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

МЕТОД ВЫБОРА ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ МЕР РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

А. В. Кузнецов[1,2*]

[1]ООО «РТК ИБ», Москва, Россия

[2]Финансовый университет при Правительстве Российской Федерации, Москва, Россия

✉ *1283_my@mail.ru

ДЛЯ ЦИТИРОВАНИЯ

Кузнецов А. В. Метод выбора технической реализации мер реагирования на инциденты // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 22–31. DOI: 10.66424/2071-8217-2026-2-2

ПОСТУПИЛА 16.02.2026
ПРИНЯТА 27.04.2026
ОПУБЛИКОВАНА 15.06.2026

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Принимая во внимание возрастающее значение своевременности реагирования на инциденты информационной безопасности предложен метод выбора технической реализации мер реагирования на инциденты информационной безопасности без участия группы реагирования. Метод принимает во внимание заданные ограничения на предоставленные манданты и покрытие средствами реагирования. В рамках метода, в отличие от известных, рассматривается задача выбора как задача целочисленного (булевого) линейного программирования, в которой члены целевой функции являются логическими переменными, учитывающими логические действия по локализации инцидентов информационной безопасности, предусмотренные планами реагирования. Применение метода позволяет минимизировать время, затрачиваемое на локализацию инцидентов информационной безопасности.

КЛЮЧЕВЫЕ СЛОВА

Средство реагирования, группа реагирования, локализация (сдерживание) инцидента, автоматическое реагирование, мандат на действие, план реагирования

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

THE METHOD FOR SELECTING TECHNICAL IMPLEMENTATION OF INCIDENT RESPONSE MEASURES

A. V. Kuznetsov[1,2*]

[1]RTK IB LLC, Moscow, Russia

[2]Financial University under the Government of the Russian Federation, Moscow, Russia

✉ *1283_my@mail.ru

FOR CITATION

Kuznetsov A. V. The method for selecting technical implementation of incident response measures. *Problems of information security. Computer systems*. 2026. No. 2, pp. 22–31. DOI: 10.66424/2071-8217-2026-2-2 (In Russian)

ABSTRACT

Considering the increasing importance of timely response to information security incidents, the method for selecting technical implementation of information security incident response measures without the involvement of a response team is proposed. The method considers specified constraints on provided mandates and the coverage of response tools. Unlike known methods, this method considers the selection problem as an integer (boolean) linear programming problem. The terms of the objective function are logical variables for the infor-

RECEIVED 16.02.2026
ACCEPTED 27.04.2026
PUBLICATION 15.06.2026

mation security incident localization that included into response plans. Thereby minimizing the time spent for information security incident localization.

KEYWORDS

Response tool, response team, incident (containment) localization, automated response, action mandate, response plan

1. ВВЕДЕНИЕ

По итогам 2025 г. сразу несколько российских организаций, специализирующихся на оказании услуг по контролю и анализу защищенности информационных (компьютерных) систем, отметили, что современные атакующие (нарушители) все чаще преследуют цель полного уничтожения информационной инфраструктуры и накопленных в ней данных, в том числе резервных копий [1, 2].

В сложившейся ситуации обеспечение своевременности и корректности технической реализации мер реагирования на инциденты информационной безопасности (ИБ), возникающие вследствие компьютерных атак (кибератак), является актуальным направлением исследований. При этом стоит отметить, что для технической реализации мер реагирования на возникающие инциденты ИБ в организациях могут применяться различные средства реагирования. К таким средствам можно отнести как специализированные средства защиты информации (Endpoint Detection and Response, Network Detection and Response, Extended Detection and Response) [3], так и встроенные в общесистемное или прикладное программное обеспечение (ПО) механизмы управления и защиты информации (табл. 1). Например, сетевая изоляция хоста компьютерной сети может быть реализована

Таблица 1 | Сравнение средств реагирования

Table 1 | Comparison of response tools

Наименование средства	Область применения	Основные возможности по локализации
Endpoint Detection and Response	Серверы и рабочие станции (общесистемное ПО)	•Остановка служб, процессов; • изолирование «зараженных» объектов; • сетевая изоляция
Network Detection and Response	Каналы связи	• Запрет (блокирование, ограничение) прохождения сетевого трафика; • сетевая изоляция
Extended Detection and Response	Серверы и рабочие станции (общесистемное ПО), каналы связи	• Остановка служб, процессов; • изолирование «зараженных» объектов; • сетевая изоляция; • запрет (блокирование, ограничение) прохождения сетевого трафика
Межсетевые экраны уровня сети (тип «А»), веб-сервера (тип «Г»), узла (тип «В»)	Периметр сети, веб-сайты, серверы и рабочие станции	Запрет (блокирование, ограничение) прохождения сетевого трафика
Средства антивирусной защиты (типы «Б», «В», «Г»)	Серверы и рабочие станции	• Удаление вредоносного ПО; • изолирование «зараженных» объектов
Встроенные механизмы управления доступом общесистемного или прикладного ПО	Общесистемное ПО, прикладное ПО	• Блокировка учетных записей; • ограничение прав учетных записей; • остановка служб, процессов

различными средствами реагирования: встроенными или наложенными персональными межсетевыми экранами, активным сетевым оборудованием или сетевыми средствами защиты информации. Другой пример – блокировка скомпрометированной учетной записи, которая может быть реализована различными техническими способами: временная блокировка или постоянное отключение в централизованной службе каталогов (Directory Service, DS) или в системе класса Identity and Access Management (IdM), перенос в специальную группу или назначение специальной роли в DS, IdM и/или в прикладном ПО, дополнительно могут быть сброшены открытые сетевые сессии, а также изменен пароль или другой аутентификатор. Поддерживать различные технические варианты реагирования затратно, требуется время и профильная экспертиза, также обычно каждый коннектор к средству реагирования лицензируется отдельно [4], т.е. целесообразно минимизировать их количество.

На практике для выбора того или иного технического действия даже при наличии плана (сценария) реагирования применяются экспертные методы и системы [5, 6], напрямую зависящие от квалификации привлекаемых членов (экспертов) групп реагирования на инциденты ИБ. Применение экспертных методов усугубляется дефицитом кадров в области обеспечения ИБ [7] и не всегда позволяет обеспечивать воспроизводимость принимаемых решений, особенно при высокой вариативности технических действий. Это не позволяет перевести реализацию мер реагирования на возникающие инциденты ИБ в автоматический режим, т.е. без участия сил групп реагирования на инциденты ИБ [8]. Особенно актуальна данная ситуация в масштабах крупных территориально распределенных гетерогенных информационных инфраструктур, где квалификация и доступность членов групп реагирования на инциденты ИБ может разниться от площадки к площадке. Таким образом, задача оптимального выбора технического действия в рамках реагирования является актуальной и требует решения путем формирования метода выбора технической реализации мер реагирования на возникающие инциденты ИБ, направленного на минимизацию участия сил групп реагирования на инциденты ИБ и сокращение времени реагирования.

В рамках исследования будут приняты следующие ограничения:

• не рассматривается задача формирования планов (сценариев) реагирования, они выступают исходными данными, содержащими логические действия, такие как изоляция хоста компьютерной сети, блокировка скомпрометированной учетной записи, завершение работы приложения и т.п. (требования к содержанию планов реагирования определены ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами»);

• в части мер реагирования на инциденты ИБ рассматриваются только действия по локализации (сдерживанию) инцидентов ИБ, направленные на активное противодействие атакующему [9] (методы и средства расследования инцидентов ИБ не рассматриваются);

• локализация предусмотрена только для подтвержденных инцидентов ИБ, не требующих дополнительного расследования [10] (методы и средства подтверждения инцидентов ИБ не рассматриваются);

• исследование инвариантно к используемому терминологическому аппарату: «инцидент ИБ», «компьютерный инцидент», «инцидент защиты информации» и «киберинцидент».

Объектом исследования выступают процессы выбора технических мер реагирования на инциденты ИБ в рамках распределенной защищаемой информационной инфраструктуры, размещенной на P площадок, с использованием средств реагирования, реализующих R технических действий. Предметом исследования выступают методы выбора (оптимизации) технических мер локализации инцидентов ИБ.

Цель исследования – синтез метода выбора технической реализации мер реагирования на инциденты ИБ, позволяющего минимизировать время, затрачиваемое на непосредственную реализацию технических мероприятий по локализации инцидентов ИБ (T_{Me}), за счет формализации процесса выбора в терминах теории исследования операций.

2. МЕТОДЫ

Обозначим $\overline{X_1}$ вектором переменных все технические действия по локализации инцидентов ИБ, которые потенциально можно выполнить группе реагирования на инциденты ИБ, а $\overline{X_2}$ – вектором технических действий, выбранных группой реагирования на инциденты ИБ:

$$x_r = \begin{cases} 1, \text{техническое действие выбрано} \\ 0, \text{техническое действие не выбрано} \end{cases}, (1)$$

под методом выбора технической реализации мер реагирования на инциденты ИБ будем понимать отображение $M_{loc}: \overline{X_1} \to \overline{X_2}$. Разрабатываемый метод должен обладать свойством масштабируемости и учитывать гетерогенность используемых средств реагирования.

Сравнение возможностей применения наиболее популярных средств реагирования для реализации технических действий по локализации инцидентов ИБ приведено в табл. 1.

Важно задать ограничения на выбор тех или иных технических действий с учетом возможности реализации данных действий в автоматическом режиме, т.е. без непосредственного участия членов групп реагирования на инциденты ИБ.

Первоначальным ограничением выступает минимизация количества выбираемых технических действий, что позволяет поддерживать меньшее количество технических интеграций (сокращает стоимость лицензий), минимизирует нагрузку на силы групп реагирования на инциденты ИБ и сами средства реагирования:

$$\sum_{r=1}^{R} x_r \to \min. \quad (2)$$

Одним из первичных ограничений выступает наличие покрытия средствами реагирования защищаемой информационной инфраструктуры (размещения компонентов средств реагирования), так как если нет покрытия, то нет технической возможности реализовать меру по локализации инцидента ИБ ни в автоматическом, ни в ручном режиме.

Указанные ограничения задаются матрицей $S = \|s_{pr}\|_{P,R}$ (табл. 2), где $s_{pr} \in \{0;1\}$ – булевая (логическая) переменная, отражающая наличие покрытия средствами реагирования для выполнения r технического действия на p-й площадке информационной инфраструктуры, $p = \overline{1,P}$, $r = \overline{1,R}$.

Еще одним из первичных ограничений выступает наличие мандата (отсутствие мандата) на автоматическое выполнение технического действия, так как если его нет, то требуется вовлечение для реализации членов группы реагирования на инциденты ИБ в ручном режиме.

Мандат представляет собой цифровую запись, например, в системе классов Incident Response Platform или Security Orchestration, Automation and Response [11, 12], содержащую идентификационную информацию, характеризующую условия локализации инцидента ИБ, с учетом заданных критериев, характерных для конкретной организации и ее информационной инфраструктуры (например: по территории, информационном системам, периоду времени и т.п.) [13].

Указанные ограничения задаются матрицей $M = \|m_{pr}\|_{P,R}$ (табл. 3), где $m_{pr} \in \{0;1\}$ – булевая (логическая) переменная, отражающая предоставление мандата на r техническое действие на p-й площадке

Таблица 2 | Фрагмент матрицы *S* (пример)

Table 2 | Fragment of matrix *S* (example)

S		***r***				
		1	*2*	…	*R–1*	*R*
p	*1*	0	1	…	1	1
	…	0	1	…	0	1
	P	1	0	…	1	1

информационной инфраструктуры, $p=\overline{1,P}$, $r=\overline{1,R}$.

Формируется $P\times R$ систем условий, отражающих техническую возможность выполнить *r* техническое действие на *p*-й площадке информационной инфраструктуры без участия сил группы реагирования на инциденты ИБ:

$$\begin{cases} s_{pr}x_r=1 \\ m_{pr}x_r=1 \end{cases} \text{ для } p=const. \qquad (3)$$

Для совокупности используемых в организации документированных планов реагирования формируется матрица $D=\|d_{kl}\|_{K,L}$, отражающая вхождение в них логических действий по локализации инцидентов ИБ (табл. 4), где $d_{kl}\in[0;1]$ – переменная, отражающая вклад *l* логического действия в *k*-й план реагирования, с соблюдением условия:

$$\sum_{l=1}^{L} d_{kl}=1 \text{ для } k=const. \qquad (4)$$

Для сопоставления логических и технических действий по локализации инцидентов ИБ сформирована булевая матрица $A=\|a_{rl}\|_{R,L}$ (табл. 5), где $a_{rl}\in\{0;1\}$ – булевая (логическая) переменная, отражающая возможность реализации *l* логического действия *r*-м техническим действием, т. е. средством реагирования.

Формируется *L* условий, отражающих возможность реализации *l* логического действия как минимум одним техническим действием:

Таблица 3 | Фрагмент матрицы *M* (пример)

Table 3 | Fragment of matrix *M* (example)

M		***r***				
		1	*2*	…	*R–1*	*R*
p	*1*	1	0	…	1	0
	…	0	1	…	0	1
	P	1	1	…	0	1

Таблица 4 | Фрагмент матрицы *D* (пример)

Table 4 | Fragment of matrix *D* (example)

D		***l***				
		1	*2*	…	*L–1*	*L*
k	*1*	0,5	0	…	0	0,5
	…	0,25	0,25	…	0,25	0,25
	K	1	0	…	0	0

Таблица 5 | Фрагмент матрицы *A* (пример)

Table 5 | Fragment of matrix *A* (example)

A		***l***				
		1	*2*	…	*L–1*	*L*
r	*1*	0	0	…	1	1
	…	1	1	…	0	0
	R	1	1	…	0	1

$$y_l(x) = \sum_{r=1}^{R} a_{rl} x_r \geq 1 \text{ для } l = \text{const}. \quad (5)$$

С учетом условия (5) формируется $\overline{Y}$ – вектор возможности выполнения логических действий, зависящий от $\overline{X_2}$:

$$y_l(x) = \begin{cases} 1, \text{ логическое действие реализовать возможно} \\ 0, \text{ логическое действие реализовать невозможно} \end{cases}. \quad (6)$$

Вводится член целевой функции I_k, отражающий автоматическое выполнение k-го плана реагирования, содержащего набор логических действий y_l, реализация которых возможна выбранными техническими действиями x_r (т.е. характеризующей автоматическую локализацию инцидента ИБ):

$$I_k = \sum_{l=1}^{L} d_{kl} y_l(x), \quad (7)$$

где

$$I_k = \begin{cases} I_k = 1, \text{ автоматическая реализация плана реагирования;} \\ I_k \neq 1, \text{ неавтоматическая реализация плана реагирования, тогда } I_k = 0 \end{cases}. \quad (8)$$

Сокращение времени, затрачиваемого на непосредственную реализацию технических мероприятий по локализации инцидентов ИБ в информационной инфраструктуре T_{ME}, и минимизация участия сил групп реагирования на инциденты ИБ в этом предусматривает увеличение количества планов реагирования, выполняемых в автоматическом режиме, т. е. целевая функция F принимает вид:

$$F = \sum_{k=1}^{K} I_k \to \max \Rightarrow T_{Me} \to \min. \quad (9)$$

Целевая функция F является линейной функцией. Таким образом, поставленная задача сводится к задаче поиска экстремума на множествах, заданных системами линейных равенств и неравенств (3), (5) с целочисленными (булевыми) переменными x_r, т. е. является задачей целочисленного (булевого) линейного программирования [14, 15]. Таким образом, в такой постановке задачи возникает интерпретация теории исследования операций применительно к принятию решений в рамках реагирования на инциденты ИБ.

В качестве математического метода решения выбран метод ветвей и границ [15, 16], который модифицирован в части учета того, что члены целевой функции являются логическими переменными (8), определяемыми планами реагирования и возможностью их реализации техническим действиями с учетом заданных ограничений на мандаты и покрытие средствами реагирования.

Предложенный метод M_{loc} (последовательность действий, приводящая к выбору оптимального набора технических действий) включает в себя следующие шаги и применяется последовательно:

1. Формирование матрицы S ограничений на покрытие средствами реагирования с учетом реального размещения компонентов средств реагирования (агентов и/или шлюзов).

2. Формирование матрицы M ограничений на предоставленные манданты согласно политике управления доступом в информационной инфраструктуре.

3. Формирование матрицы D ограничений на состав планов реагирования в части логических действий согласно документированным планам реагирования.

4. Формирование матрицы A ограничений на реализацию логических действий техническими действиями с учетом технических возможностей применяемых средств реагирования.

5. Формирование условий (3) и (5).

6. Поиск решения с применением модифицированного метода ветвей и границ.

По результатам применения метода M_{loc} будут установлены: минимальное количество и состав необходимых (оптимальных) технических действий $\overline{X_2}$; количество автоматически выполняемых планов реагирования F.

3. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Предложенный метод применен на следующем контрольном примере, в котором матрицы S, M и A сформированы с использованием генераторов псевдослучайных чисел, а в матрице D предусмотрено по четыре логических действия для каждого плана реагирования ($d_{kl} = 0{,}25$), остальные параметры задачи принимали следующие значения: $R = 4$; $P = 4$; $L = 8$; $K = 4$, чтобы в качестве проверки провести исчерпывающий перебор. Результаты применения метода и проверки совпали (табл. 6).

Таким образом, существует оптимальный набор технических действий, выбранных группой реагирования на инциденты ИБ, позволяющий обеспечить реализацию максимального количества планов реагирования в автоматическом режиме.

Принимая во внимание, что согласно исследованию компании Logshero среднее время реагирования на инциденты ИБ занимает у 82 % организаций более одного часа [17], а реализация данного метода и выбранных в рамках него технических действий по локализации – менее одной минуты (шестой шаг), то время, затрачиваемое на непосредственную реализацию технических мероприятий по локализации инцидентов ИБ, сокращается в 60 раз.

4. ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования предложен метод выбора технической реализации мер реагирования на инциденты ИБ, принимающий во внимание заданные ограничения на предоставленные манданты и покрытие средствами реагирования, в рамках которого задача выбора рассмотрена как задача целочисленного (булевого) линейного программирования, в которой члены целевой функции являются логическими переменными, учитывающими логические действия по локализации инцидентов ИБ, предусмотренные планами реагирования. Применение данного метода позволяет максимизировать количество планов реагирования, выполняемых в автоматическом режиме (без участия сил реагирования на инциденты ИБ), тем самым минимизировать время, затрачиваемое на локализацию инцидентов ИБ.

Применение результатов исследования дает положительный эффект в области технических наук (методы и системы защиты информации, информационная безопасность) и наиболее значимо для владельцев (операторов) распределенных информационных (компьютерных) систем и входящих в их состав групп реагирования на инциденты ИБ.

Предложенный метод проходит практическую апробацию на базе крупнейшего в России коммерческого центра мониторинга и реагирования на кибератаки ООО «РТК ИБ».

Таблица 6 | Значения для контрольного примера

Table 6 | Values for the test case

Вар-т	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	***10***	*11*	*12*	*13*	*14*	*15*	*16*
x_1	1	0	1	1	1	1	0	0	1	**1**	0	1	0	0	0	0
x_2	1	1	0	1	1	1	0	1	0	**0**	1	0	1	0	0	0
x_3	1	1	1	0	1	0	1	1	0	**1**	0	0	0	1	0	0
x_4	1	1	1	1	0	0	1	0	1	**0**	1	0	0	0	1	0
F	4	0	4	4	4	2	0	0	0	**4**	0	0	0	0	0	0

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Автор заявляет об отсутствии конфликта интересов / The author declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. От выявления компрометации до реагирования: как российские компании справлялись с кибератаками в 2025 году. URL: https://bi.zone/expertise/insights/ot-otsenki-komprometatsii-do-reagirovaniya-kak-rossiyskie-kompanii-spravlyalis-s-kiberatakami-v-2025/ (дата обращения: 12.02.2026).
2. Курс на антихрупкость стратегический обзор киберугроз 2025. URL: https://jetcsirt.su/analytics/kurs-na-antikhrupkost-strategicheskiy-obzor-kiberugroz-2025/ (дата обращения: 12.02.2026).
3. **Метельков А. Н.** Многоликость мониторинга в обеспечении информационной безопасности // Правовая информатика. 2025. № 4. С. 69–78.
4. Security Vision 5: эволюция автоматизации. URL: https://safe.cnews.ru/articles/2021-11-01_security_vision_5_evolyutsiya_avtomatizatsii (дата обращения: 03.04.2026).
5. **Голицын С. А., Шульженко А. Д.** Концептуальный подход к построению центра мониторинга системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Globus: Технические науки. 2021. Т. 7. № 1 (37). С. 40–43.
6. **Микрюков А. А., Куулар А. В.** Совершенствование процесса управления инцидентами на основе прецедентного подхода // Открытое образование. 2021. Т. 25. № 4. С. 47–54.
7. 41 % компаний испытывают нехватку специалистов в области информационной безопасности. URL: https://www.kaspersky.ru/about/press-releases/globalnoe-issledovanie-laboratorii-kasperskogo-41-kompanij-ispytyvayut-nehvatku-specialistov-v-oblasti-informacionnoj-bezopasnosti (дата обращения: 12.02.2026).
8. **Кузнецов А. В.** Эволюция реагирования на инциденты информационной безопасности // Защита информации. Инсайд. 2024. № 5 (119). С. 14–20.
9. **Милославская Н. Г., Толстой А. И.** Управление инцидентами информационной безопасности. М. : Горячая Линия – Телеком, 2024. С. 105–109; 169–193.
10. **Чижевский М. А., Серпенинов О. В., Лапсарь А. П.** Оптимизация алгоритма расследования компьютерных инцидентов в SIEM-системах // Проблемы информационной безопасности. Компьютерные системы. 2025. № 3 (66). С. 69–80. DOI: 10.48612/jisp/rmzt-68hn-ung8.
11. **Мухитов А. А., Шафиков М. Р.** Проблематика автоматизации процесса реагирования на инциденты ИБ // Advances in Science and Technology : сборник статей LX международной научно-практической конференции, 30 апреля 2024 г., Москва, Россия. М. : ООО АКТУАЛЬНОСТЬ.РФ, 2024. С. 90–93.
12. **Власова А. В., Дударев В. А., Новикова Т. И.** Обзор основных направлений и технологий применения систем SOC в системе информационной безопасности // Фундаментальные и прикладные научные исследования: инноватика в современном мире: сборник научных статей по материалам IX Международной научно-практической конференции, 25 ноября 2022 г., Уфа, Россия. Уфа : ООО «Научно-издательский центр «Вестник науки»», 2022. С. 235–239.
13. **Кузнецов А. В.** Анализ критериев предоставления мандата на локализацию инцидента информационной безопасности // Инженерный вестник Дона. 2025. № 3 (123). С. 217–226.
14. **Трушков А. С.** Задача целочисленного программирования с булевыми переменными // Актуальные вопросы современной информатики : материалы IX Всероссийской научно-практической конференции, 1–15 апреля 2019 г., Коломна, Россия. Коломна : Государственный социально-гуманитарный университет, 2019. С. 87–95.

15. **Дейкина А. С., Червякова М. В.** Метод ветвей и границ для решения задачи линейного программирования с булевыми переменными // Материалы секционных заседаний 57-й студенческой научно-практической конференции ТОГУ, 17–27 апреля 2017 г., Хабаровск, Россия. В 2 т. Хабаровск : Тихоокеанский государственный университет, 2017. С. 16–21.
16. Применение Метода ветвей и границ для решения Экстремальных задач. URL: https://naukamirowozreniya.ru/public/202511/application/1764226987579351894/primenenie-metoda-vetvej-i-granic-dlya-resheniya-ekstremalnyh-zadach.pdf (дата обращения: 12.02.2026).
17. 2024 Observability Pulse Report. URL: https://logz.io/observability-pulse-2024/?utm_medium=referral&utm_source=cncf#executive-summary (дата обращения: 12.02.2026).

REFERENCES

1. From compromise detection to response: How Russian companies coped with cyberattacks in 2025. URL: https://bi.zone/expertise/insights/ot-otsenki-komprometatsii-do-reagirovaniya-kak-rossiyskie-kompanii-spravlyalis-s-kiberatakami-v-2025/ (accessed: 12.02.2026). (In Russian)
2. Antifragility: A Strategic Cyber Threat Review 2025. URL: https://jetcsirt.su/analytics/kursna-antikhrupkost-strategicheskiy-obzor-kiberugroz-2025/ (accessed: 12.02.2026). (In Russian)
3. **Metelkov A. N.** Diversity of monitoring in ensuring information security. *Legal Informatics*. 2025. No. 4, pp. 69–78. (In Russian)
4. Security Vision 5: evolution of automation. URL: https://safe.cnews.ru/articles/2021-11-01_security_vision_5_evolyutsiya_avtomatizatsii (accessed: 03.04.2026). (In Russian)
5. **Golitsyn S. A., Shulzhenko A. D.** Conceptual approach to the construction of a monitoring center for detection, prevention and elimination of the consequences of computer attacks. *Globus: Technical Sciences*. 2021. Vol. 7. No. 1 (37), pp. 40–43. (In Russian)
6. **Mikryukov A. A., Kuular A. V.** Improving the incident management process based on a use case approach. *Open Education*. 2021. Vol. 25. No. 4, pp. 47–54. (In Russian)
7. 41 % of companies are experiencing a shortage of information security specialists. URL: https://www.kaspersky.ru/about/press-releases/globalnoe-issledovanie-laboratorii-kasperskogo-41-kompanij-ispytyvayut-nehvatku-specialistov-v-oblasti-informacionnoj-bezopasnosti (accessed: 12.02.2026). (In Russian).
8. **Kuznetsov A. V.** The evolution of information security incident response. *Zaŝita informacii. Inside*. 2024. No. 5 (119), pp. 14–20. (In Russian)
9. **Miloslavskaya N. G., Tolstoy A. I.** Information Security Incident Management. Moscow : Hot Line – Telecom, 2024, pp. 105–109; 169–193. (In Russian)
10. **Chizhevsky M. A., Serpeninov O. V., Lapsar A. P.** Optimization of computer incident investigation algorithm in siem systems. *Problems of information security. Computer systems.* 2025. No. 3 (66), pp. 69–80. DOI: 10.48612/jisp/rmzt-68hn-ung8. (In Russian)
11. **Mukhitov A. A., Shafikov M. R.** Problems of automation of the process of response to information security incidents. Advances in Science and Technology. Collection of articles of the LX international scientific and practical conference, 30 April 2024, Moscow, Russia. Moscow: OOO AKTUAL'NOST'.RF, 2024, pp. 90–93. (In Russian)
12. **Vlasova A. V., Dudarev V. A., Novikova T. I.** Review of the main directions and technologies for the application of SOC systems in the information security system. Fundamental and applied scientific research: innovation in the modern world. Collection of scientific articles based on the materials of the IX International scientific and practical conference, 25 November 2022, Ufa, Russia. Ufa : OOO "Nauchno-izdatel'skij centr "Vestnik nauki", 2022, pp. 235–239. (In Russian)
13. **Kuznetsov A. V.** The analysis of criteria for granting a mandate to an information security incident localization. *Engineering Journal of Don*. 2025. No. 3 (123), pp. 217–226. (In Russian)

14. **Trushkov A. S.** Integer programming problem with Boolean variables. Actual issues of modern informatics. Proceedings of the IX All-Russian scientific and practical conference, 1–15 April 2019, Kolomna, Russia. Kolomna, Gosudarstvennyj social'no-gumanitarnyj universitet, 2019, pp. 87–95. (In Russian)
15. **Deikina A. S., Chervyakova M. V.** Branch and bound method for solving a linear programming problem with Boolean variables. Materials of sectional meetings of the 57th student scientific and practical conference, 17–27 April 2017, Khabarovsk, Russia. In 2 volumes. Khabarovsk, Pacific National University, 2017, pp. 16–21. (In Russian)
16. Application of the Branch and Bound Method to Solve Extremal Problems. URL: https://naukamirowozreniya.ru/public/202511/application/1764226987579351894/primenenie-metoda-vetvej-i-granic-dlya-resheniya-ekstremalnyh-zadach.pdf (accessed: 12.02.2026). (In Russian)
17. 2024 Observability Pulse Report. URL: https://logz.io/observability-pulse-2024/?utm_medium=referral&utm_source=cncf#executive-summary (accessed: 12.02.2026).

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT AUTHOR

КУЗНЕЦОВ Александр Васильевич – канд. техн. наук, руководитель отдела комплексных технических решений, ООО «РТК ИБ», Россия, 125009, Москва, пер. Никитский, д. 7, стр. 1; доцент, Финансовый университет при Правительстве Российской Федерации, Россия, 125167, Москва, пр-т Ленинградский, д. 49/2
E-mail: 1283_my@mail.ru
ORCID: 0000-0002-7160-1845

KUZNETSOV Aleksandr V. – Candidate of Engineering Sciences, Head of Integrated Technical Solutions Department, RTK IB LLC, Russia, 125009, Moscow, Nikitsky Lane, 7, build. 1; Associate Professor, Financial University under the Government of the Russian Federation, Russia, 125167, Moscow, Leningradsky ave., 49/2