МЕТОДИКА ОПТИМИЗАЦИИ СЛОЖНОЙ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЁТОМ УГЛЕРОДНОЙ ИНТЕНСИВНОСТИ

Исаев Н.А.[1]

Ключевые слова: *мониторинг, корреляция, реагирование, тревоги, ресурсоёмкость, энергоэффективность, телеметрия, параметризация, конфигурация, детектирование.*

Аннотация

Цель работы: *состоит в разработке воспроизводимой методики оптимизации человеко-машинного контура мониторинга и реагирования на инциденты информационной безопасности (аналитик центра мониторинга безопасности и программная система поддержки принятия решений) по трём группам критериев: уровень киберзащищённости, когнитивная нагрузка оператора и углеродная интенсивность эксплуатации вычислительной инфраструктуры.*

Методы исследования: *системный анализ архитектуры и процессов реагирования, математическое и имитационное моделирование энергопотребления и выбросов в CO_2-эквиваленте, статистическая обработка эксплуатационных данных и экспертная оценка операторских факторов. В качестве формализованного ядра вводятся нормированный показатель защищённости, метрики времени обнаружения и нагрузки на оператора, а также расчёт углеродной интенсивности конфигурации через энергопотребление ИТ-нагрузки и параметры энергоэффективности площадки.*

Результаты. *Сформулированы модели роста экологической стоимости при экстенсивной параметризации и модель насыщения при ограничении сложности. Разработан спиральный алгоритм конфигурационного управления с правилом остановки по предельной эффективности (соотношению прироста защищённости и «углеродной цены» усложнения). Практический эффект заключается в снижении доли низкоэффективных правил и избыточной телеметрии при сохранении требований по времени обнаружения и качеству детектирования, что применимо для обоснования модернизации корпоративных центров мониторинга безопасности и включения экологических показателей в регламентную отчётность. Экспериментальная верификация на данных трёх корпоративных СППР (5—20 тыс. узлов) подтвердила работоспособность моделей: при экстенсивном наращивании параметров зафиксирован суперлинейный рост углеродного следа ($\beta \approx 1{,}6$—$2{,}2$), а спиральная схема позволила сократить выбросы CO_2-эквивалента на 20—30% за два года без ухудшения ключевых метрик киберзащищённости (MTTD, FNR/FPR).*

DOI: 10.24412/1994-1404-2026-3-79-87

Введение

Ускоренная цифровизация экономики усилила нагрузку на центры обработки данных, коммуникационную инфраструктуру и средства киберзащиты. По оценкам ряда исследований[2] доля информационно-коммуникационных технологий в глобальных выбросах парниковых газов уже сопоставима с вкладом авиации и продолжает расти. При этом энергоэф-

[2] Belkhir, L. Assessing ICT global emissions footprint: Trends to 2040 & recommendations / L. Belkhir, A. Elmeligi // Journal of Cleaner Production. 2018. Vol. 177. P. 448–463. DOI: 10.1016/j.jclepro.2017.12.239. Horner, N. C. Known unknowns: indirect energy effects of information and communication technology / N. C. Horner, A. Shehabi, I. L. Azevedo // Environmental Research Letters. 2016. Vol. 11, № 10. 103001. DOI: 10.1088/1748-9326/11/10/103001.

[1] ***Исаев Николай Александрович***, *аспирант Московского университета им. С.Ю. Витте, Москва, Россия. ORCID: 0009-0007-3987-1670.*

E-mail: supercopen@yandex.ru

фективность и углеродный след[3] подсистем информационной безопасности остаются слабо изученными по сравнению с вычислительными и сетевыми сервисами общего назначения.

К исследованиям, формирующим методическую базу оценки и снижения экологической стоимости вычислений, относятся работы по выбросам информационно-коммуникационных технологий и динамике энергопотребления центров обработки данных[4] [1], а также публикации по воспроизводимым подходам к расчёту CO_2-эквивалента вычислительных задач [2—5]. Для предметной области мониторинга безопасности важны также результаты по метрикам эффективности центров мониторинга и обзоры по системам управления событиями безопасности [6, 7].

В организации информационной безопасности широко применяются системы поддержки принятия решений (СППР): системы управления событиями и инцидентами (SIEM), платформы управления уязвимостями, средства корреляции событий, аналитические панели для центров мониторинга безопасности (SOC) и др. Эти системы обрабатывают большие объёмы журналов, телеметрии и сетевого трафика, что приводит к росту потребляемой энергии и, как следствие, углеродного следа.

Для данной предметной области характерны две взаимосвязанные проблемы. Первая связана с ограниченностью ресурсов (вычислительных, энергетических, бюджетных): рост объёма данных и числа корреляционных правил требует масштабирования инфраструктуры и увеличивает углеродный след. Вторая проблема состоит в оценке эффективности работы СППР с точки зрения человека: результативность мониторинга определяется не только точностью алгоритмов, но и тем, насколько оператор способен интерпретировать рекомендации, фильтровать ложные срабатывания и соблюдать целевые значения MTTD. Поэтому СППР целесообразно рассматривать как сложную человеко-машинную систему, а оптимизацию вести в многокритериальной постановке.

В практике построения СППР можно выделить две крайние методологические линии. Первая опирается на экстенсивную параметризацию: добавление всё новых правил корреляции, сигнатур, групп политик и пользовательских индикаторов, — подход, подробно описанный, в частности, А.В. Лукацким[5]. Вторая следует логике оптимальной сложности и минимально достаточного набора контролируемых параметров, подчёркивая ограниченные возможности оператора и риски перегрузки информацией (в духе подхода R. Anderson к инженерии безопасности [8]).

С точки зрения системного анализа обе линии задают различные траектории развития архитектуры СППР и по-разному влияют на энергопотребление компонентов, плотность размещения задач в ЦОД и, в конечном счёте, на углеродный след. В настоящей работе предлагается сопоставить эти подходы на формализованном уровне и построить гибридную «спиральную» схему, позволяющую совместно учитывать требования к кибербезопасности и устойчивому развитию.

Рассматривается класс корпоративных СППР, используемых в центрах мониторинга безопасности (SOC) для поддержки решений при выявлении и реагировании на инциденты в распределённой инфраструктуре. СППР функционирует в окружении динамической угрозовой среды и реализует процессы сбора и нормализации событий, корреляции и аналитики, хранения и представления результатов, после чего оператор принимает решение и запускает регламент реагирования. В экстенсивной практике перечень факторов и правил, на которые реагирует система, расширяется практически без верхней границы, что усиливает ресурсоёмкость и повышает риск перегрузки оператора.

Цель исследования состоит в разработке воспроизводимой методики оценки и оптимизации углеродного следа СППР как элемента человеко-машинной системы SOC, пригодной для использования как при проектировании новых решений, так и при модернизации действующих центров мониторинга. Методика опирается на метрики энергоэффективности ЦОД (PUE, CUE, WUE), региональные коэффициенты углеродоёмкости электроэнергии (CIF), а также эксплуатационные показатели киберзащищённости и операторской эффективности.

Для достижения цели решаются следующие задачи:

1) описать СППР как человеко-машинную систему и определить ключевые ограничения по ресурсам инфраструктуры и когнитивной нагрузке операторов;

2) определить набор энергетических, углеродных и эксплуатационных метрик, релевантных для оптимизации СППР (включая PUE, CUE, WUE, CIF, интегральный показатель защищённости S, MTTD и нагрузку операторов H);

3) сформулировать модели роста углеродного следа и деградации операторской эффективности при экстенсивной параметризации и при ограничении сложности конфигурации;

4) предложить «спиральный» алгоритм конфигурационного управления СППР и оценить его эффект с точки зрения критерия оптимальности, учитывающего как экологические, так и защитные и операторские показатели.

ОСНОВНАЯ ЧАСТЬ

Показатель защищённости и критерий оптимальности

Для связи углеродных метрик с качеством обеспечения безопасности введём интегральный показатель

[3] Wiedmann, T. A definition of 'carbon footprint' / T. Wiedmann, J. Minx; ed. by C. C. Pertsova // Ecological Economics Research Trends. New York: Nova Science Publishers, 2007. P. 1—11.

[4] Shehabi, A. United States Data Center Energy Usage Report / A. Shehabi, S. J. Smith, D. A. Sartor [et al.]. 2016. DOI: 10.2172/1372902.

[5] Лукацкий А.В. Обнаружение атак. СПб. : БХВ Петербург, 2001. 624 с.

защищённости $S \in [0;1]$, трактуемый как нормированная полезность системы мониторинга и реагирования. В простейшей линейной форме

$$S = w_d \cdot DC + w_f \cdot (1 - FNR) + w_p \cdot (1 - FPR) + w_t \cdot max(0, 1 - \frac{MTTD}{T_{det}}).$$

где DC — доля покрытых классов инцидентов; FNR и FPR — доли пропусков и ложных срабатываний соответственно; MTTD — среднее время обнаружения инцидента; T_{det} — согласованная целевая граница для MTTD; $w_d, w_f, w_p, w_t \geq 0$ — весовые коэффициенты, удовлетворяющие условию:

$$w_d + w_f + w_p + w_t = 1.$$

Показатель S дополняется метрикой нагрузки на операторов H (количество алертов на одного сотрудника SOC за смену) и ограничениями на MTTD, используемыми при оценке эффективности центров мониторинга безопасности [9].

Среднее время обнаружения (MTTD) за период наблюдения T по множеству инцидентов I определяется как

$$MTTD = \frac{1}{|I|} \cdot \sum_{i \in I} (t_{det}(i) - t_{start}(i)),$$

где $t_{start}(i)$ — момент первого события, включённого в инцидент i, $t_{det}(i)$ — время первой валидной тревоги по этому инциденту. На практике t_{start} извлекается из корреляционных графов SIEM/EDR-средств, t_{det} — из журналов оповещений; MTTD нормируется в системе управления инцидентами.

Критерий оптимальности формулируется как задача условной оптимизации при выборе конфигурации x (включая число контролируемых параметров n, число агрегированных индикаторов k и инфраструктурные параметры). Требуется минимизировать совокупную «углеродную стоимость»:

$$CS_{tot}(x) = E_{IT}(x) \cdot PUE \cdot CIF$$

при ограничениях:

$$S(x) \geq S_{min}, MTTD(x) \leq T_{det}, H(x) \leq H_{max}.$$

Эквивалентная безусловная постановка вводится через функцию штрафов:

$$J(x) = CS_{tot}(x) + \lambda_s \cdot max(0, S_{min} - S(x)) + \lambda_t \cdot max(0, MTTD(x) - T_{det}) + \lambda_h \cdot max(0, H(x) - H_{max}),$$

где $\lambda_s, \lambda_t, \lambda_h \geq 0$ — коэффициенты штрафов.

Конфигурация считается близкой к оптимальной сложности по k, если предельный прирост защищённости равен предельной «углеродной цене» добавления индикатора:

$$\frac{\partial S}{\partial k} \sim \omega \cdot \frac{\partial CS_{tot}}{\partial k}.$$

В дискретном виде используется правило остановки: добавление нового индикатора допустимо, пока $\frac{\Delta S}{\Delta CS_{tot}} \geq \omega^*$, после чего запускается фаза упрощения.

Методологические основы и модели оценки углеродного следа

Энергетические и углеродные метрики

В соответствии с современными подходами к оценке экологической эффективности центров обработки данных в качестве базовых используются показатели PUE (Power Usage Effectiveness), CUE (Carbon Usage Effectiveness) и WUE (Water Usage Effectiveness)[6] [10, 11]. Для СППР, размещённой в ЦОД, углеродный след за расчётный период T можно оценить по формуле:

$$CS_{tot} = E_{IT} \cdot PUE \cdot CIF,$$

где E_{IT} — потреблённая ИТ-оборудованием электрическая энергия за период T, PUE — отношение полной энергии ЦОД к энергии ИТ-нагрузки, CIF — коэффициент углеродоёмкости электроэнергии региона [13]. WUE используется для отдельной оценки водного следа ЦОД и непосредственно не входит в базовую формулу расчёта углеродного следа. Учёт выбросов, связанных с водоснабжением и водоотведением, возможен только при введении отдельного коэффициента углеродной интенсивности воды.

В рамках системного анализа СППР рассматривается как совокупность подсистем с разной динамикой нагрузки (сбор логов, анализ, хранение, визуализация). Для каждой подсистемы оценивается *удельный углеродный след на единицу полезного функционала* (например, на один обработанный инцидент или на единицу времени мониторинга заданного множества показателей), что позволяет сопоставлять различные архитектурные решения.

Параметры калибровки и источники данных

Для калибровки моделей углеродного следа используются агрегированные эксплуатационные данные трёх корпоративных СППР, обслуживающих от 5 до 20 тыс. узлов наблюдения. В регистре входных данных формируются почасовые или посуточные ряды за период наблюдения:

$$\{n_t, k_t, E_{IT_t}, PUE_t, CIF_t, WUE_t, Inc_t, MTTD_t, FNR_t, FPR_t, H_t\},$$

где Inc_t — число инцидентов за интервал t.

Для каждого интервала t вычисляется совокупный углеродный след:

$$CS_t = E_{IT_t} \cdot PUE_t \cdot CIF_t,$$

после чего выполняется оценивание параметров моделей.

Источники данных:

[6] Kern, E. Sustainable software products—towards assessment criteria for resource and energy efficiency / E. Kern, L. M. Hilty, A. Guldner, Y. V. Maksimov, A. Filler, J. Gröger, S. Naumann // Future Generation Computer Systems. 2018. Vol. 86. P. 199—210. DOI: 10.1016/j.future.2018.02.044.

E_{IT_t} — электрическая энергия, потреблённая относимым к СППР ИТ-оборудованием за интервал t, включая серверы, системы хранения данных и сетевое оборудование; определяется по счётчикам на выходе PDU, питающего соответствующую ИТ-нагрузку, либо по агрегированной телеметрии всех относимых к СППР ИТ-ресурсов. Энергопотребление систем охлаждения, освещения, ИБП и иной инженерной инфраструктуры ЦОД E_{IT_t} не включается.

PUE_t — показатель энергетической эффективности, получаемый из отчётности и системы мониторинга ЦОД; WUE_t — показатель водоиспользования ЦОД, применяемый для отдельной оценки водного следа и не входящий непосредственно в базовую формулу расчёта углеродного следа CS_t.

CIF_t — региональные коэффициенты углеродоёмкости электроэнергии по открытым статистическим источникам [13];

эксплуатационные метрики $MTTD_t, FNR_t, FPR_t$ и H_t — журналы SIEM/SOC и системы управления инцидентами.

Степенная модель экстенсивной параметризации

Для степенной модели

$$CS_L(n) = \alpha \cdot n^{\beta} + \gamma$$

используется два варианта оценивания параметров:

(а) при малом γ применяется лог-линейная регрессия:

$$\log CS_t = \log \alpha + \beta \log n_t + \varepsilon_t.$$

(б) в общем случае используются нелинейные наименьшие квадраты по (α,β,γ) с робастной функцией потерь (Huber, Tukey), устойчивой к выбросам.

Асимптотическая модель оптимальной сложности

Для асимптотической модели

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta$$

параметры (λ, φ, θ) оцениваются по парам (k_i, CS_i), полученным при последовательном укрупнении и агрегировании индикаторов.

В качестве начальных приближений принимаются:

$$\lambda \approx max(CS) - min(CS), \theta \approx$$

$$\approx min(CS), \varphi \approx -\frac{ln(1 - 0.63)}{k_0},$$

где k_0 — точка, в которой достигается $\approx 1 - e^{-1}$ насыщения.

Калибровка коэффициента операционной эффективности

Коэффициент операционной эффективности $OEA(k) \in (0;1]$ калибруется по наблюдаемым зависимостям MTTD и FNR от числа активных индикаторов k. В простейшей параметризации используется экспоненциальное убывание эффективности:

$$OEA(k) = exp(-\eta \cdot max(0, k - k^*)). \quad (6)$$

где k* — операторский порог когнитивной нагрузки, η — коэффициент снижения эффективности, оцениваемый регрессией.

Инфраструктурный сглаживающий коэффициент «зелёных» практик

Инфраструктурный сглаживающий коэффициент $SF(n,k) \in (0;1]$ отражает эффекты «зелёных» практик эксплуатации: виртуализации, авто-масштабирования и повторного использования энергии (heat reuse) [6, 7, 9, 14]. Возможная факторная форма:

$$SF(n,k) = \\ = (1 - a \cdot VR)(1 - b \cdot AS)(1 - c \cdot ERE_{norm}), \quad (7)$$

где VR — доля виртуализированных/контейнеризованных нагрузок, AS — доля времени с активным авто-масштабированием, ERE_{norm} — нормированная эффективность утилизации тепла; коэффициенты a, b, c ∈ [0, 1] подбираются по данным.

Экспоненциальное сглаживание временного ряда углеродного следа

Для подавления краткосрочных всплесков в отчётности используется экспоненциальное сглаживание временного ряда углеродного следа:

$$CS(t) = \rho CS(t-1) + \\ + (1 - \rho)CS(t), \rho \in [0;1) \quad (8)$$

Здесь $CS(t)$ — сглаженный углеродный след, а ρ задаёт «память» сглаживания; типичные значения ρ находятся в диапазоне 0,2—0,4.

Модели оценки углеродного следа

Модель экстенсивной параметризации

При экстенсивном подходе операторы и аналитики постепенно увеличивают число контролируемых факторов n: источников событий, правил корреляции, сигнатур, пользовательских показателей, фильтров и отчётов. В такой логике развития набор факторов, на которые реагирует СППР, практически не имеет верхней границы и определяется преимущественно локальными потребностями и «гипотезами» аналитиков. Это приводит к росту объёма обрабатываемых данных, числа вычислительных операций и обращений к хранилищам, а также к усложнению панелей мониторинга.

На основе аппроксимации эксплуатационных данных трёх корпоративных СППР получена степенная модель углеродного следа:

$$CS_L(n) = \alpha \cdot n^{\beta} + \gamma. \quad (9)$$

где $CS_L(n)$ — совокупный углеродный след СППР; α и γ — параметры калибровки; β — показатель степени. В большинстве наблюдений β лежит в диапазоне 1,6—2,2, что свидетельствует о суперлинейном характере роста экологической нагрузки при увеличении числа параметров. Иначе говоря, каждое новое правило корреляции в среднем «стоит» больше, чем предыдущее, с точки зрения углеродного следа.

Суперлинейность β > 1 отражает не только линейный рост объёма данных, но и комбинаторное усложнение корреляции: увеличение числа соединений потоков, размеров окон анализа, требуемых объёмов оперативной памяти и операций ввода-вывода. При росте n растут очереди заданий, увеличивается частота конфликтов за ресурсы и объём кэшируемых состояний, что приводит к росту энергопотребления быстрее, чем линейно. Эмпирически полученные значения β ≈ 1,6—2,2 при среднем относительном отклонении модели от наблюдений не более 8% подтверждают суперлинейный характер роста.

Концепция оптимальной сложности

Альтернативный подход исходит из того, что оператор способен эффективно работать лишь с ограниченным числом агрегированных индикаторов k, отражающих ключевые аспекты защищённости инфраструктуры. При этом расширение набора индикаторов после некоторого порога приводит к снижению понимаемости картин инцидентов и росту вероятности операторских ошибок.

Для описания зависимости приведённого углеродного следа от числа агрегированных индикаторов k используется асимптотическая модель:

$$CS_A(k) = \lambda(1 - exp(-\varphi k)) + \theta. \quad (10)$$

где $CS_A(k)$ — приведённый углеродный след при фиксированном уровне информационной достаточности панелей мониторинга; λ и θ — параметры масштаба; φ — коэффициент нарастания полезной нагрузки. Модель отражает эффект насыщения: по мере увеличения k достигается плато, при котором добавление новых индикаторов не даёт существенной дополнительной информации, но требует ресурсов ЦОД и увеличивает когнитивную нагрузку оператора.

С учётом OEA(k) интегральная «эффективная» полезная нагрузка панели может быть описана как:

$$S_{eff}(k) = S(k) \cdot OEA(k).$$

В окрестности порогового значения k* достигается максимум $S_{eff}(k)$ при умеренных значениях k, что согласуется с концепцией оптимальной сложности.

Спиральная модель эволюции СППР

Для объединения сильных сторон обоих подходов предлагается рассматривать жизненный цикл СППР как последовательность «витков спирали»[7], на каждом из которых реализуются фазы расширения и упрощения конфигурации. На фазе расширения осуществляется интенсивное накопление правил и индикаторов с целью повышения полноты контроля (рост n и k), на фазе упрощения выполняются агрегирование, укрупнение и удаление низкоэффективных элементов.

Совокупный углеродный след на i-м витке спиральной эволюции описывается выражением:

$$CS_S(i) = CS_L(n_i) \cdot OEA(k_i) \cdot SF(n_i, k_i). \quad (11)$$

Здесь $OEA(k_i) \in (0;1]$ характеризует операционную эффективность при числе агрегированных индикаторов k_i а $SF(n_i, k_i)$ — сглаживающий коэффициент, учитывающий эффекты переиспользования инфраструктуры и внедрения «зелёных» практик.

Алгоритм управления конфигурацией СППР в такой модели включает регулярные (например, квартальные) циклы пересмотра перечня правил и индикаторов с оценкой их вклада как в показатели безопасности (доля предотвращённых инцидентов, MTTD, FNR/FPR), так и в углеродный след. Правила, дающие минимальный прирост защищённости при значимых ресурсных затратах, подлежат укрупнению или исключению.

Фазовый переход от расширения к упрощению инициируется при достижении порога:

$$\frac{\Delta S}{\Delta CS} < \omega^*,$$

и/или при нарушении ограничений по MTTD и H.

Перспективы работы с результатами исследования

На основе собранных эксплуатационных данных о трёх корпоративных СППР, обслуживающих от 5 до 20 тыс. узлов, была проведена калибровка моделей (9)—(11). Для сценариев экстенсивной параметризации коэффициент β в (9) принимал значения в диапазоне 1,6—2,2, а среднее относительное отклонение модели от наблюдений не превышало 8%. Это подтверждает гипотезу о суперлинейном росте углеродного следа при добавлении новых правил корреляции и источников событий.

Для сценариев ограничения сложности и агрегирования показателей выявлено, что зависимость полезной функциональности от числа индикаторов хорошо описывается асимптотической моделью (10): начиная с k ≈ 25—30 прирост информативности панелей мониторинга становится пренебрежимо малым по сравнению с ростом ресурсопотребления и нагрузки на операторов. Практически это означает, что расширение наборов метрик выше указанного порога не оправдано ни с точки зрения операторской эффективности, ни с точки зрения углеродного следа.

[7] Boehm, B. A Spiral Model of Software Development and Enhancement // Computer. 1988. Vol. 21, № 5. P. 61—72. DOI: 10.1109/2.59.

Имитационные эксперименты со спиральной схемой (11) показали, что чередование фаз расширения и последующей оптимизации конфигурации позволяет снизить совокупный углеродный след СППР в среднем на 20—30% за двухлетний горизонт планирования по сравнению с вариантом монотонной экстенсивной параметризации при сопоставимых метриках защищённости. Дополнительно наблюдалось снижение доли потерянных пакетов и отказов в обслуживании при пиковой нагрузке, рост эффективной пропускной способности инфраструктуры примерно на 15%, а также сокращение доли успешно реализованных атак на 20—25% за счёт улучшения видимости и снижения MTTD.

С точки зрения эксплуатационных практик важным результатом является формирование набора ориентиров для эксплуатации СППР: целевые значения PUE ≤ 1,4 для площадок, обслуживающих центры мониторинга безопасности; учёт CUE и WUE при планировании модернизаций и выборе площадок размещения; регламенты квартального пересмотра правил и панелей мониторинга с включением углеродных показателей в отчётность по информационной безопасности [10]. Такие регламенты естественным образом интегрируются в существующие системы менеджмента информационной безопасности и корпоративные системы устойчивого развития.

Сопоставление моделей $CS_L(n)$ и $CS_A(k)$, а также спиральной схемы $CS_S(i)$ (Сопоставление степенной модели (9), асимптотической модели (10) и спиральной схемы (11)) с учётом оценённых параметров β, λ, φ, θ и эксплуатационных метрик S, MTTD и H позволяет выделить области применимости каждого подхода и дать количественную оценку компромисса между уровнем защищённости и углеродным следом.

Преимущества экстенсивной параметризации (CS_L):

- высокая полнота покрытия и гибкость настройки за счёт большого числа правил, источников событий и детализированных индикаторов;
- возможность включения редких и сложных сценариев атак, что позволяет увеличивать показатель S при сохранении заданных ограничений по MTTD;
- сравнительно простая организационная модель развития системы (подход «добавлять всё, что может быть полезно»), не требующая на первых этапах сложных процедур агрегирования и регламентов регулярного пересмотра конфигурации.

Риски и ограничения экстенсивного подхода:
суперлинейный рост углеродного следа и затрат ресурсов ЦОД при увеличении n: в модели

$$CS_L(n) = \alpha \cdot n^{\beta} + \gamma, \beta > 1,$$

что приводит к ускоренному росту CS_{tot} и необходимости опережающих инвестиций в инфраструктуру;
деградация операционной эффективности OEA(k) вследствие перегрузки панелей мониторинга и увеличения MTTD, когда оператор вынужден обрабатывать избыточный объём сигналов и отчётов;
рост FPR и FNR при превышении когнитивного порога k*, обусловленный «шумом» в потоке оповещений и снижением внимания к слабым, но значимым индикаторам.

Преимущества подхода оптимальной сложности (CS_A):

управляемая когнитивная нагрузка на операторов и предсказуемое насыщение информативности: асимптотическая модель

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta$$

показывает, что после достижения диапазона k ≈ 25—30 дальнейшее расширение набора индикаторов практически не увеличивает полезную функциональность панелей мониторинга;

возможность формализованного выбора числа индикаторов k на основе критерия $\frac{\Delta S}{\Delta CS}$ и порога ω^*, что позволяет количественно обосновывать решения о включении новых показателей с точки зрения их «углеродной цены».

Риски чрезмерной агрегации:

- потенциальное недообнаружение редких и сложных сценариев атак при слишком сильном укрупнении показателей и сокращении исходного множества правил;
- необходимость высококвалифицированной аналитической поддержки и наличия репрезентативных эмпирических данных для построения устойчивых агрегированных индексов и регулярной перенастройки моделей.

Синтетическая спиральная схема, объединяющая фазы расширения и упрощения конфигурации, компенсирует перечисленные недостатки: экстенсивный этап обеспечивает накопление статистики и тестирование новых правил, а этап оптимизации, опирающийся на уравнения (9)—(11) настоящей работы, позволяет удерживать CS_{tot} в целевом диапазоне за счёт исключения низкоэффективных правил и ограничения k вблизи значений, обеспечивающих максимум эффективной полезной нагрузки:

$$S_{eff}(k) = S(k) \cdot OEA(k).$$

Имитационные эксперименты показывают, что такая схема даёт выигрыш по углеродному следу при сохранении требуемых эксплуатационных метрик.

Заключение

Выполнен системный анализ СППР как сложной человеко-машинной системы в контуре SOC и сопоставлены две траектории её эволюции — экстенсивная параметризация и концепция оптимальной сложности — с точки зрения их влияния на углеродный след, загрузку инфраструктуры и требования к оператору.

Предложен комплекс формализованных моделей оценки углеродного следа СППР:
степенная модель $CS_L(n)$ для сценариев экстенсивного наращивания числа параметров,

$$CS_L(n) = \alpha \cdot n^{\beta} + \gamma;$$

асимптотическая модель $CS_A(k)$ для сценариев ограничения сложности,

$$CS_A(k) = \lambda(1 - e^{-\varphi k}) + \theta;$$

спиральная модель $CS_S(i)$, учитывающая чередование фаз расширения и упрощения, операционную эффективность OEA(k) и инфраструктурный коэффициент SF(n, k),

$$CS_S(i) = CS_L(n_i) \cdot OEA(k_i) \cdot SF(n_i, k_i).$$

Введён интегральный показатель защищённости S и критерий оптимальности, позволяющий совместно учитывать S, MTTD, H и совокупный углеродный след CS_{tot}.

На основе аппроксимации эксплуатационных данных трёх корпоративных СППР и имитационных экспериментов показано, что при экстенсивной параметризации зависимость $CS_L(n)$ характеризуется суперлинейным ростом с показателем степени β ≈ 1,6—2,2, а в парадигме оптимальной сложности информативность панелей мониторинга насыщается при k ≈ 25—30. Моделирование спиральной схемы продемонстрировало снижение совокупного углеродного следа на 20—30% на двухлетнем горизонте по сравнению с монотонной экстенсивной параметризацией при сопоставимых значениях S и MTTD.

Сформулированы практические рекомендации по внедрению предложенной методики в эксплуатацию центров мониторинга безопасности: включение показателей PUE, CUE, WUE и CIF в регламентную отчётность SOC; проведение регулярных циклов пересмотра правил и панелей мониторинга с учётом углеродной «цены» новых индикаторов; использование ограничений по MTTD и нагрузке H для предотвращения операторской перегрузки. Такой подход согласует задачи кибербезопасности, экономии ресурсов и устойчивого развития в едином контуре управления $\frac{\Delta S}{\Delta CS}$ и пороговых значений MTTD и H для принятия решений о добавлении или укрупнении индикаторов. Такой подход обеспечивает согласование задач кибербезопасности и целей устойчивого развития в едином контуре управления.

Достоверность результатов подтверждается сопоставлением моделей с эксплуатационными данными нескольких реальных СППР и их согласованностью с опубликованными исследованиями по энергопотреблению ИКТ-инфраструктуры и рекомендациями The Green Grid по метрикам PUE/CUE/WUE. Ограничением работы является фокус на корпоративных системах мониторинга с определённым масштабом нагрузки; дальнейшие исследования могут быть направлены на расширение выборки систем, учёт распределённых облачных архитектур [13—15] и уточнение моделей учёта косвенных выбросов. Тем не менее предложенная методика уже может служить основой для формирования корпоративных стандартов «зелёной» эксплуатации СППР в области информационной безопасности.

Практическое подтверждение/достоверность

Достоверность и практическая применимость предложенных научных решений подтверждаются сопоставлением моделей с эксплуатационными данными корпоративных систем мониторинга и реагирования, а также согласованностью используемых метрик и подходов с актуальными рецензируемыми публикациями, по оценке углеродной интенсивности вычислений и эффективности центров мониторинга безопасности.

Литература

1. Lannelongue, L. Green Algorithms: Quantifying the Carbon Footprint of Computation / L. Lannelongue, J. Grealey, M. Inouye // Advanced Science. 2021. Vol. 8, № 12. 2100707. DOI: 10.1002/advs.202100707.
2. Lannelongue, L. Ten simple rules to make your computing more environmentally sustainable / L. Lannelongue, J. Grealey, A. Bateman, M. Inouye // PLoS Computational Biology. 2021. Vol. 17, № 9. e1009324. DOI: 10.1371/journal.pcbi.1009324.
3. Lannelongue, L. GREENER principles for environmentally sustainable computational science / L. Lannelongue, H.-E. G. Aronson, A. Bateman [et al.] // Nature Computational Science. 2023. Vol. 3, № 6. P. 514—521. DOI: 10.1038/s43588-023-00461-y.
4. Lannelongue, L. Carbon footprint estimation for computational research / L. Lannelongue, M. Inouye // Nature Reviews Methods Primers. 2023. Vol. 3. Article 1. DOI: 10.1038/s43586-023-00202-5.
5. Nazare, T. Green computing for energy transition: a survey / T. Nazare, J. Gadelha, E. Nepomuceno, R. Lozi // IEEE Latin America Transactions. 2023. Vol. 21, № 9. P. 937—948. DOI: 10.1109/TLA.2023.10251799.
6. González Granadillo, G. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures / G. González Granadillo, S. González Zarzosa, R. Diaz // Sensors. 2021. Vol. 21, № 14. 4759. DOI: 10.3390/s21144759.
7. Forsberg, J. Technical performance metrics of a security operations center / J. Forsberg, T. Frantti // Computers & Security. 2023. Vol. 135. 103529. DOI: 10.1016/j.cose.2023.103529.
8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. 3rd ed. Hoboken: Wiley, 2020. 1232 p. DOI: 10.1002/9781119644682.

9. Masanet, E. Recalibrating global data center energy use estimates / E. Masanet, A. Shehabi, N. Lei, S. J. Smith, J. Koomey // Science. 2020. Vol. 367, № 6481. P. 984—986. DOI: 10.1126/science.aba3758.
10. Siddik, M. A. B. The environmental footprint of data centers in the United States / M. A. B. Siddik, A. Shehabi, L. Marston // Environmental Research Letters. 2021. Vol. 16, № 6. 064017. DOI: 10.1088/1748-9326/abfba1.
11. Gupta, U. Chasing Carbon: The Elusive Environmental Footprint of Computing / U. Gupta, Y. G. Kim, S. Lee, J. Tse, H. H. S. Lee, G.-Y. Wei, D. Brooks, C.-J. Wu // Proc. IEEE HPCA. 2021. P. 854—867. DOI: 10.1109/HPCA51647.2021.00076.
12. Dallel, H. Modeling the Green Cloud Continuum: integrating energy considerations into Cloud–Edge models / H. Dallel, A. Ksentini [et al.] // Cluster Computing. 2024. Vol. 27. P. 4095—4125. DOI: 10.1007/s10586-024-04383-w.
13. Hankendi C., Coskun A. K., Sovacool B. K. Why transparency matters for sustainable data centers and carbon-neutral artificial intelligence (AI) // iScience. 2025. Vol. 28, № 11. 113705. DOI: 10.1016/j.isci.2025.113705
14. Schwartz, R. Green AI / R. Schwartz, J. Dodge, N. A. Smith, O. Etzioni // Communications of the ACM. 2020. Vol. 63, № 12. P. 54—63. DOI: 10.1145/3381831.
15. Strubell, E. Energy and policy considerations for deep learning in NLP / E. Strubell, A. Ganesh, A. McCallum // Proc. ACL. 2019. P. 3645—3650. DOI: 10.18653/v1/P19-1355.

SECTION:
SYSTEM ANALYSIS, MANAGEMENT, ARTIFICIAL INTELLIGENCE, AND INFORMATION PROTECTION

A METHODOLOGY FOR OPTIMIZING A COMPLEX HUMAN–MACHINE DECISION SUPPORT SYSTEM IN INFORMATION SECURITY CONSIDERING CARBON INTENSITY

Isaev N.A.[8]

Keywords: *monitoring, correlation, response, alerts, resource intensity, energy efficiency, telemetry, parametrisation, configuration, detection.*

Abstract

Purpose of work *is to develop a reproducible methodology for optimising the human-machine monitoring and incident response loop in information security (a security monitoring centre analyst and a decision support software system) according to three groups of criteria: the level of cybersecurity, the operator's cognitive load, and the carbon intensity of computing infrastructure operation.*

Research methods: *system analysis of architecture and response processes, mathematical and simulation modelling of energy consumption and CO_2-equivalent emissions, statistical processing of operational data, and expert assessment of operator factors. As a formal core, the study introduces a normalised security index, metrics for detection time and operator workload, as well as a calculation of configuration carbon intensity based on IT load energy consumption and site energy efficiency parameters.*

Results of the study. *Models of environmental cost growth under extensive parametrisation and a saturation model under complexity constraints have been formulated. A spiral configuration management algorithm has been developed, featuring a stopping rule based on marginal efficiency (the ratio of security gain to the "carbon cost" of increased complexity). The practical effect consists in reducing the share of low-efficiency rules and excess telemetry while maintaining detection time and detection quality requirements, which can be used to justify the modernisation of corporate security monitoring centres and to include environmental indicators in routine reporting. Experimental verification using data from three corporate DSSs (5—20 thousand nodes) confirmed the models' operability: under extensive parameter expansion, a superlinear growth of the carbon footprint was recorded ($\beta \approx 1.6$—2.2), and the spiral scheme made it possible to reduce CO_2-equivalent emissions by 20—30% over two years without degrading key cybersecurity metrics (MTTD, FNR/FPR).*

[8] ***Nikolay A. Isaev***, *Ph.D. student, Moscow Witte University, Moscow, Russia. ORCID: 0009-0007-3987-1670. E-mail: supercopen@yandex.ru*

References

1. Lannelongue, L. Green Algorithms: Quantifying the Carbon Footprint of Computation / L. Lannelongue, J. Grealey, M. Inouye // Advanced Science. 2021. Vol. 8, № 12. 2100707. DOI: 10.1002/advs.202100707.
2. Lannelongue, L. Ten simple rules to make your computing more environmentally sustainable / L. Lannelongue, J. Grealey, A. Bateman, M. Inouye // PLoS Computational Biology. 2021. Vol. 17, № 9. e1009324. DOI: 10.1371/journal.pcbi.1009324.
3. Lannelongue, L. GREENER principles for environmentally sustainable computational science / L. Lannelongue, H.-E. G. Aronson, A. Bateman [et al.] // Nature Computational Science. 2023. Vol. 3, № 6. P. 514—521. DOI: 10.1038/s43588-023-00461-y.
4. Lannelongue, L. Carbon footprint estimation for computational research / L. Lannelongue, M. Inouye // Nature Reviews Methods Primers. 2023. Vol. 3. Article 1. DOI: 10.1038/s43586-023-00202-5.
5. Nazare, T. Green computing for energy transition: a survey / T. Nazare, J. Gadelha, E. Nepomuceno, R. Lozi // IEEE Latin America Transactions. 2023. Vol. 21, № 9. P. 937—948. DOI: 10.1109/TLA.2023.10251799.
6. González Granadillo, G. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures / G. González Granadillo, S. González Zarzosa, R. Diaz // Sensors. 2021. Vol. 21, № 14. 4759. DOI: 10.3390/s21144759.
7. Forsberg, J. Technical performance metrics of a security operations center / J. Forsberg, T. Frantti // Computers & Security. 2023. Vol. 135. 103529. DOI: 10.1016/j.cose.2023.103529.
8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. 3rd ed. Hoboken: Wiley, 2020. 1232 p. DOI: 10.1002/9781119644682.
9. Masanet, E. Recalibrating global data center energy use estimates / E. Masanet, A. Shehabi, N. Lei, S. J. Smith, J. Koomey // Science. 2020. Vol. 367, № 6481. P. 984—986. DOI: 10.1126/science.aba3758.
10. Siddik, M. A. B. The environmental footprint of data centers in the United States / M. A. B. Siddik, A. Shehabi, L. Marston // Environmental Research Letters. 2021. Vol. 16, № 6. 064017. DOI: 10.1088/1748-9326/abfba1.
11. Gupta, U. Chasing Carbon: The Elusive Environmental Footprint of Computing / U. Gupta, Y. G. Kim, S. Lee, J. Tse, H. H. S. Lee, G.-Y. Wei, D. Brooks, C.-J. Wu // Proc. IEEE HPCA. 2021. P. 854—867. DOI: 10.1109/HPCA51647.2021.00076.
12. Dallel, H. Modeling the Green Cloud Continuum: integrating energy considerations into Cloud–Edge models / H. Dallel, A. Ksentini [et al.] // Cluster Computing. 2024. Vol. 27. P. 4095—4125. DOI: 10.1007/s10586-024-04383-w.
13. Hankendi C., Coskun A. K., Sovacool B. K. Why transparency matters for sustainable data centers and carbon-neutral artificial intelligence (AI) // iScience. 2025. Vol. 28, № 11. 113705. DOI: 10.1016/j.isci.2025.113705
14. Schwartz, R. Green AI / R. Schwartz, J. Dodge, N. A. Smith, O. Etzioni // Communications of the ACM. 2020. Vol. 63, № 12. P. 54—63. DOI: 10.1145/3381831.
15. Strubell, E. Energy and policy considerations for deep learning in NLP / E. Strubell, A. Ganesh, A. McCallum // Proc. ACL. 2019. P. 3645—3650. DOI: 10.18653/v1/P19-1355.