Секция «Цифра, финансы и право - взгляд молодых ученых»

Антифрод: перспективы внедрения в систему внутреннего государственного финансового контроля

Научный руководитель – Плужникова Татьяна Владимировна

Колоскова Людмила Георгиевна
Студент (бакалавр)
Финансовый университет, Финансовый факультет, Москва, Россия
E-mail: koloskova.mila2000@yandex.ru

Чтобы укрепить имеющиеся позиции функционирования государственного сектора следует обращаться к заимствованию опыта в инструментально-методическом обеспечении в области других секторов экономики. Система ГФК нельзя исключать, поскольку выделяются перспективные направления развития инструментального подхода к внедрению и реализации ВГФК, такие как антифрод [1] или фрод-мониторинг. Говоря о заимствовании у других секторов, так вот этот то самый пример, поскольку антифрод берет свое начало в банковском секторе. Эта система позволяет создать процесс для подразделения клиентов в группы, тем самым выводить информацию о том какие действия они совершают, место и время и объём операции фиксируется. Данный инструмент направлен на минимизацию мошеннических действий. Для этого следует придерживаться основных элементов, для качественного функционирования системы (рис.1).

Данный инструмент выделяется как перспективный, поскольку в системе ВГФК фрод-мониторинг позволит обрести возможность обмена информации в режиме онлайн, что сократит время для фиксирования операций, проводимых мошенниками, что в дальнейшем даст эффективно противодействовать мошенничеству.

Теперь перейдем к рассмотрению содержательных качеств и преимуществ системы фрод-мониторинга. Так, основными целями антифрод является (рис. 2). При внедрении данного аппарата в систему ГФК направлениями развития будут выделяться (рис. 3).

Антифрод дает нам возможность провести анализ и вести контроль за операциями финансово-бюджетного характера, прослеживать активность в системе транзакционных казначейских платежей, к тому же можно проследить активность систем аналитического и бухгалтерского учета. Фрод-мониторинг поможет обеспечить прозрачность действий уполномоченных сотрудников в государственных информационных и иных автоматизированных системах. В сомнительные моменты, а именно непредвиденные или же их можно назвать аномальные транзакционных операции, что даст контролирующим органам выявить рискоемкие действия и присвоить им признаки. Также с точки зрения упущенных выгод, предусматривается возможность мониторинга недополученных доходов, которые могли быть получены, если бы правонарушения не были выявлены. Данная автоматизированная система даст в дальнейшем возможность оперативно и точечно выявить и впоследствии свести к минимуму убытки, что приведет к прозрачности управления финансовыми ресурсами государственного сектора. Это открывает новый риск, которым следует научится учесть, как квалификация контролирующих органов, чтобы они были ознакомлены с возможностями автоматизированных систем фрод-мониторинга.

Для более качественного внедрения необходимо провести анализ зарубежных практик их реализации в корпоративном секторе, далее потратить время на эксперименты, то есть точечно внедрить систему и обучить персонал, после можно провести тестовую апробацию, что даст возможность более глубоко понять проблематику внедрения и разработать методику применения к возникающих правонарушениям.

Для внедрения системы фрод-мониторинга важно подготовить ряд нормативных актов, которые будут регламентировать полномочия органов ГФК, к тому же следует издать соответствующие методические и организационные документы, в которых будут прописаны требования по реализации антифрод системы с детализацией по штрафным санкциям в случае неисполнения функциональной обеспеченности. Кроме того, важно оценить технические возможности, чтобы определить если нужда в совершенствовании существующих информационных систем, для более легкого процесса оптимизации действующего функционала органов ВГФК.

Для внедрения предлагаемого инструментария предусматривается ряд мер для снижения уровня злоупотреблений со средствами бюджетов бюджетной системы Российской Федерации (рис.4.). Говоря о проблематике по снижению бюджетных рисков, необходимо придерживаться 8 ключевых моментов для обеспечения надежного программного обеспечения (рис. 5).

На рис. 5 проиллюстрирована система управления рисками мошеннических операций. Представленные элементы связаны с подготовкой контроля за борьбой с мошенничеством, также можно разработать механизм рассмотрения жалоб, что в дальнейшем можно сгруппировать данные для более простого процесса обнаружения. Последние элементы данного рисунка необходимо рассматривать как процедуры реагирования.

Рассмотрим существующий инструмент. Например, AFDS [2] с его помощью возможно обеспечить защиту приложения интернет-банкинга и их пользователей от киберпреступности, обнаруживая мошенничество в онлайн-среде. К тому же эта система обнаруживает активность финансовых вредоносных программ, попытки захвата учетных записей, фишинга, мошеннических операций несанкционированной доступ к функциям, попыткам атак веб приложений и попыткам связанных с частой авторизацией. Основными характеристиками рассматриваемой системы являются (рис. 6).

Так, благодаря системе фрод-мониторинга можно отследить финансово-бюджетные потоки бюджетов бюджетной системы Российской Федерации. Изменения в контроле за соблюдением использования бюджетных средств делают его более эффективным и надежным. Все этапы движения бюджетных средств можно отследить. Вся цепочка от того, кто направил до того, как потрачены средства видна контролирующим органам из-за цифровизации процесса. Функции журналов и записи сеансов приведут к выбору потенциального злоумышленника пути решения: нарушать закон или нет. Эти элементы в целом усложняют систему обхода и фиксирует все движения, совершаемые работником. Выявление и упразднение фишинговых атак будет на этапе их определения и внесение этих программ в реестр вредоносных.

Для того чтобы построить и внедрить национальную систему борьбы с мошенничеством (антифрод), необходимо понять, как она функционирует. Итак, изначально создаются алгоритмы для обнаружения "подозрительных объектов", то есть устанавливаются фильтры и определяются модели аномального/мошеннического поведения злоумышленников. Кроме того, при обнаружении определенного алгоритма начисляются баллы, при этом баллы ранжируются и отсеиваются наиболее подозрительные. Обратите внимание, что система не может функционировать без источника данных, поэтому для сбора анализа ее необходимо подключить к базе данных «Электронного бюджета» или другому источнику данных. Это связано с тем, что мошенники будут искать другие способы преодоления барьеров системы защиты от мошенничества. После некоторых из этих операций алгоритм необходимо усовершенствовать, чтобы быстрее и точнее выявлять мошенничество. Алгоритм анализа системы защиты от мошенничества можно проиллюстрировать графически (рис. 7).

В целом, было бы желательно перенять описанный выше опыт. Однако предлагает-

ся, чтобы система изначально внедрялась снизу вверх, то есть на местном и региональном уровнях управления, а не сверху вниз. Если результаты покажут положительный эффект, то дальше трансформация будет продолжаться и на остальных уровнях, на горизонтальном и на вертикальном уровне структуре органов государственного внутреннего финансового контроля.

Другим вектором развития соответствующей системы представляется опыт обмена данными между федеральными фондами. В Российской Федерации, например, Пенсионный фонд (ПФР) и Фонд социального страхования (ФСС) с 1 января 2023 года будут объединены в один государственный внебюджетный социальный фонд. На их основе внедрение такого инструмента, как Arachne, позволит выявить риски мошенничества в отношении каждого элемента и его основных функций. В качестве примера рассмотрим функции, связанные с предоставлением средств материнского (семейного) капитала. Как только система обнаруживает признаки мошеннических операций с этими средствами, она применяет функцию флажков в отношении ранжирования рисков и конфликтующих лиц, в результате чего эти субъекты попадают в категорию риска и усиливается контроль со стороны подающих документы органов. Анализируя данные, система выявляет риски мошенничества и отмечает их "красными флажками". Это помогает выявлять и предотвращать мошенничество в проектах, бенефициарах, контрактах и подрядчиках. При этом используются такие инструменты предотвращения мошенничества, как базы данных, использование альтернативных ИТ-методов и баз данных, оценка конфликта идентификации и ранжирование рисков.

Поэтому система антифрод является перспективным инструментом, поскольку она может упростить процедуры функционирования системы внутреннего государственного финансового контроля. Форд-мониторинг в сочетании с цифровой трансформацией государственного управления поможет бороться с возникновением очагов мошенничества и нарушением закона.

Источники и литература

1) The Implementation of Fraud Risk Assessment and Anti-Fraud Strategy in Government Institution XYZ; Volume 6, Issue 2 (July-December) 2021 [Электронный ресурс] // URL: a6143223c4d1aa31818fd2345854463291e3.pdf (semanticscholar.org)
2) Антифрод-система – пять шагов к успеху от НИП «Информзащита» [Электронный ресурс] // URL: Внедрение Anti Fraud системы ДБО ЮЛ на базе (infosec.ru)

Иллюстрации

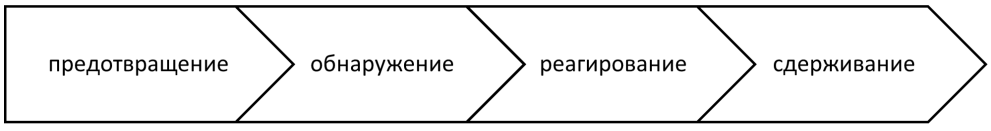

Рис. 1. Основные элементы функционирования системы фрод-мониторинга (составлено автором)

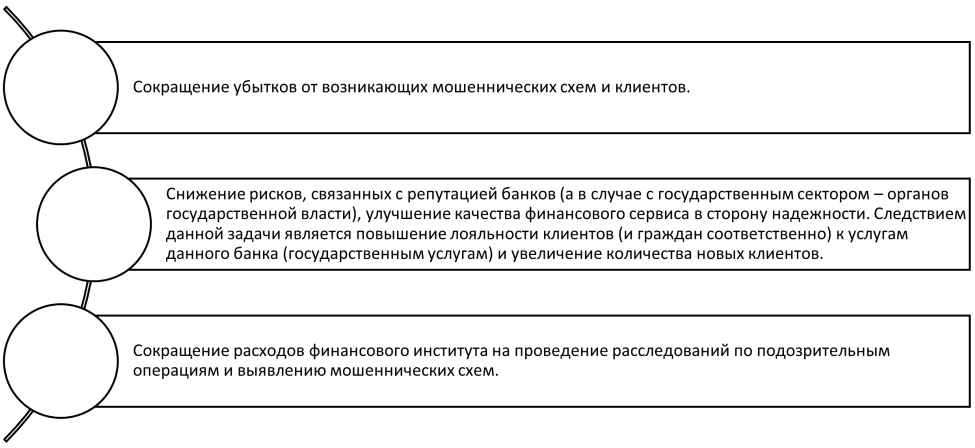

Рис. 2. Цели антифрод

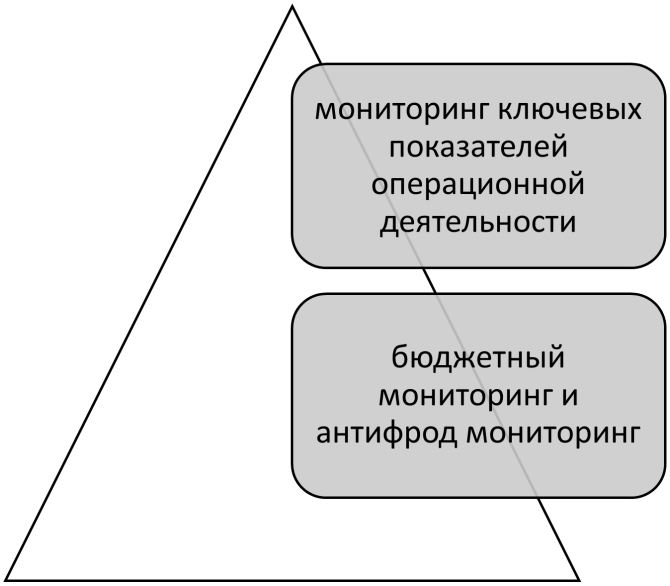

Рис. 3. Направления развития

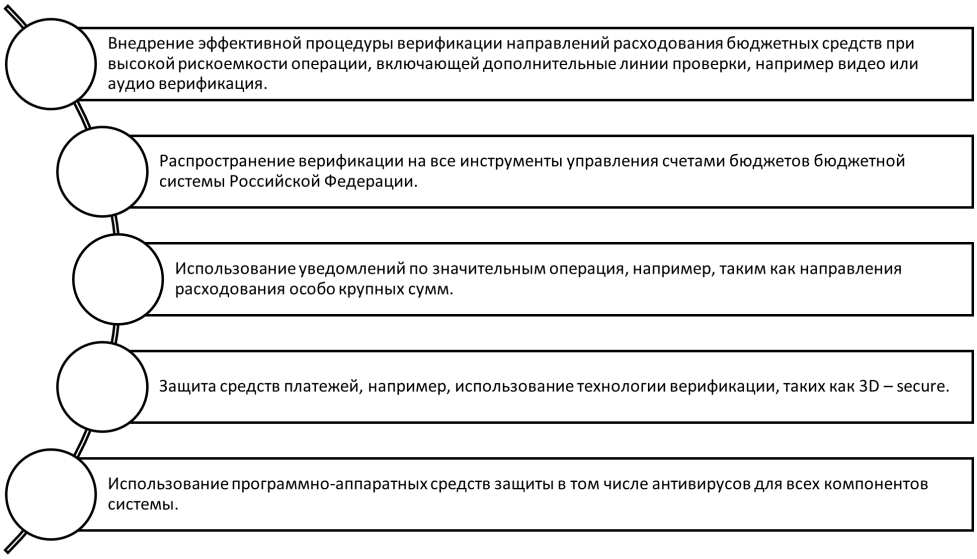

Рис. 4. Меры для снижения уровня злоупотребления со средствами бюджетов бюджетной системы РФ

Рис. 5. Элементы прочного программного обеспечения борьбы с мошенническими операциями

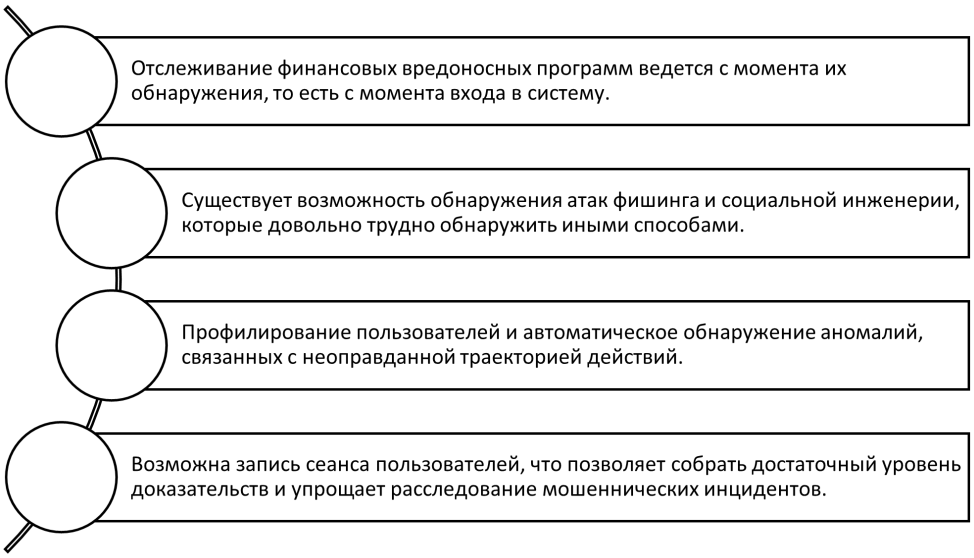

Рис. 6. Основные характеристики системы

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. 7. Алгоритмы анализа антифрод систем