

УДК 004.056

Имитационная модель обеспечения безопасности автоматизированной информационной системы на основе реконfigurирования параметров системы защиты

Басыров Александр Геннадьевич — доктор техн. наук, профессор. Профессор кафедры информационно-вычислительных систем и сетей. Научные интересы: моделирование информационных систем. E-mail: alexanderbas@mail.ru

Неаскин Станислав Романович — адъюнкт Военного института (научно-исследовательского). Научные интересы: информационная безопасность. E-mail: stasneas@bk.ru

Военно-космическая академия имени А. Ф. Можайского, Россия, 197198, Санкт-Петербург, ул. Ждановская, 13

Для цитирования: Басыров А. Г., Неаскин С. Р. Имитационная модель обеспечения безопасности автоматизированной информационной системы на основе реконfigurирования параметров системы защиты // Интеллектуальные технологии на транспорте. 2026. № 3 (47). С. 5–17. DOI: 10.20295/2413-2527-2026-347-5-17

Аннотация. *Представлено исследование, посвященное разработке имитационной модели автоматизированной информационной системы в условиях штатной нагрузки и деструктивных воздействий. Цель: повышение устойчивости системы к возмущающим воздействиям за счет своевременного обнаружения нештатного состояния и последующего реконfigurирования параметров защиты. Методы: имитационное моделирование, последовательный анализ Вальда, анализ Парето, взвешенная свертка критериев потенциального ущерба и ресурсных затрат. Результаты: модель позволяет формировать штатный профиль событий, выявлять отклонения в потоках системных журналов, классифицировать характер воздействия и выбирать рациональную конфигурацию защиты. Практическая значимость: сокращение времени восстановления работоспособности системы и снижение потенциального ущерба при деструктивных воздействиях. Дальнейшее развитие модели связано с расширением состава источников событий и уточнением параметров оценки потенциального ущерба. Исследование может быть использовано при анализе устойчивости и защищенности автоматизированных систем.*

Ключевые слова: автоматизированная информационная система, последовательный анализ Вальда, множество Парето, реконfigurирование, журналы событий системы

2.3.6 — методы и системы защиты информации, информационная безопасность (технические науки);
1.2.2 — математическое моделирование, численные методы и комплексы программ (технические науки)

Введение

Современные автоматизированные информационные системы (АИС) функционируют в условиях постоянного изменения сетевой нагрузки,

программных отказов, эксплуатационных сбоев и целенаправленных действий нарушителя. Одним из подходов к диагностике состояния таких систем

является постоянный анализ системных журналов в режиме реального времени [1]. При этом практическая задача защиты не сводится только к обнаружению факта воздействия на систему. После обнаружения необходимо определить, какие параметры защиты следует активировать, чтобы снизить потенциальный ущерб, связанный с деструктивными воздействиями, не перегрузив систему избыточными вычислительными и сетевыми затратами [2–6].

На практике эта задача осложняется несколькими обстоятельствами. Во-первых, события безопасности поступают из разных источников: операционной системы, активного сетевого оборудования (АСО), прикладного программного обеспечения и др. [7]. Во-вторых, часть событий является штатной и не должна приводить к ложной тревоге. В-третьих, реакция системы должна учитывать компромисс между уровнем защиты и затратами включаемых механизмов парирования.

Предлагаемая модель функционирования автоматизированной информационной системы позволяет воспроизводить поток событий, обнаруживать нештатное состояние статистическим методом и выбирать рациональную конфигурацию защиты с учетом остаточного ущерба и вычислительных затрат.

Научная новизна имитационной модели заключается в возможности не только обнаружения деструктивного воздействия на АИС, но и восстановления ее работоспособного состояния за счет реконfigurирования. В единую модель объединены генерация разнородных журналов auditd, АСО и прикладного программного обеспечения передачи информации, построение штатного профиля интенсивности событий, последовательный анализ Вальда, классификация характера воздействия и выбор рациональной конфигурации защиты.

Практическая значимость работы состоит в том, что модель позволяет проводить вычислительные эксперименты без вмешательства в реальную автоматизированную информационную систему. С ее помощью можно оценивать влияние длительности окна агрегации и выбранных конфигураций безопасности на скорость обнаружения воздействия, потенциальный ущерб и ресурсные затраты.

Структура имитационной модели и постановка задачи

Имитационная модель состоит из следующих основных компонентов, представленных в табл. 1. Особенностью модели является наличие обратной связи: выбранная рациональная конфигурация влияет на дальнейшую генерацию событий, снижая интенсивность потока и вероятность появления деструктивных признаков. Это позволяет имитировать не только обнаружение воздействия, но и последующее изменение поведения системы после реконfigurирования.

Таблица 1

Основные компоненты модели

Компонент	Назначение
Модуль генерации логов	Формирует штатные и нештатные события из системных журналов
Модуль парсинга	Извлекает временные метки, источники и типы событий из строк журналов
Модуль агрегации	Группирует события по временным окнам и рассчитывает признаки воздействия
Модуль штатного профиля	Строит зависимость штатной интенсивности $\lambda_0(t)$ от времени
Модуль анализа Вальда	Выполняет последовательную проверку гипотез H_0 и H_1
Модуль классификации	Определяет тип воздействия по весовым признакам
Модуль оптимизации конфигураций	Рассчитывает потенциальный ущерб, затраты, множество Парето и рациональную конфигурацию
Модуль обратной связи	Применяет выбранную конфигурацию к дальнейшей имитации потока событий
Графический интерфейс	Обеспечивает управление моделью, визуализацию данных и вывод результатов

Рассматривается АИС, в которой во времени формируется поток событий системных журналов. Источниками событий выступают журнал аудита операционной системы auditd, сообщения АСО и сообщения программного обеспечения передачи информации. Общая схема работы имитационной модели представлена на рис. 1.

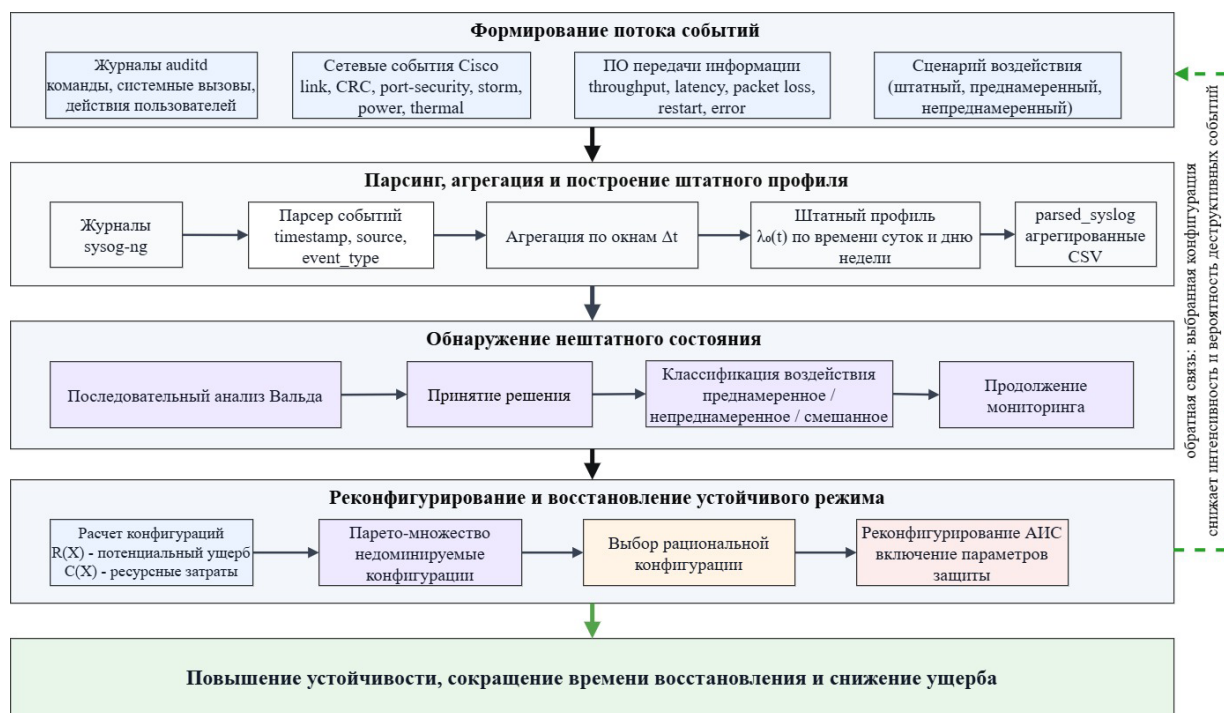


Рис. 1. Общая схема работы имитационной модели

С течением времени система может находиться в одном из трех состояний:

- штатное функционирование;
- преднамеренное деструктивное воздействие;
- непреднамеренное деструктивное воздействие.

Требуется:

- сформировать штатный профиль интенсивности значимых событий;
- обнаруживать переход в нештатное состояние;
- классифицировать характер воздействия;
- рассчитать допустимые конфигурации параметров безопасности;
- выделить множество Парето недоминируемых конфигураций;
- выбрать рациональную конфигурацию с учетом потенциального ущерба и вычислительных затрат;
- вывести результаты в виде таблиц и графиков.

Модель потока событий и моделируемые воздействия

Поток событий рассматривается по временным окнам длительностью Δt . Количество строк журналов в окне моделируется распределением Пуассона:

$$N(t) \sim \text{Poisson}(\lambda(t)).$$

Интенсивность штатного потока зависит от времени суток, дня недели и случайных колебаний:

$$\lambda(t) = \lambda_{\text{base}} \cdot K_{\text{day}}(t) \cdot K_{\text{week}}(t) \cdot K_{\text{trend}}(t),$$

где λ_{base} — базовая интенсивность;

$K_{\text{day}}(t)$ — суточный коэффициент активности;

$K_{\text{week}}(t)$ — недельный коэффициент активности;

$K_{\text{trend}}(t)$ — случайные малые колебания.

Табл. 2 содержит используемые коэффициенты генерации штатного потока.

Таблица 2

Коэффициенты генерации штатного потока

Параметр	Значение	Назначение
λ_{base}	65 событий за базовое окно 300 секунд	базовая интенсивность
K_{day}	1,7 с 09:00 до 18:00	повышенная дневная активность
K_{day}	0,55 с 00:00 до 06:00	пониженная ночная активность
K_{day}	1,0 в остальное время	средний режим
$K_{\text{week}}(t)$	1,0 в рабочие дни	обычная недельная активность
$K_{\text{week}}(t)$	0,65 в выходные дни	пониженная активность
$K_{\text{trend}}(t)$	1,0 + random (0; 0,12)	случайные малые колебания

В модели рассматриваются две основные группы деструктивных воздействий: преднамеренные и непреднамеренные. Преднамеренные воздействия связаны с действиями нарушителя, использованием сетевых утилит, попытками повышения привилегий и нарушением сетевого обмена. Непреднамеренные воздействия связаны с отказами оборудования, деградацией канала, питанием, перегревом и ошибками программного обеспечения.

После парсинга событий рассчитываются два весовых показателя:

$$\text{Sintentional} = 7 \cdot \text{audit_exec} + 6 \cdot \text{audit_privilege} + 5 \cdot \text{cisco_port_security} + 4 \cdot \text{cisco_storm};$$

$$\text{Sunintentional} = 6 \cdot \text{power_event} + 6 \cdot \text{thermal_event} + 5 \cdot \text{transmission_degradation} + 4 \cdot \text{cisco_crc} + 4 \cdot \text{cisco_link_down} + 3 \cdot \text{service_restart} + 3 \cdot \text{software_error}.$$

Эти показатели используются для классификации обнаруженного воздействия. Весовые признаки воздействия представлены в табл. 3.

Обнаружение воздействия последовательным анализом Вальда

Для обнаружения нештатного состояния используется последовательный анализ Вальда [8].

В каждом временном окне определяется количество значимых событий $x(t)$. По предварительно сформированной штатной неделе строится профиль ожидаемой интенсивности:

$$\lambda_0(t) = E[x(t)].$$

Проверяются две гипотезы:

$$H0: \lambda = \lambda_0(t),$$

$$H1: \lambda = \lambda_1(t) = k \cdot \lambda_0(t),$$

где k — коэффициент роста интенсивности при воздействии, который задает, насколько в гипотезе $H1$ поток «выше нормы».

Например, $k = 2,5$ означает: при $H1$ ожидается поток примерно в 2,5 раза выше, чем обычно.

При $k > 2,5$ система ожидает более сильную аномалию и может быть менее чувствительной к слабым отклонениям.

Если $1 < k < 2,5$, то система чувствительнее к небольшим отклонениям, но риск ложных срабатываний выше.

Для пуассоновского потока логарифм отношения правдоподобия имеет вид

$$\ln L = x \cdot \ln \frac{\lambda_1}{\lambda_0} - (\lambda_1 - \lambda_0).$$

Таблица 3

Признаки воздействия

Признак	Вес	Тип воздействия	Обоснование
audit_exec	7	Преднамеренное	Запуск сетевых и системных утилит является сильным индикатором действий нарушителя
audit_privilege	6	Преднамеренное	Попытки повышения привилегий напрямую связаны с нарушением политики доступа
cisco_port_security	5	Преднамеренное	Признак появления нежелательного устройства или превышения ограничений
cisco_storm	4	Преднамеренное	Может указывать на сетевую атаку или неправильное подключение
power_event	6	Непреднамеренное	События питания часто приводят к отказу или деградации системы
thermal_event	6	Непреднамеренное	Перегрев оборудования является критическим эксплуатационным фактором
transmission_degradation	5	Непреднамеренное	Потери, задержки и снижение пропускной способности влияют на устойчивость обмена
cisco_crc	4	Непреднамеренное	CRC-ошибки отражают проблемы физического или канального уровня
cisco_link_down	4	Непреднамеренное	Падение интерфейса нарушает связность
service_restart	3	Непреднамеренное	Перезапуск службы может быть следствием сбоя
software_error	3	Непреднамеренное	Ошибки ПО указывают на нестабильность программного компонента

Накопленная статистика Вальда рассчитывается по формуле

$$S_n = S(n-1) + \ln L.$$

Пороги принятия решений определяются через вероятности ошибок первого и второго рода:

$$\ln A = \ln \frac{(1-\beta)}{\alpha}, \quad \ln B = \ln \frac{\beta}{(1-\alpha)}.$$

Правило принятия решения:

$S_n \geq \ln A$ — принимается гипотеза $H1$;

$S_n \leq \ln B$ — принимается гипотеза $H0$;

$\ln B < S_n < \ln A$ — продолжить наблюдение.

В этой имитационной модели включение признака воздействия не приводит к мгновенному принятию гипотезы $H1$. Включение режима воздействия меняет вероятностные характеристики генератора событий, но конкретное число событий в окне остается случайной величиной. Поэтому статистика Вальда накапливает доказательства постепенно. Если в одном окне число значимых событий близко к штатному уровню, вклад $\ln L$ может быть отрицательным и S_n уменьшится.

Параметры последовательного анализа Вальда представлены в табл. 4.

Для наглядности в интерфейсе отображается не только S_n , но и $\ln L$. Это позволяет видеть, какое именно окно сдвинуло статистику к гипотезе $H1$ или, наоборот, к $H0$.

Параметры реконфигурирования

После обнаружения нештатного состояния модель переходит к выбору конфигурации защиты. В рассматриваемой имитационной модели используются 26 параметров конфигурации (табл. 5), включающих усиленный аудит, межсетевую фильтрацию, IPS, криптографические механизмы, маршрутизацию и средства сетевой телеметрии.

Условные затраты C_i отражают вычислительную и эксплуатационную цену включения параметра (нагрузку на процессор, возможное снижение пропускной способности, сложность сопровождения и влияние на сетевой обмен).

Таблица 4

Параметры последовательного анализа Вальда

Параметр	Смысл	Влияние на модель
α	Вероятность ложной тревоги	Чем меньше α , тем выше верхний порог $\ln A$ и тем сложнее принять $H1$
β	Вероятность пропуска воздействия	Чем меньше β , тем ниже допустимость пропуска, но выше требовательность критерия
k	Ожидаемый рост интенсивности при $H1$	Определяет, насколько сильное отклонение ожидает анализатор
$\lambda_0(t)$	Штатная интенсивность	Рассчитывается по baseline-профилю
$\lambda_1(t)$	Интенсивность при воздействии	Рассчитывается как $k \cdot \lambda_0(t)$
$\ln L$	Вклад текущего окна	Показывает, увеличивает или уменьшает окно статистику S_n
S_n	Накопленная статистика	Используется для принятия $H0$ или $H1$

Таблица 5

Параметры конфигурации безопасности

Параметр	Назначение	Тип	Условные затраты C_i
Усиленный auditd	Расширенное журналирование команд, системных вызовов и действий пользователей	Аудит/обнаружение	7
Zone-Based Firewall (ZBFW)	Межсетевой экран L3–L7	Защита сети	38
CBAC stateful firewall	Stateful firewall старого типа	Защита сети	30

Окончание табл. 5

Параметр	Назначение	Тип	Условные затраты C_i
IOS IPS	Сигнатурное обнаружение и блокирование атак	IDS/IPS	62
IPsec AES-256/SHA-256 software	Программное шифрование трафика	Криптозащита	75
IPsec с AIM–VPN	Шифрование с аппаратным ускорителем	Криптозащита	35
PFS DH group	Обеспечение секретности сеансовых ключей	Криптозащита	14
GRE over IPsec	Защищенный туннель с инкапсуляцией	Туннель/криптозащита	78
DMVPN mGRE + NHRP + IPsec	Динамический защищенный оверлей	Туннель/криптозащита	86
L2TP/IPsec	L2-туннель с IPsec	Туннель/криптозащита	70
IPsec compression LZS	Сжатие трафика внутри IPsec	Оптимизация	50
Debug logging по трафику	Подробное отладочное логирование сетевого трафика	Аудит/диагностика	42
TCP intercept/inspect	Защита от SYN flood и инспекция TCP	Защита сети	24
Policy-Based Routing	Маршрутизация по правилам	Управление маршрутом	14
QoS classification NBAR	DPI-классификация трафика	QoS/анализ	16
NetFlow v9/IPFIX export	Экспорт телеметрии потоков	Мониторинг	13
Shaping 25M	Формирование трафика до 25 Мбит/с	QoS/ограничение	20
Policing 30M малый burst	Жесткое ограничение трафика	QoS/ограничение	16
NAT/PAT overload	Трансляция адресов	Сетевая функция	11
NAT ALG FTP/SIP	Инспекция прикладных протоколов FTP/SIP	NAT/инспекция	9
MPLS LFIB labels	Маркировка и пересылка MPLS	Маршрутизация	11
VRF MPLS/VPN lite	Разделение таблиц маршрутизации	Сегментация	8
uRPF antispoofing	Антиспуфинг источника пакетов	Защита сети	9
ACL расширенные	Фильтрация L3/L4 по адресам, портам и протоколам	Защита сети	7
OSPF area timers	Динамическая маршрутизация OSPF	Маршрутизация	5
BGP edge	Граничная динамическая маршрутизация	Маршрутизация	8

Расчет потенциального ущерба и затрат

Множество параметров конфигурации безопасности X включает настройки и механизмы средств защиты информации, которые могут быть активированы или отключены в зависимости от состояния системы и характера воздействия [9].

x_i — бинарная переменная, определяющая i -й параметр конфигурации безопасности системы,

которая принимает значение, равное 1, если параметр применен в конфигурации, и 0 в обратном случае (параметр отключен), $x_i \in \{0, 1\}$. Под совокупностью возможных к использованию параметров безопасности в общем их количестве n будем понимать структуру вида $X_n = \{x_1, x_2, \dots, x_n\}$, где параметр данной их конфигурации определен в момент времени t и может быть настроен (включен)

в том числе удаленно. Тогда конкретная конфигурация безопасности задается вектором

$$X(t) = \{x_1(t), x_2(t), \dots, x_i(t)\}.$$

Для конфигурации X рассчитывается суммарная защищенность системы от j -го деструктивного воздействия при активированном i -м параметре безопасности:

$$E_{ji}(X) = \sum E_{ji} \cdot x_i.$$

Значение защищенности ограничивается сверху:

$$E_{ji}(X) \leq 0,92.$$

Такое ограничение введено потому, что модель не рассматривает защиту как абсолютную: даже при включении большого числа механизмов остаточный риск сохраняется.

Остаточный потенциальный ущерб после применения конфигурации:

$$R(X) = \sum P_j \cdot D_j \cdot (1 - E_{ji}(X)),$$

где P_j — вероятность j -й угрозы;

D_j — ущерб от j -й угрозы;

E_{ji} — степень защищенности i -го параметра против j -й угрозы;

x_i — включение i -го параметра.

Затраты на применение конфигурации:

$$C(X) = \sum C_i \cdot x_i,$$

где C_i — условная стоимость параметра защиты.

В табл. 6 представлены рассматриваемые типовые воздействия для расчета потенциального ущерба.

Суммарный ожидаемый потенциальный ущерб без дополнительных мер защиты составляет 85,7. Именно поэтому штатная конфигурация, в которой все рассматриваемые параметры выключены, имеет максимальный нормированный потенциальный ущерб среди сравниваемых решений.

Результативность защиты

Матрица защищенности [9] задает вклад каждого параметра в снижение конкретной угрозы. Данная величина количественно характеризует результативность использования соответствующего параметра и принимает значения в диапазоне от 0 до 1. В табл. 7 приведены только ненулевые значения матрицы.

В модели используется не полный перебор параметров для формирования вариантов конфигураций, а ограниченное множество допустимых конфигураций. Такой подход ближе к практической эксплуатации (администратор безопасности обычно выбирает не произвольный набор команд, а один из осмысленных профилей). Дополнительно генерируются случайные комбинации, расширяющие поисковое пространство.

Таблица 6

Рассматриваемые деструктивные воздействия

Воздействие	Класс	Вероятность P_j	Ущерб D_j	Исходный ожидаемый ущерб $P_j \cdot D_j$
Несанкционированное использование системных и сетевых утилит	Антропогенный	0,40	80	32,0
Нарушение сетевого обмена из-за действий нарушителя	Антропогенный	0,25	70	17,5
Отказ ПО передачи информации	Техногенный	0,25	50	12,5
Обрыв или деградация канала связи	Техногенный	0,15	40	6,0
Скачки напряжения и отключение питания	Техногенный	0,18	65	11,7
Перегрев передающего или сетевого оборудования	Стихийный	0,10	60	6,0

Таблица 7

Результативность параметров защиты

Воздействие	Параметр	Степень защищенности E_{ji}
Несанкционированное использование утилит	Усиленный auditd	0,30
	ZBFW	0,35
	CBAC	0,22
	IOS IPS	0,42
	Debug logging	0,18
	TCP intercept	0,25
	PBR	0,20
	NetFlow	0,18
	uRPF	0,25
	ACL расширенные	0,28
Нарушение сетевого обмена нарушителем	Усиленный auditd	0,12
	ZBFW	0,32
	IOS IPS	0,35
	GRE over IPsec	0,28
	DMVPN	0,30
	TCP intercept	0,30
	PBR	0,25
	NBAR	0,20
	NetFlow	0,20
	uRPF	0,30
Отказ ПО передачи информации	Усиленный auditd	0,10
	Debug logging	0,12
	NBAR	0,18
	NetFlow	0,25
	Shaping	0,20
	Policing	0,18
	OSPF	0,12
	BGP	0,10
Деградация канала связи	IPsec с AIM–VPN	0,25
	DMVPN	0,28
	PBR	0,18
	NBAR	0,25
	Shaping	0,38
	Policing	0,25
	MPLS	0,18
	VRF	0,22
	OSPF	0,20
	BGP	0,20

Окончание табл. 7

Воздействие	Параметр	Степень защищенности E_{ji}
Скачки напряжения и питание	Усиленный auditd	0,08
	DMVPN	0,18
	PBR	0,15
	NetFlow	0,18
	Shaping	0,20
	MPLS	0,15
	VRF	0,18
	OSPF	0,15
	BGP	0,15
Перегрев оборудования	Усиленный auditd	0,05
	NBAR	0,15
	NetFlow	0,18

Анализ Парето и выбор рациональной конфигурации

На рис. 2 показан пример множества Парето-конфигураций системы защиты. Серые точки соответствуют всем допустимым конфигурациям, синие — недоминируемым конфигурациям. Синим крестом выделена штатная конфигурация, звездой — рациональная конфигурация. Оранжевый круг — выбранная конфигурация, зеленый круг — активная конфигурация.

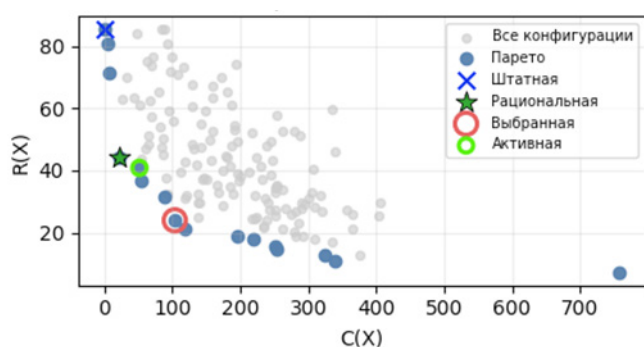


Рис. 2. Отображение множества Парето в интерфейсе модели

После расчета потенциального ущерба $R(X)$ и вычислительных затрат $C(X)$ для всех допустимых вариантов выделяется множество Парето. Конфигурация исключается, если существует другая конфигурация, которая имеет не больший остаточный ущерб, не большие затраты и строго лучше хотя бы по одному критерию [10, 11].

Далее выполняется нормирование критериев:

$$R_n(X) = \frac{(R(X) - R_{\min})}{(R_{\max} - R_{\min})}, \quad C_n(X) = \frac{(C(X) - C_{\min})}{(C_{\max} - C_{\min})}.$$

Рациональная конфигурация выбирается по функции:

$$F(X) = (1-a) \cdot R_n(X) + a \cdot C_n(X),$$

где a — вес вычислительных затрат. При малом a модель предпочитает сильное снижение ущерба, при большом a — более экономные конфигурации.

Результаты имитационного эксперимента

На рис. 3 показан пример фрагмента окна мониторинга функционирования АИС. Поток событий, влияющий на защищенность АИС, имеет дискретную природу и изменяется по окнам.

В ходе эксперимента была сформирована неделя штатных логов, построен базовый профиль $\lambda_0(t)$, после чего был запущен мониторинг с окном агрегации 3 секунды. На графиках отображались:

- поток значимых событий после парсинга;
- штатное ожидание $\lambda_0(t)$;
- адаптивный порог $\lambda_0(t) + 3\sigma\lambda_0(t)$;
- накопленная статистика Вальда S_n ;
- верхний и нижний пороги принятия решений.

Полученные результаты показывают, что статистика Вальда не реагирует мгновенно на включение

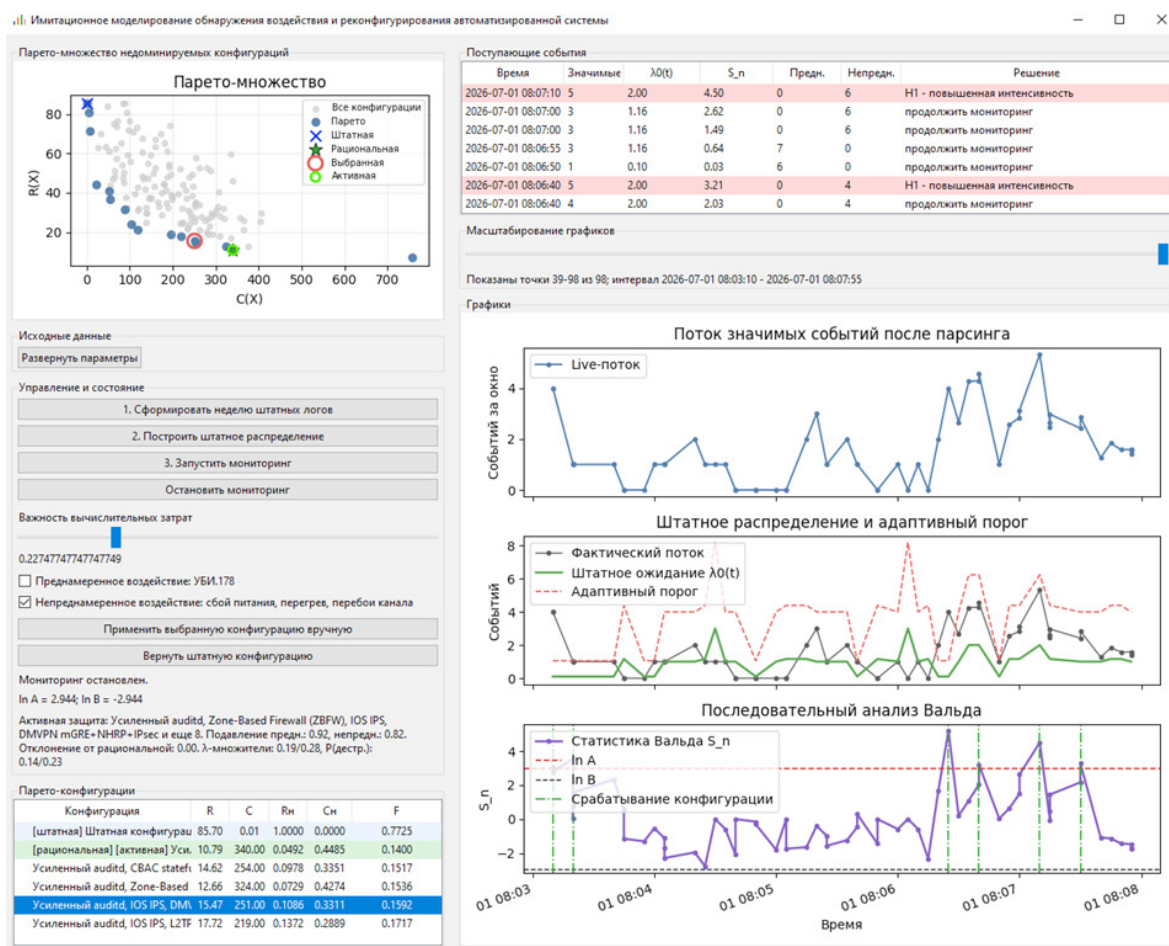


Рис. 3. Динамика значимых событий, адаптивного порога и статистики Вальда

режима воздействия. Это соответствует сути последовательного критерия: решение принимается не по факту включения сценария, а по накопленному статистическому отличию наблюдаемого потока от штатного профиля. В отдельном окне вклад $\ln L$ может быть положительным или отрицательным. Если число значимых событий выше ожидаемого, S_n растет. Если поток близок к штатному, статистика снижается или сбрасывается при принятии H_0 .

В табл. 8 приведен пример интерпретации одного шага анализа Вальда.

После принятия H_1 модель позволяет выбрать рациональную конфигурацию и применять ее к дальнейшей генерации событий.

Проведенное моделирование показывает существенное влияние выбора параметров окна агрегации и коэффициента k на принятие решений.

Коэффициент k задает ожидаемый рост интенсивности при воздействии. Если k слишком велик, анализатор ожидает резкий скачок потока и может

медленнее реагировать на слабые воздействия. Если k мал, модель становится чувствительнее, но возрастает риск ложной тревоги.

Анализ Парето показывает, что максимальная конфигурация не всегда является рациональной. Несмотря на минимальный потенциальный ущерб, она может иметь чрезмерно высокие ресурсные затраты. Поэтому практически значимым является поиск недоминируемых решений, находящихся между штатным режимом и максимальным включением всех параметров.

Отличительной особенностью модели является наличие обратной связи: выбранная конфигурация влияет на дальнейшее течение имитационного процесса, снижая интенсивность деструктивных событий и остаточный ущерб. За счет этого модель позволяет исследовать не только момент обнаружения нештатного состояния, но и переход системы к более устойчивому режиму после применения защитных параметров.

Пример интерпретации одного шага анализа Вальда

Показатель	Пример значения	Описание
s	3	Значимых событий в текущем окне
$\lambda_0(t)$	1	Ожидаемое штатное значение
k	2,5	Ожидаемый рост интенсивности при воздействии
$\lambda_1(t)$	2,5	Интенсивность по гипотезе $H1$
$\ln L$	1,25	Текущее окно сдвигает статистику к $H1$
S_n	2,1	Накопленная статистика
$\ln A$	2,94 при $\alpha = 0,05, \beta = 0,05$	Верхний порог принятия $H1$
Решение	Продолжить наблюдение	Доказательства пока недостаточно для $H1$

Заключение

В работе представлена имитационная модель автоматизированной информационной системы в условиях деструктивных воздействий. Модель воспроизводит поток событий журналов системы, строит штатное распределение интенсивности, обнаруживает нештатное состояние по последовательному анализу Вальда и выполняет выбор рациональной конфигурации защиты на основе анализа Парето.

Предложенный подход позволяет исследовать не только момент обнаружения воздействия, но и последующую реакцию системы. Это делает мо-

дель пригодной для анализа устойчивости автоматизированных систем, оценки вариантов реконфигурирования и исследования компромисса между снижением потенциального ущерба и ростом вычислительных затрат.

Дальнейшее развитие модели может быть связано с использованием реальных журналов событий, расширением набора источников данных, добавлением вероятностной классификации типа воздействия и применением ситуационного подхода реконфигурирования системы в зависимости от текущего режима функционирования.

СПИСОК ИСТОЧНИКОВ

1. Ефимова Ю. В., Гаврилов А. Г. Моделирование системы информационной безопасности на основе анализа системных журналов // Инженерный вестник Дона. 2019. № 6 (57). 11 с.
2. Малюк А. А., Пазизин С. В., Погужин Н. С. Введение в защиту информации в автоматизированных системах: учебное пособие для вузов. М.: Горячая линия — Телеком, 2001. 147 с.
3. Анализ решений в области средств защиты информации в автоматизированной системе / К. В. Стародубов [и др.] // Проектное управление в строительстве. 2023. № 2 (29). С. 81–85.
4. Баринов А. Е., Богер А. М. Классификация каналов деструктивного информационного воздействия на программируемые логические контроллеры сетей АСУ ТП // Цифровая индустрия: состояние и перспективы развития (ЦИСП-2023): сборник статей Всероссийской научной конференции с международным участием (Челябинск, Россия, 21–23 ноября 2023 г.). Челябинск: Издательский центр Южно-Уральского гос. ун-та, 2024. С. 88–94.
5. Попов А. М., Филатов В. И. Устойчивость распределенной автоматизированной системы управления с учетом модели прогнозирования последствий непреднамеренных деструктивных воздействий // Проблемы машиностроения и надежности машин. 2024. № 4. С. 84–89. DOI: 10.31857/S0235711924040111
6. Optimal Security Hardening on Attack Tree Models of Networks: A Cost-Benefit Analysis / R. Dewri [et al.] // International Journal of Information Security. 2012. Vol. 11, iss. 3. Pp. 167–188. DOI: 10.1007/s10207-012-0160-y

7. Кротова Е. Л., Андреев Р. А., Андреева П. А. Обзор методов статической и динамической кластеризации журналов событий безопасности // Международный научно-исследовательский журнал. 2021. № 4-1 (106). С. 32–35. DOI: 10.23670/IRJ.2021.106.4.005
8. Вальд А. Последовательный анализ = Sequential Analysis / пер. с англ. П. А. Бакута [и др.]; под ред. Б. А. Севастьянова. М.: Физматгиз, 1960. 328 с.
9. Неаскин С. Р., Соловьев И. А. Математическая модель управления конфигурацией безопасности автоматизированной системы в условиях деструктивных воздействий // Труды Военно-космической академии имени А. Ф. Можайского. 2025. Вып. 698. С. 245–258.
10. Подиновский В. В., Ногин В. Д. Парето-оптимальные решения многокритериальных задач. М.: Наука. Главная редакция физико-математической литературы, 1982. 256 с.
11. Москвин Б. В. Теория принятия решений: учебник. СПб.: ВКА имени А. Ф. Можайского, 2014. 364 с.

Дата поступления: 07.08.2026

Решение о публикации: 24.08.2026

An Imitation Model for Ensuring the Security of an Automated Information System Based on Reconfiguring the Protection System Parameters

Alexander G. Basyrov — Dr. Sci. in Engineering, Full Professor. Professor of the Department of Information and Computing Systems and Networks. Research interests: modeling of information systems.
E-mail: alexanderbas@mail.ru

Stanislav R. Neaskin — Adjunct at the Military Institute (Research). Research interests: information security.
E-mail: stasneas@bk.ru

Mozhaisky Military Aerospace Academy, 13 Zhdanovskaya str., Saint Petersburg, 197198, Russia

For citation: Basyrov A. G., Neaskin S. R. An Imitation Model for Ensuring the Security of an Automated Information System Based on Reconfiguring the Protection System Parameters, *Intellectual Technologies on Transport*, 2026, no. 3 (47), pp. 5–17. DOI: 10.20295/2413-2527-2026-347-5-17 (In Russian)

Abstract. *The study presents research devoted to the development of a simulation model of an automated information system under normal load conditions and destructive influences. **Purpose:** is to improve the system's resilience by timely detection of abnormal conditions and subsequent reconfiguration of protection parameters. **Methods:** simulation modeling, sequential Wald analysis, Pareto analysis, and weighted aggregation of criteria for potential damage and resource costs. **Results:** show that the model makes it possible to generate a standard event profile, identify deviations in system log flows, classify the nature of the impact, and select an optimal protection configuration. **Practical significance:** lies in reducing the time required to restore system functionality and minimizing potential damage in the event of destructive impacts. Further development of the model is related to expanding the range of event sources and refining the parameters for assessing potential damage. The research can be used in the analysis of the stability and security of automated systems.*

Keywords: *automated information system, sequential Wald analysis, Pareto set, reconfiguration, system event logs*

REFERENCES

1. Efimova J. V., Gavrilov A. G. Modelirovanie sistemy informatsionnoy bezopasnosti na osnove analiza sistemnykh zhurnalov [Modeling of Information Security System Based on Analysis of System Logs], *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 2019, no. 6 (57), 11 p. (In Russian)
2. Malyuk A. A., Pazizin S. V., Pogozhin N. S. Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh: uchebnoe posobie dlya vuzov [Introduction to Information Security in Automated Systems: A Textbook for Universities]. Moscow, "Goryachaya liniya — Telekom" Publishing House, 2001, 147 p. (In Russian)
3. Starodubov K. V., et al. Analiz resheniy v oblasti sredstv zashchity informatsii v avtomatizirovannoy sisteme [Analysis of Solutions in the Field of Information Security in an Automated System], *Proektnoe upravlenie v stroitelstve*, 2023, no. 2 (29), pp. 81–85. (In Russian)
4. Barinov A. E., Boger A. M. Klassifikatsiya kanalov destruktivnogo informatsionnogo vozdeystviya na programmiruemye logicheskie kontroliery setey ASU TP [Classification of Channels of Destructive Information Impact on Programmable Logic Controllers of Automated Process Control Systems], *Tsifrovaya industriya: sostoyanie i perspektivy razvitiya (TsISP'2023): sbornik statey Vserossiyskoy nauchnoy konferentsii s mezhdunarodnym uchastiem [The 2023 Global Smart Industry Conference (GloSIC'2023): Collection of Articles from the All-Russian Scientific Conference with International Participation]*, Chelyabinsk, Russia, November 21–23, 2023. Chelyabinsk: Publishing Center of the South Ural State University, 2024, pp. 88–94. (In Russian)
5. Popov A. M., Filatov V. I. Ustoychivost raspredelennoy avtomatizirovannoy sistemy upravleniya s uchetom modeli prognozirovaniya posledstviy neprednamerennykh destruktivnykh vozdeystviy [Stability of a Distributed Automated Control System Taken into Account in a Model for Predicting the Consequences of Unintentional Destructive Impacts], *Problemy mashinostroeniya i nadezhnosti mashin*, 2024, no. 4, pp. 84–89. DOI: 10.31857/S0235711924040111 (In Russian)
6. Dewri R., et al. Optimal Security Hardening on Attack Tree Models of Networks: A Cost-Benefit Analysis, *International Journal of Information Security*, 2012, vol. 11, iss. 3, pp. 167–188. DOI: 10.1007/s10207-012-0160-y
7. Krotova E. L., Andreev R. A., Andreeva P. A. Obzor metodov staticheskoy i dinamicheskoy klasterizatsii zhurnalov sobytiy bezopasnosti [Overview of Methods for Static and Dynamic Clustering of Security Event Logs], *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal [International Research Journal]*, 2021, no. 4-1 (106), pp. 32–35. DOI: 10.23670/IRJ.2021.106.4.005 (In Russian)
8. Wald A. Posledovatelnyy analiz [Sequential Analysis]. Moscow, Fizmatgiz Publishing House, 1960, 328 p. (In Russian).
9. Neaskin S. R., Solovyov I. A. Matematicheskaya model upravleniya konfiguratsiey bezopasnosti avtomatizirovannoy sistemy v usloviyakh destruktivnykh vozdeystviy [A Mathematical Model for Managing the Security Configuration of an Automated System under Conditions of Destructive Influences], *Trudy Voenno-kosmicheskoy akademii imeni A. F. Mozhayskogo [Proceedings of the Mozhaisky Military Space Academy]*, 2025, iss. 698, pp. 245–258. (In Russian)
10. Podinovskiy V. V., Nogin V. D. Pareto-optimalnye resheniya mnogokriterialnykh zadach [Pareto-Optimal Solutions to Multi-Criteria Problems]. Moscow, Nauka Publishers, 1982, 256 p. (In Russian)
11. Moskvina B. V. Teoriya prinyatiya resheniy: uchebnik [The Theory of Decision-Making: A Textbook]. Saint Petersburg, Mozhaisky Military Aerospace Academy, 2014, 364 p. (In Russian)

Received: August 07, 2026

Accepted: August 24, 2026