УДК 004.77
DOI 10.17513/snt.40619

МАТЕМАТИЧЕСКИЙ АППАРАТ И АЛГОРИТМ ОПТИМИЗАЦИОННОГО ВЫБОРА КОНТРМЕР ПРОТИВ УГРОЗ БЕЗОПАСНОСТИ В СИСТЕМАХ WI-FI SENSING

Сарайкин А.И. ORCID ID 0009-0005-3954-8027,
Парфёнов Д.И. ORCID ID 0000-0002-1146-1270

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», Оренбург, Российская Федерация, e-mail: saraikin-a@yandex.ru

Цель исследования – разработка комплексного математического аппарата и алгоритмического инструментария для оптимизированного выбора защитных контрмер в системах мониторинга и распознавания объектов на основе беспроводных сетей стандарта IEEE 802.11 (WI-FI Sensing). Исследование направлено на решение задачи достижения максимального уровня информационной безопасности при соблюдении заданных бюджетных ограничений и строгих требований к производительности системы. В рамках работы предложены детализированные формальные модели для описания угроз и средств защиты, интегрирующие количественные оценки критичности угроз, эффективности контрмер, их стоимости и влияния на быстродействие системы. Ключевой научной новизной является механизм учета синергетических и антагонистических эффектов, возникающих при комбинированном применении различных мер защиты, что позволяет избежать как избыточных затрат, так и недооценки эффективности правильно сформированного набора решений. Для решения поставленной оптимизационной задачи разработан алгоритм на основе модифицированной жадной стратегии, обеспечивающий поиск субоптимального набора контрмер. Наглядным результатом исследования стала трехмерная модель, визуализирующая зависимость остаточного риска от бюджета и производительности. Полученные результаты подтверждают необходимость применения комплексного, количественно обоснованного подхода к проектированию безопасных систем Wi-Fi Sensing, выходящего за рамки интуитивного выбора защитных мер.

Ключевые слова: Wi-Fi Sensing, кибербезопасность, оптимизация выбора контрмер, математическое моделирование

MATHEMATICAL FRAMEWORK AND ALGORITHM FOR THE OPTIMIZATION-BASED SELECTION OF COUNTERMEASURES AGAINST SECURITY THREATS IN WI-FI SENSING SYSTEMS

Saraykin A.I. ORCID ID 0009-0005-3954-8027,
Parfenov D.I. ORCID ID 0000-0002-1146-1270

Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", Orenburg, Russian Federation, e-mail: saraikin-a@yandex.ru

The aim of the research is to develop a comprehensive mathematical framework and algorithmic toolkit for the optimized selection of protective countermeasures in object monitoring and recognition systems based on IEEE 802.11 wireless networks (Wi-Fi Sensing). The study is aimed at solving the problem of achieving the maximum level of information security while complying with specified budget constraints and stringent system performance requirements. The paper proposes detailed formal models for describing threats and protective measures, integrating quantitative assessments of threat criticality, countermeasure effectiveness, their cost, and their impact on system performance. A key scientific novelty is the mechanism for accounting for synergistic and antagonistic effects arising from the combined application of various protective measures, which makes it possible to avoid both excessive costs and underestimation of the effectiveness of a properly formed set of solutions. To solve the stated optimization problem, an algorithm based on a modified greedy strategy has been developed, ensuring the search for a suboptimal set of countermeasures. A visual result of the study is a three-dimensional model that visualizes the dependence of residual risk on budget and performance. The obtained results confirm the necessity of applying a comprehensive, quantitatively justified approach to designing secure Wi-Fi Sensing systems, going beyond the intuitive selection of protective measures.

Keywords: Wi-Fi Sensing, cybersecurity, countermeasure optimization, mathematical modeling

Введение

Бурное развитие и внедрение технологии Wi-Fi Sensing, превращающей стандартную инфраструктуру беспроводных сетей IEEE 802.11 в инструмент пассивного мониторинга окружающего пространства, открывает беспрецедентные возможности в сферах умных помещений, телемедицины, промышленной автоматизации и систем безопасности. Фундаментальная возможность пассивного мониторинга окружающего пространства через анализ искажений радиосигнала – параметров его мощности (RSSI), состояния канала (CSI) и времени пролета (ToF/TDoA) – одновременно является источником уязвимостей этой техно-

логии. Пассивный характер сбора высокодетализированных поведенческих данных, отсутствие явных индикаторов наблюдения и физическая природа атак формируют уникальные уязвимости, систематизированные в рамках предшествующих патентных и аналитических исследований. Как показывают работы [1, 2], данные CSI позволяют дистанционно восстанавливать широкий спектр действий. Включая ввод текста и паролей, что создает прямую угрозу конфиденциальности [3–5]. При этом патенты [6, 7] прямо указывают на уязвимость систем к атакам типа adversarial, приводящим к созданию «фантомных» объектов. Дальнейшие исследования углубляют анализ, рассматривая уязвимости систем, основанных на времени пролета сигнала (ToF) [8, 9]. Отдельно рассматриваются угрозы доступности, реализуемые через атаки на уровне RSSI [10–12]. Современная практика инженерии безопасности зачастую опирается на качественные или полуколичественные методологии управления рисками, такие как модель ФСТЭК, OCTAVE или NIST Cybersecurity Framework (CSF) [13]. Эти подходы, будучи ценными для формирования общей стратегии, демонстрируют существенные ограничения применительно к сложным, технологически специфичным системам, подобным Wi-Fi Sensing. Они плохо масштабируются для анализа десятков взаимосвязанных угроз и контрмер, не обеспечивают количественного обоснования выбора конкретных средств защиты и, что наиболее важно, практически не учитывают эффекты синергии и антагонизма между различными контрмерами при их совместном применении. В то же время продвинутые математические методы, включая многокритериальный анализ (MCDM) [14] и целочисленное линейное программирование (ILP) [15], хотя и предлагают формальный оптимизационный аппарат, обычно применяются в отрыве от глубокой специфики предметной области. Как следствие, они не позволяют корректно учесть такие особенности Wi-Fi Sensing, как различная критичность угроз для разных физических параметров сигнала (CSI, RSSI, ToF) или комплексное воздействие гибридных атак.

Особую актуальность приобретает задача учета синергетических эффектов. Современные исследования, включая систематические обзоры [16], указывают на доминирование в литературе анализа антагонизмов между мерами безопасности, в то время как потенциальные синергии, способные привести к сверхаддитивному повышению уровня защиты при рациональной комбинации контрмер, изучены недостаточно. Игнорирование этого фактора на практике может приводить к двум негативным сценариям: перерасходу бюджета на внедрение избыточных или конфликтующих мер и, наоборот, к недооценке эффективности правильно скомбинированного, но на первый взгляд скромного набора решений. Таким образом, формируется четко выраженный научно-практический пробел: между детальным качественным описанием уникальных угроз Wi-Fi Sensing и существующими общими методами оптимизации отсутствует связующее звено – специализированный количественный аппарат.

Цель исследования – разработка математического аппарата и алгоритмического инструментария для выбора и оптимизации контрмер, обеспечивающих максимальную безопасность систем мониторинга и распознавания объектов на основе беспроводных сетей стандарта IEEE 802.11 при заданных бюджетных ограничениях и требованиях к производительности.

Материалы и методы исследования

В работе применялся комплекс теоретико-прикладных методов, включающий математическое моделирование для формализации угроз и контрмер, количественную оценку рисков на основе интегральных показателей, методы оптимизации с бюджетными и эксплуатационными ограничениями, а также алгоритмический подход, реализующий жадную стратегию выбора контрмер. Для анализа компромиссов использованы методы визуализации данных, в частности построение трехмерной поверхности решений. Исследование опирается на разработанный математический аппарат (система расчетных формул, матрица эффективности), структурированные экспертные оценки угроз Wi-Fi Sensing, а также специализированное программное обеспечение, реализующее предложенные модели и алгоритмы.

Результаты исследования и их обсуждение

Модель оценки угроз

Пусть у нас есть множество угроз $T = \{t_1, t_2, \ldots, t_N\}$ и множество контрмер $C = \{c_1, c_2, \ldots, c_M\}$.

Для каждой угрозы t_i оценивается ее критичность по трем критериям: нарушение конфиденциальности ($У_1$); нарушение целостности ($У_2$); нарушение доступности ($У_3$).

Цель: найти подмножество контрмер $C^* \subseteq C$, максимизирующее общий уровень безопасности при ограничениях на бюджет и производительность.

Для каждой угрозы $t_i \in T$ необходимо определить: потенциальный ущерб $У_i$, вероятность реализации $В_i$ и радиус воздействия $Р_i$.

Потенциальный ущерб оценивается по трем аспектам: конфиденциальность, целостность и доступность.

$$У_i = w_{\text{conf}} \cdot S_{\text{conf}} + w_{\text{int}} \cdot S_{\text{int}} + w_{\text{avail}} \cdot S_{\text{avail}},$$

где $S_{\text{conf}}, S_{\text{int}}, S_{\text{avail}} \in \{1,5\}$ – оценки нарушения конфиденциальности, целостности и доступности соответственно; $w_{\text{conf}}, w_{\text{int}}, w_{\text{avail}}$ – весовые коэффициенты, причем $w_{\text{conf}} + w_{\text{int}} + w_{\text{avail}} = 1$.

Вероятность реализации угрозы определяется как

$$В_i = (Т_с + О_с + Д_с) / 3,$$

где $Т_с \in \{1,5\}$ – техническая сложность реализации атаки; $О_с \in \{1,5\}$ – доступность необходимого оборудования; $Д_с \in \{1,5\}$ – требуемый уровень знаний атакующего.

Интегральный показатель угрозы (риск) при этом будет

$$Рискі = У_i \cdot В_i \cdot Р_i,$$

где $Р_i \in \{0,1\}$ – доля системы, подверженная угрозе.

Далее разрабатывается модель оценки контрмер.

Для каждой контрмеры $c_j \in C$ необходимо определить: вектор эффективности $Э_j$; вектор стоимости $С_j$; вектор совместимости $К_j$; сложность интеграции $П_j$.

Вектор эффективности:

$$Э_j = w_{\text{cover}} \cdot E_{\text{cover}} + w_{\text{maturity}} \cdot E_{\text{maturity}} + w_{\text{resistance}} \cdot E_{\text{resistance}},$$

где $E_{\text{cover}}, E_{\text{maturity}}, E_{\text{resistance}} \in \{1,5\}$ – оценки покрытия угроз, технологической зрелости и сложности обхода соответственно; $w_{\text{cover}}, w_{\text{maturity}}, w_{\text{resistance}}$ – весовые коэффициенты, в сумме равные 1.

Вектор стоимости:

$$С_j = w_{\text{fin}} \cdot S_{\text{fin}} + w_{\text{perf}} \cdot S_{\text{perf}} + w_{\text{oper}} \cdot S_{\text{oper}},$$

где $S_{\text{fin}} \in \{1,5\}$ – финансовые затраты (1 – высокие, 5 – низкие); $S_{\text{perf}} \in \{1,5\}$ – влияние на производительность (1 – сильное, 5 – отсутствует); $S_{\text{oper}} \in \{1,5\}$ – сложность эксплуатации (1 – сложная, 5 – простая); весовые коэффициенты $w_{\text{fin}}, w_{\text{perf}}, w_{\text{oper}}$ в сумме равны 1. Обратная шкала применяется для того, чтобы более низкая стоимость напрямую увеличивала итоговую ценность контрмеры. Количественная оценка того, насколько легко и эффективно контрмера может быть интегрирована в существующую инфраструктуру Wi-Fi Sensing без необходимости кардинальной перестройки системы, выражается вектором совместимости:

$$К_j = w_{\text{standards}} \cdot K_{\text{standards}} + w_{\text{integration}} \cdot K_{\text{integration}} + w_{\text{scalability}} \cdot K_{\text{scalability}},$$

где $K_{\text{standards}} \in \{1,5\}$ – оценка соответствия контрмеры отраслевым стандартам и протоколам; $K_{\text{integration}} \in \{1,5\}$ – оценка сложности интеграции контрмеры в существующую инфраструктуру; $K_{\text{scalability}} \in \{1,5\}$ – оценка способности контрмеры масштабироваться в системах разного размера; $w_{\text{standards}}, w_{\text{integration}}, w_{\text{scalability}}$ – весовые коэффициенты, причем $w_{\text{standards}} + w_{\text{integration}} + w_{\text{scalability}} = 1$.

Соответствие контрмеры отраслевым стандартам и протоколам оценивает, насколько контрмера соответствует общепринятым стандартам (например, IEEE 802.11bf, WPA3). Оценка близкая к 5 означает, что контрмера использует стандартные протоколы и легко встраивается в стандартную инфраструктуру. Оценка близкая к 1 указывает на использование уникальных решений, которые могут вызвать проблемы совместимости.

Сложность интеграции отражает трудоемкость внедрения контрмеры. Оценка 5 означает, что контрмера легко внедряется (например, путем обновления программного обеспечения), а оценка 1 – что требуется значительная перестройка инфраструктуры или замена оборудования.

Масштабируемость показывает, насколько хорошо контрмера работает в системах разного масштаба. Оценка 5 означает, что контрмера эффективно масштабируется без потери эффективности, 1, что она применима только в ограниченных условиях.

Весовые коэффициенты определяют важность каждого аспекта для конкретной системы. Матрица эффективности при этом будет иметь вид

$$E = [e_{ij}]_{n\times m},$$

где e_{ij} – эффективность контрмеры c_j против угрозы t_i вычисляется следующим образом:

$$e_{ij} = \alpha\cdot Э_j + \beta\cdot СпецЭ_{ij}.$$

Специализированная эффективность ($СпецЭ_{ij} \in \{0,1\}$) – это точечная мера того, насколько конкретная контрмера c_j целенаправленно защищает от конкретной угрозы t_i. $СпецЭ_{ij} = 1$ – контрмера c_j идеально и целенаправленно блокирует угрозу t_i. Например, аппаратное шифрование CSI-данных (c_j) против перехвата CSI-паттернов (t_i). $СпецЭ_{ij} = 0$ – контрмера не оказывает никакого специфического воздействия на данную угрозу. Например, система фильтрации сетевых пакетов (c_j) против атак на алгоритмы машинного обучения (t_i). $0 < СпецЭ_{ij} < 1$ – частичная эффективность, когда контрмера косвенно или ограниченно влияет на угрозу. Таким образом, параметр специализированной эффективности дает возможность учесть ситуацию, когда контрмера, демонстрируя среднюю общую эффективность, может быть максимально результативной против конкретной угрозы.

Весовые коэффициенты α и β определяют баланс между: универсальностью контрмеры (α), ее общей эффективностью $Э_j$ против широкого спектра угроз и β – специализацией контрмеры (ее точечным воздействием $СпецЭ_{ij}$ на конкретную угрозу). При этом $\alpha + \beta = 1$.

Типичные сценарии балансировки: $\alpha = 0.7$, $\beta = 0.3$, приоритет универсальным решениям (например, при ограниченном бюджете); $\alpha = 0.3$, $\beta = 0.7$, приоритет специализированной защите (например, для критических угроз); $\alpha = 0.5$, $\beta = 0.5$, сбалансированный подход.

Функция целевой эффективности

Показатель ценности для пары угроза – контрмера отражает, насколько эффективно контрмера нейтрализует конкретную угрозу с учетом степени ее совместимости и совокупных затрат на внедрение, позволяя сравнивать различные средства защиты между собой и выбирать решения с максимальной отдачей на единицу вложенных ресурсов:

$$ЦК_{ij} = \frac{Риск_i \cdot e_{ij}}{С_j \cdot К_{ij}},$$

где $К_{ij} \in \{0,1\}$ – коэффициент совместимости контрмеры c_j с существующей инфраструктурой при противодействии угрозе t_i.

Общий показатель ценности контрмеры при этом

$$ЦК_j = \frac{\sum_{i=1}^{n} ЦК_{ij} \cdot I_{ij}}{\sum_{i=1}^{n} I_{ij}},$$

где I_{ij} – индикатор применимости контрмеры c_j к угрозе t_i:

$$I_{ij} = \begin{cases} 1, \text{ если контрмера } c_j \text{ применима к угрозе } t_i \\ 0, \text{ иначе} \end{cases}$$

Для учета взаимодействия контрмер при их совместном применении вводится матрица синергии:

$$S = [s_{jk}]_{m\times m}, s_{jk} \in \{-1,1\},$$

где s_{jk} – коэффициент синергии между контрмерами c_j и c_k.

Общая формула коэффициента синергии:

$$s_{jk} = w_f \cdot s_{jk}^{(f)} + w_c \cdot s_{jk}^{(c)} + w_r \cdot s_{jk}^{(r)} + w_i \cdot s_{jk}^{(i)},$$

где w_f, w_c, w_r, w_i – весовые коэффициенты компонентов синергии; $s_{jk}^{(f)}$ – компонент функциональной синергии; $s_{jk}^{(c)}$ – компонент синергии покрытия; $s_{jk}^{(r)}$ – компонент ресурсной синергии; $s_{jk}^{(i)}$ – компонент информационной синергии. При этом условие нормировки весовых коэффициентов: $w_f + w_c + w_r + w_i = 1$.

Функциональная синергия отражает взаимное усиление функциональных возможностей контрмер:

$$s_{jk}^{(f)} = \frac{1}{\left|T_{jk}\right|} \sum_{t_i \in T_{jk}} \frac{\min\left(e_{ij}, e_{ik}\right)}{e_{\max}} - \gamma_{jk},$$

где $T_{jk} = \{t_i \in T \mid e_{ij} > \theta \wedge e_{ik} > \theta\}$ – множество угроз, против которых эффективны обе контрмеры; e_{ij}, e_{ik} – эффективности контрмер c_j и c_k против угрозы t_i; $e_{\max} = 5$ – максимальное значение эффективности; $\gamma_{jk} \in \{0, 0.5\}$ – корректирующий коэффициент за функциональные конфликты между контрмерами; $\theta = 0{,}3$ – порог значимой эффективности.

Синергия покрытия:

$$s_{jk}^{(c)} = \frac{\left|T_j \cup T_k\right| - \max\left(\left|T_j\right|, \left|T_k\right|\right)}{|T| - \min\left(\left|T_j\right|, \left|T_k\right|\right)},$$

где $\mathrm{T}_j = \{\mathrm{t}_i \in \mathrm{T} \mid \mathrm{e}_{ij} > \theta\}$ – множество угроз, эффективно покрываемых контрмерой c_j; $\mathrm{T}_k = \{\mathrm{t}_i \in \mathrm{T} \mid \mathrm{e}_{ik} > \theta\}$ – множество угроз, эффективно покрываемых контрмерой c_k; $|\mathrm{T}|=\mathrm{n}$ – общее количество угроз; $\left|\mathrm{T}_j \cup \mathrm{T}_k\right|$ – мощность объединения множеств.

Ресурсная синергия:

$$s_{jk}^{(r)} = \frac{R_{jk}^{\text{shared}} - R_{jk}^{\text{extra}}}{C_j + C_k},$$

где R_{jk}^{shared} – экономия ресурсов за счет совместного использования инфраструктуры; R_{jk}^{extra} – дополнительные затраты на интеграцию контрмер; C_j и C_k – стоимости внедрения контрмер c_j и c_k.

Информационная синергия:

$$s_{jk}^{(i)} = \frac{I_{jk}^{\text{shared}}}{I_j^{\text{total}} + I_k^{\text{total}}},$$

где I_{jk}^{shared} – объем полезной информации, которую контрмера c_j может предоставить c_k; $I_j^{\text{total}}, I_k^{\text{total}}$ – общий объем информации, обрабатываемой контрмерами.

Синергетическая эффективность контрмеры:

$$e_{ij}^{\text{syn}} = e_{ij} \cdot \left(1 + \beta \cdot \frac{1}{\left|C^*\right| - 1} \sum_{\substack{c_k \in C^* \\ k \neq j}} s_{jk}\right),$$

где e_{ij}^{syn} – эффективность контрмеры c_j против угрозы t_i с учетом синергии; e_{ij} – базовая эффективность контрмеры; $\beta \in \{0{,}0{,}3\}$ – коэффициент влияния синергии на эффективность; C^* – выбранное подмножество контрмер; $|C^*|$ – количество контрмер в выбранном подмножестве.

После количественной оценки угроз и анализа эффективности контрмер необходимо определить такое подмножество контрмер, которое обеспечивает максимальное снижение совокупного риска при соблюдении бюджетных ограничений, требований к производительности системы и гарантированном покрытии критических угроз. Формализация этой задачи в виде целевой функции с системой ограничений и разработка эффективного алгоритма решения позволят произвести рациональное распределение ресурсов безопасности.

Формулировка задачи оптимизации

Максимизировать целевую функцию для выбираемого подмножества контрмер:

$$F\left(C^*\right) = \sum_{j \in C^*} \sum_{i=1}^{n} \text{Риск}_i \cdot e_{ij} \cdot x_{ij} + \mu \cdot \text{SynergyEffect}\left(C^*\right),$$

где Риск_i – интегральный риск i-й угрозы; e_{ij} – эффективность контрмеры c_j против угрозы t_i; $x_{ij} \in \{0{,}1\}$ – индикатор применения контрмеры c_j к угрозе t_i; $\mu \geq 0$ – коэффициент значимости синергии.

При бюджетном ограничении:

$$\sum_{j\in C^*} C_j^{\text{fin}} \le \text{Budget}_{\max},$$

где C_j^{fin} – финансовый компонент стоимости контрмеры c_j.; $B_{\max}$ – максимально допустимый бюджет

Ограничение на производительность:

$$\prod_{j\in C^*} C_j^{\text{perf}} \ge \text{Perf}_{\min},$$

где C_j^{perf} – компонент производительности контрмеры c_j; $\text{Perf}_{\min}$ – минимально допустимый уровень производительности системы.

Ограничение на покрытие критических угроз:

$$\forall t_i \in T_{\text{critical}} : \sum_{j\in C^*} e_{ij} \cdot x_{ij} \ge \text{Cover}_{\min},$$

где $\text{T}_{\text{critical}} \subseteq \text{T}$ – множество критических угроз; $\text{Cover}_{\min}$ – минимальный требуемый уровень снижения риска для критических угроз; $x_{ij} \in \{0,1\}$ – индикатор применения контрмеры c_j к угрозе t_i.

Ограничение на совместимость контрмер (синергия):

$$\forall c_j, c_k \in C^* : s_{jk} \ge \theta_{\min},$$

где $\theta_{\min} \in \{-0.3, 0\}$ – минимально допустимый уровень синергии.

Ограничение на обязательные контрмеры:

$$\forall c_j \in C_{\text{mandatory}} : c_j \in C^*,$$

где $C_{\text{mandatory}} \subseteq C$ – множество обязательных контрмер (например, по требованиям регуляторов).

Логические ограничения:

$$x_{ij} \le y_j, \forall i, j \quad \sum_{j\in C} x_{ij} \ge 1, \forall t_i \in T_{\text{critical}},$$

где $y_j \in \{0,1\}$ – бинарная переменная выбора контрмеры c_j в набор C^*; $x_{ij} \in \{0,1\}$ – бинарная переменная применения контрмеры c_j к угрозе t_i.

Ограничение на максимальное количество контрмер:

$$|C^*| = \sum_{j\in C} y_j \le N_{\max},$$

где $N_{\max}$ – максимальное количество контрмер (ограничение сложности системы).

Синергетический эффект:

$$\text{SynergyEffect}\left(C^*\right) = \sum_{i=1}^{n} \text{Риск}_i \cdot \left(\max_{j\in C^*} e_{ij}^{\text{syn}} \max_{j\in C^*} e_{ij} \right),$$

где $e_{ij}^{\text{syn}} = e_{ij} \cdot \left(1 + \beta \cdot \overline{s}_j\left(C^*\right)\right)$ – эффективность с учетом синергии; $\overline{s}_j\left(C^*\right) = \dfrac{1}{|C^*|-1} \sum_{\substack{k\in C^* \\ k\ne j}} s_{jk}$ – средняя синергия контрмеры c_j с другими выбранными контрмерами; $\beta \in \{0,1\}$ – коэффициент влияния синергии на эффективность.

Остаточный риск после внедрения контрмер:

$$\text{ResidualRisk}_i\left(C^*\right) = \text{Риск}_i \cdot \prod_{j\in C^*} \left(1 - e_{ij}^{\text{syn}} \cdot x_{ij}\right).$$

Алгоритм оптимизации набора контрмер с учетом ограничений на бюджет, производительность и покрытие критических угроз представлен на рис. 1.

На первом шаге для каждой контрмеры $c_j \in C_{\text{cand}}$ производится расчет модифицированного прироста целевой функции на единицу затрат:

$$\Delta F_j^{\text{syn}} = \frac{F\left(C^* \cup \{c_j\}\right) + \mu \cdot \text{SynergyEffect}\left(C^* \cup \{c_j\}\right) - F_{\text{current}}^{\text{syn}}}{C_j^{\text{fin}}},$$

где $F_{\text{current}}^{\text{syn}} = F\left(C^*\right) + \mu \cdot \text{SynergyEffect}\left(C^*\right)$ – текущее значение целевой функции с учетом синергии, SynergyEffect(C^*) вычисляется в соответствии с представленной моделью.

На втором шаге осуществляется выбор контрмеры с максимальным приростом. Из множества кандидатов выбирается контрмера:

$$c_{\text{best}} = \arg\max_{c_j \in C_{\text{cand}}} \Delta F_j^{\text{syn}}.$$

Если $\max \Delta F_j^{\text{syn}} \le 0$, алгоритм переходит к Шагу 5 (Завершение).

На третьем шаге происходит проверка ограничений для контрмеры c_{best}. Перед добавлением контрмеры в оптимальный набор выполняется комплексная проверка выполнения бюджетного ограничения, ограничений производительности, покрытия критических угроз и совместимости (синергии) для временного множества $C_{\text{temp}} = C^* \cup \{c_{\text{best}}\}$. Если все ограничения выполняются, алгоритм переходит к Шагу 4. В противном случае контрмера c_{best} исключается из множества кандидатов ($C_{\text{cand}} = C_{\text{cand}} \setminus \{c_{\text{best}}\}$) и осуществляется возврат к Шагу 2 для выбора следующего наилучшего кандидата.

На четвертом шаге контрмера c_{best} добавляется в оптимальный набор, а все связанные переменные и множества обновляются:

$$C^* = C^* \cup \{c_{\text{best}}\}, \quad \text{Cost}_{\text{current}} = \text{Cost}_{\text{current}} + C_{\text{bestfin}},$$

$$\text{Perf}_{\text{current}} = \text{Perf}_{\text{current}} \cdot P_{\text{best}}, \quad F_{\text{currentsyn}} = F(C^*) + \mu \cdot \text{SynergyEffect}(C^*).$$

Из C_{cand} исключается выбранная контрмера, а также все контрмеры, имеющие с ней недопустимый антагонизм:

$$C_{\text{cand}} = C_{\text{cand}} \setminus \{c_{\text{best}}\} \setminus \{c_j \in C_{\text{cand}} \mid s_{\text{best},j} < \theta_{\min}\}.$$

После обновления данных осуществляется возврат к Шагу 1 для следующей итерации основного цикла.

На пятом шаге алгоритм завершает работу, когда множество кандидатов пусто ($C_{\text{cand}} = \varnothing$) или не осталось контрмер, дающих положительный прирост эффективности ($\max \Delta F_j^{\text{syn}} \le 0$). На выходе алгоритма возвращается найденное оптимальное (субоптимальное) множество контрмер C^* и рассчитываются итоговые показатели: общая стоимость внедрения, остаточный риск, интегральный коэффициент синергии, эффективность использования бюджета.

Общая стоимость внедрения:

$$\text{Cost}_{\text{total}} = \sum_{j \in C^*} C_j^{\text{fin}}.$$

Остаточный риск с учетом синергетического повышения эффективности контрмер:

$$\text{Risk}_{\text{residual}}^{\text{syn}} = \sum_{i=1}^{n} \text{Риск}_i \cdot \prod_{j \in C^*} \left(1 - e_{ij} \cdot \left(1 + \beta \cdot \overline{s}_j\right)\right),$$

где $\overline{s}_j = \frac{1}{|C^*| - 1} \sum_{k \in C^*, k \ne j} s_{jk}$ – средняя синергия контрмеры c_j с другими выбранными средствами защиты.

Интегральный коэффициент синергии для выбранного набора:

$$\overline{s}\left(C^*\right) = \frac{1}{|C^*|\left(|C^*| - 1\right)} \sum_{j,k \in C^*, j \ne k} s_{jk}.$$

Эффективность использования бюджета:

$$\text{BudgetEfficiency} = \frac{F_{\text{current}}^{\text{syn}}}{\text{Cost}_{\text{total}}}.$$

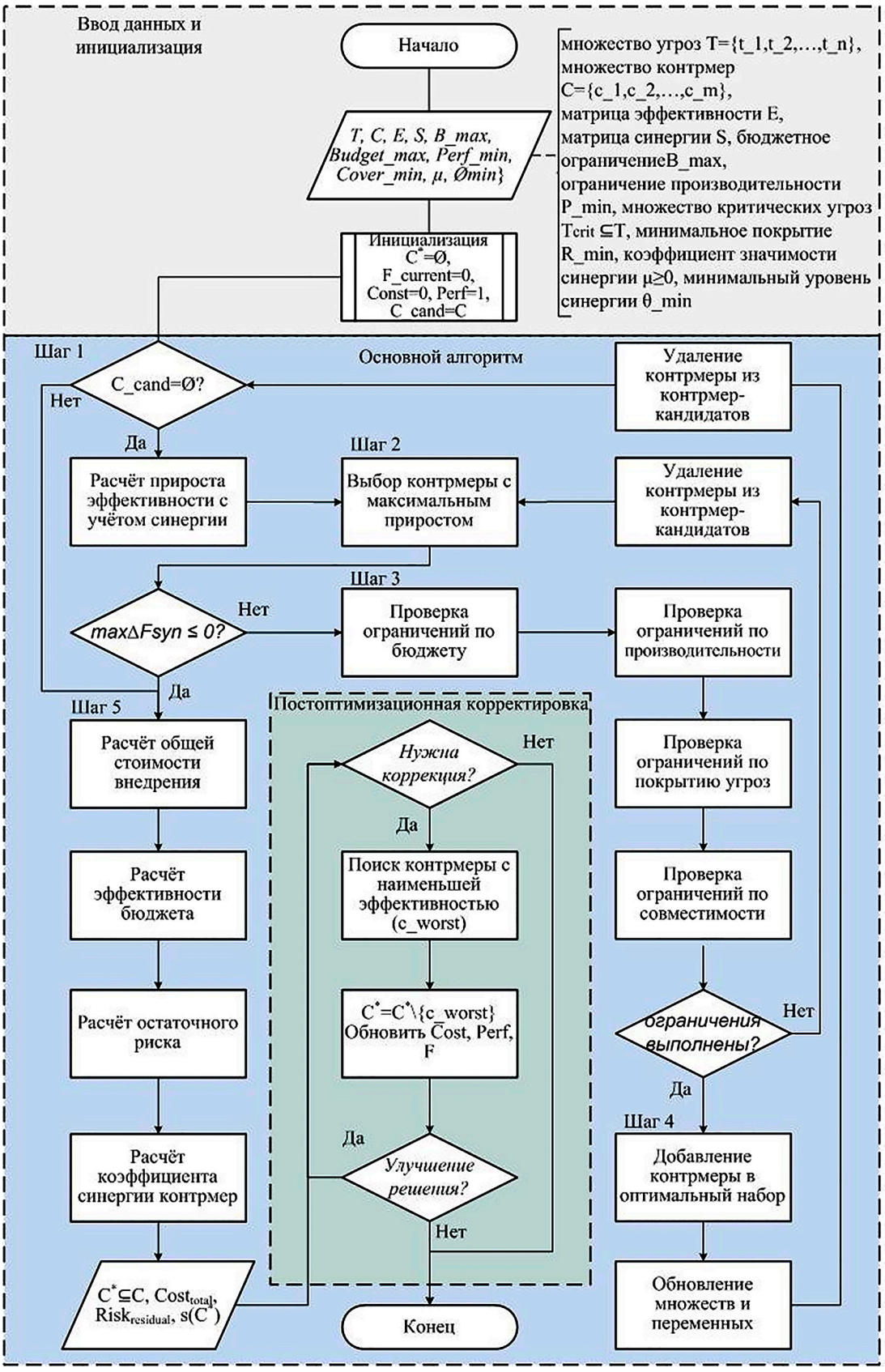

Рис. 1. Алгоритм оптимизации набора контрмер с учетом ограничений на бюджет, производительность и покрытие критических угроз
Примечание: составлен авторами по результатам данного исследования

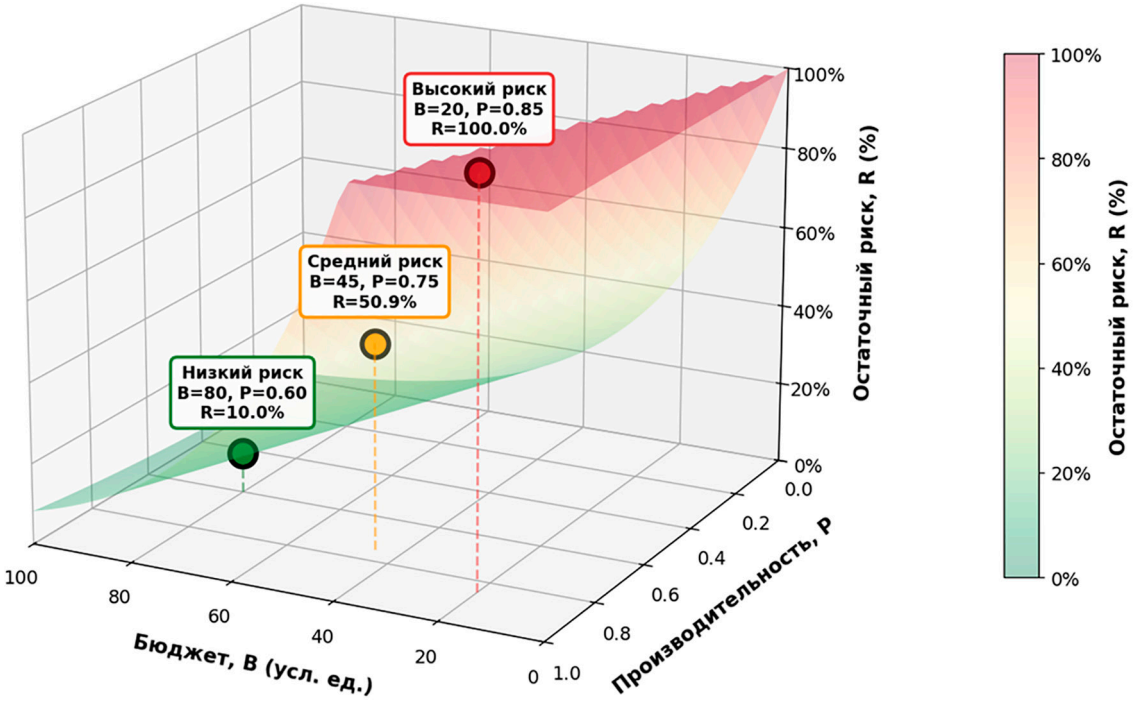

Рис. 2. Трехмерная модель зависимости остаточного риска от бюджета и требований к производительности
Примечание: составлен авторами по результатам данного исследования

Для получения более сбалансированного решения опционально можно произвести постоптимизационную корректировку, в ходе которой из набора C^* последовательно удаляются наименее эффективные с точки зрения отношения $\Delta F_j^{\text{syn}} / C_j^{\text{fin}}$ контрмеры до тех пор, пока не будут выполнены все ограничения. Это позволяет освободить бюджет для потенциально более выгодных комбинаций контрмер на последующих итерациях модифицированного алгоритма.

Разработанный математический аппарат позволяет не только рассчитывать оптимальный набор средств защиты, но и наглядно анализировать фундаментальный компромисс между тремя ключевыми параметрами системы: бюджетом, минимальной производительностью и остаточным риском. Для визуальной наглядности была построена трехмерная модель зависимости остаточного риска от бюджета и требований к производительности (рис. 2).

Представленная трехмерная модель отражает общие закономерности поведения системы, однако для получения точных, пригодных для реализации результатов необходимо применять разработанный оптимизационный алгоритм. Это связано с тем, что алгоритм учитывает дискретную природу выбора контрмер, что может приводить к ступенчатому характеру зависимостей. Таким образом, визуализация служит эффективным инструментом для выявления трендов и поддержки стратегических решений на этапе предпроектного анализа, в то время как алгоритм обеспечивает точное количественное обоснование для итогового проектирования.

Заключение

В ходе исследования разработан комплексный математический аппарат для оптимизации выбора средств защиты в системах Wi-Fi Sensing. Аппарат включает формальные модели угроз и контрмер, метод расчета интегрального риска, механизм оценки эффективности контрмер, целевую функцию с системой ограничений, а также алгоритм последовательного выбора оптимального набора защитных мер. Данный инструментарий позволяет перейти от качественного описания уязвимостей к количественному обоснованию решений по кибербезопасности и предоставляет архитекторам систем формальную основу для принятия взвешенных решений. Однако эффективное применение этого аппарата требует понимания фундаментального компромисса, лежащего в основе любого проектирования системы безопасности.

Этот компромисс заключается в треугольнике взаимоисключающих требований:

стремление обеспечить высокую производительность системы при минимальном финансировании мер безопасности закономерно ведет к существенному остаточному риску. Подобный подход может быть допустим лишь для систем, работающих с некритичными данными, где последствия реализации угроз являются приемлемыми. Для ответственных применений Wi-Fi Sensing оптимальная стратегия защиты должна формироваться не интуитивно, а на основе комплексного анализа всей поверхности решений, рассматривающей взаимосвязь бюджета, производительности и уровня риска, а не фокусироваться на отдельных изолированных сценариях. Разработанный математический аппарат, таким образом, служит основой для построения и анализа такой многомерной поверхности компромиссов, позволяя найти рациональный баланс между противоречивыми целями проектирования.

Практическая значимость работы заключается в предоставлении специалистам методической основы для обоснованного выбора контрмер, позволяющей избежать как недостаточного, так и избыточного инвестирования в безопасность.

Список литературы

1. Li M., Meng Y., Liu J., Zhu H., Liang X., Liu Y., Ruan N. When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals // Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. P. 1068–1079. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=cgjqyuoAAAAJ&citation_for_view=cgjqyuoAAAAJ:zYLM7Y9cAGgC (дата обращения: 26.12.2025). DOI: 10.1145/2976749.2978397.

2. Qi F., Zhao Y., Bhuiyan M.Z.A., Hai T., Islam M., Zhang S., Tang Z. Unauthorized and privacy-intrusive human activity watching through Wi-Fi signals: An emerging cybersecurity threat // Concurrency and Computation: Practice and Experience. 2023. Vol. 35. Is. 19. P. e7313. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=JqHr6TcAAAAJ&cstart=100&pagesize=100&citation_for_view=JqHr6TcAAAAJ:CCeGMaHljPEC (дата обращения: 26.12.2025). DOI: 10.1002/cpe.7313.

3. Wang C.-P., Lee C.-D., Chen P.-Y., Chiu H.-C., Lu Y.-C. Artificial intelligence (AI)-channel state information (CSI) automated labeling method. Patent 2024. № US20240144098A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20240144098A1/en (дата обращения: 25.12.2025).

4. Prasant Mohapatra, Parth H. Pathak Yunze Zeng. WiFi-based person-identification technique for use in smart spaces. Patent 2018. № US10045717B2. [Электронный ресурс]. URL: https://patents.google.com/patent/US10045717B2/en (дата обращения: 26.12.2025).

5. Ying Chen, Jie Yang, Yan Wang, Jian Liu, Marco Gruteser. Device-free activity identification using fine-grained wifi signatures. Patent 2023. № US20230053685A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20230053685A1/en?q=(Device-free+activity+identification+fine-grained+wifi+signatures)&oq=Device-free+activity+identification+using+fine-grained+wifi+signatures (дата обращения: 28.12.2025).

6. Hang L., Tong W., Yaqi R., Huihui L., Zhixiang W., Dawei G. A method of people detection based on WIFI signal. Patent CN 2021. № CN110149604B.

7. Lau K.H., Sung L., Chan W.C., Ng W.F., Lee K.F. Methods and Systems for Offloading Pose Processing to a Mobile Device for Motion Tracking on a Hardware Device without a Camera. Patent US 2024. № 2024/0310921 A1. URL: https://patents.google.com/patent/CN110149604B/en?oq=CN+2021+110149604B+ (дата обращения: 23.12.2025).

8. Excofiler D., Phan Huy D.T. Method for detecting the presence of a person using a communicating device within an environment of interest. Patent 2024. № EP4360338A1. [Электронный ресурс]. URL: https://patents.google.com/patent/EP4360338A1/en?oq=EP+2024;+No.+4360338+A1+ (дата обращения: 24.12.2025).

9. Poupyrev I., Schwesig C., Schulze J. Gesture detection and interactions. Patent US 2020. № US10572027B2. [Электронный ресурс]. URL: https://patents.google.com/patent/US10572027B2/en?oq=US+2020;+No.+10%2c572%2c027+B2+ (дата обращения: 24.12.2025).

10. Schweizer B., Dash D. Basic Sensing by Proxy and Doze Mode for IEEE 802.11BF Communications. Patent US 2025. № US20250159533A1. [Электронный ресурс]. URL: https://patents.google.com/patent/US20250159533A1/en?oq=Patent+US+2025;+No.+20250159533+A1+ (дата обращения: 24.12.2025).

11. Сарайкин А.И., Макаров В.С., Лушников М.Е. Программа для исследования зависимости уровня и времени прохождения сигнала от расстояния между устройствами передачи данных в беспроводных компьютерных сетях. Свид. о рег. прогр. ср-ва № RU 2024662941; заявитель и обладатель ОГУ. зарег. 03.06.2024. 36 Мбайт. Электронный ресурс. URL: https://elibrary.ru/item.asp?id=67984069 (дата обращения: 24.12.2025).

12. Сарайкин А.И., Макаров В.С., Лушников М.Е. Влияние расстояния между устройствами передачи данных на уровень и время прохождения сигнала в беспроводных компьютерных сетях. Свид. о рег. базы данных № RU 2024622257; заявитель и обладатель ОГУ. зарег. 03.06.2024. 20 Кбайт. [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=67981841 (дата обращения: 23.12.2025).

13. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). 2018. [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата обращения: 23.12.2025).

14. Horta A., Holanda R.. A Multi-criteria Approach to Improve the Cyber Security Visibility Through Breach Attack Simulations // Brazilian Computer Science. 2022. P. 330–343. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=k4V7sM8AAAAJ&citation_for_view=k4V7sM8AAAAJ:-vzq6BoH5oUC (дата обращения: 23.12.2025). DOI: 10.5753/sbseg.2022.224454.

15. Saygin C., Zarreh A., Zarreh M., Wan H. Optimizing cybersecurity in cyber-physical manufacturing systems: A game-theoretic approach and quantal response equilibrium study // Journal of Future Sustainability. 2025. Vol. 5. Is. 3. P. 179–194. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=BOhaCCAAAAAJ&citation_for_view=BOhaCCAAAAAJ:dhFuZR0502QC (дата обращения: 24.12.2025). DOI: 10.5267/j.jfs.2025.9.002.

16. Zimmermann V., Fanconi L., Sievers H., Isenring Y. From antagonisms to synergies: A systematic review of safety-security interrelations // International Journal of Critical Infrastructure Protection. 2025. Vol. 51. P. 100808. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=tuSCDYAAAAAJ&cstart=20&pagesize=80&citation_for_view=tuSCDYAAAAAJ:4OULZ7Gr8RgC (дата обращения: 24.12.2025). DOI: 10.1016/j.ijcip.2025.100808.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.