таких событий. В E(g,t) включаются только события, которые по заранее утверждённому правилу должны быть формально эскалированы. Тобъект→эск отсчитывается от первого объективно квалифицируемого события по журналам систем управления событиями ИБ (SIEM), автоматизации реагирования (SOAR) или управления IT-услугами (ITSM) до формальной эскалации. Событие, которое не должно эскалироваться, в E(g,t) не попадает. Горизонт τ одинаков для всех команд и фиксируется до рандомизации. Если событие не эскалировано до τ, ему присваивается Tτ(e) = τ, поэтому такой эпизод не может улучшить результат команды. Неделя без подходящих событий имеет N(g,t) = 0 и неопределённый Yop. Она не кодируется нулём, а число событий и индикатор такой недели анализируются отдельно.

Для четырёхнедельного периода Yop рассчитывается по всем подходящим событиям, а не как среднее недельных значений. Если событий нет, Yop остаётся неопределённым. Параметры стандартизации фиксируются по общему калибровочному периоду. Индикатор Shock отмечает тяжёлые инциденты, массовые сбои инструментов и резкие изменения состава команды. Повторные

открытия и просроченная очередь рассматриваются как вторичные исходы, сверхурочная работа, восстановление и усталость - как сводный показатель устойчивости Ysust, почти произошедшие или своевременно предотвращённые инциденты (near miss) и ложные эскалации - как ограничители безопасности.

Формулируются четыре гипотезы. H1: увеличение WCR связано с последующим ростом STR и BO. H2: рост WCR связан с увеличением SIL через параллельные пути STR и BO, а SIL связано с последующим ухудшением Yop. H3: небезопасность занятости усиливает, а психологическая безопасность ослабляет связь WCR со STR и BO. H4: внедрение КПР-ИБ уменьшает Yop по принципу анализа согласно первоначальному назначению команд (intention-to-treat, ITT) без ухудшения Ysust и неприемлемого роста ложных эскалаций. H1-H3 оцениваются как вторичные временно упорядоченные гипотезы о предполагаемом механизме. Причинный вывод первичного анализа относится к H4 и рандомизированному графику внедрения. В H4 ITT означает оценку команд по первоначально назначенному графику внедрения независимо от полноты выполнения отдельных элементов.

Контур психосоциального риска ИБ-команды

Предлагаемый КПР-ИБ переносит объект управления с отдельного «проблемного сотрудника» на команду и устройство работы и воздействует на первичные источники профессионального стресса. Четыре взаимосвязанных элемента КПР-ИБ представлены в таблице 2.

Таблица 2. Элементы КПР-ИБ

Элемент	Целевая проблема	Механизм	Основные метрики	Что исключено
Управление требованиями и рабочей ёмкостью	Незавершённая работа (WIP), поток сигналов, дежурства, дефицит нужных навыков	Лимиты параллельной работы, приоритизация, настройка шумных правил, карта навыков, защищённая передача смены	WCR, накопленная очередь	Норма героизма и оценка по часам присутствия
Безопасная эскалация и ясность занятости	Страх санкции, слухи о сокращении, задержка сомнения	Прозрачная коммуникация решений, право остановить и запросить проверку, ясные маршруты эскалации	JI, PS, SIL, Тобъект→эск	Обещание отсутствия изменений и безусловная безответственность
Командное обучение	Скрытие ошибки, повторные инциденты, дефицит голоса	Разбор хронологии и системных условий без поиска виновного при сохранении стандартов качества	Почти произошедшие инциденты, повторные открытия, PS	Индивидуальные лидерборды

Элемент	Целевая проблема	Механизм	Основные метрики	Что исключено
Восстановление	Накопленная усталость после интенсивных периодов	Гибкие микропаузы, смена типа задачи, защищённое время после инцидента, устойчивые дежурные ротации	STR, BO, усталость, сверхурочная работа	Универсальный режим 52/17

Микропаузы могут улучшать самочувствие, но метаанализ не подтверждает единую оптимальную длительность и показывает зависимость эффекта результативности от вида задачи [35]. Поэтому восстановление задаётся гибко. Также формальное присутствие сотрудника не приравнивается к эффективности: метаанализ презентеизма показывает сложную систему организационных и индивидуальных коррелятов работы в состоянии сниженной функциональности [36]. КПР-ИБ не обещает повысить результативность без ресурсов: снижение WIP, обучение, передача смены и восстановление требуют времени и управленческой поддержки. Последовательность сбора данных, внедрения КПР-ИБ и проверки эффекта показана на рисунке 2.

Рисунок 2. Цикл сбора данных, вмешательства и проверки эффекта в КПР-ИБ

Данные, измерение и защита участников

Процессные данные собираются для единицы «команда-неделя», опросные - для четырёхнедельного периода. Пульс проводится перед неделей 1 и после недель 4, 8, 12 и 16 как пять независимых анонимных срезов. Идентификатор сотрудника не создаётся, ответы между волнами не связываются. Командный результат публикуется только при наличии не менее семи ответов и не менее 60% состава команды. Для команды из восьми человек требуется семь ответов.

Ролевые срезы подчиняются тому же порогу. JI, STR, BO и PS используются только как командные показатели после проверки согласия ответов [37]. Персональные сообщения, нажатия клавиш, видео, биометрия и скрытая оценка поведения не собираются. Состав данных, правила их агрегации и ограничения использования приведены в таблице 3.

Таблица 3. Минимальный набор данных и ограничения использования

Показатель	**Источник**	**Агрегация**	**Назначение**	**Защита и проверка**
JI, STR, BO, SIL, PS	Независимый анонимный пульс до недели 1 и после недель 4, 8, 12 и 16	Команда / 4 недели без связи ответов между волнами	Вторичные предикторы, медиаторы и модераторы	Не менее 7 ответов и не менее 60% состава команды. Для PS проверяются ICC(1), ICC(2) и rWG(j)
D_k и CAP_k	SIEM/SOAR/ITSM, сменный журнал, карта навыков	Команда–неделя	Расчёт WCR по классам задач	Остаток трудочасов - распределение q_{jk} - шкала s_{jk} - аудит качества
Тобъект→эск	ITSM и журнал решений	Событие и команда–неделя	Первичный исход Yop в минутах	Объективное стартовое событие - единый τ - неэскалированные эпизоды получают τ - N = 0 не кодируется нулём

Показатель	Источник	Агрегация	Назначение	Защита и проверка
Подтверждённое повторное открытие, просроченная очередь	ITSM и график дежурств	Команда–неделя	Вторичные операционные исходы	Подтверждение дефекта закрытия - поправка на приоритет, роль и сложность
Почти произошедший инцидент, ложная эскалация	SOAR/ITSM и независимая проверка	Команда–неделя	Ограничители безопасности	Нет штрафа за добросовестный отчёт - анализ отдельно от Yop
Сверхурочная работа, REC, усталость	График дежурств и короткий пульс	Команда–неделя и команда / 4 недели	Отдельный блок устойчивости Ysust	Не входят в D и Yop - анализируются отдельно

В формуле порога публикации nответ означает число полученных ответов, Nкоманды - численность команды, ceil - округление вверх. Показатели ICC(1), ICC(2) и rWG(j) используются для проверки обоснованности объединения индивидуальных ответов в командный показатель. До сбора данных фиксируются словарь событий, классы задач, правила расчёта D, CAP и Yop, горизонт наблюдения, обработка недель без событий, вторичные исходы и план пропусков. Опросы проводит независимый оператор. Технические токены не содержат исследовательского идентификатора и удаляются до формирования набора данных. Руководитель получает только командный профиль. Результаты запрещено использовать для увольнения, премирования или ранжирования сотрудников.

Обобщение собранных данных показывает, что актуальность методики определяется наложением трёх процессов. Широкий IT-рынок России охлаждается, тогда как сегмент кибербезопасности сохраняет спрос при несовпадении навыков, опыта кандидатов и бюджета [5-7]. Российские и западные источники фиксируют устойчивую интенсивность угроз [8-11], а отраслевые опросы ИБ-специалистов - перегруженность, недоукомплектованность и рост субъективной стрессогенности роли [12, 13]. Исследования связывают превышение рабочих требований над ресурсами со стрессом, истощением и снижением качества решений, а небезопасность занятости и низкую психологическую безопасность - с защитным молчанием и задержкой эскалации [14-34]. Поэтому оценка риска требует перехода от общих чисел атак и вакансий к локальным D, CAP, STR, BO, SIL и Yop конкретной команды. КПР-ИБ обеспечивает такой переход и соответствует системной логике ISO 45001 и ISO 45003 [2-4].

Методы разработки модели и вычислительный эксперимент

Для последующей полевой проверки модели разработан протокол ступенчато-кластерного исследования в логике SPIRIT 2025 и расширения CONSORT для исследований со ступенчатым внедрением [38, 39]. Кластером является ИБ-команда, периодом - одна неделя. До рандомизации проводится восьминедельный калибровочный период для словаря событий, базовых трудозатрат, выбора единого τ и параметров вторичной стандартизации Yop. Он не входит в 16-недельный анализ внедрения. В анализируемом периоде все команды остаются в контроле на неделях 1-3. Четыре равные последовательности начинают КПР-ИБ в начале недель 4, 7, 10 и 13 и получают соответственно 13, 10, 7 и 4 недели доступа к вмешательству. В первую неделю каждой последовательности экспозиция задаётся как 0,5, далее - как 1. Для 12, 36, 72 и 96 команд в каждой последовательности находятся соответственно 3, 9, 18 и 24 команды.

Первичная оцениваемая величина - средний ITT-эффект назначения доступа к КПР-ИБ по рандомизированной последовательности на Yop.

AssignedExposure(g,t) обозначает назначенную долю доступа к КПР-ИБ по графику независимо от полноты фактического выполнения отдельных элементов. Основная модель включает фиксированные эффекты команды и недели, кластерно-робастные стандартные ошибки с поправкой CR1 по команде и не корректируется на WCR, STR, BO и SIL, измеренные после рандомизации. Такой анализ поддерживает причинную интерпретацию общего эффекта внедрения при соблюдении рандомизации, отсутствии межкомандного переноса и корректной регистрации исхода. Нарушения графика и межкомандное заимствование практик фиксируются и анализируются отдельно.

Для оценки статистической мощности выполнен вычислительный эксперимент для 12, 36, 72 и 96 команд. Восемь сотрудников на команду используются только для оценки ожидаемой опросной нагрузки. Статистической единицей остаётся «команда-неделя». В каждом прогоне сначала генерировалось число событий, подлежащих эскалации. Модель допускала как недели без событий, так и недели с резким ростом потока. Затем для каждого события создавалось время до эскалации, ограниченное горизонтом τ, и по тем же правилам рассчитывался Yop. Общий шок мог одновременно увеличить число событий и ухудшить время до эскалации. В базовом сценарии в среднем задавалось два события на команду-неделю, что дало около 24% недель без Yop. Это плановый сценарий, а не оценка реального SOC.

$$Yop(g,t) = \delta ITT\ AssignedExposure(g,t) + TeamFE(g) + WeekFE(t) + \varepsilon(g,t).$$

Здесь δITT обозначает средний эффект назначения доступа к КПР-ИБ, TeamFE(g) - фиксированный эффект команды, WeekFE(t) - фиксированный эффект недели, ε(g,t) - остаточную ошибку.

Для каждого сценария выполнено 10 000 прогонов с фиксированным начальным значением генератора случайных чисел (seed) 20260820. В каждом прогоне оценивалась та же intention-to-treat модель с фиксированными эффектами команды и недели. Стандартная ошибка корректировалась по командам. Статистическая мощность равна доле тестов, отклонивших нулевую гипотезу при уровне 0,05. Интервалы Монте-Карло рассчитывались по формуле

Уилсона. Сценарий d = 0 контролирует ошибку первого рода. Полный исполняемый код сохранён в файле stress_stepped_wedge_event_power_supplement.py.

Вторичный анализ H1-H3 сохраняет временной порядок WCRprev(g,p) → {STR(g,p), BO(g,p)} → SIL(g,p+1) → Yop(g,p+2), учитывает назначенную экспозицию, календарный период и заранее определённые тяжёлые инциденты. Пути через STR и BO оцениваются раздельно, а взаимодействия WCR с JI и PS проверяются в H3. Неопределённость оценивается повторным расчётом с поочерёдным исключением команд. Разделение изменений внутри команды и различий между командами снижает риск ошибочного переноса межкомандных связей на динамику одной команды, но не превращает вторичные связи в причинные оценки [40].

В расчётах d обозначает модуль стандартизованного эффекта. Значение d = 0,4 соответствует изменению Yop на 0,4 стандартного отклонения. Обозначение G указывает общее число команд. Результаты вычислительного эксперимента для всех сценариев представлены в таблице 4.

Таблица 4. Статистическая мощность событийных вычислительных сценариев

Сценарий	**G**	**Недель без Yop**	**Мощность**	**95% интервал МК**
Базовый	12	24,3%	0,1444	0,1376-0,1514
Базовый	36	24,3%	0,3728	0,3634-0,3823
Базовый	72	24,3%	0,6651	0,6558-0,6743
Базовый	96	24,3%	0,7918	0,7837-0,7996
Редкие события	96	47,6%	0,5737	0,5640-0,5834
Повышенная зависимость	96	24,3%	0,5494	0,5396-0,5591
Замедленное внедрение	96	24,3%	0,6069	0,5973-0,6164

Сценарий	G	Недель без Yop	Мощность	95% интервал МК
Совмещённый неблагоприятный	96	54,5%	0,2186	0,2106-0,2268

Примечание: недели с N(g,t) = 0 не входят в модель Yop. Для всех сценариев d = 0,4. МК - интервал Монте-Карло по 10 000 прогонам.

Результаты вычислительного эксперимента и обсуждение

При нулевом эффекте доля ложных отклонений составила 0,0401-0,0488 и оставалась близкой к заданным 0,05. Средняя оценка эффекта в базовом сценарии была близка к заданному значению. Это подтверждает корректность реализованного алгоритма для плановых сценариев.

В базовом сценарии статистическая мощность при d = 0,4 составила 0,6651 для 72 и 0,7918 для 96 команд. Анализ чувствительности показал снижение статистической мощности при редких событиях, сильной связи между соседними неделями и замедленном внедрении. В совмещённом неблагоприятном сценарии около 55% недель не имели Yop, а статистическая мощность снизилась до 0,2186. Поэтому исследование 8-12 команд рассматривается как пилот осуществимости, после которого параметры уточняются для подтверждающего многоорганизационного этапа.

Связь с ростом киберугроз оценивается после перехода от внешнего фона к локальным требованиям D, дисбалансу WCR, STR, BO, SIL и последующему Yop. Показатели JI и PS задают проверяемую модерацию влияния WCR. Охлаждение рынка измеряется через JI, тогда как вакансии и зарплаты задают контекст. Тяжёлые инциденты учитываются в анализе чувствительности. Разнонаправленная динамика широкого IT-найма и отдельных ИБ-вакансий отражает сегментацию по навыкам, опыту и бюджету.

Область применимости и направления дальнейшего исследования

Разработанная модель характеризует высокий профиль рабочих требований ИБ и обосновывает приоритетность управления психосоциальными рисками в этих командах. Межролевые различия внутри IT требуют отдельного

исследования с едиными психометрическими и операционными показателями. Рыночные данные и показатели угроз интерпретируются только в пределах определений каждого источника [6, 7, 12, 13]. Пилот уточняет вариативность команд, частоту событий, скорость внедрения и свойства Yop. Конфиденциальность обеспечивают отсутствие продольного идентификатора, минимальный порог ответов, независимый сбор и запрет дисциплинарного использования данных. Отдельные отчёты по малым ролевым группам не выпускаются.

Заключение

Высокая интенсивность и сложность угроз сами по себе не являются показателем стресса сотрудников. Согласно разработанной модели, они становятся психосоциальным риском, когда преобразуются в локальный поток приоритетной работы D, превышающий доступную рабочую ёмкость CAP ИБ-команды. Дисбаланс WCR формирует проверяемую связь с профессиональным стрессом STR, выгоранием BO и снижением операционной надёжности Yop. Небезопасность занятости усиливает, а психологическая безопасность ослабляет предполагаемые последствия WCR, в том числе через защитное молчание SIL.

Рынок труда России 2025–2026 гг. характеризуется разнонаправленной динамикой: широкая IT-категория охлаждается и становится более конкурентной, тогда как отдельный сегмент кибербезопасности сохраняет рост вакансий и выраженное несовпадение навыков, опыта и бюджета. Российские и западные данные характеризуют устойчивую интенсивность угроз в рамках методики каждого источника. Эмпирическая проверка выстраивается по пути от внешнего контекста к D, CAP и WCR конкретной команды.

КПР-ИБ объединяет управление нагрузкой и рабочей ёмкостью, безопасную эскалацию, командное обучение и восстановление. Базовый сценарий показал статистическую мощность 0,665 при 72 командах и 0,792 при 96 командах для d = 0,4, а анализ чувствительности подтвердил необходимость пилотной калибровки перед многоорганизационным этапом. Страх потери работы и низкая психологическая безопасность выступают модераторами

последствий дисбаланса нагрузки и ресурсов, а защитное молчание - проверяемым звеном между психосоциальным состоянием и последующей операционной надёжностью.

Список литературы

1. World Health Organization. Burn-out an occupational phenomenon: International Classification of Diseases [Электронный ресурс]. URL: https://www.who.int/standards/classifications/frequently-asked-questions/burn-out-an-occupational-phenomenon (дата обращения: 21.08.2026).
2. ГОСТ Р ИСО 45001-2020. Системы менеджмента безопасности труда и охраны здоровья. Требования и руководство по применению [Электронный ресурс]. URL: https://protect.gost.ru/gost/details/7edf6db7-ef4d-4655-89e9-f546d8de3045 (дата обращения: 21.08.2026).
3. Росстандарт. Уведомление об утверждении ГОСТ Р ИСО 45003-2026 (приказ от 16.06.2026 № 668-ст) [Электронный ресурс]. URL: https://uvedns.gostinfo.ru/uveddetails?id=196186 (дата обращения: 21.08.2026).
4. ISO 45003:2021. Occupational health and safety management - Psychological health and safety at work - Guidelines for managing psychosocial risks [Электронный ресурс]. URL: https://www.iso.org/standard/64283.html (дата обращения: 21.08.2026).
5. hh.ru. Краткий обзор рынка труда. Россия, июнь 2026 [Электронный ресурс]. URL: https://stats.hh.ru/api/v1/monthly-report/f-e945e3b9-d3da-49cb-9f51-d57ea337baca (дата обращения: 21.08.2026).
6. Спрос на специалистов по кибербезопасности вырос на 35% за пять лет // Коммерсантъ. 17.03.2026 [Электронный ресурс]. URL: https://www.kommersant.ru/doc/8514071 (дата обращения: 21.08.2026).
7. ГК «Солар». Исследование «Солар» и hh.ru: российские компании готовы платить на 36% больше профессионалам в кибербезопасности. 03.06.2025 [Электронный ресурс]. URL: https://rt-solar.ru/events/news/5585/ (дата обращения: 21.08.2026).
8. ГК «Солар». DDoS-атаки-2025: 665 тыс. атак и рекорд мощности 11 Тбит/с [Электронный ресурс]. URL: https://rt-solar.ru/analytics/reports/6480/ (дата обращения: 21.08.2026).
9. F6. Cybercrime Trends 2025–2026: ежегодный отчёт [Электронный ресурс]. URL: https://www.f6.ru/cybercrime-trends-annual-report-2025-2026/ (дата обращения: 21.08.2026).

10. ENISA. ENISA Threat Landscape 2025 [Электронный ресурс]. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата обращения: 21.08.2026).
11. UK National Cyber Security Centre. Annual Review 2025: Incident management [Электронный ресурс]. URL: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk/incident-management (дата обращения: 21.08.2026).
12. ISC2. 2025 Cybersecurity Workforce Study [Электронный ресурс]. URL: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study (дата обращения: 21.08.2026).
13. ISACA. Cybersecurity Staffing Challenges Persist With Adaptability and Soft Skills in High Demand. 2025 [Электронный ресурс]. URL: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-19/cybersecurity-staffing-challenges-persist-with-adaptability-and-soft-skills-in-high-demand (дата обращения: 21.08.2026).
14. 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. URL: https://jisp.spbstu.ru/article/2026.26.5/
15. Резниченко С.И., Подтягина П.О. Офисная среда и параметры профессионального опыта как предикторы профессионального выгорания у специалистов IT-индустрии // Экспериментальная психология. 2024. Т. 17, № 1. С. 181–197. DOI: 10.17759/exppsy.2024170112. URL: https://psyjournals.ru/journals/exppsy/archive/2024_n1/Reznichenko_Podtiagina
16. Джумагулова А.Ф., Водопьянова Н.Е., Гофман О.О., Никифоров Г.С. Профессиографические особенности деятельности IT-специалистов как рискогенные факторы выгорания // Вестник РУДН. Серия: Психология и педагогика. 2024. Т. 21, № 1. С. 220–241. DOI: 10.22363/2313-1683-2024-21-1-220-241. URL: https://journals.rudn.ru/psychology-pedagogics/article/view/41499/ru_RU
17. Гофман О.О., Водопьянова Н.Е., Джумагулова А.Ф., Никифоров Г.С. Проблема профессионального выгорания специалистов в сфере информационных технологий: теоретический обзор // Организационная психология. 2023. Т. 13, № 1. С. 117–144. DOI:

10.17323/2312-5942-2023-13-1-117-144. URL: https://doi.org/10.17323/2312-5942-2023-13-1-117-144

18. Singh T., Johnston A.C., D'Arcy J., Harms P.D. Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research // Organizational Cybersecurity Journal: Practice, Process and People. 2023. Vol. 3, no. 2. P. 100–126. DOI: 10.1108/OCJ-06-2022-0012. URL: https://doi.org/10.1108/OCJ-06-2022-0012

19. Gupta V., Rangarajan A., Nobles C. Burnout in the Cybersecurity Profession: A Scoping Review // MWAIS 2024 Proceedings. 2024. Paper 20. URL: https://aisel.aisnet.org/mwais2024/20/

20. Reeves A., Pattinson M., Butavicius M. The sleepless sentinel: factors that predict burnout and sleep quality in cybersecurity professionals // Information & Computer Security. 2024. Vol. 32, no. 4. P. 477–491. DOI: 10.1108/ICS-11-2023-0222. URL: https://doi.org/10.1108/ICS-11-2023-0222

21. Ogbanufe O., Jones M.C., Hancock J.I. Job demands, identity, and outcomes: The mediating role of cynicism among cybersecurity-focused employees // Computers & Security. 2025. Vol. 150. Art. 104277. DOI: 10.1016/j.cose.2024.104277. URL: https://doi.org/10.1016/j.cose.2024.104277

22. Mulgund P., Singh R., Li Y., Chew S.L., Higgins K. A Qualitative Examination of Stressors Contributing to Burnout Among Chief Information Security Officers (CISOs) // Information Systems Journal. 2026. Vol. 36, no. 4. P. 556–581. DOI: 10.1111/isj.70020. URL: https://onlinelibrary.wiley.com/doi/10.1111/isj.70020

23. Tariq S., Baruwal Chhetri M., Nepal S., Paris C. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities // ACM Computing Surveys. 2025. Vol. 57, no. 9. Art. 224. P. 1–38. DOI: 10.1145/3723158. URL: https://doi.org/10.1145/3723158

24. Arora S., Hastings J.D. A Survey-Based Quantitative Analysis of Stress Factors and Their Impacts Among Cybersecurity Professionals. 2024. arXiv:2409.12047. URL: https://arxiv.org/abs/2409.12047

25. Dykstra J., Paul C.L. Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations // 11th USENIX Workshop on Cyber Security Experimentation and Test. 2018. URL: https://www.usenix.org/conference/cset18/presentation/dykstra

26. Bakker A.B., Demerouti E. The Job Demands–Resources model: state of the art // Journal of Managerial Psychology. 2007. Vol. 22, no. 3. P. 309–328. DOI: 10.1108/02683940710733115. URL: https://doi.org/10.1108/02683940710733115

27. Jiang L., Lavaysse L.M. Cognitive and Affective Job Insecurity: A Meta-Analysis and a Primary Study // Journal of Management. 2018. Vol. 44, no. 6. P. 2307–2342. DOI: 10.1177/0149206318773853. URL: https://doi.org/10.1177/0149206318773853

28. Vander Elst T., De Witte H., De Cuyper N. The Job Insecurity Scale: A psychometric evaluation across five European countries // European Journal of Work and Organizational Psychology. 2014. Vol. 23, no. 3. P. 364–380. DOI: 10.1080/1359432X.2012.745989. URL: https://doi.org/10.1080/1359432X.2012.745989

29. Schaufeli W.B., Desart S., De Witte H. Burnout Assessment Tool (BAT) - Development, Validity, and Reliability // International Journal of Environmental Research and Public Health. 2020. Vol. 17, no. 24. Art. 9495. DOI: 10.3390/ijerph17249495. URL: https://www.mdpi.com/1660-4601/17/24/9495

30. Edmondson A. Psychological Safety and Learning Behavior in Work Teams // Administrative Science Quarterly. 1999. Vol. 44, no. 2. P. 350–383. DOI: 10.2307/2666999. URL: https://doi.org/10.2307/2666999

31. Frazier M.L., Fainshmidt S., Klinger R.L., Pezeshkan A., Vracheva V. Psychological Safety: A Meta-Analytic Review and Extension // Personnel Psychology. 2017. Vol. 70, no. 1. P. 113–165. DOI: 10.1111/peps.12183. URL: https://doi.org/10.1111/peps.12183

32. Van Dyne L., Ang S., Botero I.C. Conceptualizing Employee Silence and Employee Voice as Multidimensional Constructs // Journal of Management Studies. 2003. Vol. 40, no. 6. P. 1359–1392. DOI: 10.1111/1467-6486.00384. URL: https://doi.org/10.1111/1467-6486.00384

33. Breevaart K., Bohle S.L., Pletzer J.L., Medina F.M. Voice and silence as immediate consequences of job insecurity // Career Development International. 2020. Vol. 25, no. 2. P. 204–220. DOI: 10.1108/CDI-09-2018-0226. URL: https://doi.org/10.1108/CDI-09-2018-0226

34. Lainidi O., Johnson J., Griffin B., Koutsimani P., Mouratidis C., Keyworth C., O'Connor D.B. Associations between burnout, employee silence and voice: a systematic review and meta-analysis // Psychology & Health. 2026. Vol. 41, no. 8. P. 1245–1265. DOI: 10.1080/08870446.2025.2509074. URL: https://pubmed.ncbi.nlm.nih.gov/40437815/

35. Albulescu P., Macsinga I., Rusu A., Sulea C., Bodnaru A., Tulbure B.T. “Give me a break!” A systematic review and meta-analysis on the efficacy of micro-breaks for increasing well-being and

performance // PLOS ONE. 2022. Vol. 17, no. 8. Art. e0272460. DOI: 10.1371/journal.pone.0272460. URL: https://doi.org/10.1371/journal.pone.0272460

36. Miraglia M., Johns G. Going to work ill: a meta-analysis of the correlates of presenteeism and a dual-path model // Journal of Occupational Health Psychology. 2016. Vol. 21, no. 3. P. 261–283. DOI: 10.1037/ocp0000015. URL: https://doi.org/10.1037/ocp0000015

37. LeBreton J.M., Senter J.L. Answers to 20 Questions About Interrater Reliability and Interrater Agreement // Organizational Research Methods. 2008. Vol. 11, no. 4. P. 815-852. DOI: 10.1177/1094428106296642.

38. Butcher N.J., Monsour A., Mew E.J., et al. SPIRIT 2025 statement: updated guideline for protocols of randomised trials // BMJ. 2025. Vol. 389. Art. e081477. DOI: 10.1136/bmj-2024-081477. URL: https://www.bmj.com/content/389/bmj-2024-081477

39. Hemming K., Taljaard M., McKenzie J.E., et al. Reporting of stepped wedge cluster randomised trials: extension of the CONSORT 2010 statement with explanation and elaboration // BMJ. 2018. Vol. 363. Art. k1614. DOI: 10.1136/bmj.k1614. URL: https://www.bmj.com/content/363/bmj.k1614

40. Maxwell S.E., Cole D.A. Bias in cross-sectional analyses of longitudinal mediation // Psychological Methods. 2007. Vol. 12, no. 1. P. 23-44. DOI: 10.1037/1082-989X.12.1.23.

41. Burr H., Berthelsen H., Moncada S., et al. The Third Version of the Copenhagen Psychosocial Questionnaire // Safety and Health at Work. 2019. Vol. 10, no. 4. P. 482-503. DOI: 10.1016/j.shaw.2019.10.002. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6933167/

42. Novikova A.V., Shirokov V.A., Kuzmin S.V., Novikov A.A., Perevezentseva A.S. Validation of the Russian version of the Copenhagen Psychosocial Questionnaire // Journal of Occupational and Environmental Hygiene. 2026. Online ahead of print. P. 1-14. DOI: 10.1080/15459624.2026.2649753. URL: https://pubmed.ncbi.nlm.nih.gov/41980050/