УДК 004.94
DOI: 10.26102/2310-6018/2026.55.4.019

Применение марковского процесса принятия решений при разработке стратегии информационной безопасности

К.В. Зубченко✉, Н.З. Султанов, Г.А. Шевцова

Российский государственный гуманитарный университет, Москва, Российская Федерация

Резюме. Актуальность исследования обусловлена ростом количества и сложности кибератак, в частности, необходимостью постоянного повышения уровня защиты организаций, а также постоянного планирования и моделирования стратегии защиты в условиях ограниченности ресурсов. Данная работа направлена на разработку модели, позволяющей осуществлять разработку стратегии информационной безопасности заданной организации с учетом экономических показателей. Основными методами исследования являются моделирование, сравнительный анализ и синтез. В работе содержатся характеристики смоделированных организаций, использованные в прототипе формулы и алгоритмы, а также числовые показатели критериев и параметров. Представлены зависимости между параметрами модели. В результате выявлена работоспособность модели на смоделированных организациях: получены оптимальные стратегии для каждой из них, коррелирующие с общепризнанными подходами к построению стратегий в реальных компаниях. Продемонстрированы результирующие графики состояния систем. Для всех организаций наиболее оптимальными оказались комплексные стратегии. В краткосрочной перспективе использование марковского процесса принятия решений позволяет успешно оптимизировать управленческие решения, независимо от степени зрелости компании. Выделение большого бюджета на информационную безопасность оказывает существенное влияние на эффективность только для компаний с низкой степенью зрелости. Результаты работы представляют практическую ценность для специалистов и руководителей по информационной безопасности, предоставляя инструмент для разработки оптимальной стратегии информационной безопасности в рамках заданного бюджета.

Ключевые слова: марковский процесс принятия решений, стратегия информационной безопасности, моделирование стратегии защиты, экономические затраты, оптимизация стратегии.

Для цитирования: Зубченко К.В., Султанов Н.З., Шевцова Г.А. Применение марковского процесса принятия решений при разработке стратегии информационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2026;14(4). URL: https://moitvivt.ru/ru/journal/article?id=2217 DOI: 10.26102/2310-6018/2026.55.4.019

Application of Markov decision process in developing an information security strategy

K.V. Zubchenko✉, N.Z. Sultanov, G.A. Shevtsova

Russian State University for the Humanities, Moscow, the Russian Federation

Abstract. The relevance of this study is driven by the growing number and complexity of cyberattacks, in particular the need to continually improve organizations' security levels, as well as the ongoing planning and modeling of security strategies in the face of limited resources. This work aims to develop a model for developing an information security strategy for a given organization, taking into account economic indicators. The primary research methods are modeling, comparative analysis, and synthesis. The paper contains the characteristics of the simulated organizations, the formulas and algorithms used in the prototype, as well as numerical indicators of criteria and parameters. The relationships between

the model parameters are presented. As a result, the model's performance on the simulated organizations was demonstrated: optimal strategies were obtained for each of them, correlating with generally accepted approaches to developing strategies in real companies. The resulting graphs of the system states are demonstrated. For all organizations, integrated strategies proved to be the most optimal. In the short term, the use of a Markov decision process allows for the successful optimization of management decisions, regardless of the company's maturity level. Allocating a large budget for information security has a significant impact on efficiency only for companies with a low maturity level. The results of the work are of practical value to information security specialists and managers, providing a tool for developing an optimal information security strategy within a given budget.

Keywords: Markov decision process, information security strategy, security strategy modeling, economic costs, strategy optimization.

For citation: Zubchenko K.V., Sultanov N.Z., Shevtsova G.A. Application of Markov decision process in developing an information security strategy. *Modeling, Optimization and Information Technology.* 2026;14(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2217 DOI: 10.26102/2310-6018/2026.55.4.019

Введение

В связи со значительно возросшей цифровизацией, сфера информационной безопасности (ИБ) столкнулась с огромным количеством вызовов. При решении поставленных задач все чаще прибегают к стратегическому планированию и моделированию угроз [1].

При построении долгосрочной стратегии необходимо учитывать ряд факторов, при этом опираясь на модель угроз. Моделирование угроз для конкретной организации зачастую строится на основе методического документа Федеральной службы по техническому и экспортному контролю (ФСТЭК)[1], однако, в силу разнообразия технического обеспечения разных отраслей, регулирующие документы являются скорее шаблоном, которые необходимо адаптировать под собственные реалии. При этом разработка модели угроз методом «мозгового штурма» допускает наличие человеческого фактора и является индуктивным методом, который зачастую показывает лишь проблемы, а не решения. В том числе существует ряд проблем при построении стратегии информационной безопасности:

1. Экономическая проблема. Ситуация в сфере ИБ такова, что организации в основном руководствуются требованиями регулятора, а не реальным обеспечением защищенности [2]. Кроме того, часто не учитываются возможные выгоды от развития ИБ в организации.

2. Проблема ландшафта угроз. За счет уже упомянутого разнообразия отраслей, стратегия информационной безопасности для каждого из предприятий является индивидуальной и должна пересматриваться на постоянной основе. Для реализации качественного подхода приходится разрабатывать собственные метрики эффективности защиты, поскольку для многих сфер отсутствуют отраслевые стандарты ИБ [3].

3. Эффективность по Парето. Для достижения высоких показателей эффективности ИБ организации достаточно найти управленческие решения, которые позволят балансировать между экономическими затратами и эффективностью [4]. Поиск таких решений затруднен предыдущими проблемами, что приводит к нерациональному использованию ресурсов и, как итог, к серьезным уязвимостям.

[1] *Методика оценки угроз безопасности информации от 5 февраля 2021 г.* ФСТЭК России. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 03.02.2026).

Для решения данных проблем, в частности для эффективного стратегического планирования развития ИБ компании, могут применяться марковские процессы принятия решений (МППР). Их применение позволит находить оптимальные управленческие решения. Злоумышленники уже используют искусственный интеллект в кибератаках [5], поэтому оптимизация и автоматизация принятия решений может предоставить возможность проактивно реагировать на эти угрозы. Исследования возможности применения МППР в областях моделирования кибератак и анализа защищенности проводились в следующих публикациях [6, 7].

Целью данной работы является разработка модели, позволяющей осуществлять разработку стратегии ИБ с использованием МППР, с учетом экономических показателей затрат.

В ходе исследования будут смоделированы 5 абстрактных организаций с различными состояниями систем. Результаты данной работы могут быть полезны при построении модели угроз, составлении стратегии ИБ и разработке систем поддержки принятия решений с учетом ограничений.

Для достижения поставленной цели потребуется решение следующих задач:

1. Формализация задачи и разработка алгоритма на основе МППР;
2. Моделирование 5 абстрактных организаций для проверки гипотезы;
3. Разработка прототипа системы, реализующей алгоритм;
4. Сравнительный анализ результатов работы системы.

Материалы и методы

В ходе работы применялись следующие общенаучные методы: синтез, сравнительный анализ, сбор данных, моделирование. В качестве метода реализации МППР выбрана итерация состояния среды (Value iteration). Разработка прототипа системы производилась с использованием языка программирования Python.

Формализация задачи. Марковский процесс принятия решений (МППР, MDP) – это математическая структура, используемая для моделирования принятия решений в ситуациях, когда результаты частично случайны, а частично находятся под контролем лица, принимающего решение [8].

Необходимо задать пространство состояний S, которое отражает текущее состояние системы, и пространство действий A, определяющее множество дискретных управленческих решений (вмешательств).

Каждое состояние системы S включает в себя следующие атрибуты:

– Уровень угроз. Это экзогенный стохастический фактор, принимающий значения из ординарной шкалы (Низкий, Средний, Высокий, Критический). Он показывает количественную и качественную характеристику угроз безопасности для данной системы.

– Бюджет. Финансовый ресурс, определяющий доступность управленческих решений.

– Состояние отдельных технических компонентов. Могут быть бинарными («Наличие EDR», «Наличие SIEM») или порядковыми («Состояние межсетевого экранирования», «Осведомленность сотрудников», «Состояние резервного копирования»).

В Таблице 1 приведены 5 абстрактных систем с их параметрами (пространство состояний S). Параметры П4–П8 были сформированы на основании перечня типовых прямых затрат на информационную безопасность [2].

Таблица 1 – Список абстрактных систем (пространство состояний)
Table 1 – List of abstract systems (state space)

Параметр	Орг. 1	Орг. 2	Орг. 3	Орг. 4	Орг. 5
Бюджет (у. е.) (П1)	100000	100000	150000	500000	500000
Горизонт планирования (лет) (П2)	1	2	2	3	5
Уровень угроз (Низкий/Средний/Высокий) (П3)	Низкий	Средний	Средний	Низкий	Высокий
Состояние межсетевого экранирования (1–3) (П4)	1	1	2	2	1
Наличие EDR агентов в инфраструктуре (НЕТ/ДА) (П5)	НЕТ	НЕТ	ДА	ДА	НЕТ
Наличие SIEM в инфраструктуре (НЕТ/ДА) (П6)	НЕТ	НЕТ	НЕТ	НЕТ	ДА
Осведомленность сотрудников (1–3) (П7)	1	1	1	2	2
Состояние системы резервирования (1–3) (П8)	1	1	2	2	2
Вероятность взлома (1–100 %) (П9)	1,96	5,88	1,20	0,30	1,89
Оценка безопасности (1–100 %) (П10)	32	12	40	66	18

В Таблице 2 приведены управленческие решения (пространство действий A). Каждое действие имеет параметры стоимости (в условных единицах), времени выполнения и вероятности успеха. При этом «Бездействие» не имеет стоимости и всегда длится 1 день с вероятностью 1,0. Во время выполнения одного действия, остальные выполняться не могут. Вероятность успеха обуславливает возможность действия не быть исполненным. В таком случае длительность учтется, стоимость отнимется от бюджета, но никакого эффекта не будет.

Таблица 2 – Демонстрационный список руководящих действий (пространство действий)
Table 2 – Demo list of guiding actions (action space)

Действие	Стоимость (у. е.)	Длительность (дн.)	Вероятность успеха
Бездействие (DO_NOTHING) (A1)	0	1	1,0
Улучшение межсетевого экранирования (UPGRADE_FIREWALL) (A2)	8000	14	0,95
Внедрение EDR агента (DEPLOY_EDR) (A3)	12000	21	0,9
Подключение узла к SIEM (IMPLEMENT_SIEM) (A4)	20000	60	0,85

Таблица 2 (продолжение)
Table 2 (continued)

Повышение осведомленности сотрудников (CONDUCT_TRAINING) (A5)	4000	7	0,95
Улучшение резервного копирования (ENHANCE_BACKUP) (A6)	6000	14	0,9

Для формализации задачи необходимо определить функцию переходов (P) и функцию вознаграждения (R).

Функция переходов определяет вероятностную модель динамики системы и зависит от текущего состояния (s) и выбранного управленческого действия (a). При этом (s') является следующим состоянием после выполнения действия a из состояния s. Стоит отметить, что вероятность изменения угрозы задается не стационарно и зависит от выбранного действия (например, «Бездействие» повышает вероятность ухудшения). При успешном выполнении, действие модифицирует соответствующие бинарные или порядковые параметры состояния системы. Полная функция переходов задается следующей формулой:

$$P(s'|s,a) = \sum_{\text{П3}'}[P_{\text{П3}}(\text{П3}' \mid \text{П3}, a) \cdot \alpha(A) \cdot P_s(s'|s,a,\text{П3}') + (1 - \alpha(A) \cdot P_F(s'|s,a,\text{П3}'))],$$

где $\alpha(A)$ – вероятность успешного действия, P_F – вероятность неудачного перехода, P_S – вероятность успешного перехода.

Функция вознаграждения вычисляет скалярное вознаграждение и является компромиссом между финансовыми затратами и эффективностью.

$$r(s,a,s') = \sum R_i + \gamma^t,$$

где R_i – штраф или премия за определенное действие, i – индекс компонента вознаграждения, t – дискретный временной шаг действия из Таблицы 2.

При этом введен коэффициент дисконтирования $\gamma = 0{,}98$ для предпочтения немедленных вознаграждений перед будущими.

Цель алгоритма: найти оптимальную функцию ценности состояния $V*(s)$ и детерминированную оптимальную политику $\pi*(s)$, максимизирующую ожидаемую дисконтированных сумму вознаграждений.

$$V*(s) = max_a\big[P(s'|s,a)\big(R(s,a,s') + \gamma V*(s')\big)\big],$$

$$\pi*(s) = arg\ max_a \sum_{s'} P\big(s'|s,a\big)\big(R(s,a,s') + \gamma V*(s)\big).$$

Алгоритм итеративно обновляет значения для всего пространства состояний (S) до достижения критерия сходимости. Для каждого состояния выполняется полный перебор допустимых действий и вычисление ожидаемого значения через взвешенную сумму по возможным следующим состояниям. Итеративное обновление задается формулой:

$$V_{k+1}(s) = max_a Q_k(s,a),$$

где $Q_k(s,a) = \sum_{s'} P(s'|s,a)\big(R(s,a,s') + \gamma V_k(s')\big)$, k – номер итерации.

Критерий остановки равен:

$$max_s|V_{k+1}(s) - V_k(s)| < \varepsilon,$$

где $\varepsilon = 0{,}01$, k – номер итерации.

Для оценки политики выполняется N симуляций Монте-Карло (в рамках прототипа $N = 30$):

$$V(\pi) = \frac{1}{N}\sum_{i=1}^{N}\sum_{t=0}^{H}\gamma^t r_t^{(i)},$$

где H – горизонт планирования, $r_t^{(i)}$ – вознаграждение на шаге t в симуляции i.

Вычисление параметров. Эффективность руководящих действий задается мультипликативными коэффициентами α, от которых зависит параметр П9:

$$П9(s) = P_{П3} \cdot \alpha_{П4} \cdot \alpha_{П5} \cdot \alpha_{П6} \cdot \alpha_{П7} \cdot \alpha_{П8},$$

где $P_{П3}$ принимает значения от 0,05 до 0,5 в случаях низкой и критической угрозах соответственно.

П10 зависит от суммы всех остальных параметров, скорректированных в соответствии с выполненными действиями.

$$П10(s) = 100 - П3 \cdot 20 - (3 - П4) \cdot 8 - П5(0|15) - П6(0|15) - (3 - П7) \cdot 6 - (3 - П8) \cdot 5.$$

Ограничения. Представленная модель имеет ряд ограничений. Текущая реализация использует дискретизацию непрерывных параметров, что может приводить к потере информации. Модель также ограничена стационарными вероятностными переходами. Некоторые внешние факторы не учитываются, что в реальных условиях может приводить к неверной оптимизации. Также модель ограничена пространством действий, которые должны быть расширены в соответствии с возможностями применения в используемых системах. Бюджетная сумма не должна быть меньше минимальной стоимости действия и не должна равняться нулю.

Результаты

Результаты проведенных симуляций представлены в Таблице 3. Оптимизированные параметры отмечены зеленым цветом, без изменений – желтым, ухудшенные – красным.

Таблица 3 – Результаты проведенных симуляций для всех рассматриваемых организаций
Table 3 – Results of the simulations conducted for all the organizations under consideration

Параметр	Орг. 1	Орг. 2	Орг. 3	Орг. 4	Орг. 5
Бюджет (у. е.) (П1). Остаток	37 200	24 000	103 067	437 733	407 467
Уровень угроз (Низкий/Средний/Высокий) (П3)	Низкий	Высокий	Высокий	Высокий	Высокий
Состояние межсетевого экранирования (1–3) (П4)	2	1	3	3	3
Наличие EDR агентов в инфраструктуре (НЕТ/ДА) (П5)	ДА	ДА	ДА	ДА	ДА
Наличие SIEM в инфраструктуре (НЕТ/ДА) (П6)	ДА	ДА	ДА	ДА	ДА

Таблица 3 (продолжение)
Table 3 (continued)

Осведомленность сотрудников (1–3) (П7)	1	3	3	3	3
Состояние системы резервирования (1–3) (П8)	1	1	2	2	2
Вероятность взлома (1–100 %) (П9)	1,52	2,05	0,48	0,25	0,26
Оценка безопасности (1–100 %) (П10)	54	16	42	50	49

Также были сформированы графики для наглядной демонстрации изменения состояния систем. На графиках в окне «распределение действий» показано количество предпринятых действий в соответствии с пространством действий. Для удобства интерпретации результатов введена метрика «Риск», которая является зеркальным и линейно зависимым отображением П10 («Защищенность системы»). «Риск» высчитывается в процентах по следующей формуле:

$$\text{Риск} = 100 - \text{П10}.$$

Изменения состояний систем представлены на Рисунках 1–5.

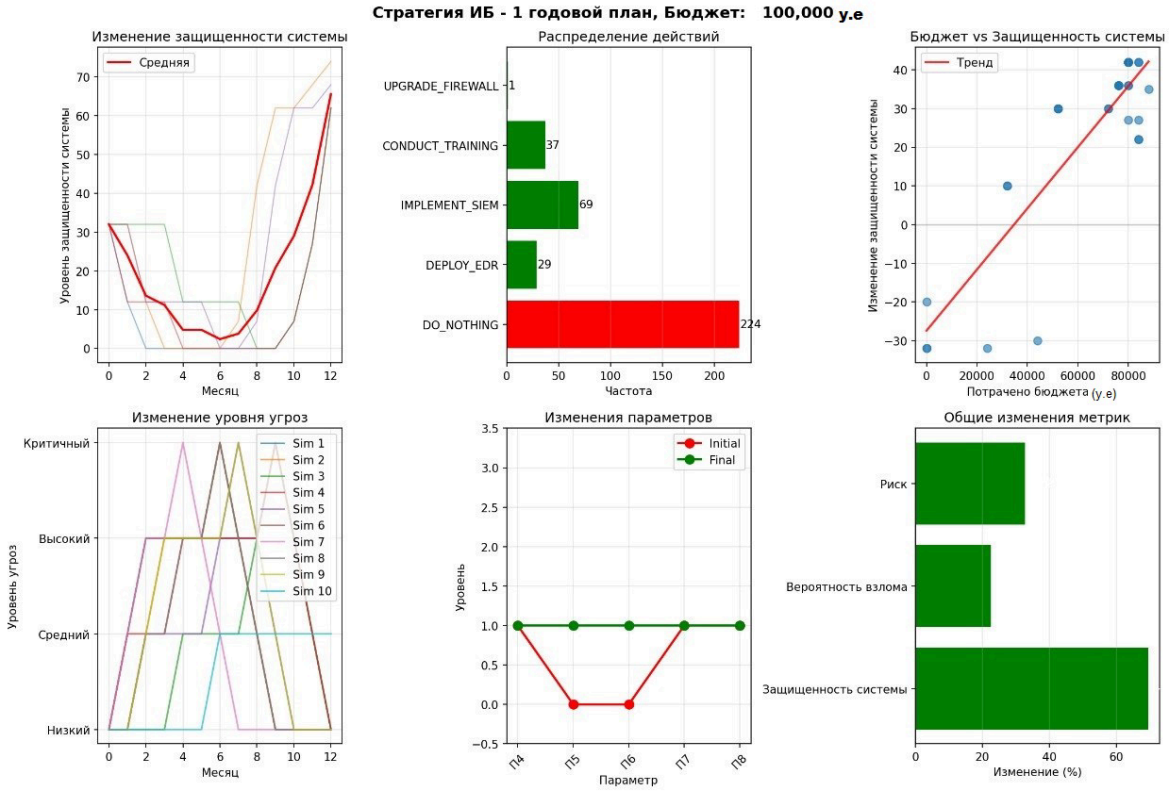

Рисунок 1 – Сводные графики результата оптимизации стратегии для Орг. 1
Figure 1 – Summary graphs of the strategy optimization results for Org. 1

Для организации 1 можно увидеть значительное повышение уровня некоторых параметров (П5 и П6), а также значительное улучшение среднего уровня защищенности системы. При этом уровень комплексной защищенности системы увеличился более чем на 60 %.

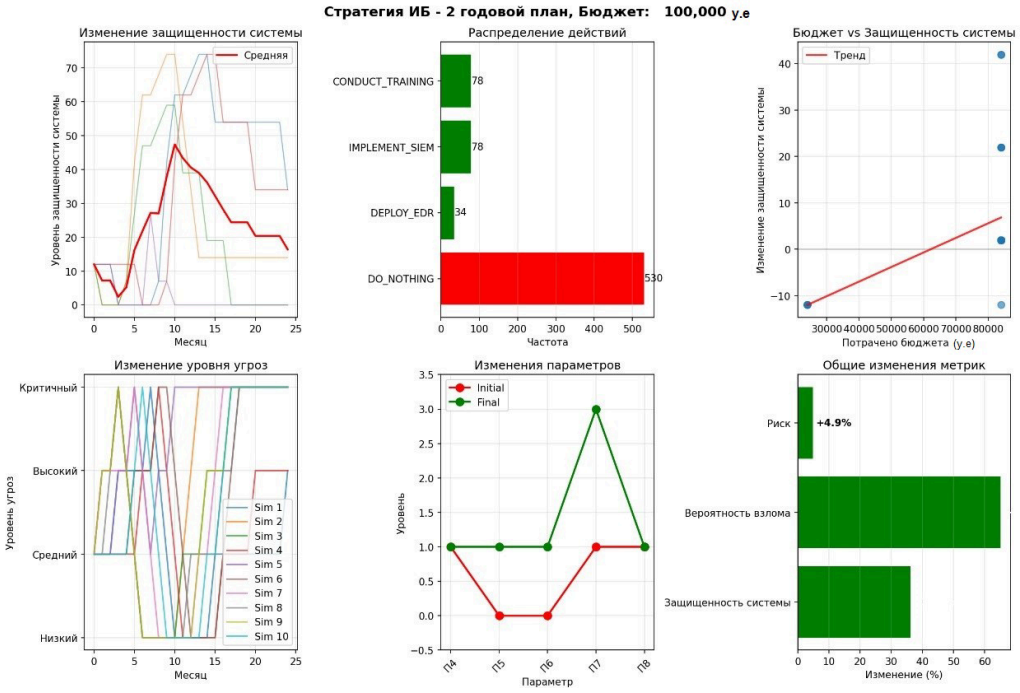

Рисунок 2 – Сводные графики результата оптимизации стратегии для Орг. 2
Figure 2 – Summary graphs of the strategy optimization results for Org. 2

Для организации 2 прослеживается улучшение большей части всех параметров (П5, П6, П7), но функция отношения затраченного бюджета к результирующей защищенности системы имеет менее выраженный положительный тренд, чем для организации 1. Улучшение уровня защищенности системы составило 35 %. Среднее изменение защищенности системы в первый год росло, а затем начало падать, предположительно, в связи с нехваткой бюджета на такой срок.

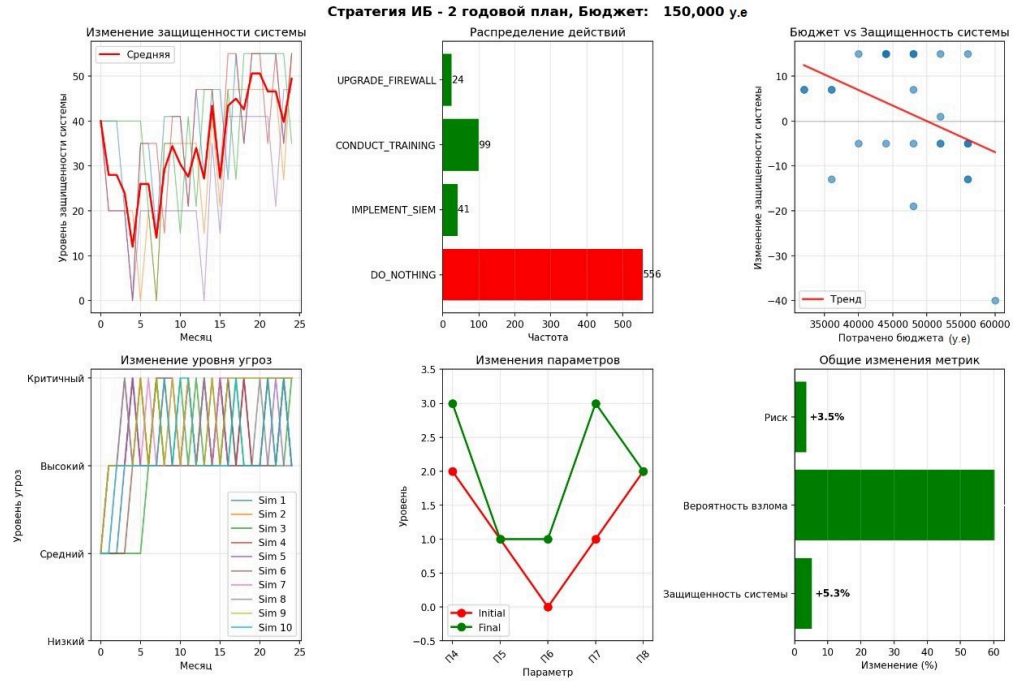

Рисунок 3 – Сводные графики результата оптимизации стратегии для Орг. 3
Figure 3 – Summary graphs of the strategy optimization results for Org. 3

Для организации 3 можно констатировать улучшение параметров П4, П6 и П7. При этом среднее изменение защищенности системы на протяжении всего периода было стабильно положительным. В связи с изначально высокой оценкой безопасности (40 %), улучшение было незначительным: +5,3 %. Однако, уровень угроз повысился в связи с длительностью рассматриваемого диапазона и сопряженными с этой длительностью изменениями ландшафта угроз. При этом вероятность взлома понизилась – это показатель того, что даже при низких рисках для конкретной организации за счет правильной стратегии, общемировой уровень угроз растет, и без внедрения новых эффективных управленческих решений на длительном промежутке времени рано или поздно достигнет высоких значений.

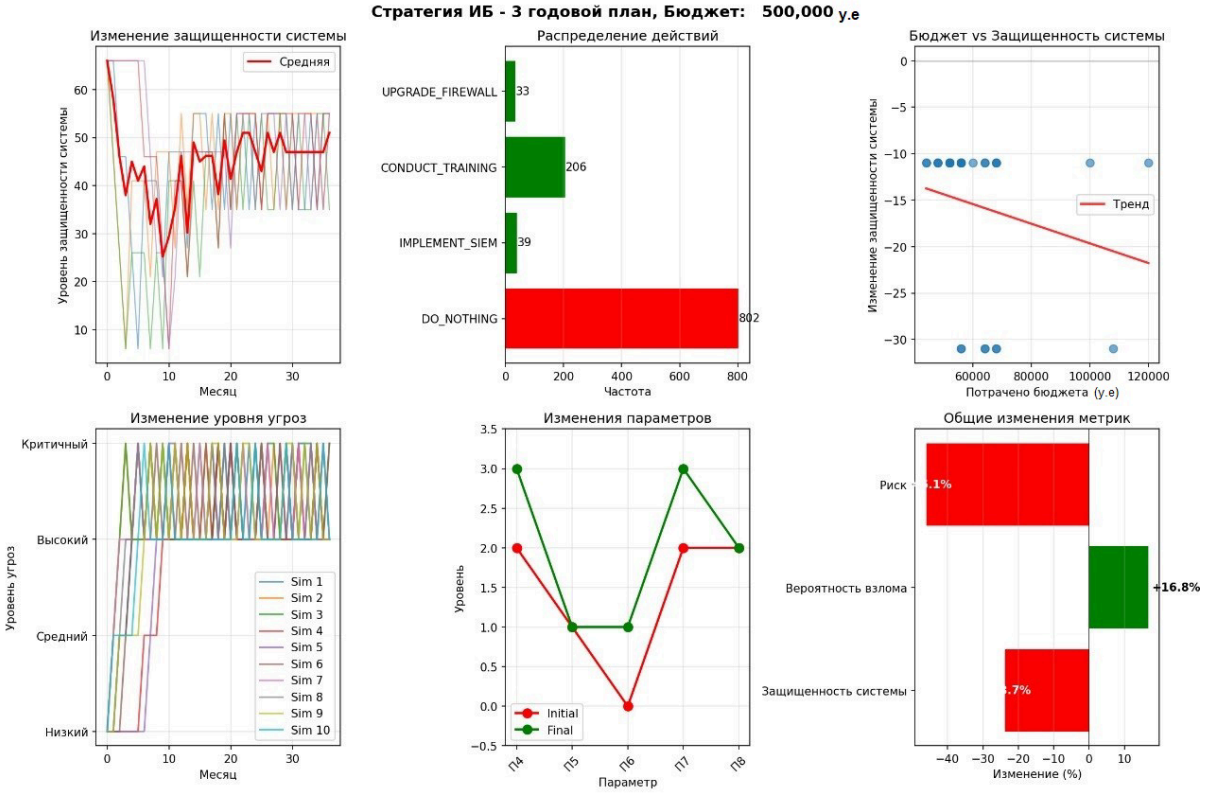

Рисунок 4 – Сводные графики результата оптимизации стратегии для Орг. 4
Figure 4 – Summary graphs of the strategy optimization results for Org. 4

Для организации 4 можно констатировать уменьшение защищенности системы на 23,7 %. При одновременных улучшениях параметров П4, П6, П7. Такие результаты свидетельствуют о том, что возник дефицит эффективных управленческих решений на горизонте 3 лет. При максимизации параметров П4, П5, П6, П7 уровень угроз все равно достиг критического уровня, а тренд корреляции между затраченным бюджетом и защищенностью системы стал отрицательным – вложенные условные единицы перестали увеличивать эффективность из-за высокого изначального уровня защищенности организации. Для получения положительных результатов уровня защищенности системы на таком горизонте необходим расширенный список управленческих действий.

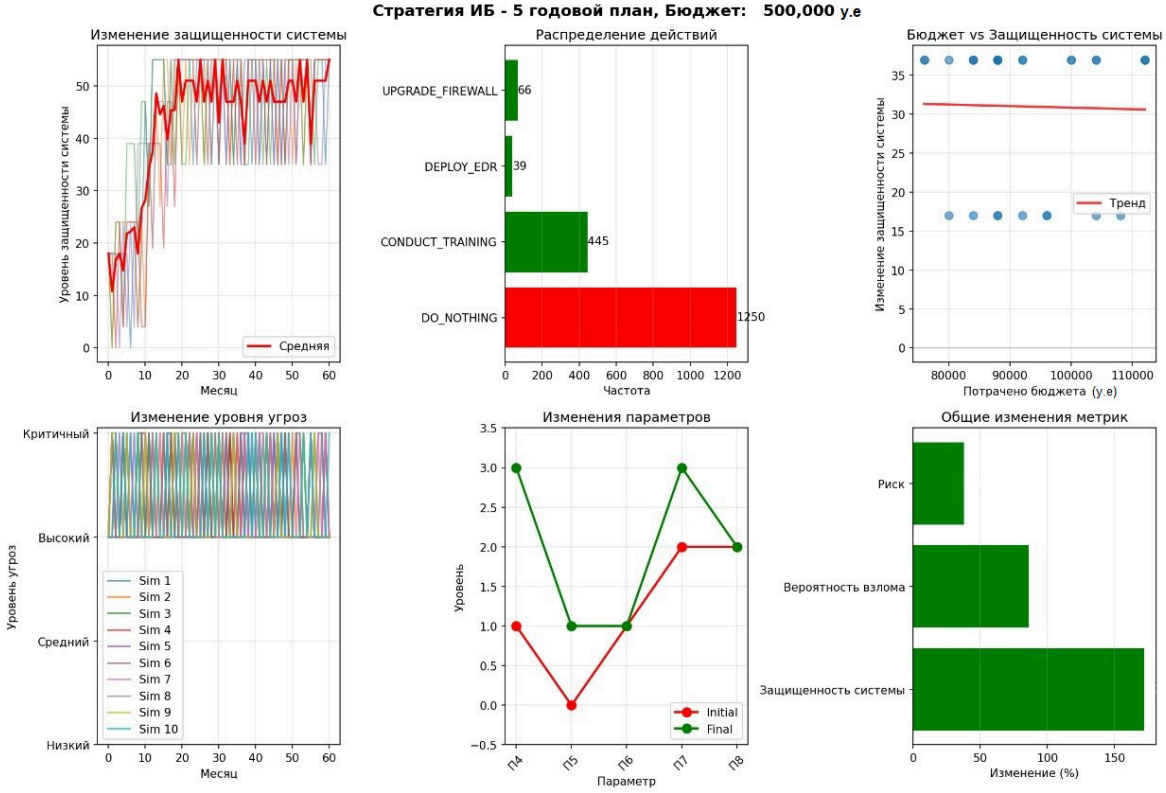

Рисунок 5 – Сводные графики результата оптимизации стратегии для Орг. 5
Figure 5 – Summary graphs of the strategy optimization results for Org. 5

Организация 5 изначально имела один из самых низких уровней защищенности, однако располагая крупным бюджетом на длительный срок в среднем защищенность системы выросла до определенного уровня (примерно 50 %), после чего остановилась. Это свидетельствует об ограниченных управленческих действиях. Данный тезис подтверждает тренд корреляции бюджета с уровнем защищенности – он слабо-отрицательный. Тем не менее, общий уровень защищенности системы вырос более чем на 150 %. В результате симуляций оптимальная стратегия вывела организацию 5 на уровень плато. Для дальнейшего улучшения показателей увеличение бюджета не приведет к значимым улучшениям без реализации качественно новых управленческих решений.

Обсуждение

На основе полученных данных можно сделать следующие выводы:

1. Для организаций с низким уровнем зрелости модель улучшает параметры системы даже при небольшом горизонте планирования. Для таких организаций бюджет крайне важен и играет ключевую роль, что видно из графиков «Бюджет VS защищенность системы» на Рисунке 1 и 2.

2. Для организаций с высоким уровнем зрелости необходима более широкая вариативность действий при моделировании, поскольку, достигнув максимального значения параметров, модель выбирает действие A1, которое на большом промежутке времени сильно ухудшает показатели.

3. На коротком горизонте планирования (до 3 лет) удалось значительно повысить уровень защищенности рассматриваемых организаций, при этом уложившись в требуемый бюджет.

4. Дисконтирование вознаграждения в МППР отлично отражает реальную ценность управленческих решений в сфере ИБ. Со временем даже самое лучшее управленческое решение устаревает и перестает быть эффективным в силу смены ландшафта угроз

5. Наибольшую эффективность показали комплексные стратегии, применяющие максимальное количество доступных действий. Стратегии, делающие упор только на внедрение (EDR или SIEM), или только на организационные мероприятия, ухудшили общее состояние систем.

6. Сумма выделенных средств (бюджет) оказывает существенное влияние на оценку защищенности организации в долгосрочной перспективе. Это можно увидеть при сравнительном анализе результатов Орг. 1 и Орг. 2 (графики «Изменение защищенности системы»), у которых исходные параметры одинаковые, но горизонт планирования отличается. График уровня защищенности Орг. 2 в первый год практически повторяет график Орг. 1, а затем заканчивается бюджет, и общая оценка защищенности начинает падать.

Данные выводы коррелируют с общепринятыми подходами к стратегическому планированию ИБ [9, 10]. Из этого следует, что МППР, с учетом ограничений, может быть использован для планирования стратегии ИБ организации. При этом ни одна из организаций не вышла за пределы своего бюджета.

Также стоит отметить, что бездействие (A1) во всех случаях более всего влияет на отрицательную оценку защищенности. Это значит, что даже управленческое решение с минимальной эффективностью уменьшает риски для ИБ.

Заключение

Поставленная цель исследования достигнута: разработан прототип системы, реализующий МППР с учетом экономических ограничений, позволяющий оптимизировать стратегическое планирование информационной безопасности. На основе проведенного сравнительного анализа сформулированы следующие выводы:

1. В краткосрочной перспективе (от 1 года до 2 лет) МППР обеспечивает эффективную оптимизацию управленческих решений для всех рассмотренных абстрактных организаций, независимо от их степени зрелости.

2. Оптимизированные стратегии коррелируют с подходами к построению защищенных систем в сфере ИБ.

3. Наибольшей эффективности можно добиться только комплексным применением мер обеспечения ИБ.

4. Выделение большого бюджета на ИБ влияет на эффективность только в контексте организаций с низким уровнем зрелости.

Перспективным направлением дальнейших исследований в данной области является использование МППР в системах поддержки принятия решений и внедрение имитационного моделирования для постоянной коррекции коэффициентов и расширения параметров и действий.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Заводцев И.В., Борисов М.А., Бондаренко Н.Н., Мелешко В.А. Моделирование угроз безопасности информации и определение их актуальности для информационных систем объектов информатизации федеральных органов исполнительной власти. *Computational Nanotechnology*. 2022;9(1):106–114. https://doi.org/10.33693/2313-223X-2022-9-1-106-114

Zavodtsev I.V., Borisov M.A., Bondarenko N.N., Meleshko V.A. Modeling Information Security Threats and Determination of Their Relevance for Information Systems of Informatization Objects of Federal Executive Authorities. *Computational Nanotechnology*. 2022;9(1):106–114. (In Russ.). https://doi.org/10.33693/2313-223X-2022-9-1-106-114

2. Козырь Н.С. Затраты и выгоды информационной безопасности бизнеса. *Управление*. 2023;11(4):110–118. https://doi.org/10.26425/2309-3633-2023-11-4-110-118
Kozyr N.S. Costs and benefits of business information security. *Management (Russia)*. 2023;11(4):110–118. (In Russ.). https://doi.org/10.26425/2309-3633-2023-11-4-110-118
3. Георгиевский А.Д., Черемухина Ю.Ю. Система обеспечения информационной безопасности и внедрение механизмов управления. *Компетентность*. 2025;(10):41–43. https://doi.org/10.24412/1993-8780-2025-10-41-43
Georgievskiy A.D., Cheremukhina Yu.Yu. System for ensuring information security and implementation of management mechanisms. *Competency (Russia).* 2025;(10):41–43. (In Russ.). https://doi.org/10.24412/1993-8780-2025-10-41-43
4. Санакоев Р.Г., Плешаков В.В. Математические модели и методы оптимизации в управлении организационными системами: теория, методология и практика применения в экспертной деятельности. *Инженерный вестник Дона*. 2026;(2). URL: https://www.ivdon.ru/ru/magazine/archive/n2y2026/10755
Sanakoev R.G., Pleshakov V.V. Mathematical models and optimization methods in the management of organizational systems: theory, methodology, and practice of application in expert activity. *Engineering Journal of Don.* 2026;(2). (In Russ.). URL: https://www.ivdon.ru/en/magazine/archive/n2y2026/10755
5. Намиот Д.Е. О кибератаках с помощью систем Искусственного интеллекта. *International Journal of Open Information Technologies*. 2024;12(9):132–141.
Namiot D. On cyberattacks using Artificial Intelligence systems. *International Journal of Open Information Technologies.* 2024;12(9):132–141. (In Russ.).
6. Ветров И.А., Подтопельный В.В. Особенности использования марковских процессов принятия решений при моделировании атак на системы искусственного интеллекта. *Вестник Самарского университета. Естественнонаучная серия.* 2024;30(4):147–160. https://doi.org/10.18287/2541-7525-2024-30-5-147-160
Vetrov I.A., Podtopelny V.V. Features of using Markov decision-making processes when modeling attacks on artificial intelligence systems. *Vestnik of Samara University. Natural Science Series.* 2024;30(4):147–160. (In Russ.). https://doi.org/10.18287/2541-7525-2024-30-5-147-160
7. Трапезников Е.В., Магазев А.А., Касенов А.А. Марковская модель кибератак и ее применение к анализу защищенности информации в автоматизированных системах. *Моделирование, оптимизация и информационные технологии.* 2024;12(2). https://doi.org/10.26102/2310-6018/2024.45.2.011
Trapeznikov E.V., Magazev A.A., Kasenov A.A. The Markov model of cyber attacks and its application to the analysis of information security in automated systems. *Modeling, Optimization and Information Technology.* 2024;12(2). (In Russ.). https://doi.org/10.26102/2310-6018/2024.45.2.011
8. Емшиков Б.М., Овезбердиев Г.Д. Марковские процессы принятия решений: современные подходы и применение в интеллектуальных системах. *Символ науки*. 2024;2(12-1):41–42.
9. Качаева Г.И., Султанов Н.Г. Стратегии защиты от угроз безопасности: развитие системы обеспечения кибербезопасности. *Вестник Дагестанского*

государственного технического университета. Технические науки. 2025;52(2):107–115. https://doi.org/10.21822/2073-6185-2025-52-2-107-115
Kachaeva G.I., Sultanov N.G. Security threat protection strategies: development of a cybersecurity system. *Herald of Dagestan State Technical University. Technical Sciences.* 2025;52(2):107–115. (In Russ.). https://doi.org/10.21822/2073-6185-2025-52-2-107-115

10. Плохута К.Д. Управление рисками информационной безопасности и комплаенс. *Компетентность.* 2025;(5):19–25. https://doi.org/10.24412/1993-8780-2025-5-19-25
Plokhuta K.D. Information Safety Risk Management and Compliance. *Competency (Russia).* 2025;(5):19–25. (In Russ.). https://doi.org/10.24412/1993-8780-2025-5-19-25

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTORS

Зубченко Константин Вадимович, аспирант, Российский государственный гуманитарный университет, Москва, Российская Федерация.
e-mail: zkonst12@gmail.com

Konstantin V. Zubchenko, Postgraduate, Russian State University for the Humanities, Moscow, the Russian Federation.

Султанов Наиль Закиевич, доктор технических наук, профессор, профессор кафедры информационных технологий и систем, Российский государственный гуманитарный университет, Москва, Российская Федерация.
e-mail: sultanovnz@mail.ru

Nail Z. Sultanov, Doctor of Engineering Sciences, Professor, Professor at the Department of Information Technologies and Systems, Russian State University for the Humanities, Moscow, the Russian Federation.

Шевцова Галина Александровна, кандидат исторических наук, доцент, директор института информационных наук и технологий безопасности, Российский государственный гуманитарный университет, Москва, Российская Федерация.
e-mail: shevtsova-g@mail.ru

Galina A. Shevtsova, Candidate of Historical Sciences, Associate Professor, Director of the Institute of Information Sciences and Security Technologies, Russian State University for the Humanities, Moscow, the Russian Federation.

Статья поступила в редакцию 10.02.2026; одобрена после рецензирования 13.04.2026; принята к публикации 20.04.2026.

The article was submitted 10.02.2026; approved after reviewing 13.04.2026; accepted for publication 20.04.2026.