

Научная статья
DOI 10.66424/2071-8217-2026-3-9
УДК 004.056.53

МЕТОДИКА ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ АВИАПРЕДПРИЯТИЯ НА ОСНОВЕ МЕТОДА ВЕТВЕЙ И ГРАНИЦ

А. А. Антонов*

Финансовый университет при Правительстве Российской Федерации, Москва, Россия

✉ *alaantonov@fa.ru

ДЛЯ ЦИТИРОВАНИЯ

Антонов А. А. Методика выбора средств защиты информации авиапредприятия на основе метода ветвей и границ // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 120–130.
DOI: 10.66424/2071-8217-2026-3-9

ПОСТУПИЛА 05.05.2026

ПРИНЯТА 03.08.2026

ОПУБЛИКОВАНА 13.10.2026

© Антонов А. А.

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Современные требования к рациональному использованию сетей авиапредприятия и их информационной безопасности обуславливают выбор актуальных средств защиты информации. Рынок предлагает множество сертифицированных средств защиты информации, что затрудняет выбор оптимального варианта. Для решения задачи выбора средств защиты информации для обработки персональных данных в информационных системах авиапредприятия предложена методика, основанная на применении метода ветвей и границ. Использование данной методики позволяет найти оптимальное решение в рамках принятой детерминированной линейной модели задачи дискретной оптимизации, исключая неэффективные варианты на начальных этапах.

КЛЮЧЕВЫЕ СЛОВА

Методика, метод ветвей и границ, защита информации, авиапредприятие, угрозы, дискретная оптимизация, средства защиты информации

Original article
DOI 10.66424/2071-8217-2026-3-9

METHODOLOGY FOR SELECTING INFORMATION SECURITY TOOLS FOR AN AIRLINE BASED ON THE BRANCH-AND-BOUND METHOD

A. A. Antonov*

Financial University under the Government of the Russian Federation, Moscow, Russia

✉ *alaantonov@fa.ru

FOR CITATION

Antonov A. A. Methodology for selecting information security tools for an airline based on the branch-and-bound method. *Problems of information security. Computer systems*. 2026. No. 3, pp. 120–130. DOI: 10.66424/2071-8217-2026-3-9 (In Russian)

RECEIVED 05.05.2026

ACCEPTED 03.08.2026

PUBLICATION 13.10.2026

ABSTRACT

Modern requirements for the rational use of aircraft enterprise networks and their information security determine the choice of relevant information security tools. Currently, the market offers a wide range of certified information security tools, making it difficult to choose the optimal option. To address this issue, the article proposes a methodology based on the branch-and-bound method for selecting information security tools for processing personal data in aircraft enterprise information systems. This methodology allows for finding the optimal solution within the framework of a deterministic linear model of discrete optimization, eliminating inefficient options in the initial stages.

KEYWORDS

Methodology, branch and bound method, information security, airline, threats, discrete optimization, information security tools

1. ВВЕДЕНИЕ

В соответствии с доктриной информационной безопасности Российской Федерации [1] и Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры»¹, к критической информационной инфраструктуре относится авиационная отрасль. Отказ в обслуживании таких систем, как автоматическое зависимое наблюдение-вещание (АЗН-В), может привести к негативным последствиям, включая угрозу безопасности полетов [2, 3].

В контексте деятельности авиапредприятия актуальной является проблема обработки значительного объема конфиденциальной информации, включая персональные данные, а также обеспечения кибербезопасности критических систем связи, таких как АЗН-В.

Авиапредприятия, являющиеся объектами критической информационной инфраструктуры и операторами персональных данных, обязаны исполнять требования Федерального закона № 152-ФЗ «О персональных данных» [4] и сопутству-

ющих нормативных актов, в частности приказа ФСТЭК России № 21 [5]. Определение фактических угроз организовано на основе модели угроз по методике ФСТЭК, к типовым угрозам относятся [3, 6]: нарушение целостности данных за счет воздействия вредоносного программного обеспечения; уязвимость программного обеспечения и операционных систем персональных компьютеров; ограничения доступа к ресурсам и другим видам деятельности.

Целью исследования является разработка и апробация методики выбора оптимального набора средств защиты информации для информационных систем авиапредприятий на основе метода ветвей и границ. Предлагаемая методика позволяет формализовать процесс принятия решений, обеспечить строгое соблюдение регуляторов и минимизировать стоимость при заданном уровне защищенности.

2. МЕТОДЫ

Под методикой понимается совокупность этапов решения задачи выбора средств защиты информации (СЗИ): постановка задачи; формирование критериев и ограничений; экспертная оценка параметров СЗИ (в том числе с применением метода анализа иерархий); применение математического метода ветвей и границ для поиска оптимального набора;

¹ Концепция внедрения автоматического зависимого наблюдения на основе единого стандарта с развитием до функционала многопозиционных систем наблюдения в Российской Федерации (утв. распоряжением Минтранса России от 25.04.2018 № МС-68-Р).

интерпретация результата и проверка на соответствие требованиям регуляторов.

Для решения задачи дискретной оптимизации в научной литературе рассматриваются различные математические методы, включая полный перебор, динамическое программирование и генетические алгоритмы. Приведем обоснование выбора метода ветвей и границ. Полный перебор гарантирует нахождение оптимума, однако его вычислительная сложность делает его неприменимым при количестве кандидатов более 15–20. Динамическое программирование эффективно для задач с малой размерностью, но плохо масштабируется при введении нескольких разнородных ограничений. Генетические алгоритмы позволяют находить приближенные решения за приемлемое время, однако не гарантируют достижения глобального оптимума. Метод ветвей и границ обеспечивает точное решение задачи целочисленного программирования при существенно меньшем переборе вариантов за счет раннего отсека неперспективных ветвей, что делает его предпочтительным для задачи выбора СЗИ в условиях жестких регуляторных и бюджетных ограничений.

Для количественной оценки эффективности методов рассмотрим гипотетический сценарий с $N=30$ кандидатами СЗИ. При полном переборе потребуется проверить более миллиарда комбинаций, что практически нереализуемо. Динамическое программирование в данном случае неприменимо из-за разнородных ограничений (бюджет, совместимость, уровни доверия). Генетические алгоритмы способны найти хорошее приближенное решение, но не гарантируют глобальный оптимум, что критично для задач защиты критической информационной инфраструктуры. Метод ветвей и границ в рассматриваемой постановке позволяет сократить пространство поиска на 60–80 % за счет раннего отсека неперспективных ветвей по верхней границе целевой функции, сохраняя при этом гарантию оптимальности в рамках принятой модели. Поскольку целевая функция и все ограничения линейны, ослабленная задача является задачей линей-

ного программирования и решается точно (симплекс-методом), что гарантирует точность верхней границы и корректность отсека.

Таким образом, в основе предложенной методики лежит математический метод ветвей и границ [7], который позволяет формализовать задачу выбора средства защиты информации как задачу целочисленного программирования и найти оптимум с ограничениями, избегая полного перебора всех вариантов решения [8, 9]. Основная идея метода заключается в следующем: множество всех допустимых решений последовательно разбивается на подмножества (ветви). Каждая ветвь представляет собой часть пространства решений с дополнительными ограничениями. Для каждого подмножества вычисляется оценка (граница) целевой функции: верхняя граница – для задач максимизации; нижняя граница – для задач минимизации.

Если оценка для «ветви» хуже, чем значение уже найденного лучшего решения, эта ветка отбрасывается и не исследуется дальше. Таким образом, определяются: целевая функция (максимизация эффективности защиты при соблюдении требований установленного уровня защищенности); система ограничений (бюджет, требования регуляторов, совместимость); переменные решения (константы – обязательные меры базового набора, переменные – дополнительные меры).

Множество возможных СЗИ разбивается на подмножества. На каждом уровне дерева принимается решение о включении или исключении конкретного СЗИ из конфигурации защиты.

Для каждого узла дерева вычисляется верхняя граница возможного значения целевой функции: это делается путем решения «ослабленной» задачи – без условия целочисленности переменных. Поскольку математическая модель задачи является линейной, ослабленная (непрерывная) задача решается точно и дает допустимую верхнюю границу целевой функции в рамках принятой линеаризации. Это обеспечивает корректность отсека в рамках модели, однако точность границы зависит от адекватности линеаризации исходных

зависимостей. При появлении существенных нелинейных эффектов погрешность оценки верхней границы может возрастать, что потенциально снижает эффективность отсечений либо приводит к потере перспективных ветвей. В представленном примере задача остается линейной и детерминированной, что позволяет корректно применять отсечения и находить оптимальное решение в рамках принятых допущений. Сравнение верхней границы ветки с текущим решением: если граница ниже, ветвь исключается из рассмотрения.

Для определения параметров задачи привлекают специалистов защиты информации. Вводятся следующие ограничения:

- СЗИ должны быть сертифицированы (ФСТЭК России, а также требованиям Федеральных авиационных правил и рекомендаций ИКАО оснащению воздушных судов оборудованием АЗН-В)²;

- должны соответствовать классу защищенности не ниже требуемого и уровня доверия;

- должны быть совместимы с существующей инфраструктурой;

- стоимость внедрения не должна превышать выделенный бюджет. Для авиационных систем критически важна совместимость с бортовым оборудованием, работающим в реальном времени [10], и наземными станциями многопозиционных систем наблюдения. Недопустимо внесение задержек более 0,1 с.

Математическая модель задачи может быть описана следующим образом.

Пусть имеется n кандидатов на выбор средств защиты информации. Множество кандидатов I разделяется на два подмножества: I_{base} – средства защиты, необходимые для реализации мер адаптированного базового набора; I_{add} – дополнительные средства защиты.

Используемые переменные в решении:

$x_i = 1$ для всех $i \in I_{base}$ (фиксированное значение, мера обязательна);

$x_i \in \{0, 1\}$ для всех $i \in I_{add}$ (выбираются в ходе оптимизации).

$x_i = 1$, если i -е СЗИ выбрано;

$x_i = 0$, если i -е СЗИ не выбрано.

Параметры для каждого СЗИ: P_i – уровень защиты (в баллах, 0–100), представляет собой интегральный показатель (функциональность, сертификация, стоимость владения, совместимость и т.д.), рассчитываемый с помощью анализа иерархии [11]. Использование аппарата метода анализа иерархий на этапе формирования параметра P_i позволяет экспертам заранее учесть веса различных векторов угроз и степень дублирования функций СЗИ до этапа дискретной оптимизации. Параметр может включать не только общий «уровень защиты», но и способность СЗИ противодействовать конкретным атакам на авиационные протоколы (например, подмена сообщений АЗН-В [2, 3, 12], глушение сигнала на частоте 1090 МГц [13], интерференция); C_i – стоимость внедрения; K_i – класс защиты по ФСТЭК (1, 2, 3, ...); T_i – уровень доверия к СЗИ (1–6); S_i – показатель совместимости (0–1).

Целевая функция должна максимизировать эффективность защиты при соблюдении требований установленного уровня защищенности:

$$Z_{\max} = \sum_{i=1}^n P_i x_i.$$

Система ограничений:

- ограничение № 1, бюджет: $\sum (C_i x_i) \leq B_{\max}$, где $B_{\max}$ – максимальный бюджет;

- ограничение № 2, класс защиты и уровень доверия: для всех i , где $x_i = 1$;

- $K_i \geq K_{\min}$ и $T_i \geq T_{\min}$, где $K_{\min}$, $T_{\min}$ – минимальные требуемые класс и уровень доверия;

- ограничение № 3, совместимость: $\sum (S_i x_i) \geq S_{\min} \sum x_i$, где $S_{\min}$ – минимальный показатель совместимости, при условии $\sum x_i > 0$;

- ограничение № 4, область определения переменных: $x_i = 1$, для всех $i \in I_{base}$; $x_i \in \{0, 1\}$, для всех $i \in I_{add}$.

Временная совместимость: суммарное время на внедрение и настройку выбранных СЗИ не должно превышать допустимый

² Концепция внедрения автоматического зависимого наблюдения на основе единого стандарта с развитием до функционала многопозиционных систем наблюдения в Российской Федерации (утв. распоряжением Минтранса России от 25.04.2018 № МС-68-Р).

срок, критичный для непрерывности бизнес-процессов авиапредприятия.

Важно отметить, что предварительная фильтрация кандидатов по жестким требованиям регуляторов (класс защиты, уровень доверия, минимальная совместимость) исключает из рассмотрения заведомо недопустимые комбинации, что снижает риск выбора набора с формально высоким баллом, но низкой надежностью. Таким образом, оптимизация ведется уже внутри множества заведомо допустимых СЗИ.

В самой оптимизационной модели взаимовлияния между СЗИ не учитываются напрямую: суммарная эффективность считается аддитивно, в более сложных сценариях целевая функция может быть расширена за счет аддитивных поправочных коэффициентов, отражающих парные эффекты совместимости и синергии, что позволит учесть как усиление, так и конфликт функций без перехода к полной нелинейной постановке. Это допущение оправдано для упрощенной постановки и позволяет продемонстрировать работу метода ветвей и границ.

Рассмотрим задачу выбора оптимального набора условных средств защиты информации из семи кандидатов для защиты информационной системы авиапредприятия, обрабатывающей персональные данные на 200 рабочих мест. В рамках методического примера параметры кандидатов (см. таблицу) сформированы на ос-

нове экспертных оценок с применением метода анализа иерархий. Данный подход позволяет привести характеристики СЗИ к единой количественной шкале, что обеспечивает корректность дальнейшей модели. В реальных условиях эксплуатации авиапредприятия указанные значения рассчитываются профильными специалистами по ИБ.

Показатель совместимости S_i в таблице является экспертной оценкой, рассчитанной по методике, основанной на методе анализа иерархий.

Ограничения задачи для предприятия (200 сотрудников): максимальный бюджет $B_{\max} = 18\,000\,000$ руб; минимальный класс защиты $K_{\min} = 2$; минимальный уровень доверия $T_{\min} = 4$; минимальная совместимость $S_{\min} = 0,85$;

Предварительная фильтрация кандидатов:

- по классу защиты ($K_i \geq 2$): исключаются № 2, 6 ($K = 1$);
- по уровню доверия ($T_i \geq 4$): исключаются № 2, 6 ($T = 3$);
- по совместимости ($S_i \geq 0,85$): из оставшихся исключается № 7 ($S = 0,70$).

Следовательно, допустимое множество ограничилось четырьмя вариантами: $I_{add} = \{1, 3, 4, 5\}$, т.е. имеется $n = 4$.

Система ограничений следующая:

- по бюджету $\sum (C_i x_i) \leq 18\,000\,000$;
- по классу защиты и уровню доверия: для всех i , где $x_i = 1$: $K_i \geq 2$ и $T_i \geq 4$;
- по совместимости $\sum (S_i x_i) \geq 0,85 \sum x_i$;

Параметры кандидатов для выбора средств защиты информации

Parameters for selecting information security tools

Наименование СЗИ	Уровень защиты	Стоимость внедрения	Класс защиты	Уровень доверия	Показатель совместимости
АПМ «Соболь»	85	1 600 000	2	4	0,95
«Криптон-замок»	70	2 640 000	1	3	0,90
АПМ «Аккорд»	90	1 500 000	2	4	0,85
Diamond VPN/FW	60	1 000 000	2	4	0,92
«Континент-АП»	75	2 060 000	2	4	0,88
С-Терра Клиент	65	700 000	1	3	0,94
КриптоПро NGate	55	400 000	2	4	0,70

• по области определения переменных: $x_i = 1$, для всех $i \in I_{base}$; $x_i \in \{0, 1\}$, для всех $i \in I_{add}$.

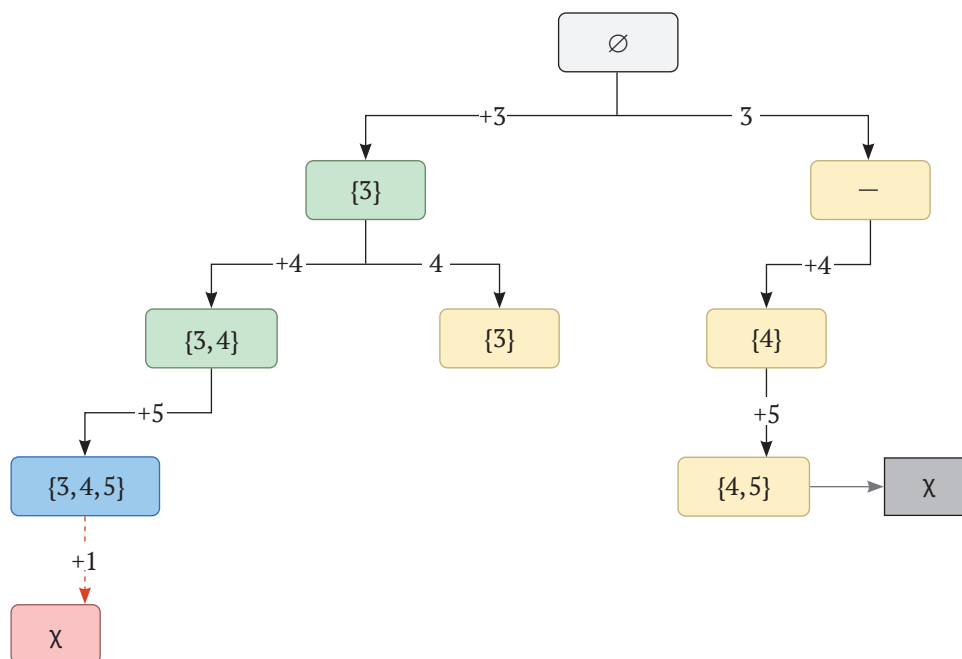
Апробация разработанной методики на примере задачи выбора СЗИ. Первый шаг – предварительная оценка эффективности. Для каждого кандидата вычислим отношение P_i/C_i – эффективность затрат: № 3 – $90/1\,500\,000 = 0,000060$; № 4 – $60/1\,000\,000 = 0,000060$; № 5 – $75/2\,060\,000 \approx 0,000036$; № 1 – $85/16\,000\,000 \approx 0,000005$. Таким образом, чем выше значение, тем «дешевле» получается защита. Порядок ветвления выбирается по убыванию этого показателя.

Второй шаг – формирование дерева решений и вычисление верхних границ. Дерево решений для рассматриваемого примера представлено на рисунке (+3, –3, +4, –4, +5, +1 – включение/исключение СЗИ № 3, 4, 5, 1).

Для каждого узла вычисляется верхняя граница – максимально возможная суммарная защита, которую можно получить, добавив к текущему набору любых из оставшихся кандидатов.

Если эта верхняя граница ниже текущего лучшего найденного решения, ветка отсекается и не исследуется. Следует учитывать, что верхняя граница, вычисляемая по ослабленной задаче без условия целочисленности, является допустимой, но может быть грубой при существенных нелинейных эффектах. В рамках принятой линейной модели это не приводит к ложному отсечению перспективных ветвей. При увеличении числа переменных и появлении нелинейных зависимостей погрешность оценки границы может возрастать, что потенциально снижает эффективность отсечений. В представленном примере задача остается линейной и детерминированной, что обеспечивает корректность отсечений и нахождение оптимального решения в рамках модели.

Для первого узла: набор {3}; текущая защита $Z=90$ баллов; бюджет 1,5 млн руб.; совместимость $0,85 \geq 0,85$; оставшиеся кандидаты (по убыванию P_i) – № 4 (60), 5 (75), 1 (85); верхняя граница $90 + 60 + 75 + 85 = 310$ баллов.



Дерево решений метода ветвей и границ для выбора СЗИ авиапредприятия

The decision tree of the branch-and-bound method for selecting information security measures for an airline

Для второго узла: набор {3, 4}; $Z = 90 + 60 = 150$ баллов; бюджет 2,5 млн руб.; совместимость $0,85 + 0,92 = 1,77 \geq 0,85 \cdot 2 = 1,70$; верхняя граница $150 + 75 + 85 = 310$ баллов.

Для третьего узла: набор {3, 4, 5}; $Z = 150 + 75 = 225$ баллов; бюджет 4,56 млн руб.; совместимость $0,85 + 0,92 + 0,88 = 2,65 \geq 2,55$; верхняя граница $225 + 85 = 310$ баллов; фиксируем решение $Z = 225$ баллов.

Условие по совместимости проверяется через суммарный показатель: его значение должно быть не ниже минимально допустимого, умноженного на число выбранных средств защиты. В данном примере требование выполнено.

Для четвертого узла: попытка добавить № 1 к {3, 4, 5}, т.е. переход к набору {1, 3, 4, 5}; бюджет $4,56 + 16 = 20,56$ млн руб. Тут имеем превышение ($20,56 > 18$), набор недопустим. Ветка закрывается.

Третий шаг – отсечение по верхней границе. Теперь проверим, нужно ли рассматривать ветку, где № 3 не включен, а начинается с № 4 или 5. Если рассмотрим узел, где № 3 исключен, но включен № 4 и 5 (набор {4, 5}), получаем: $Z = 60 + 75 = 135$ баллов; бюджет 3,06 млн руб.; совместимость $0,92 + 0,88 = 1,80 \geq 1,70$; оставшийся вариант № 1 (85); верхняя граница $135 + 85 = 220$ баллов. При сравнении с существующим решением даже в лучшем случае эта ветвь не превысит уже найденное решение.

Данное отсечение позволит сократить пространство поиска на 50 % относительно метода полного перебора. В реальных условиях, где количество потенциальных СЗИ может превышать 30 ед., подобное раннее отсечение позволит сократить вычислительные ресурсы на формирование необходимой конфигурации без потери точности.

Четвертый шаг – это оптимальное решение. Алгоритм завершает поиск на комбинации {3, 4, 5}, которая формирует необходимый набор СЗИ. Итоговые параметры будут следующие: суммарный показатель защиты $Z = 225$ баллов, совокупная стоимость внедрения 4 560 000 руб., остаток бюджета 13 440 000 руб. Взаимовлияния

между СЗИ (синергия или конфликты) учтены на предварительном этапе при расчете интегрального показателя методом анализа иерархий. Сравнение оптимального набора {3, 4, 5} с альтернативным {1, 3} показывает, что последний при схожих затратах дает меньший уровень защиты, не обеспечивает эшелонированности и оставляет критически малый остаток бюджета, что подтверждает адекватность модели и оптимальность выбранного решения.

В данном примере рассматривается лишь четыре допустимых СЗИ, что не выявляет полного потенциала алгоритма, сама структура задачи относится к классу NP-трудных, но при расширении количества СЗИ до 15 компонентов метод полного перебора потребует анализа более 4000 вариантов.

3. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

С вычислительной точки зрения задача выбора СЗИ относится к классу комбинаторных оптимизационных задач. При использовании метода полного перебора пространство решений растет экспоненциально, а применение метода ветвей и границ позволяет существенно сократить перебор за счет раннего отсечения неперспективных ветвей по верхней границе целевой функции, среднее время работы снижается на 50–70 %. Механизм отсечения по верхней границе в таких случаях исключает до 60 % заведомо неоптимальных ветвей на ранних уровнях дерева решений, что делает предложенную методику выбора средств защиты информации авиапредприятия на основе метода ветвей и границ применимой для авиакомпаний.

Представленная модель является детерминированной и предполагает фиксированные значения параметров. На практике эти величины могут носить стохастический характер, также совместимость может быть нетранзитивной. В текущей постановке эти эффекты исключены для

упрощения демонстрации работы метода ветвей и границ; их учет требует перехода к стохастическим и нелинейным моделям, что является направлением дальнейших исследований.

Следует подчеркнуть, что в рамках приведенного численного примера, где число кандидатов невелико, а все ограничения линейны, метод ветвей и границ гарантирует нахождение глобального оптимума. Обсуждение возможной грубости верхней границы при нелинейных эффектах относится к перспективным усложнениям модели и не снижает достоверности полученного в данной работе результата. Для реальных задач с $N > 30$ и нелинейными ограничениями требуется адаптация процедур вычисления границ, что выносится в отдельное исследование.

Таким образом, в рамках принятой детерминированной линейной постановки задачи использование разработанной методики позволяет найти оптимальный набор СЗИ. При переходе к более реалистичным сценариям с неопределенностью, нелинейными взаимодействиями и нетранзитивными ограничениями требуется расширение модели и адаптация процедур вычисления границ. В частности, учет нетранзитивной совместимости в перспективе может быть реализован через введение бинарных матриц попарных ограничений (запрет на одновременное использование определенных пар СЗИ) или логических условий, что требует модификации процедуры ветвления. Выбранная конфигурация обеспечивает максимальный уровень защиты при соблюдении всех требований приказа ФСТЭК России № 21.

4. ЗАКЛЮЧЕНИЕ

Перспективными направлениями развития являются:

- переход к вероятностной постановке задачи с введением распределений;
- интеграция алгоритма в автоматизированные системы управления информационной безопасностью авиапредприятия;
- адаптация методики для выбора средств защиты бортовых систем связи и наземной инфраструктуры управления воздушным движением с учетом требований ИКАО по кибербезопасности;
- переход к стохастическим и нелинейным моделям, учитывающим неопределенность векторов угроз, синергию и конфликты между СЗИ, вариативность стоимости, нетранзитивный характер совместимости СЗИ (с введением бинарных ограничений на пары несовместимых средств) и формализацию требований временной совместимости. Перспективным направлением является усложнение целевой функции за счет введения аддитивных поправочных коэффициентов для парной совместимости, что однако выводит задачу из класса линейных и потребует адаптации процедуры вычисления границ для таких сценариев.

Кроме того, актуальность предложенной методики возрастает при переходе на стандарт АЗН-В 1090ES [14, 15] и отказе от первичных радиолокаторов, что требует оснащения воздушных судов новыми СЗИ. Таким образом, предложенная методика и применяемый в ее рамках математический метод ветвей и границ обеспечивают строгое и воспроизводимое решение задачи выбора СЗИ.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

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

³ Концепция внедрения автоматического зависимого наблюдения на основе единого стандарта с развитием до функционала многопозиционных систем наблюдения в Российской Федерации (утв. распоряжением Минтранса России от 25.04.2018 № МС-68-Р).

СПИСОК ИСТОЧНИКОВ

1. **Колтунова Т. В., Колтунов Н. Л.** Правовые аспекты обеспечения информационной безопасности в критической информационной инфраструктуре // Евразийский юридический журнал. 2022. № 3(166). С. 413–416. EDN: GBXTYW.
2. **Петров В. И.** Решение проблем кибербезопасности в гражданской авиации // Гражданская авиация на современном этапе развития науки, техники и общества. М. : ИД Академии Жуковского, 2021. С. 16–19. EDN: YTFJNR.
3. **Пригонюк Н. Д., Бунин А. В.** Защита информации на воздушных судах гражданской авиации от угроз и уязвимостей программного обеспечения систем // Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества», 16–17 мая 2018 г., Москва, Россия. М. : Академия имени Н. Е. Жуковского, 2018. С. 262. EDN: YHJPXF.
4. **Токарев Е. В.** Анализ современного законодательства и его влияние на защиту данных // Научный аспект. 2024. Т. 37. № 1. С. 4757–4762. EDN: AWICFA.
5. **Дроботенко И. А.** Проблемы реализации требований по информационной безопасности в соответствии с нормативными требованиями ФСТЭК России // Материалы научно-технической конференции «Микроэлектроника и информатика – 2024», 25–26 апреля 2024 г., Москва – Зеленоград. М.: Национальный исследовательский университет «Московский институт электронной техники», 2024. С. 60–64. EDN: BFFSMB.
6. **Матыюк С. П.** Исследование уязвимостей информационно-вычислительных систем воздушного транспорта // Сборник научных статей III международной научной конференции «Приоритетные направления инновационной деятельности в промышленности», 30–31 марта 2021 г., Казань, Россия. Казань : КОНВЕРТ, 2021. С. 181–182. EDN: SRRNSM.
7. **Курочкин В. А.** Применение метода ветвей и границ для решения минимаксной обобщенной задачи о назначениях // Материалы XIX международной молодежной научной конференции по естественнонаучным и техническим дисциплинам «Научному прогрессу творчество молодых», 19–20 апреля 2024 г., Йошкар-Ола. 2024. С. 754–756. EDN: NIVIQS.
8. **Елина Т. Н., Мыльников В. А.** Методика оценки экономической эффективности внедрения комплексной системы защиты информации на предприятии // Сборник докладов XVII Международной конференции по электромеханике и робототехнике «Зава-лишинские чтения 22», 12–14 апреля 2022 г., Санкт-Петербург, Россия. СПб. : ГУАП, 2022. С. 42–46. DOI: 10.31799/978-5-8088-1705-0-2022-17-42-46. EDN: EIHVRV.
9. **Гусеница Я. Н., Тимонов А. А., Чикирев А. А.** Методика выбора оптимального средства защиты информации для объекта вычислительной техники при ограничениях на вычислительные ресурсы // Техника средств связи. 2025. № 3(171). С. 57–66. DOI: 10.24412/2782-2141-2025-3-57-66. EDN: EKAAPY.
10. **Сбитнев А. В., Аникаев К. П.** Автоматизация контроля выполнения команд диспетчера экипажем воздушного судна // Гражданская авиация на современном этапе развития науки, техники и общества : сборник тезисов докладов Международной научно-технической конференции, посвященной 50-летию МГТУ ГА, 25–26 мая 2021 г., Москва, Россия. М.: ИД Академии Жуковского, 2021. С. 353–354. EDN: IVJFWT.
11. **Симонова Л. А., Вафин И. И., Вильданов А. Г.** Решение задач организации и планирования выбора спецтехники при формировании заявок на основе метода Саати // Техничко-технологические проблемы сервиса. 2023. № 1(63). С. 23–28. EDN: BBEHJN.
12. **Антонов А. А., Повалишина М. А.** Исследование эффективности методов шифрования в системе автоматического зависимо-го наблюдения-вещания // Научные труды КубГТУ. 2024. № 2. С. 111–121. DOI: 10.26297/2312-9409.2024.2.10. EDN: QGNSIP.
13. **Емельянов В. Е.** Оценка живучести информационных сетей средств навигации и управления воздушным движением // Вестник науки и образования Северо-Запада России. 2022. Т. 8. № 3. С. 52–56. EDN: KZVSYU.
14. **Антонов А. А.** Методика выбора средств защиты информации авиапредприятия на основе метода анализа иерархий // Научные

труды КубГТУ. 2023. № 1. С. 86–93. EDN: DPWHET.

15. **Косинский Т. В.** Проблема доктрины информационной безопасности как составной

части стратегии национальной безопасности Российской Федерации // Закон. Право. Государство. 2023. № 3(39). С. 87–90. EDN: OPUCEP.

REFERENCES

1. **Koltunova T. V., Koltunov N. L.** The legal aspects of ensuring of information security in the critical information infrastructure. *Eurasian Law Journal*. 2022. No. 3(166), pp. 413–416. EDN: GBXTYW. (In Russian)
2. **Petrov V. I.** Solving Cybersecurity Problems in Civil Aviation. *Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva*. Moscow : ID Akademii Zhukovskogo, 2021, pp. 16–19. EDN: YTFJNR. (In Russian)
3. **Prigonyuk N. D., Bunin A. V.** Protection of information on civil aviation aircraft from threats and vulnerabilities of system software. *Mezhdunarodnaya nauchno-tehnicheskaya konferentsiya "Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva"*, 16–17 maya 2018 g., Moskva, Rossiya. Moscow: Akademiya imeni N. E. Zhukovskogo, 2018, pp. 262. EDN: YHJPXF. (In Russian)
4. **Tokarev E. V.** Analysis of modern legislation and its impact on data protection. *Nauchnyy aspekt*. 2024. Vol. 37. No. 1, pp. 4757–4762. EDN: AWICFA. (In Russian)
5. **Drobotenko I. A.** Problems of implementing information security requirements in accordance with the regulatory requirements of the FSTEC of Russia. *Materialy nauchno-tehnicheskoy konferentsii "Mikroelektronika i informatika – 2024"*, 25–26 aprelya 2024 g., Moskva – Zelenograd. Moscow : Nacional'nyj issledovatel'skij universitet "Moskovskij institut ehlektronnoj tekhniki", 2024, pp. 60–64. EDN: BFFSMB. (In Russian)
6. **Matyuk S. P.** Research into the vulnerabilities of information and computing systems in air transport. *Sbornik nauchnykh statej III mezhdunarodnoj nauchnoj konferentsii "Prioritetnye napravleniya innovacionnoj deyatel'nosti v promyshlennosti"*, 30–31 marta 2021 g., Kazan', Rossiya. Kazan : KONVERT, 2021, pp. 181–182. EDN: SRRNSM. (In Russian)
7. **Kurochkin V. A.** Application of the branch and bound method to solve the minimax generalized assignment problem. *Materialy XIX mezhdunarodnoj molodezhnoj nauchnoj konferentsii po estestvennonauchnym i tehnicheskim disciplinam "Nauchnomu progressu tvorchestvo molodyh"*, 19–20 aprelya 2024 g., Joshkar-Ola. 2024, pp. 754–756. EDN: NIVIQC. (In Russian)
8. **Elina T. N., Mylnikov V. A.** Methodology for Assessing the Economic Efficiency of Implementing a Comprehensive Information Security System at a Company. *Sbornik dokladov XVII Mezhdunarodnoj konferentsii po ehlektromehanike i robototekhnike "Zavalishinskie chteniya 22"*, 12–14 aprelya 2022 g., St. Petersburg, Russia. St. Petersburg : GUAP, 2022, pp. 42–46. DOI: 10.31799/978-5-8088-1705-0-2022-17-42-46. EDN: EIHVRV. (In Russian)
9. **Gusenitsa Ya. N., Timonov A. A., Chikirev A. A.** Methodology for selecting the optimal information protection means for a computing equipment object under constraints on computing resources. *Means of communication equipment*. 2025. No. 3(171), pp. 57–66. DOI: 10.24412/2782-2141-2025-3-57_66. EDN: EKAAPY. (In Russian)
10. **Sbitnev A. V., Anikaev K. P.** Automation of monitoring the execution of a dispatcher's commands by the aircraft crew. *Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva : sbornik tezisov dokladov Mezhdunarodnoj nauchno-tehnicheskoy konferentsii, posvyashchennoj 50-letiyu MGTU GA*, 25–26 maya 2021 g., Moskva, Russia. Moscow : ID Akademii Zhukovskogo, 2021, pp. 353–354. EDN: IVJFWT. (In Russian)
11. **Simonova L. A., Vafin I. I., Vildanov A. G.** Solving the problems of organizing and planning the selection of special equipment when forming applications on the basis of the Saati method. *Tekhniko-tehnologicheskie problemy servisa*. 2023. No. 1(63), pp. 23–28. EDN: BBEHNJ. (In Russian)
12. **Antonov A. A., Povalishina M. A.** Investigation of the effectiveness of encryption methods in the system of automatic dependent surveillance-broadcasting. *Scientific Papers of Kuban State Technological University*. 2024.

- No. 2, pp. 111–121. DOI: 10.26297/2312-9409.2024.2.10. EDN: QGNSIP. (In Russian)
13. **Emelyanov V. E.** Assessment of the survivability of information networks of navigation and air traffic control. *Journal of Science and Education of North-West Russia*. 2022. Vol. 8. No. 3, pp. 52–56. EDN: KZVSYU. (In Russian)
14. **Antonov A. A.** The methodology of choosing the means of protecting the information of an airline based on the method of hier. *Scientific Papers of Kuban State Technological University*. 2023. No. 1, pp. 86–93. EDN: DPWHET. (In Russian)
15. **Kosinskiy T. V.** The problem of the information security doctrine as an integral part of the national security strategy of the Russian Federation. *Lex. Jus. Civitas*. 2023. No. 3(39), pp. 87–90. EDN: OPUCEP. (In Russian)

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT AUTHOR

АНТОНОВ Александр Александрович – канд. техн. наук, доцент, Финансовый университет при Правительстве Российской Федерации, Россия, 125167, Москва, пр-т Ленинградский, д. 49/2
E-mail: alaantonov@fa.ru
ORCID: 0000-0002-1787-6522

ANTONOV Alexander A. – Candidate of Engineering Sciences, Associate Professor, Financial University under the Government of the Russian Federation, Russia, 125167, Moscow, Leningradsky ave., 49/2