УДК 336.13

А.А. Лысенко, Л.Г. Колоскова
Финансовый университет при Правительстве Российской Федерации, г. Москва,
email: analysenko@fa.ru, koloskova.mila2000@yandex.ru.

ИНСТРУМЕНТАРИЙ АНТИФРОД: ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ В СИСТЕМУ ВНУТРЕННЕГО ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ключевые слова: внутренний государственный финансовый контроль, Федеральное казначейство, антифрод, цифровая платформа, инструменты финансового контроля.

В статье представлен комплексный анализ перспектив внедрения передового инструмента внутреннего государственного финансового контроля – системы антифрод. Рассмотрены сущностные характеристики и преимущества системы фонд-мониторинг, элементы надежного программного обеспечения борьбы с мошенническими операциями, а также алгоритмы анализа антифрод систем.

A.A. Lysenko, L.G. Koloskova
Financial University under the Government of the Russian Federation, Moscow,
email: analysenko@fa.ru, koloskova.mila2000@yandex.ru.

ANTIFRAD TOOL: PROSPECTS FOR INTRODUCTION IN THE SYSTEM OF INTERNAL STATE FINANCIAL CONTROL OF THE RUSSIAN FEDERATION

Keywords: internal state financial control, Federal Treasury, Antifraud, digital platform, financial control tools.

The article presents a comprehensive analysis of the prospects for the introduction of an advanced tool for internal state financial control – the anti-fraud system. The essential characteristics and advantages of the fund-monitoring system, elements of reliable software for combating fraudulent transactions, as well as algorithms for analyzing anti-fraud systems are considered.

Необходимость укрепления потенциала функционирования государственного сектора обуславливает тенденцию заимствования опыта инструментально-методического обеспечения иных секторов экономики. Система государственного финансового контроля не является исключением. Так перспективным направлением развития инструментального подхода к реализации внутреннего государственного финансового контроля является внедрение такого инструмента, как антифрод, или фрод-мониторинг [1]. Система антифрод берёт своё развитие в банковском секторе. Данная система подразделяет клиентов так, чтобы получать информацию о том, какие действия, в каком регионе, в какое время и в каких объемах выполнял конкретный субъект установленные операции. Согласно теории рационального выбора, при увеличении возможности обнаружения мошенничества организация нацелена на предотвращение подобных инцидентов для того, чтобы вызвать сомнения у потенциального мошенника. В любой борьбе с мошенничеством важно придерживаться четырёх основных компонентов: предотвращение, обнаружение, реагирование и сдерживание. Перспективы рассматриваемого инструментального направления в контексте внедрения в систему внутреннего государственного финансового контроля связаны с возможностью обмена информацией в режиме онлайн, что позволят сократить время для фиксирования мошеннических операций и, как следствие, приводит к более эффективному противодействию мошенничеству.

Рассмотрим основные содержательные характеристики и преимущества системы антифрод. Так, основными задачами форд-мониторинга являются:

1. Сокращение убытков от возникающих мошеннических схем и клиентов.

2. Снижение рисков, связанных с репутацией банков (а в случае с государственным сектором – органов государственной власти), улучшение качества

финансового сервиса в сторону надежности. Следствием данной задачи является повышение лояльности клиентов (и граждан соответственно) к услугам данного банка (государственным услугам) и увеличение количества новых клиентов.

3. Сокращение расходов финансового института на проведение расследований по подозрительным операциям и выявлению мошеннических схем.

Внедрение антифрод в систему государственного финансового контроля имеет свои перспективы. Так основными направлениями развития автоматизированного мониторинга могут являться: мониторинг ключевых показателей операционной деятельности, бюджетный мониторинг и антифрод мониторинг. Форд-мониторинг позволит анализировать и контролировать операции финансово-бюджетных потоков, прослеживать транзакционную активность системы казначейских платежей, а также транзакционную активность систем бухгалтерского и аналитического учета (что особо актуально в условиях централизации бюджетного учета). Помимо этого, рассматриваемая система позволит обеспечить прозрачность функционирования уполномоченных сотрудников в государственных информационных и иных автоматизированных системах. В момент непредвиденных и/или аномальных транзакционных операций контролирующие органы смогут выявлять признаки, рискоемкие операции, связанные с нанесением ущерба государству, осуществлять мониторинг расходов, которые произведены или планируются к исполнению в будущем периоде.

С другой стороны, при рассмотрении и анализе упущенных выгод, предусматривается возможность отслеживания недополученных доходов, которые должны были быть реализованы при условии отсутствия правонарушений. Автоматизированная антифрод система позволит в дальнейшем своевременно выявлять и минимизировать убытки, что приведет к прозрачности управления финансовыми ресурсами государственного сектора. В связи с этим контролирующие лица будут обучены и ознакомлены с возможностями автоматизированных антифрод систем государственного финансового контроля, что позволит ускорить процесс их внедрения и поможет качественно и с наибольшей эффективностью выявлять случаи мошенничества для их последующего их пресечения.

Для того чтобы внедрить антифрод в систему государственного финансового контроля, необходимо проанализировать ряд практику его реализации в корпоративном секторе, провести ряд экспериментов и тестовую апробацию, что позволит разработать задачи и методику применения для выявление соответствующих нарушений.

Для обеспечения внедрения антифрод в минимальный срок и в максимальной комплектации, одним из возможных направлений является включение в нормативные акты, регламентирующие полномочия органов государственного финансового контроля, а также издание соответствующих организационно-распорядительных и методических документов, включающих требования по реализации форд-мониторинга с указанием штрафных санкций при отсутствии соответствующей функциональной обеспеченности. Помимо этого, необходимо предусмотреть соответствующее техническое обслуживание и доработку существующих информационных систем для возможности оптимизации действующего функционала органов внутреннего государственного финансового контроля. Как следствие, реализация указанного инструментария приведет к развитию системы в целом и условий в частности, управления финансово-бюджетными потоками государственного сектора.

Внедрение предлагаемого инструментария предусматривает ряд мер и инструментов для снижения уровня мошенничества и злоупотреблений со средствами бюджетов бюджетной системы Российской Федерации:

1. Внедрение эффективной процедуры верификации направлений расходования бюджетных средств при высокой рискоемкости операции, включающей дополнительные линии проверки, например видео или аудио верификация.

2. Распространение верификации на все инструменты управления счетами бюджетов бюджетной системы Российской Федерации.

3. Использование уведомлений по значительным операция, например, таким как направления расходования особо крупных сумм.

4. Защита средств платежей, например, использование технологии верификации, таких как 3D – secure [2].

5. Использование программно-аппаратных средств защиты в том числе антивирусов для всех компонентов системы.

Относительно проблематики снижения бюджетных рисков, необходимо придерживаться 8 ключевых моментов для обеспечения надежного программного обеспечения (рис.1).

На рис. 1 представлена система управления рисками мошеннических операций, стратегии, планируемых действий по борьбе с мошенничеством и процедуры контроля за борьбой с мошенничеством, что следует рассматривать как превентивные меры. Элементы, связанные с контролем за борьбой с мошенничеством, разработкой механизмов рассмотрение жалоб и исследования данных процессов следует группировать в процесс их обнаружения. Последние элементы данного рисунка необходимо рассматривать как процедуры реагирования.

Проанализируем существующие направления антифрод систем для возможности их адаптации к государственному финансовому контролю. Например, Advanced Fraud Detection System позволяет обеспечить защиту приложения интернет-банкинга и их пользователей от киберпреступности, обнаруживая мошенничество в онлайн-среде [5]. При этом обеспечивается возможность ведения журнала действий пользователей. Более того, система способна обнаруживать активность финансовых вредоносных программ, попытки захвата учетных записей, фишинга, мошеннических операций, несанкционированного доступа к функциям пользователей, а также попыткам атак веб-приложений, связанных с частой авторизации. Основными характеристиками рассматриваемой системы являются:

1. Отслеживание финансовых вредоносных программ ведется с момента их обнаружения, то есть с момента входа в систему.

2. Существует возможность обнаружения атак фишинга и социальной инженерии, которые довольно трудно обнаружить иными способами.

3. Профилирование пользователей и автоматическое обнаружение аномалий, связанных с неоправданной траекторией действий.

4. Возможна запись сеанса пользователей, что позволяет собрать достаточный уровень доказательств и упрощает расследование мошеннических инцидентов.

Обращаясь к возможности применения рассматриваемого инструментария в системе государственного финансового контроля, необходимо выделить ряд преимуществ, обуславливающих процедуру заимствования методического инструментария из иных секторов экономики. Так, благодаря системе антифрод, представляется возможность отслеживать финансово-бюджетные потоки бюджетов бюджетной системы Российской Федерации.

Следующий шаг – контроль исполнения бюджетных средств, реализация которого становится возможной в более технологичном формате. Данная система позволит организовать прозрачную систему финансово-бюджетных поток, которая предоставить возможность видеть, кто распределял, получал и совершал какие-либо иные действия со средствами бюджетов бюджетной системы. Такая трансформационная составляющая контроля позволит в перспективе оптимизировать фактическое предоставление средств, то есть органы государственной власти, используя антифрод, будут знать сколько на самом деле необходима, что, в свою очередь, обеспечить целесообразность, эффективность и целевой характер использования бюджетных средств. Более того, используя такую функцию как запись сеанса, на психологическом уровне исполнитель не захочет проводить мошеннические или махинационные действия, что повлечёт за собой увеличение добросовестных сотрудников органов государственной власти. Помимо этого, представляется довольно сложным обойти систему, фиксирующую операции работников. Фишинговые атаки будут остановлены и ликвидированы на начальном этапе, вредоносные программы будут занесены в реестр подобных программ, что позволит моментально их фиксировать и нейтрализовать.

Рис. 1. Элементы надежного программного обеспечения борьбы с мошенническими операциями

Фильтры

- Прописание правил и условий, при совпадении с которыми система присваивает им определённый ранг или балл подозрительности чтобы дальше про ранжировать.

Расчёт вероятности

- На основе собственные базы данных и действия злоумышленников строится модель, которая позволит эффективнее обнаруживать подобные действия и их пресекать.

Разработка моделей аномального поведения

- На основе собственной базы данных будут прописанные алгоритмы связанных с неправомерным действиям. Постоянное обновление иных путей аномального поведение.

Обнаружение связей

- Сложных сетей взаимодействия клиентов которые позволят при анализе обнародовать взаимосвязи с дискредитированными объектами.

Обнаружение признаков дискредитации во внешних ресурсах

- Автоматическая проверка объектов в интернете и во внешних ресурсах в контексте обозначенных признаков дискредитации. анализ прямой или опосредованной взаимосвязи дискредитированными признаками.

Рис. 2. Алгоритмы анализа антифрод систем

Рассмотрим иные направления антифрод систем. Так, еще одним направлением фрод-мониторинга является ИТ-инструмент Arachne, который создает базу данных проектов европейского фонда регионального развития и европейского социального фонда на основе информации, предоставленной контрольными органами [3]. Рассматриваемый инструмент использует общедоступные данные для дополнения информации, предоставленной контрольными органами. Проанализировав данные, система выявляет риски мошенничества и помечает их «красными флажками». Тем самым система помогает выявлять и предотвращать нарушения среди проектов, бенефициаров, контрактов и подрядчиков. Данный инструмент использует такие средства борьбы с мошенничеством, как база данных, использование альтернативных методов и баз данных ИТ, оценку конфликта идентификации, ранжирование риска.

Для того, чтобы создать и внедрить национальную систему антифрод, необходимо понимать принцип ее функционирования. Так, изначально настраивается алгоритм обнаружения «подозрительности», то есть производится настройка фильтров и прописываются модели аномального/неправомерного поведения злоумышленников. Далее, присваиваются установленные баллы при обнаружении тех или иных алгоритмов, которые позволят проранжировать баллы и отсечь наименее подозрительные [4]. Необходимо отметить, что данная система не будет работать без источников данных, поэтому следует произвести подключение к источникам информации для сбора аналитики, например, к базе «Электронного бюджета». Проведя ряд указанных операций следует совершенствовать алгоритмы для более быстрого и точного обнаружения злоупотреблений, поскольку мошенники будут каждый раз искать иной путь преодоление барьеров системы антифрод. Представим схематично алгоритмы анализа антифрод (рис. 2).

Обобщая вышеизложенное, представляется целесообразным перенять рассмотренный опыт. Однако, первоначально, предлагается внедрить систему не «сверху-вниз», а, напротив, «снизу-вверх», то есть начать с местного и регионального уровней власти. После того, как трансформационные мероприятия дадут результаты, возможно постепенное дальнейшее подключение и остальных уровней, как в горизонтальной, так и вертикальной структуре органов внутреннего государственного финансового контроля.

Другим вектором развития рассматриваемой системы представляется опыт обмена данными между федеральными фондами. Так в Российской Федерации с 1 января 2023 года Пенсионный фонд (ПФР) и Фонд социального страхования (ФСС) будут объединяться в один государственный внебюджетный Социальный Фонд. На их базе возможно внедрение такого инструмента, как Arachne, который позволит выявить риски мошенничества на каждом элементе и в разрезе основных функций. Для примера рассмотрим функцию, связанную с предоставлением материнского (семейного) капитала. На моменте обнаружения признаков мошеннической операции со средствами будут применяться функция пометки, связанная с ранжированием рисков, конфликтных персон, что впоследствии поместит указанные объекты в рискоемкую категорию и обусловит более тщательное внимание со стороны представляющих средства органов. Проанализировав данные, система выявляет риски мошенничества и помечает их «красными флажками». Тем самым система помогает выявлять и предотвращать нарушения среди проектов, бенефициаров, контрактов и подрядчиков. Данный инструмент использует такие средства борьбы с мошенничеством, как база данных, использование альтернативных методов и баз данных ИТ, оценку конфликта идентификации, ранжирование риска.

Таким образом, система антифрод является перспективным инструментальным обеспечением системы внутреннего государственного финансового контроля, поскольку способен упростить процедуры ее функционирования. Форд-мониторинг во взаимосвязи с цифровой трансформацией системы государственного управления будет способствовать противодействию возникновения очагов мошенничества и правонарушений.

Библиографический список

1. Антифрод-система – пять шагов к успеху от НИП «Информзащита». [Электронный ресурс]. URL: https://www.infosec.ru/upload/wp/2014/12/Frodmonitoring-5-shagov-k-uspehu-kratk-2.pdf (дата обращения 21.09.2022).

2. An effective anti-fraud program: how do we know? (The challenge of finding an anti-fraud program in the indonesian public sectors). 2020. vol. 5. no 2. [Электронный ресурс]. URL: cea2d12ff2a1e7777a4 410aae7307dabfa23.pdf (дата обращения 21.09.2022).

3. Fraud prevention, detection and response in united nations system organizations Prepared by George A. Bartsiotas Gopinathan Achamkulangare; JIU/REP/2016/4. [Электронный ресурс]. URL: JIU_ REP_2016_4_English_website version with annexes__rev8June2016.docx (дата обращения 21.09.2022).

4. Preventing fraud and corruption in the European Structural and Investment Funds – taking stock of practices in the EU Member States; Written by Léna Bonnemains, Mélissa Campagno, Brian Kessler, Olga Mala, and Goya Razavi October 2018 [Электронный ресурс]. URL: preventing_fraud_en.pdf (дата обращения 21.09.2022).

5. The Implementation of Fraud Risk Assessment and Anti-Fraud Strategy in Government Institution XYZ. 2021. vol. 6. Is. 2. [Электронный ресурс]. URL: a6143223c4d1aa31818fd2345854463291e3.pdf (дата обращения 21.09.2022).