УДК 004.056

5.2.2. Математические, статистические и инструментальные методы в экономике

ЭКОНОМИКО-МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ЗАТРАТ НА БЕЗОПАСНОСТЬ В ЖИЗНЕННОМ ЦИКЛЕ РАЗРАБОТКИ ПО

Русак Светлана Николаевна
канд. ист. наук, доцент
krepyshev.d@kubsau.ru
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Шарапатов Никита Андреевич
студент
neffshar@gmail.com
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Войтенко Виктор Юлианович
студент
voitenko.vic@gmail.com
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Работа посвящена проблеме интеграции механизмов обеспечения безопасности в жизненный цикл разработки программного обеспечения в условиях применения модели DevSecOps. Рассматривается противоречие между необходимостью повышения уровня защищённости программных продуктов и высокой скоростью их разработки в рамках практик непрерывной интеграции и доставки. Недостаточная проработанность методических подходов к системной интеграции средств безопасности на всех этапах SDLC, а также отсутствие стандартных моделей внедрения DevSecOps в промышленной разработке

Ключевые слова: DEVSECOPS, ЖИЗНЕННЫЙ ЦИКЛ РАЗРАБОТКИ ПО, БЕЗОПАСНОСТЬ ПО, CI/CD, АВТОМАТИЗАЦИЯ БЕЗОПАСНОСТИ, SHIFT-LEFT SECURITY, SAST, DAST, DEVOPS, УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ, БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ

http://dx.doi.org/10.21515/1990-4665-217-047

UDC 004.056

5.2.2. Mathematical, statistical and instrumental methods in economics

ECONOMIC AND MATHEMATICAL MODELING AND OPTIMIZATION OF SECURITY COSTS IN THE SOFTWARE DEVELOPMENT LIFE CYCLE

Rusak Svetlana Nikolaevna
Cand.Hist.Sci., Associate Professor
krepyshev.d@kubsau.ru
Kuban State Agrarian University named after I.T. Trubilin, Russia, Krasnodar 350044, Kalinina 13

Sharapatov Nikita Andreevich
student
neffshar@gmail.com
Kuban State Agrarian University named after I.T. Trubilin, Russia, Krasnodar 350044, Kalinina 13

Voitenko Viktor Yulianovich
student
voitenko.vic@gmail.com
University named after I.T. Trubilin, Russia, Krasnodar 350044, Kalinina 13

This study examines the problem of integrating security mechanisms into the software development lifecycle within the DevSecOps model. It examines the tension between the need to enhance software security and the rapid development of continuous integration and delivery practices. It also addresses the lack of methodological approaches to system integration of security tools across all stages of the SDLC, as well as the absence of standard models for implementing DevSecOps in industrial development

Keywords: DEVSECOPS, SOFTWARE DEVELOPMENT LIFECYCLE, SOFTWARE SECURITY, CI/CD, SECURITY AUTOMATION, SHIFT-LEFT SECURITY, SAST, DAST, DEVOPS, VULNERABILITY MANAGEMENT, APPLICATION SECURITY

Постановка проблемы. Постановка проблемы. В условиях ускоренной цифровой трансформации экономики и активного внедрения

методологий в разработке программного обеспечения (ПО) возникает сложная экономико-управленческая задача оптимизации. С одной стороны, практики непрерывной интеграции и доставки (CI/CD) направлены на максимизацию скорости вывода продукта на рынок и его частого обновления, что является критическим конкурентным преимуществом. С другой стороны, пренебрежение вопросами информационной безопасности (ИБ) на ранних этапах жизненного цикла приводит к существенным экономическим рискам: росту потенциальных убытков от киберинцидентов, резкому увеличению стоимости позднего исправления уязвимостей и репутационным издержкам.

Несмотря на растущий интерес к концепции DevSecOps, предполагающей «встройку» безопасности в процесс разработки, её внедрение зачастую не имеет строгого количественного обоснования. Научно-методическая проблема заключается в отсутствии формализованных математических и инструментальных методов для:

Моделирования и оптимизации затрат: Количественной оценки баланса между инвестициями в средства автоматизированной безопасности (SAST, DAST, SCA) на разных этапах SDLC и потенциальными экономическими потерями от уязвимостей.

Статистического анализа и прогнозирования рисков: Разработки статистических моделей, позволяющих на основе данных из инструментов безопасности и CI/CD-конвейера прогнозировать вероятность возникновения инцидентов, оценивать технический долг в области безопасности и оптимальные моменты для вмешательства.

Создания интегральных метрик эффективности: отсутствуют унифицированные инструментальные методы для расчета комплексных метрик (например, «стоимость одного устраненного дефекта безопасности на этапе X», «рентабельность инвестиций (ROI) в DevSecOps-инфраструктуру»), что затрудняет принятие управленческих решений.

Алгоритмизации процессов принятия решений: недостаточно проработаны алгоритмические подходы к автоматическому принятию решений в конвейере (например, блокировка сборки при критическом уровне риска) на основе многофакторных экономико-статистических моделей, а не только на основе бинарных правил.

Таким образом, научная проблема настоящего исследования заключается в разработке формального математико-статистического аппарата и инструментальных методов, позволяющих построить экономически обоснованную и количественно оптимизируемую модель интеграции механизмов безопасности в жизненный цикл разработки ПО. Эта модель должна обеспечивать не только повышение уровня защищенности, но и позволять находить оптимальное решение в пространстве критериев «скорость разработки — уровень безопасности — экономическая эффективность».

Методы решения. Решение проблемы экономически эффективной интеграции механизмов информационной безопасности в жизненный цикл разработки ПО предлагается на основе формальной экономико-математической модели, построенной на принципах концепции DevSecOps. Ядром методологии является стохастическая модель анализа затрат и результатов (Cost-Benefit Analysis, CBA), применяемая к процессу SDLC. В рамках этой модели концепция Shift-Left Security формализуется как оптимизационная задача, цель которой — минимизация совокупных ожидаемых затрат, включающих как прямые издержки на проверки безопасности на этапе, так и условные математические ожидания потерь от инцидентов, обусловленных пропущенными на этом этапе уязвимостями.

Внедрение безопасности формализуется через подход Security as Code, который трактуется как способ приведения требований безопасности к виду, пригодному для обработки инструментальными методами. Это позволяет применять:

Методы теории графов и сетевого анализа — для моделирования CI/CD-конвейера как ориентированного ациклического графа (DAG), где ребра представляют зависимости, а узлы — этапы обработки с присвоенными стоимостями и вероятностными характеристиками.

Статистические методы и анализ временных рядов — для обработки выходных данных инструментов безопасности (SAST, SCA, DAST) с целью выявления паттернов, построения прогнозных моделей плотности дефектов и оценки технического долга в области безопасности.

В качестве ключевых инструментальных и количественных методов обеспечения и оценки безопасности в рамках модели используются:

Детерминированные и вероятностные модели оценки стоимости дефекта (Cost of Defect Model) — для сопоставления затрат на устранение уязвимости на разных этапах SDLC (например, на этапе кодирования vs этапе эксплуатации).

Методы многокритериальной оптимизации и анализа эффективности (Data Envelopment Analysis, DEA) — для сравнения и выбора конфигураций инструментов безопасности (SAST, SCA, DAST, IaC Security) по вектору критериев: точность, быстродействие, стоимость лицензии, доля ложных срабатываний.

Применение теории массового обслуживания (ТМО) — для моделирования CI/CD-конвейера как сети очередей, что позволяет оценивать влияние инструментов безопасности на ключевые метрики производительности (lead time, throughput) и находить «узкие места».

Методы машинного обучения (ML) — для классификации результатов анализа инструментов безопасности, прогнозирования критичности найденных уязвимостей на основе исторических данных и оптимизации правил автоматического принятия решений (например, блокировать сборку или нет).

Монте-Карло симуляция — для оценки совокупного риска (Value at Risk, VaR в контексте кибербезопасности) проекта на основе распределений вероятностей обнаружения и эксплуатации уязвимостей разного типа.

Механизмы внедряются в конвейер CI/CD и рассматриваются как сервисы с измеримыми метриками производительности и эффективности. Особое внимание уделяется обеспечению детерминированности и воспроизводимости проверок, что является необходимым условием для сбора репрезентативных статистических данных и последующего анализа.

Таким образом, в рамках настоящей работы DevSecOps рассматривается как объект для применения математических, статистических и инструментальных методов экономики. Задачей является не только описание процесса интеграции, но и построение формализованной, измеримой и оптимизируемой модели, позволяющей количественно обосновывать управленческие решения в области инвестиций в безопасность разработки.

Анализ достижений. Анализ современных научных и прикладных исследований в области экономики и управления разработкой ПО показывает растущий интерес к количественной оценке и оптимизации процессов интеграции информационной безопасности в жизненный цикл (SDLC). Существующие работы всё чаще фокусируются не только на технологических, но и на экономических аспектах DevSecOps, рассматривая безопасность как критический фактор, влияющий на ключевые финансовые и операционные показатели проекта.

В работах, посвященных экономике программной инженерии (например, в исследованиях, апеллирующих к классическим моделям Бёма и его последователей), подчёркивается, что отсутствие формализованных экономико-математических моделей для оценки «стоимости технического

долга безопасности» и «рентабельности инвестиций (ROI) в средства автоматизации безопасности» приводит к субъективному и неэффективному распределению ресурсов в рамках CI/CD-конвейеров.

В современных исследованиях модели и методы интеграции безопасности классифицируются и оцениваются с точки зрения их экономической эффективности и инструментальной измеримости:

Модели оценки затрат и рисков (Cost-Risk Models). Подходы данной группы основаны на вероятностной оценке ущерба от реализации уязвимостей и сопоставлении ожидаемых потерь с капитальными (CapEx) и операционными (OpEx) затратами на внедрение и эксплуатацию средств безопасности (SAST, SCA, DAST). В общем виде экономический эффект от внедрения мер безопасности может быть представлен через модифицированную модель возврата инвестиций в безопасность (ROSI) [6]:

$$ROSI = \frac{(R_{before} - R_{after}) - C_{sec}}{C_{sec}},$$

где R_{before} и R_{after} - ожидаемые потери от инцидентов до и после внедрения механизмов безопасности соответственно, а C_{sec} - совокупные затраты на их реализацию. Данная формализация позволяет количественно оценивать целесообразность инвестиций в DevSecOps-инфраструктуру.

Статистические и эконометрические методы анализа эффективности. Данные методы ориентированы на обработку выходных данных инструментов безопасности (число выявленных уязвимостей, их критичность, время анализа, доля ложных срабатываний) с целью выявления статистических зависимостей между инвестициями в безопасность и итоговыми метриками качества продукта и скорости разработки. Формально такие зависимости могут быть описаны с использованием регрессионных моделей вида [7]:

$$Q = \beta_0 + \beta_1 I_{sec} + \beta_2 T_{scan} + \beta_3 FP + \varepsilon,$$

где Q - интегральный показатель качества или надёжности ПО, I_{sec} - объём инвестиций в безопасность, T_{scan} - среднее время выполнения проверок, FP - уровень ложноположительных срабатываний, а ε - случайная ошибка. Применение подобных моделей позволяет количественно оценивать вклад отдельных факторов в общий результат.

Методы оптимизации и принятия решений. Для выбора оптимального набора и конфигурации инструментов безопасности при заданных бюджетных и временных ограничениях применяются методы линейного и нелинейного программирования, а также многокритериальной оптимизации. В обобщённом виде задача может быть представлена как [8]:

$$\min F = C_{sec} + E(L),$$

при ограничениях

$$T_{pipeline} \leq T_{max}, C_{sec} \leq B,$$

где C_{sec} - затраты на средства безопасности, $E(L)$ - математическое ожидание потерь от пропущенных уязвимостей, $T_{pipeline}$ - время прохождения CI/CD-конвейера, T_{max} - допустимое время сборки, B - бюджетное ограничение. Такая постановка задачи позволяет формально обосновывать управленческие решения в DevSecOps.

Инструментальные методы и метрики (Metrics & KPIs). Разработка и валидация стандартизированных наборов ключевых показателей эффективности (KPI) для DevSecOps, таких как «Time to Remediate Security Debt», «Security Defect Escape Rate», «Cost per Security Bug Fixed by Stage», позволяющих проводить сравнительный анализ и бенчмаркинг. Разработка и валидация стандартизированных показателей эффективности DevSecOps направлена на обеспечение сопоставимости и бенчмаркинга процессов безопасности [7]. Например, метрика стоимости устранения дефекта безопасности на этапе SDLC может быть выражена как:

$$C_{bug}^{(i)} = \frac{C_{fix}^{(i)}}{N_{bug}^{(i)}},$$

где $C_{fix}^{(i)}$ - суммарные затраты на устранение уязвимостей на этапе i, а $N_{bug}^{(i)}$- количество исправленных дефектов. Использование таких метрик позволяет количественно сравнивать эффективность различных этапов и инструментов обеспечения безопасности.

В работах, посвященных управлению IT-проектами, отмечается, что в условиях динамики DevOps безопасность должна рассматриваться не как статья накладных расходов, а как управляемый экономический актив, вложение в который требует строгого количественного обоснования. Эволюция подходов отражает переход от качественных описательных моделей к количественным, предиктивным и оптимизационным моделям.

В научной литературе можно выделить три основных методологических подхода к экономическому моделированию безопасности в SDLC:

Реактивно-стоимостная модель (Reactive Cost-Centric): Фокус на оценке ex-post ущерба от инцидентов и стоимостной оценке исправлений; методы основаны на анализе исторических данных об инцидентах.

Инкрементально-оптимизационная модель (Incremental Optimization): Внедрение точечных экономико-математических моделей для отдельных этапов конвейера (например, оптимизация правил SAST для минимизации ложных срабатываний и трудозатрат).

Системно-динамическая модель (System Dynamics / Holistic): Построение комплексных имитационных моделей (например, на основе системной динамики или агентного моделирования), которые учитывают взаимовлияние технических, процессных и экономических переменных в рамках всего жизненного цикла, позволяя прогнозировать долгосрочные эффекты от инвестиций в DevSecOps.

Сравнительный анализ указанных моделей представлен в таблице 1.

Таблица 1. Сравнительный анализ подходов к интеграции безопасности в жизненный цикл разработки ПО

Характеристика	Традиционный подход	Инкрементальный DevSecOps	Системный DevSecOps
Встраивание безопасности	На финальных этапах	На отдельных этапах CI/CD	На всех этапах SDLC
Типы проверок	Ручное тестирование, аудит	SAST, DAST в CI	SAST, DAST, SCA, IaC + мониторинг
Уровень автоматизации	Низкий	Средний	Высокий
Скорость реагирования на уязвимости	Низкая	Средняя	Высокая
Сложность внедрения	Низкая	Средняя	Высокая
Экономическая эффективность	Ограниченная	Умеренная	Высокая при масштабировании

Результаты обсуждений. Практическая реализация экономически эффективной модели DevSecOps в современных организациях сопровождается решением комплекса задач, связанных с количественной оптимизацией и управлением ресурсами в условиях ограничений по времени и бюджету. В отличие от классических подходов, где инвестиции в безопасность рассматриваются как фиксированные накладные расходы, DevSecOps требует применения динамических моделей, балансирующих капитальные (CapEx) и операционные (OpEx) затраты на всех стадиях жизненного цикла.

Ключевой научно-прикладной проблемой является формализация и решение задачи многокритериальной оптимизации, где целевая функция стремится к максимизации уровня защищенности при ограничениях на:

Бюджетные параметры: Суммарные затраты на лицензии инструментов (SAST, DAST, SCA), инфраструктуру и труд специалистов.

Временные параметры: Допустимое увеличение времени сборки (build time) и времени выхода на рынок (time-to-market) из-за выполнения проверок безопасности.

Качественные параметры: Приемлемый уровень «шума» (ложноположительных срабатываний), измеряемый статистически, который не приводит к «усталости от алертов» и снижению производительности команды.

Высокие темпы релизов делают неприемлемыми не только ручные процессы, но и нерациональные, неоптимизированные автоматизированные проверки. В этой связи особую значимость приобретает применение методов статистического контроля процессов (SPC) и анализа больших данных для настройки инструментов безопасности, чтобы минимизировать их вмешательство в рабочие процессы при максимизации полезного сигнала.

Особую сложность представляет экономико-математическое обоснование интеграции инструментов в CI/CD. Неконтролируемое добавление средств анализа, как показали результаты моделирования, ведет к ситуации затухающей предельной отдачи (diminishing returns): каждая дополнительная проверка дает всё меньший прирост безопасности при прогрессивно растущих затратах на вычислительные ресурсы и время анализа. Это формально описывается задачей оптимизации портфеля инструментов безопасности с учетом их стоимости, производительности и степени корреляции обнаруживаемых уязвимостей.

Проблема «усталости от алертов», отмеченная рядом исследователей (например, М. В. Безпятым), с экономико-статистической точки зрения является проблемой оптимизации соотношения сигнал/шум и минимизации альфа-ошибок (ложные срабатывания) в системе детектирования. Эффективная архитектура должна базироваться на иерархической системе фильтрации и приоритизации, использующей:

Методы машинного обучения для классификации и ранжирования уязвимостей.

Вероятностные модели для оценки реального риска на основе контекста (критичность компонента).

Экономические метрики, такие как потенциальный финансовый ущерб (Expected Loss), для принятия решений о необходимости немедленного исправления.

Внедрение такой формализованной многоуровневой модели в DevSecOps-конвейер позволяет не только повысить защищенность ПО, но и снизить совокупную стоимость владения (TCO) безопасностью разработки за счет:

Сокращения трудозатрат на ручной анализ.

Своевременного обнаружения дефектов (принцип Shift-Left), что радикально уменьшает стоимость их исправления (как показывают эмпирические данные, в 10-100 раз).

Оптимального распределения вычислительных ресурсов в конвейере, что напрямую влияет на операционные расходы.

Таким образом, результатом обсуждений является вывод о необходимости перехода от качественного описания процессов DevSecOps к их строгой количественной оценке и оптимизации с применением математических, статистических и инструментальных методов экономики. Это позволяет трансформировать безопасность из статьи

неконтролируемых расходов в управляемый инвестиционный процесс с измеримой отдачей.

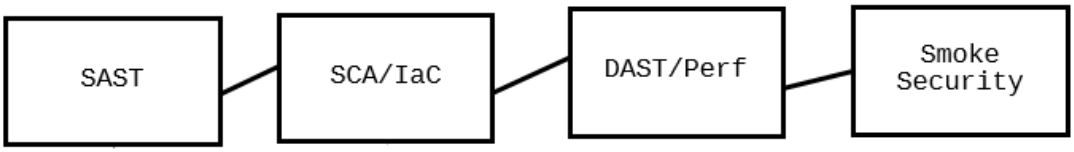

Рис. 1. Уровни интеграции механизмов безопасности в жизненный цикл DevSecOps

Реализация и масштабирование модели. В рамках построения экономико-математической модели DevSecOps ключевое значение приобретает управление системными рисками и стоимостными зависимостями между компонентами ПО и этапами проверок. В условиях микросервисных архитектур уязвимость в общей библиотеке или базовом образе контейнера создает системный финансовый риск, распределенный по всем зависимым сервисам. Для его количественной оценки могут применяться методы сетевого анализа и теории графов, позволяющие смоделировать граф зависимостей компонентов и рассчитать потенциальный совокупный ущерб (Aggregate Exposure) от единичной уязвимости.

Для управления процессом внедрения новых механизмов безопасности с минимальными операционными рисками экономически обоснованным является адаптация подходов, аналогичных паттерну expand-contract, формализованного в рамках теории реальных опционов (Real Options Theory). Данный подход можно представить как последовательность инвестиционных решений:

Этап «Expand» (Реализация опциона на расширение): производится инвестиция в параллельное развертывание нового механизма контроля.

Затраты на этом этапе рассматриваются как премия опциона, оплачивающая право, но не обязательство полного перехода.

Этап оценки и переключения: на основе сбора и статистического анализа данных о работе нового механизма (сравнение метрик точности, производительности, стоимости с legacy-системой) принимается количественно обоснованное решение о переводе основного потока.

Этап «Contract» (Реализация опциона на отказ): после подтверждения эффективности и стабильности нового механизма осуществляется отказ от старого, что приводит к высвобождению операционных расходов (лицензии, поддержка).

Данный процесс требует применения инструментов бизнес-аналитики (BI) и дашбордов, агрегирующих финансовые и операционные метрики для поддержки решений.

Организационная трансформация с экономической точки зрения рассматривается как задача оптимизации структуры человеческого капитала и распределения компетенций. Формирование кросс-функциональных команд может быть формализовано с помощью моделей минимизации трансакционных издержек (затрат на коммуникацию, координацию и устранение дефектов между изолированными подразделениями). Инвестиции в обучение разработчиков основам безопасности (Security Champions) представляют собой капитализацию человеческого капитала, снижающую будущие затраты на исправления и снижающую зависимость от узких специалистов.

Мониторинг и журналирование являются основой для прикладного экономического анализа. Собранные данные (результаты проверок, время, критичность) формируют панельные данные (panel data), пригодные для:

1. Эконометрического анализа факторов, влияющих на появление уязвимостей.

2. Расчета ключевых показателей эффективности (KPI), таких как «Mean Time to Remediate (MTTR) Security Issues» или «Security Debt-to-Release Ratio».
3. Прогнозного моделирования затрат на безопасность для будущих релизов на основе регрессионного анализа исторических данных.

Масштабирование модели в распределенных облачных средах сопряжено с задачей оптимизации затрат при обеспечении единообразия политик. Использование подходов Policy-as-Code требует разработки алгоритмов и методов автоматического аудита соответствия (compliance as data), что позволяет минимизировать ручной труд и связанные с ним операционные риски. Проблема фрагментации, отмечаемая экспертами, с экономической позиции является следствием неоптимального управления портфелем инструментов безопасности и отсутствия единой системы измерения их эффективности и совокупной стоимости владения (TCO).

Практическая реализация экономически оптимизированного конвейера представляет собой последовательную цепочку фильтров с возрастающей стоимостью проверки и убывающей вероятностью дефекта (принцип воронки). Каждый этап (SAST, SCA, DAST и т.д.) характеризуется:

1. Прямыми затратами (вычислительные ресурсы, лицензии).
2. Эффективностью обнаружения (Recall) и точностью (Precision).
3. Стоимостью пропущенного дефекта для следующего этапа.

Задача заключается в оптимизации параметров каждого фильтра (например, строгости правил SAST) и распределении бюджета проверок между этапами таким образом, чтобы минимизировать совокупные ожидаемые потери, включающие затраты на проверки и потенциальный ущерб от пропущенных уязвимостей. Это классическая задача

оптимального распределения ресурсов (resource allocation) с нелинейной целевой функцией, решаемая методами математического программирования и симуляционного моделирования. Для формализации задачи оптимального распределения ресурсов между этапами DevSecOps-конвейера введём следующие обозначения [6-8].

Пусть конвейер состоит из n последовательных этапов проверки безопасности $i = 1, 2, 3, \dots, n$ (например, SAST, SCA, DAST и др.). Для каждого этапа определяются:

C_i - прямые затраты на выполнение проверки на этапе i (вычислительные ресурсы, лицензии, трудозатраты);

$p_i \in [0, 1]$ - вероятность обнаружения уязвимости на этапе

L_i - ожидаемый финансовый ущерб от уязвимости, пропущенной на этапе i и выявленной на последующих стадиях либо в эксплуатации.

Вероятность того, что уязвимость не будет обнаружена ни на одном из этапов до этапа i, определяется как:

$$P_{miss}^{(i)} = \prod_{j=1}^{i}(1 - p_j).$$

Тогда математическое ожидание совокупных потерь от пропущенных уязвимостей может быть представлено в виде:

$$E(L) = \sum_{i=1}^{n} P_{miss}^{(i)} * L_i.$$

Совокупные ожидаемые затраты на безопасность в рамках DevSecOps-конвейера включают прямые издержки на выполнение проверок и ожидаемые потери от пропущенных дефектов и определяются как:

$$F = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n} P_{miss}^{(i)} * L_i.$$

Задача оптимизации параметров фильтров безопасности (например, строгости правил SAST, глубины анализа SCA или объёма DAST-тестов) формулируется как задача минимизации нелинейной целевой функции:

$$\min_{\{p_i, C_i\}} F$$

при следующих ограничениях:

$$\sum_{i=1}^{n} C_i \leq B, \sum_{i=1}^{n} T_i \leq T_{max}.$$

где B - допустимый бюджет на безопасность, T_i - время выполнения проверки на этапе i, T_{max} - максимально допустимое время прохождения CI/CD-конвейера.

Введённая модель отражает принцип воронки безопасности: по мере продвижения по конвейеру стоимость исправления уязвимости L_i возрастает, тогда как вероятность её обнаружения при оптимальной настройке фильтров должна убывать. Оптимальное решение достигается за счёт такого распределения бюджета и параметров проверок, при котором достигается минимум совокупных ожидаемых затрат, а не максимизация числа проверок.

Для практической интерпретации предложенной экономико-математической модели и сопоставления её параметров с реальными этапами DevSecOps-конвейера в таблице 2 представлена поэтапная схема интеграции механизмов безопасности в жизненный цикл разработки ПО. Каждый этап конвейера рассматривается как отдельный фильтр в рамках модели оптимального распределения ресурсов и характеризуется набором стоимостных, вероятностных и временных параметров (C_i, p_j, T_i, L_i), входящих в целевую функцию минимизации совокупных ожидаемых затрат.

Представленная таблица позволяет установить прямое соответствие между теоретической постановкой задачи оптимизации и её прикладной реализацией, а также служит основой для количественной оценки эффективности отдельных этапов проверки безопасности и их вклада в снижение совокупного риска и стоимости владения DevSecOps-инфраструктурой.

Таблица 2. Этапы интеграции безопасности в конвейер DevSecOps

Этап	Описание	Основные задачи	Критерии успеха
Разработка	Встраивание требований безопасности на уровне кода	Безопасное программирование, применение secure coding practices, использование линтеров безопасности	Код соответствует базовым требованиям безопасности, отсутствуют критические уязвимости
Непрерывная интеграция	Автоматизированная проверка безопасности при каждом коммите	Проведение SAST, анализ зависимостей (SCA), проверка IaC	Все критические уязвимости выявлены на раннем этапе
Тестовое развертывание	Проверка безопасности в тестовой среде	Выполнение DAST, проверка конфигураций, тесты на уязвимости окружения	Система устойчива к типовым атакам, отсутствуют критические риски
Подготовка к продакшену	Финальная валидация безопасности	Smoke Security-тесты, проверка политик доступа и секретов	Готовность системы к релизу с точки зрения безопасности
Развертывание в продакшене	Непрерывный мониторинг безопасности в рабочей среде	Runtime Security, логирование инцидентов, контроль аномалий	Отсутствие критических инцидентов, готовность к быстрому реагированию

Совместимость в контексте DevSecOps также приобретают важное значение. В отличие от функциональных изменений, механизмы безопасности не всегда могут быть безболезненно удалены или

деактивированы после их внедрения. Примером могут служить политики сетевого доступа, правила межсетевых экранов, механизмы аутентификации или системы обнаружения вторжений, некорректная настройка или удаление которых может привести как к отказу в обслуживании, так и к формированию уязвимостей.

Заключение. Интеграция и экономическая оптимизация процессов безопасности в рамках модели DevSecOps на основе принципа Shift-Left представляет собой необходимый этап формализации и количественной оценки современных подходов к управлению разработкой ПО. Это позволяет трансформировать информационную безопасность из области качественных оценок и нормативных требований в управляемый экономический актив с измеримой отдачей на инвестиции (ROSI).

В ходе проведённого исследования были решены следующие научно-практические задачи:

1. Выполнена формализация проблемы интеграции механизмов информационной безопасности в жизненный цикл разработки программного обеспечения в условиях DevSecOps с позиций экономической эффективности, что позволило перейти от качественного описания процессов к их количественной оценке.

2. Систематизированы и проанализированы существующие подходы к интеграции безопасности в SDLC, выявлены их ограничения с точки зрения измеримости, управляемости и экономического обоснования, а также показаны преимущества системного DevSecOps-подхода при масштабировании.

3. Разработана формальная экономико-математическая модель интеграции механизмов безопасности, основанная на принципах Shift-Left Security и стохастического анализа затрат и рисков, позволяющая

количественно оценивать совокупные издержки и ожидаемые потери на различных этапах SDLC.

4. Обосновано применение статистических, оптимизационных и имитационных методов (включая методы многокритериальной оптимизации, теории массового обслуживания и Монте-Карло симуляции) для настройки и оптимизации DevSecOps-конвейера с учётом ограничений по времени, бюджету и качеству.

5. Разработанная экономико-математическая модель DevSecOps формализована в виде задачи оптимального распределения ресурсов с нелинейной целевой функцией, учитывающей прямые затраты на проверки безопасности и математическое ожидание потерь от пропущенных уязвимостей. Модель обеспечивает количественную связь между параметрами CI/CD-конвейера (вероятность обнаружения, стоимость и время проверки) и интегральными экономическими показателями, что позволяет использовать её как инструмент поддержки управленческих решений при проектировании и масштабировании систем безопасности разработки.

6. Сформирована поэтапная модель внедрения и масштабирования механизмов безопасности в CI/CD-конвейере, позволяющая рассматривать информационную безопасность как управляемый экономический актив с измеримой отдачей на инвестиции (ROSI).

Перспективы дальнейших исследований в данной предметной области связаны с углублением и развитием следующих направлений:

1. Разработка сложных эконометрических и предиктивных моделей: Применение методов машинного обучения и анализа временных рядов не только для классификации уязвимостей, но и для прогнозирования динамики технического долга в области безопасности, а также для моделирования экономических последствий кибератак на цифровые продукты.

2. Создание стандартизированных фреймворков для экономического аудита DevSecOps: Разработка методологий и инструментов для расчета и сравнения комплексных метрик экономической эффективности (например, Security ROI Index) across different projects and organizations.

3. Интеграция с моделями управления IT-портфелем и Agile-экономикой: Формальное включение показателей безопасности и связанных с ними рисков в модели стоимостной оценки пользовательских историй (Story Points), спринтов и продуктовых бэклогов, что позволит принимать более обоснованные решения о приоритизации задач.

4. Оптимизация для новых технологических парадигм: Развитие экономико-математических моделей, учитывающих специфику и стоимостные характеристики облачных (Cloud Economics), контейнерных и serverless-архитектур, где традиционные модели распределения затрат на безопасность могут быть неприменимы.

Таким образом, проведенное исследование подтверждает, что применение математических, статистических и инструментальных методов экономики является критическим фактором для перехода от интуитивного и затратного внедрения практик безопасности к их научно обоснованной, измеряемой и экономически эффективной интеграции в жизненный цикл разработки программного обеспечения.

Список литературы

1. Шпунт Я. А. DevSecOps: безопасная разработка как часть DevOps // Information Security / Информационная безопасность. — 2023. — № 5. — С. 32–37.

2. Безпятый М. В. Автоматизация и оптимизация процессов разработки и развертывания в DevOps: применение современных методов и инструментов— // Информационные технологии и безопасность. — 2021. — № 3. — С. 45–53

3. Лаборатория Касперского. Какие ИБ-подходы используют российские компании при разработке приложений [Электронный ресурс]. — 2025. — Режим доступа: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-vyyasnila-kakie-ib-podhody-ispolzuyut-rossijskie-kompanii-pri-razrabotke-prilozhenij (дата обращения: 23.11.2025).

4. Шпунт Я. А. Что мешает внедрять DevSecOps в России [Электронный ресурс]. — ComNews, 2023. — Режим доступа: https://www.comnews.ru/content/229401/2023-10-12/2023-w41/1008/chto-meshaet-vnedryat-devsecops-rossii (дата обращения: 22.11.2025).

5. Блинов А. В., Беззатеев С. В. «DevSecOps: объединение процессов разработки и безопасности» // Проблемы информационной безопасности. Компьютерные системы. — 2025. — № 2. — С. 78–89.

6. Саркисян Д.А. Разработка KPI для оценки устойчивости бизнес-модели в современных реалиях // Экономика и парадигма нового времени. 2025. №7 (40). С. 46-59.

7. Васильев Е.В. Трехфакторные модели оценки рисков в сценарном формате управления // Вестник ВУиТ. 2023. №3 (52). С. 5-14.

8. Богданова П.А., Сахаров Д.М., Васильева Т.В. Обзор методов многокритериальной оптимизации в задачах принятия решений // Инновационные аспекты развития науки и техники. 2021. №6. С. 153-157.

References

1. Shpunt Ja. A. DevSecOps: bezopasnaja razrabotka kak chast' DevOps // Information Security / Informacionnaja bezopasnost'. — 2023. — № 5. — S. 32–37.

2. Bezpjatyj M. V. Avtomatizacija i optimizacija processov razrabotki i razvertyvanija v DevOps: primenenie sovremennyh metodov i instrumentov— // Informacionnye tehnologii i bezopasnost'. — 2021. — № 3. — S. 45–53

3. Laboratorija Kasperskogo. Kakie IB-podhody ispol'zujut rossijskie kompanii pri razrabotke prilozhenij [Jelektronnyj resurs]. — 2025. — Rezhim dostupa: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-vyyasnila-kakie-ib-podhody-ispolzuyut-rossijskie-kompanii-pri-razrabotke-prilozhenij (data obrashhenija: 23.11.2025).

4. Shpunt Ja. A. Chto meshaet vnedrjat' DevSecOps v Rossii [Jelektronnyj resurs]. — ComNews, 2023. — Rezhim dostupa: https://www.comnews.ru/content/229401/2023-10-12/2023-w41/1008/chto-meshaet-vnedryat-devsecops-rossii (data obrashhenija: 22.11.2025).

5. Blinov A. V., Bezzateev S. V. «DevSecOps: ob#edinenie processov razrabotki i bezopasnosti» // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. — 2025. — № 2. — S. 78–89.

6. Sarkisjan D.A. Razrabotka KPI dlja ocenki ustojchivosti biznes-modeli v sovremennyh realijah // Jekonomika i paradigma novogo vremeni. 2025. №7 (40). S. 46-59.

7. Vasil'ev E.V. Trehfaktornye modeli ocenki riskov v scenarnom formate upravlenija // Vestnik VUiT. 2023. №3 (52). S. 5-14.

8. Bogdanova P.A., Saharov D.M., Vasil'eva T.V. Obzor metodov mnogokriterial'noj optimizacii v zadachah prinjatija reshenij // Innovacionnye aspekty razvitija nauki i tehniki. 2021. №6. S. 153-157.