6 [2026]
ISBN 978-5-901722-96-1
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 338.246.018.2

ЦИФРОВЫЕ ИНСТРУМЕНТЫ МОНИТОРИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Телкова Виктория Александровна[1], студент
e-mail: *telkovavika@mail.ru*
Лыкова Елизавета Алексеевна[2], магистрант
e-mail: lisalikova@bk.ru
Лыкова Елена Сергеевна[1], к.э.н., доцент кафедры экономики и менеджмента
e-mail: likova_elena@bk.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия
[2] Московский энергетический институт, Москва, Россия

Аннотация. В статье рассматривается переход от устаревших реактивных методов экономической безопасности к проактивным цифровым инструментам. Автор анализирует пять ключевых решений: ERP-контроль лимитов, антифрод-системы, комплаенс-платформы, DLP и предиктивную аналитику. Особое внимание уделяется способности этих систем блокировать подозрительные операции в реальном времени, предотвращая вывод активов. Внедрение цифрового мониторинга, по данным статьи, снижает прямые потери от мошенничества на 40–60% уже в первый год.

Ключевые слова: проактивная безопасность, антифрод, цифровой иммунитет.

DIGITAL TOOLS FOR MONITORING THE ECONOMIC SECURITY OF AN ORGANIZATION

Victoria A. Telkova[1], Student
e-mail: telkovavika@mail.ru
Elizaveta A. Lykova[2], Master's degree Student
e-mail: lisalikova@bk.ru
Elena S. Lykova[1], Candidate of Economic Sciences, Associate Professor at the Department of Economics and Management
e-mail: likova_elena@bk.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia
[2] Moscow Power Engineering Institute, Moscow, Russia

Abstract. The article examines the transition from outdated reactive methods of economic security to proactive digital tools. The author analyzes five key solutions: ERP limit control, anti-fraud systems, compliance platforms, DLP, and predictive analytics. Special attention is paid to the ability of these systems to block suspicious transactions in real time, preventing asset withdrawal. According to the article, the implementation of digital monitoring reduces direct losses from fraud by 40–60% within the first year.

Keywords: proactive security, anti-fraud, digital immunity.

Экономическая ситуация последних трёх лет кардинально изменила правила ведения бизнеса. Курсовые колебания, санкционное давление, уход международных поставщиков и лавинообразный рост недобросовестных контрагентов превратили привычные подходы к безопасности в пережиток прошлого. Традиционная модель, опиравшаяся на ежеквартальные проверки и плановые ревизии, сегодня буксует: к моменту, когда ревизор обнаруживает хищение через сомнительного поставщика, деньги уже оказываются выведенными. Ключевая проблема кроется в скорости и человеческих возможностях. Один сотрудник службы безопасности физически не способен за день обработать 10 тысяч платежей или проверить полтысячи контрагентов. Именно поэтому отрасль вынуждена отказываться от реактивной логики («вор уже украл — теперь будем искать») в пользу проактивной («система мгновенно блокирует подозрительную операцию»). Цифровые инструменты в этих условиях становятся не дополнительной опцией, а жизненной необходимостью для сохранности активов.

Цель внедрения описываемых решений — создание непрерывного автоматизированного контроля за финансово-хозяйственной деятельностью, который позволяет перехватывать угрозу до того, как она причинит реальный ущерб.

1. ERP с функцией активного ограничения лимитов

Любая современная система управления предприятием — будь то 1С:ERP, SAP S/4HANA или «Галактика» — способна не просто фиксировать уже совершённые операции, а блокировать их на стадии создания документа. Механизм выглядит так: сотрудник оформляет заказ поставщику, а программа в режиме реального времени оценивает три ключевых параметра. Во-первых, цену: не превышает ли она среднерыночный уровень или исторические значения компании (например, не дороже 105% от цены аналогичной закупки в прошлом месяце). Во-вторых, самого контрагента: нет ли у него признаков банкротства, не значится ли он в стоп-листе. В-третьих, бюджет: достаточно ли средств по данной статье расходов.

При нарушении хотя бы одного из этих порогов система автоматически отклоняет документ и направляет запрос на подтверждение руководителю службы безопасности. Это исключает ситуацию, когда менеджер «случайно» выбирает завышенную цену или недобросовестного партнёра. Показательный случай: на одном промышленном предприятии сотрудник отдела закупок пытался приобрести смазочные материалы по цене, вдвое превышающей обычную, рассчитывая получить откат. Контроль лимитов в 1С заблокировал проведение заказа спустя полсекунды после нажатия кнопки.

2. Антифрод-системы для анализа платежей

Если ERP отвечает за первичную документацию, то антифрод-решения специализируются на движении реальных денег по банковским выпискам. Это программное обеспечение использует математические алгоритмы для поиска аномалий в платежах [1]. Среди типовых сценариев срабатывания — дробление сумм, когда крупный платёж на 10 миллионов рублей разбивается на десять платежей по 999 тысяч для обхода порога обязательного банковского контроля. Другой маркер — нехарактерное время: перевод в три часа ночи или в воскресенье с высокой вероятностью указывает на взлом или несанкционированное действие. Третий сигнал — несовпадение фамилии получателя со штатным расписанием (так называемые «мёртвые души», получающие зарплату). Четвёртый — репутация получателя: если его счёт фигурирует в базах ЦБ или ФНС как транзитный или принадлежащий фирме-однодневке. В итоге служба безопасности получает наглядный дашборд с цветовой индикацией: «красные» операции блокируются

автоматически, «жёлтые» направляются на ручную проверку, «зелёные» проходят без вмешательства.

3. Комплаенс-платформы непрерывной проверки партнёров

Даже если поставщик сегодня надёжен, завтра он может инициировать банкротство. Ручная проверка раз в квартал оставляет «окно уязвимости» длиной до 90 дней. Цифровые комплаенс-инструменты — СПАРК, Контур.Фокус, X-Compliance — работают через API, постоянно сверяя базу ваших контрагентов с данными ФНС, судов и других госорганов [2]. При каждой попытке заключить договор или провести оплату автоматически проверяются: дисквалификация или массовость руководителя (один директор на 50 фирм), наличие исполнительных производств и налоговых долгов, снижение финансового индекса (например, падение индекса «СПАРК-Риск» ниже порога «B»), а также признаки «транзитера» НДС. Самая ценная функция — проактивные алерты. Система не просто показывает данные по запросу, а сама присылает уведомление: «Контрагент ООО "Ромашка" подал иск о банкротстве 10 минут назад. Рекомендуется заморозить отгрузку».

4. DLP и SIEM в экономическом контуре безопасности

Распространённое заблуждение — считать DLP (Data Loss Prevention) инструментом только для защиты от утечек баз данных. На практике современные DLP-системы (Solar Dozor, StaffCop) и SIEM-платформы (MaxPatrol, ArcSight) являются мощным оружием против экономических преступлений — откатов, сговоров и создания фиктивных фирм [3]. DLP анализирует содержание рабочей переписки (почта, мессенджеры, внутренние чаты) по ключевым фразам: «откат», «процент», «наличные», «обналичка», «заведи свою фирму», «конкурс выиграем фиктивно». Также сравниваются файлы: если менеджер пересылает стороннему лицу коммерческое предложение конкурента или внутреннюю калькуляцию себестоимости, это сигнал о подготовке «серой» схемы. SIEM-системы, в свою очередь, собирают логи со всех компьютеров и серверов. Как только сотрудник отдела закупок копирует базу поставщиков на флешку или заходит в учётную систему с чужого рабочего места в нерабочее время — фиксируется аномалия, и инцидент отправляется экономисту по безопасности.

5. Предиктивная аналитика и поиск аномалий

Цифровая трансформация позволяет не только констатировать факт уже совершённой кражи, но и прогнозировать, где она вероятнее всего произойдёт. Для этого используются модули бизнес-аналитики (Power BI, Tableau) и математические пакеты (Python с библиотеками pandas и scikit-learn) [4]. Один из эффективных методов — закон Бенфорда. Он анализирует распределение первых цифр в суммах оплат: в реальных честных данных цифра «1» появляется примерно в 30% случаев. Если же сотрудник искусственно подгоняет суммы под лимит (например, 499 999 рублей), распределение искажается, и система подаёт сигнал тревоги. Другой подход — кластеризация поставщиков. Алгоритм самостоятельно группирует контрагентов по таким признакам, как дата регистрации, уставный капитал и уплаченные налоги. Если новый поставщик попадает в кластер «фирм-однодневок» (зарегистрирован два дня назад, капитал 10 тысяч рублей), он получает автоматический отказ. Третье направление — прогноз кассовых разрывов. Анализируя историю платежей и поступлений, искусственный интеллект предсказывает нехватку денег за три недели до её наступления, давая руководству время безопасно перераспределить ресурсы, а не брать экстренный кредит под грабительский процент.

6.Взаимосвязь с национальными и государственными программами

Внедрение цифровых инструментов мониторинга соотносится с рядом государственных инициатив и требований:

1. Требования регуляторов. В России ужесточаются нормы по защите персональных данных (152-ФЗ), финансовой отчётности, санкционному контролю [5]. Цифровые системы помогают компаниям соблюдать эти требования и избегать штрафов.

2. Программы цифровой трансформации. Государственные инициативы, направленные на развитие цифровой экономики, стимулируют бизнес к внедрению ИТ-решений для повышения эффективности и безопасности.

3. Национальная программа «Цифровая экономика Российской Федерации» [6]. Она включает меры по развитию кибербезопасности, поддержке отечественных ИТ-разработок и подготовке кадров в сфере информационных технологий.

4. Проекты по повышению производительности труда. Интеграция ERP, MES и систем мониторинга (например, MDC) позволяет оптимизировать производственные процессы, что соответствует целям таких инициатив.

Таким образом, цифровые инструменты мониторинга не только защищают бизнес, но и способствуют его соответствию государственным стандартам, повышению конкурентоспособности и участию в национальных программах развития.

Главная задача всех перечисленных решений — не дать мошеннику (внешнему или внутреннему) вывести деньги. Старая схема «украл — заметили через три месяца — пытаемся вернуть» заменяется на новую: «попытался украсть — система заметила через секунду — заблокировала — ущерба нет». По сути, это автоматический страж, который круглосуточно контролирует каждую копейку.

Почему это критически значимо в 2025–2026 годах? Причин несколько.

Рост числа фирм-однодневок. В условиях санкций и ухода крупных игроков появилось множество юридических лиц, живущих 2–3 месяца, выводящих деньги и исчезающих. Человек физически не успевает проверять каждого нового партнёра — на это уходят дни, а бизнесу нужна скорость. Цифровые комплаенс-инструменты делают ту же работу за две секунды.

Внутреннее мошенничество на подъёме. Когда реальные доходы падают, а цены растут, соблазн «подзаработать» на откатах или фиктивных поставках резко возрастает. DLP ловит переписку с обсуждением процентов, а антифрод видит фиктивные заявки на премии [7]. Раньше это обнаруживалось случайно, теперь — автоматически.

Банки ужесточают контроль. ЦБ и Росфинмониторинг требуют от кредитных организаций блокировать подозрительные транзакции. Если компания по незнанию отправит деньги «плохому» контрагенту, банк может заблокировать весь расчётный счёт на месяц. Цифровой мониторинг сверяется с базами ЦБ и ФНС за доли секунды и не даёт отправить платёж в опасное место.

Скорость как конкурентное преимущество. В современной экономике выигрывает тот, кто реагирует быстрее. Пока вы три дня вручную проверяете нового поставщика, конкурент уже отгрузил товар и получил деньги. Автоматическая проверка за две секунды позволяет работать и быстро, и безопасно.

Импортозамещение не снизило требований к безопасности. Многие опасались, что с уходом SAP контролировать станет нечем. Однако российские системы — 1С, Контур, Solar — сегодня работают в части мониторинга экономических рисков даже лучше западных, поскольку они изначально заточены под наши реалии: блокировки по 115-ФЗ, схемы обналичивания, особенности налогового администрирования.

Измеримые результаты внедрения (KPI)

Переход на цифровой мониторинг даёт конкретные бизнес-показатели:

- скорость выявления инцидентов сокращается с 14 дней (при традиционной ревизии) до 5 минут (при автоматическом алерте);

- прямые потери от мошенничества снижаются на 40–60% уже в первый год использования;

- нагрузка на персонал перераспределяется: автоматически проверяется 100% транзакций вместо выборочных 5% вручную;

- прозрачность решений возрастает, поскольку каждый запрет или блокировка сопровождается цифровой записью причины, что исключает субъективизм.

Цифровые инструменты мониторинга — это не слежка за сотрудниками, а защита прибыли компании. Внедрение ERP-контролей, антифрода, комплаенс-проверок и DLP позволяет создать так называемый «цифровой иммунитет»: система сама отсекает опасные сделки и блокирует попытки вывода активов. Начинать стоит с малого — настроить блокировку платежей сомнительным контрагентам в 1С, а затем постепенно масштабировать на предиктивную аналитику. Без этого малый и средний бизнес в текущей экономической ситуации становится лёгкой мишенью для злоумышленников — как внешних, так и внутренних.

Список литературы:

1. Баранов, А. М. Информационная безопасность и защита информации: учебник для вузов / А. М. Баранов. — 2-е изд. — М. : Юрайт, 2024. — 345 с.
2. Матвеев, И. А. Финансовый мониторинг и антифрод-защита в корпоративных информационных системах / И. А. Матвеев // Управление экономическими системами. — 2025. — № 2. — С. 45–58.
3. Лыкова, Е. С. Поиск оптимального уровня конкретизации запроса для максимизации точности релеватности ответов генеративных языковых моделей / Е. С. Лыкова, Е. А. Лыкова // Экономика и предпринимательство. – 2026. – № 2(187). – С. 1089-1094.
4. Тельнов, Ю. Ф. Предиктивная аналитика в системах экономической безопасности предприятия / Ю. Ф. Тельнов, И. Д. Козлов // Прикладная информатика. — 2024. — Т. 19. — № 4. — С. 72–83.
5. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 02.07.2021) // Собрание законодательства РФ. — 2006. — №31 (Ч. 1.). — Ст. 3451
6. Паспорт национальной программы «Цифровая экономика Российской Федерации» / [Электронный ресурс] // Правительство России: сайт. — URL: government.ru (дата обращения: 12.05.2026).
7. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изм. и доп., вступ. в силу с 01.01.2026).