АКАДЕМИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ КАЗАХСТАН

Институт дипломатии

на правах рукописи

Нургалиев Рахат Агыбаевич

ВОЗДЕЙСТВИЕ ЦИФРОВОЙ КОРРУПЦИИ НА МИРОВОЕ СООБЩЕСТВО: ПРОБЛЕМЫ И МЕТОДЫ БОРЬБЫ

Образовательная программа: «7М03111-Международные отношения»
по направлению подготовки: «7М031 Социальные науки»

Магистерский проект на соискание степени
магистра международных отношений

Научный руководитель: Сомжурек Баубек Жұмашұлы,
кандидат исторических наук,
ассоциированный профессор

Проект допущен к защите: «10» июня 2022 г.

Директор Института дипломатии: Абишева Мариан Асаровна,
кандидат политических наук

Нур-Султан, 2022

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящем магистерском проекте использованы ссылки на следующие нормативные документы:

1 Закон Республики Казахстан от 4 мая 2008 года №31-IV «О ратификации Конвенции Организации Объединенных Наций против коррупции».

2 Послание Президента Республики Казахстан Касым-Жомарта Токаева народу Казахстана «Единство народа и системные реформы – прочная основа процветания страны» от 1 сентября 2021 года.

3 Указ Президента Республики Казахстан от 2 февраля 2022 года №`802 «Об утверждении Концепции антикоррупционной политики Республики Казахстан на 2022-2026 годы и внесении изменений в некоторые указы Президента Республики Казахстан».

4 Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности (Киберщит Казахстана)».

5 Постановление Правительства Республики Казахстан «Об утверждении· Государственной программы «Цифровой Казахстан» от 12 декабря 2017 года №827.

6 Приказ Председателя Агентства Республики Казахстан по противодействию коррупции от 30 декабря 2020 года №441 «Отчет о реализации Плана развития Агентства Республики Казахстан по противодействию коррупции на 2020/2024 годы. Период отчета: 2021 год».

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Агентство	–	Агентство Республики Казахстан по противодействию коррупции
ВБ	–	Всемирный банк
ГРЕКО	–	Группа государств против коррупции
ЕАГ	–	Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма
ИИ	–	Искусственный интеллект
ИВК	–	Индекс восприятия коррупции Transparency International
ИКТ	–	Информационно-коммуникационные технологии
Конвенция	–	Конвенция ООН против коррупции
МВФ	–	Международный валютный фонд
МФЦА	–	Международный финансовый центр «Астана»
НПА	–	Нормативный правовой акт
ООН	–	Организация Объединенных Наций
ОЭСР	–	Организация экономического сотрудничества и развития
ПРООН	–	Программа развития Организации Объединенных Наций
Руководство ВБ	–	Руководство Всемирного банка по борьбе с отмыванием денег
РГТФ	–	Региональная группа по типу ФАТФ
«Эгмонт»	–	Группа подразделений финансовой разведки
ПФР	–	Подразделения финансовой разведки
FATF	–	Международная· группа разработки финансовых мер борьбы с отмыванием денег

ВВЕДЕНИЕ

Актуальность темы исследования обоснована актуальностью перехода большинства процессов государственного управления на цифровой формат, что позволяет значительно повысить его открытость, гласность и узнаваемость, распознать коррупционные сценарии, связи, усовершенствовать работу правоохранительных органов в борьбе с коррупцией и ограничить возможности коррумпированных чиновников. Но также, цифровые возможности могут создавать и новые формы коррупции.

В каждодневной жизни нашего общества стало обычным использование информационных и цифровых технологий, которые имеют широкий спектр применения. Такие технологии проникли практически во все сферы и изменили уклад современного человека.

Как мы знаем, практически всегда вместе с положительным воздействием той или иной инновации, параллельно существует и отрицательное явление.

В руках недобросовестных членов общества, цифровые технологии могут стать инструментом обхода закона и способом реализации коррупционных стратегий.

В данном контексте реализуемая в стране Антикоррупционная политика должна упреждать такие правонарушения и развивать комплексные меры по недопущению подобных фактов.

Качественная и системная работа в данном направлении обеспечена через реализацию НПА Республики Казахстан.

Кроме этого, в Послании Президента Республики Казахстан от 1 сентября 2021 года озвучено об осуществление эффективной борьбы с коррупцией [1]. Профильному агентству до конца 2021 года было поручено внести на утверждение стратегический документ, определяющий программу действий на среднесрочный период [1].

В рамках выполнения данного поручения АПК принята Концепция антикоррупционной политики Республики Казахстан на 2022-2026 годы, одной из задач которой стало применение новых технологий по минимизации коррупционных рисков [2].

Очевидно, что отслеживание, арест и возвращение активов, награбленных в результате коррупции, стали предметом серьезной озабоченности международного сообщества.

Объектом исследования является деятельность передовых стран и международных организаций по использованию цифровых технологии для противодействия коррупции, анализ состояния, проблемы, перспективы.

Предметом исследования является противодействие коррупции в контексте цифровых технологий, выработка рекомендаций по совершенствованию антикоррупционной деятельности в Республике Казахстан.

Цель исследования заключается в разработке рекомендаций и оптимальных методов противодействия цифровой коррупции.

Чтобы достичь намеченной цели в работе, необходимо решить следующие **задачи:**

- изучить теоретические аспекты в работе по борьбе с коррупцией;
- проанализировать направления и перспективы использования цифровых технологий по противодействия коррупции;
- выявить риски и новые угрозы коррупционного характера в связи с цифровизацией общественного устройства;
- определить методы борьбы с цифровой коррупцией.

Научная и практическая значимость исследования данного вопроса состоят в том, что анализ и выводы, которые содержатся в диссертации, могут быть использованы магистрантами, докторантами и исследователями в качестве основы для дальнейших научных изысканий в области противодействия цифровой коррупции, а также государственными органами при разработке стратегических документов.

Новизна работы. Несмотря на широкий спектр методов борьбы с коррупцией, используемых мировым сообществом, вопросы противодействии цифровой коррупции относятся к малоизученным. Работа направлена на комплексное изучение данной сферы с учетом современных тенденций.

Структура работы. Структура данной работы отражает цель и задачи исследования и состоит из введения, двух глав, состоящих из подпунктов, заключения, списка использованной литературы.

Анализ международной практики показал, что для получения действенных результатов от борьбы с коррупцией нужен плановый подход, сочетающий в себе детальный комплекс мероприятий.

В данном контексте, несомненным фактором снижения адм. барьеров, сокращения разрывов и повышения качества оказания гос. услуг как предпосылок для коррупции является цифровизация.

Учитывая, что феномен цифровизации охватывает практически все аспекты общественной жизни, в том числе вопросы противодействия коррупции, необходим комплексный анализ и изучение данного вопроса.

С учетом актуальности данной проблематики, была выбрана тема «Воздействие цифровой коррупции на мировое сообщество: проблемы и методы борьбы».

Гипотеза или ожидаемые результаты.

Будут выявлены положительные и отрицательные признаки применения высоких технологий в борьбе с цифровой коррупцией.

Практическая значимость.

Материалы диссертации могут быть использованы магистрантами, докторантами и исследователями в качестве основы для дальнейших научных изысканий в области противодействия цифровой коррупции, а также государственными органами при разработке стратегических документов.

Апробация результатов исследования. Основные положения магистерского проекта обсуждались на международной научно-практической

конференции «Наука и образование в эпоху цифровизации» (г. Нур-Султан, 22 апреля 2022 года).

Вместе с тем, по теме магистерского проекта опубликована научная статья «Социальные сети и кибербезопасность: современные вызовы для мирового сообщества» (30 апреля 2022 года, сборник научных статей Международного университета «Астана»).

ОБЗОР ЛИТЕРАТУРЫ

Степень изученности. В казахстанской научной среде как такового четкого определения цифровой коррупции не существует. Преступления, связанные с выводом (отмыванием) денег и применением цифровых технологии принято называть киберпреступлениями, а мероприятия направленные против них – кибербезопасностью [3].

В нашей стране термину кибербезопасности (концепция «Киберщит Казахстана») дается характеристика, когда информация обеспечена защитой в электронной форме, в том числе со средой ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационной безопасности в сфере информатизации [3].

Результаты поиска определения цифровой коррупции на пространстве интернет также показали, что данный термин является не распространенным.

Тем не менее, согласно онлайн-платформе Международного института планирования образования ЮНЕСКО (UNESCO's International for Educational Planing) под цифровой коррупцией понимается создание, неправомерное использование или манипулирование с целью незаконного извлечения выгоды посредством онлайновых или цифровых инструментов. К примеру, мошенничество на онлайн-экзаменах, создание и управление фиктивными онлайн-учреждениями, выдача поддельных цифровых степеней/дипломов, все это являются видами цифровой коррупции [4].

Как мы упомянули выше, невзирая на отсутствие определения цифровой коррупции в казахстанской научной среде, попытки разобраться в этом вопросе все-таки имеются.

Так, группой казахстанских научных соискателей А. Нуркей, А. Мукашева и Д. Едильхан в совместной статье «Модели и методы цифровых механизмов в борьбе с коррупцией, их преимущества и недостатки, а также области применения» рассмотрены приоритетные направления в борьбе с коррупцией при помощи новых цифровых технологий. В частности проанализированы преимущества и недостатки цифровизации в области решения социальных конфликтов [5].

Интересен также опыт зарубежных исследователей. К примеру, член Всемирного экономического форума (World economic forum), директор по цифровым инновациям в правительствах Банка Латинской Америки Карлос Сантис (Carlos Santiso) в своей статье «Борьба с коррупцией в цифровую эпоху: как технологии формируют будущее честности во времена кризиса» полагает, что цифровая зрелость общества и страны снижает уязвимость к коррупции. По мнению автора цифровизация и упрощение бюрократических процедур повышают эффективность, снижают затраты и упрощают обслуживание как бизнеса, так и граждан. Цифровые государственные услуги снижают риски вымогательства и возможности для взяточничества [6].

В Российской Федерации положено начало изучению воздействия цифровых продуктов как способов реализации коррупционных преступлений, противодействию им, в том числе и в государственном управлении.

Так, А.И. Овчинников в своей работе «Противодействие коррупции в условиях цифровизации: возможности, перспективы, риски» рассмотрел перспективы применения цифровых инструментов для борьбы с коррупцией. Автор считает, что цифровой потенциал позволит обстоятельно повысить открытость, гласность и узнаваемость, усовершенствует работу правоохранительных органов в борьбе с коррупцией и ограничит возможности коррумпированных лиц [7].

В работе российских исследователей Кравченко А.Г., Овчинникова А.И., Мамычева А.Ю. и Воронцова С.А. «Использование цифровых технологий в сфере противодействия коррупции» представлен потенциал усилий по борьбе с коррупцией в условиях системного внедрения ИКТ в сфере гос. управления [8].

Авторы считают, что новые цифровые технологии, возможно, смогут изменить саму парадигму коррупции, когда сам факт ее совершения станет невозможным и нецелесообразным в силу изменения современного мира в пользу цифровизации процессов взаимодействия общества и государства [8].

МЕТОДЫ ИССЛЕДОВАНИЯ

При написании данной магистерской диссертации использованы методологические принципы, которые позволяют объективно исследовать проблематику противодействия цифровой коррупции в Республике Казахстан.

В качестве общенаучных использованы теоретический метод и метод экспертной оценки, которые позволили обощить понятия «цифровой коррупции» в научной литературе иностранных и казахстанских авторов, синтезировать собственное представление термина и определить его содержание.

В аналитической части исследования использованы методы сравнительного анализа и контент-анализа в контексте основных положений и концепций теории международных отношений.

Применение метода сравнительного анализа позволило выявить новые возможности использования таких цифровых технологий как: искусственный интеллект, блокчейн, и большие данные. Помимо реализации потенциала данных технологий стали понятны, какие возможны риски и ограничения.

В результате применения вышеназванных методов исследования осуществлено обобщение материалов, выработка рекомендаций и ключевых моментов на которые в будущем следует обратить внимание.

1 ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ

1.1 Оценка рисков новых коррупционных преступлений

Согласно государственной программе «Цифровой Казахстан» использование цифровых технологий, в средней срочной перспективе возможно позволит ускорить темпы развития национальной экономики и улучшить качество жизни населения [9].

Государственная программа принята в 2017 году и действует до нынешнего 2022 года, в ней сформированы 17 инициатив и более 100 мероприятий.

Через подобные правительственные программы, государство воздействует на остро нуждающиеся сферы и отрасли, в которых накоплены не решенные проблематики. Такой проблематикой, проникшей во все сферы жизни общества и государства является коррупция. Она на протяжении долгого периода с начала обретения Казахстаном своей независимости стала препятствием для его развития.

Как принято в мировой практике, реформа государственного управления прямо или косвенно зависит от достижений технологического развития, что приводит к использованию новых технологий, в том числе для борьбы с коррупцией.

В данном аспекте для своевременного решения проблемы, возможно, послужат цифровые технологии. Но перед тем как раскрыть потенциал таких технологий, возможно, будет не лишним оценить уровень новых коррупционных преступлений в эпоху цифровизации.

В современном мире цифровые технологии стали достаточно широко использоваться, в том числе в оперативной и следственной работе правоохранительных органов.

Если в привычном материальном мире принято искать улики, то так называемый «виртуальный след» [7] показывает процесс совершения конкретных действий в онлайн среде, трансформаций в инфраструктурах хранения компьютерной информации, имеющих непосредственное отношение к правонарушениям.

Как показывает мировая практика виртуальные следы чаще всего остаются в памяти электронных устройств-гаджетов либо в цифровом пространстве, т.е. в Интернете [7].

Учитывая, что цикл жизни человеческого общества на современном этапе все больше подвергается масштабной цифровизации, закономерным является реинжиниринг процессов деятельности государственных органов, главным образом правоохранительных. Впоследствии специальным службам уже не понадобится привлечение понятых, чтобы зафиксировать то или иное правонарушение. Поиск и сбор доказательств будут осуществлять профессионалы в области высоких технологий.

Подобные изменения, несомненно, окажут прямое влияние на раскрываемость преступлений, повысят эффективность принятия судебных

решений. Фактор прозрачности будет все больше вызывать доверие среди населения.

Тем не менее, имеется также обратная сторона медали от применения цифровых технологий. Факторами риска может быть недобросовестность пользователей цифровой среды, которые способны в свою очередь спекулировать на торговле Big data (большие данные), а также производить всевозможные виды махинаций и мошенничества как кража денег, шантаж личной информацией и т.д. Для отражения таких угроз существуют специальные государственные программы, как например, в Казахстане – «Кибер щит» [3].

Вместе с тем, стоит отметить: «лица, контролирующие цифровые технологии, попадают в ситуацию, способствующую коррупции, так как обладают уникальными знаниями, компетенциями и навыками, позволяющими обойти программные коды и избежать ответственности» [7, с.8·].

В результате, очевидно, что определенные риски с использованием цифровых технологий в борьбе с коррупцией существуют, и в большинстве случаев они взаимосвязаны с отмыванием денег.

В следующем разделе будет рассмотрено, каким образом осуществляется данный вид коррупционного преступления в отличие от других разновидностей коррупции.

1.2 Отмывание денег

Общеизвестно, что частым инструментом для реализации коррупционных замыслов служит взятка, которая передается в качестве наличных либо перечисляется на банковский счет иностранного государства. В случае, когда сумма денег существенна, то получателю взятки нужно установить отправную точку, позволяющей управлять средствами без вызова подозрения к преступным действиям, являющейся их источником, либо к субъектам, которые принимают участие в ней.

В большинстве случаев отмывание денежных средств производиться через международные переводы, которые затем направляются в страну депозитария.

Само действие по скрытию либо укрывательству поступивших от теневых оборотов денег, а также легитимизация по их предстоящему использованию именуется отмыванием [10].

Злоумышленники отмывают противоправно приобретенные средства, маскируя их происхождение и правообладателя, трансформируя их форму или же перемещая в те юрисдикции, где они не влекут излишнего интереса [10].

Большей частью, отмывание средств не дает надзорным и правоохранительным органам определять нелегальные прибыли, ставить связь средств с криминальной работой и конфисковать сбережения [10].

Установившаяся практика по противодействию коррупции демонстрирует, собственно, что надобность в отмывании прибылей от коррупции находится в зависимости от объемов взяток и их сосредоточении:

чем более размер и меньше количество лиц, получающих прибыли от коррупции, тем выше необходимость в отмывании средств [10].

Случаи коррупционных злодеяний с отмыванием средств послужило фундаментом для борьбы с данным злом на интернациональной арене.

Бесспорно, что противодействие отмыванию средств диктует взаимное, межстрановое взаимодействие. Важно выстроить ясные и действенные мосты международного сотрудничества.

С юридической позиции, чтобы отмыть денежные средства необходимо применить довольно распространенные махинации. Как это выглядит? Все достаточно просто: осуществляется денежный перевод на имя члена семьи или иного лица. Но иногда перевод принимает сложную форму в виде транснационального механизма. При данных условиях идентификация и поиск может быть трудоемким, дорогим, в редком случае и невозможным [9, с.490-494].

Существует три основных этапа в отмывании средств:

1) размещение денег, поступивших от действий криминала;

2) маскировка следов;

3) инвестирование денег в предпринимательство или в финансовые институты [9, с.490-494].

Согласно Руководству ВБ [9, с.494], после того как совершено преступление, противоправно полученные средства разграничиваются от криминального источника и далее помещаются в отечественном либо иностранном банке. К примеру, наличность от коррупционного действия используются, чтобы официально оформить депозит в банке. В дальнейшем он будет использоваться для покупки товаров либо услуг.

Как таковое, приобретенные на такие деньги товарные объекты подлежат перепродаже за легальные средства. Полученная выручка вкладывается в активы либо инвестируется в проекты для покупки ценных бумаг.

«На стадии интеграции доходов, незаконно полученные средства возвращаются в законную экономику страны. К примеру, создается требующий значительного оборота денежных средств бизнес: ресторан или крупный магазин, в который можно внести значительное количество незаконно полученных средств и вывести их в виде фиктивной прибыли»· [9, с.494].

Следуя содержанию данного раздела, становится очевидным, что все старания членов международного сообщества могут быть осуществлены на деле, если то или иное государство-участник Конвенции [11] реализует строгие мероприятия, нацеленные для ведения систематической работы в этом направлении.

В данном контексте существуют определенные стандарты, утвержденные FATF, образованной в 1989 году по предложению 7 передовых стран для борьбы с отмыванием денег и торговли наркотиками. На протяжении своей деятельности до настоящего времени данная организация вырабатывает и совершенствует четкие установки по противодействию отмыванию средств [10].

Помимо самих рекомендаций, согласно стандартам FATF в стране-участнике данной организации должно быть создано ПФР [12]. В Казахстане ПФР представлен в лице Агентства РК по финансовому мониторингу. По всему миру более ста стран-участников FATF создали у себя данные подразделения, которые непосредственно занимаются обработкой данных вызывающих те или иные подозрения [12].

Следует обратить внимание, что в настоящее время отчеты, содержащие сведения о подозрительных махинациях в части коррупционной составляющей, используются не совсем эффективно. Борьба с отмыванием денег также выстроена в контроле финансовых организаций, чтобы они осуществляли мониторинг функционеров имеющих высокие должности. Данные действия позволят иметь о них предварительную информацию до совершения ими незаконных финансовых операций [12].

В целом следует обратить внимание, что в государствах с существенными коррупционными преступлениями, отсутствует соответствие инсутрументам, которые необходимы для борьбы с отмыванием денег [12].

Для сравнения, к примеру, в передовых государствах реализуется практика, когда все юрисдикции обязаны держать под контролем валютные переводы и иные транзакции с большими суммами. для того идентифицировать фальсификациию аккаунтов, не исключая счета за странные консультационные услуги и не контролируемые технические составные части, и обычной контрабанды очень дорогих предметов.

Таким образом, закономерным остается вопрос, что необходимо реализовать правительствам, чтобы добиться более значимых совместных усилий в борьбе с отмыванием денег и коррупцией?

Ответом на данный вопрос может быть имплементация рекомендаций, разработанные группой подразделений ВБ [10, с.522-523]:

1) государствам необходимо самостоятельно продолжать осуществление оценок состояния коррупциогенной ситуации, в частности определять наиболее уязвимые участки по отмыванию денег. Разрабатывать программные документы и направлять деятельность правоохранительных органов исходя из результатов оценок;

2) все сотрудники правоохранительных и судебных органов, привлеченные к антикоррупционной деятельности должны проходить обучение по изучению международного законодательства об отмывании денег, повышая тем самым свою квалификацию по обнаружению и мониторингу движения противоправно полученных средств за границей. Им необходимо владеть знаниями по применению процедур замораживания, конфискации· и возврату авктивов;

3) сотрудничество на всех уровнях судебных и правоохранительных органов, а также ПФР для противодействия коррупционным случаям и фактам отмывания денег;

4) обеспечить следователей, прокуроров и судей возможностью применения способов финансового расследования, разработанных для

противодействия отмыванию денег, и технической помощью в процессах, имеющих связь с судебным преследованием высоко/должностной коррупции;

5) все результаты расследований без каких-либо утаиваний должны отражаться в СМИ. Данная мера получит положительный отклик от общественности, которое сможет поверить в эффективность действующего законодательства;

6) приложить усилия по возврату коррупционных прибылей. Требовать их прозрачного применения, чтобы компенсировать пострадавшим лицам убытки [10, с.522-523].

1.3 Международные службы финансовой разведки

В стремительно меняющемся мире, где каждый день появляются новые угрозы международной безопасности, государства объединяют свои усилия и создают международные организации и структуры для противодействия различным угрозам, в том числе отмыванию денег.

В разделе 1.2 мы рассказывали о деятельности FATF, которое на сегодняшний день является одним из основных акторов в борьбе с указанным явлением.

В целом, алгоритм работы ПФР основан на поступающей от финансовых организаций и других структур сведений о подозрительных операциях [10]. Далее проанализированная и подготовленная на основе таких сообщений информация направляется местным правоохранительным службам и членам FATF в целях борьбы с отмыванием денег.

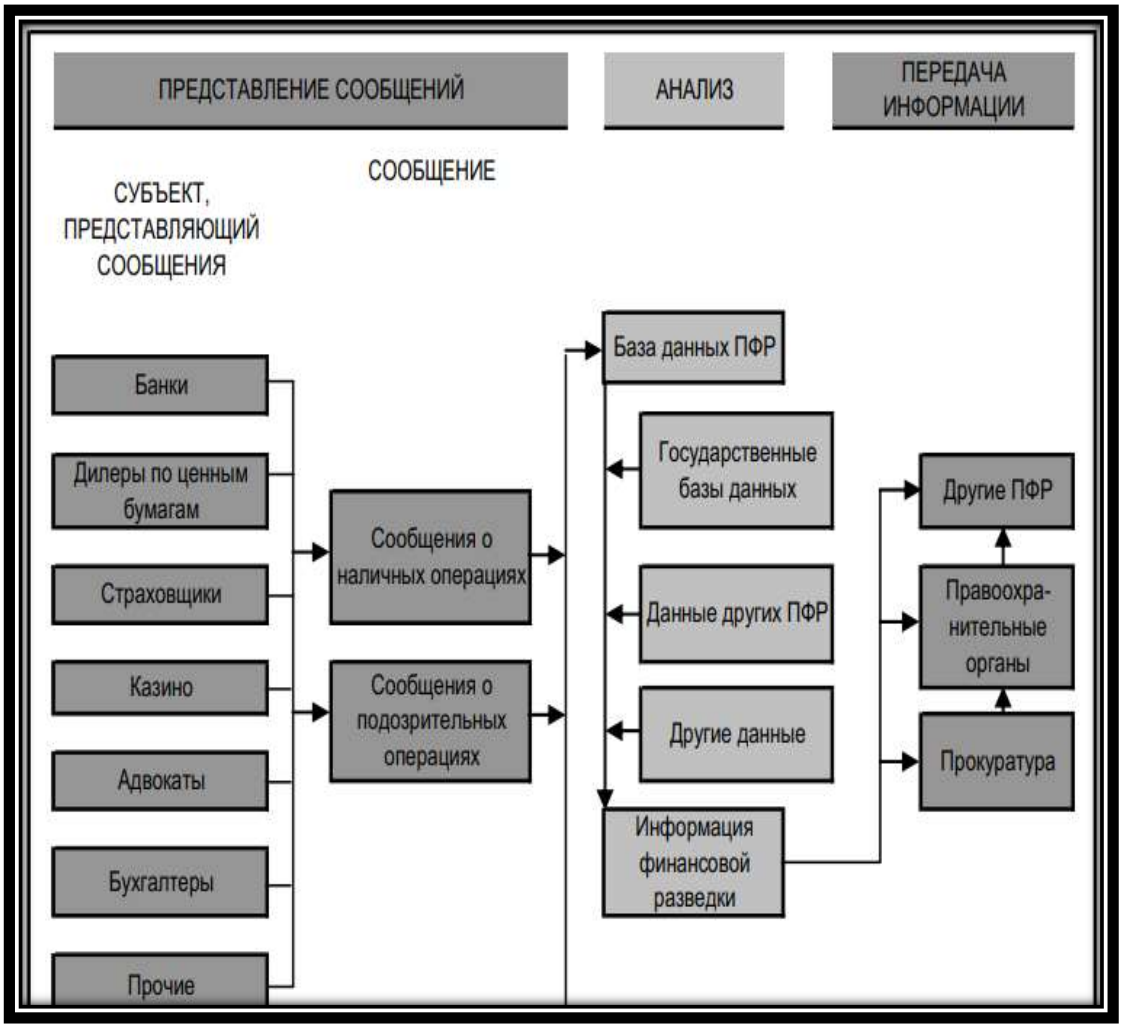

Рисунок 1 – Потоки информации типичного ПФР

Примечание – Составлено автором на основании источника [20]

Периодически, FATF на основе анализа отчетов деятельности компетентных органов стран-участниц, осуществляет выработку рекомендаций по совершенствованию их законодательства [10].

Помимо FATF существуют также так называемые РГТФ, объединяющие в себя группу стран. РГФТ и FATF входят в одну международную сеть по борьбе с отмыванием денег [10].

В РГТФ, также именуемое как ЕАГ входит и Казахстан. Начиная с 2011 года организация является межправительственным органом [12].

В нынешнем году Казахстану предстоит прохождение Второго раунда по Взаимной оценке ЕАГ на соответствие рекомендациям FATF. Оценка подразумевает обзор национальной системы противодействия отмыванию доходов и финансированию терроризма, а также эффективность ее работы [12].

Кроме этого с 1995 года осуществляет свою деятельность организация неофициального формата «Эгмонт», в рамках ·международной институциональной системы противодействия отмыванию денег и финансированию терроризма. Миссия группы «Эгмонт» - предоставить

платформу для эффективного сотрудничества ПФР во всем мире, помимо этого они борются с отмыванием денег и финансированием терроризма [12].

Агентство РК по финансовому мониторингу включен в Группу «Эгмонт» в июле 2011 года [12].

Кроме вышеназванных международных организаций по финансовой разведке существует также региональные организации как Комитет экспертов Совета Европы по оценке мер борьбы с отмыванием денег (Moneyval). Moneyval также имеет структуру по типу FATF. Основной задачей данной организации является обеспечение в странах Европы применения международных стандартов в сфере противодействия отмыванию денег.

Таким образом, Moneyval производит анализ деятельности по борьбе с отмыванием денег и финансированием терроризма в странах - участниках Совета Европы, которые не являются членами ФАТФ. Помимо стран, членами-наблюдателями являются международные организации как Всемирный банк, «Эгмонт», Интерпол и т.д. [12].

2 ЦИФРОВАЯ КОРРУПЦИЯ

2.1 Случаи цифровой коррупции в мире

Как показывает мировой рейтинг ИВК наиболее существенных успехов в деле противодействия коррупции добились европейские страны, в частности государства Скандинавии (Дания, Норвегия, Швеция, Финляндия), Америки (Канада, США) и немного в Азии (Израиль, Сингапур, Япония) [7].

«Коррупция сегодня превратилась в преступно-аморальное явление, причиняющее невосполнимый материальный, политический и моральный вред не только национальным интересам, конкретным компаниям и гражданам, но и интересам всего мирового сообщества.»· [7, с.169].

Факты коррупции в вышеуказанных странах отслеживаются и анализируются тщательным образом. Примечательно, что данные страны не ограничиваются лишь репрессированными методами, наоборот, в процентном соотношении в них преобладает превентивные меры, чтобы не допустить проявления коррупционных случаев априори [7, с.170].

Накопленный мировым сообществом опыт свидетельствует, что наибольших успехов добились те страны, где:

1) деятельность по противодействию коррупции возведена в ранг государственной политики;
2) работа системно институционализирована;
3) обеспечена широкая гласность с использованием СМИ;
4) уделяется должное внимание кадровым отношениям – в борьбе с коррупцией неприкасаемых лиц не существует;
5) работает норма о «конфискации неправомерно нажитого имущества»;
6) информаторы о коррупционных преступлениях находятся под надежной защитой государства;
7) поощряется антикоррупционная деятельность институтов гражданского общества [7, с.170].

Но мы говорим о традиционных видах коррупции. Вызывает определенный интерес, как же обстоят дела в передовых странах по борьбе с цифровой коррупцией. Будет не лишним рассмотреть их опыт и практику.

Современные коррупционеры достаточно активно используют биткоины для получения вознаграждений. Исполнение данных целей осуществляется через использование электронного кошелька, куда поступают деньги, а затем переводятся в криптовалюты для того, чтобы их нельзя было привязать к человеку ни фактически, ни юридически.

В таком случае для правоохранительных органов не остается возможностей использовать их в качестве доказательства, а после того как виртуальная валюта перемещается за пределами страны, невозможной становится и ее конфискация (7, с.10).

Фактически в интернет-пространстве имеется достаточное количество советов и рекомендаций как бороться с коррупцией применяя цифровые технологии, но очень мало четких кейсов как выглядят виртуальные схемы самой коррупции.

Например, в Российской Федерации в последнее время стала появляться информации о фигурировании криптовалюты в коррупционных делах в качестве взятки.

В целях недопущения в ближайшей перспективе подобных факторов, Правительство России в настоящее время разрабатывает поправки в свои УК и УПК, чтобы позволить компетентным органам конфисковать цифровые активы, принесшие прибыль от криминальной деятельности.

По словам российских специалистов, существует несколько методов для конфискаций цифровых активов:

1) добровольное осуществление перевода средств на электронный кошелек государственных финансовых организаций по итогам решения суда;

2) конфискация SSID (имя локального WI FI), логина или пароля в рамках оперативно-розыскных действий, также и по решению суда;

3) заморозка денег на регулируемых криптобиржах, прошедших регистрацию в юрисдикциях Российской Федерации. После этого средства переводятся в соответствующие гос.организации по официальному запросу.

В США и странах Европы для конфискации преступных криптовалют применяются специальные программы, разработанные для осуществления контроля за транзакциями, которые связывают оформленные на кого-либо ключи шифрования с прошедшими идентификацию лицами в сети интернет. Однако в статье упоминается, что на самом деле как показывает практика, это достигается не легким путем [13].

Как факт, видов криптовалюты очень много и некоторые из них не подвергаются контролю, такие как Monero [13].

Принимая во внимание, что интернет сам по себе децентролизован, отдельного контроля по поступлению криптовалюты и доступа к ней практически невозможно [13].

Специалистам правоохранительных органов, в крайнем случае, остается только конфисковать криптовалюту путем изъятия секретных ключей [13].

В 2018 году Министерство юстиции США конфисковала 17 млн. долларов в биткоинах у наркоторговцев, в том же году почти половину от вышеназванной суммы конфисковали у пользователе теневого виртуального рынка AlphaBay [13].

В Англии местная полиция изъяла почти 300 биткоинов у картеля по наркоторговле. После чего был осуществлен перевод на специально созданный криптовалютный кошелек. После этих действий данные средства по курсу были обменены на фунты-стерлинги и внесены в республиканский бюджет.

Показанные выше примеры осуществимы только в случае если имеется доступ к ключам шифрования, которые были найдены в процессе обыска на флеш-картах либо компьютере. Если таковых ключей нет, и они находятся в сервере, к которому нет доступа, то изъятие не осуществимо. Практика по выходу из данной ситуации не имеется [13].

2.2 Ситуация в Республике Казахстан

В результате системной превентивной работе Агентства РК по противодействию коррупции, переходу на трехзвенную модель уголовного процесса, количество зарегистрированных в Казахстане фактов коррупции снизилось на 29% [14].

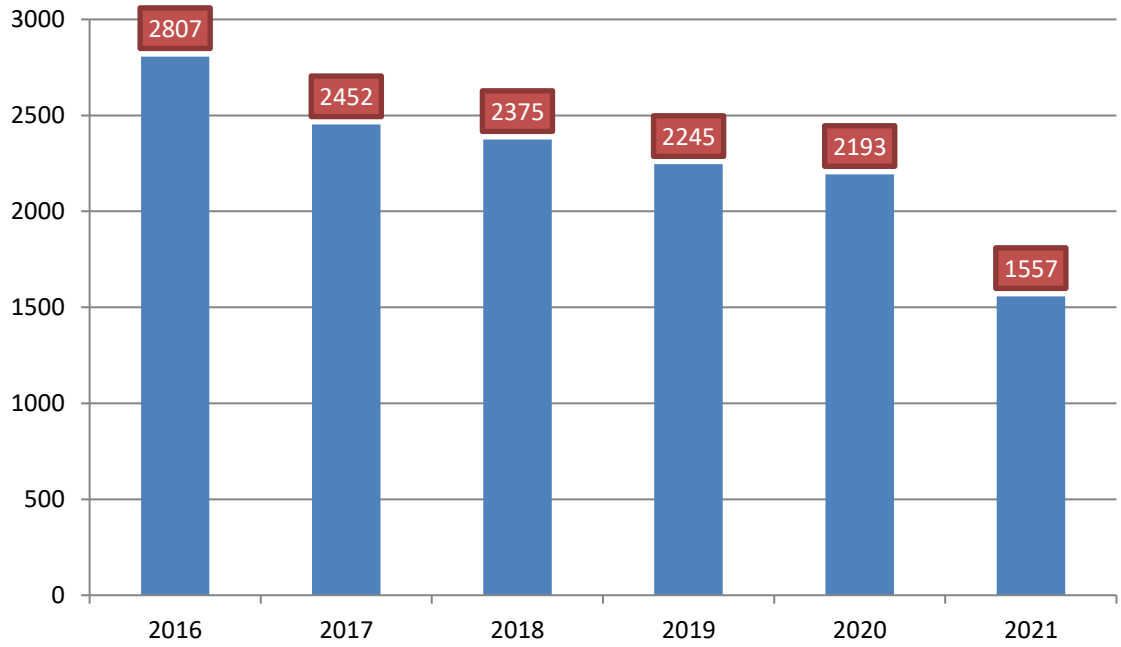

Рисунок 2 – Динамика коррупционной преступности

Примечание – Составлено автором на основании источника [14]

В 2021 году Агентство возместило 20,4 млрд тенге или 86% (из 23,8 млрд тенге установленного ущерба) [14].

Делая исторический экскурс, следует отметить, что Агентством (с 2015 года) пересмотрены методы борьбы с коррупцией, основным регулирующим документом, которого стал – Закон Республики Казахстан от 18 ноября 2015 года № 410-V «О противодействии коррупции» [14].

В соответствии с социальным исследованием Transparency International Kazakhstan в 2019 году выявлено, что в Казахстане 54,4% опрошенных, считают, что количество коррупционных случаев за последний год в их населенном пункте скорее снизилось [15].

Вместе с тем, данное исследование показало, что доля тех, кто считает, что в стране можно решать вопросы, не прибегая к коррупционным схемам (35,8%), в два раза ниже суммарной доли тех, кто считает, что коррупция является неотъемлемой частью наших ежедневных практик (56,3%) [15].

По цифровым данным, которые указаны выше мы видим, что в целом ситуации с коррупцией в Казахстана более или менее контролируема [15].

Тем не менее, новым вызовом для нашей страны будет являться цифровая коррупция, по которой в Казахстане нет четкого законодательного определения, а также методов борьбы с ней.

Помимо этого поиск зафиксированных коррупционных фактов с использованием цифровых инструментов в виде криптовалюты не дал результатов.

Если говорить о самой криптовалюте, то в 2020 году в Казахстане принят закон, где криптовалюта признана имуществом и которая не может служить средством платежа. Выпуск и оборот криптовалюты позволено только на территории МФЦА, имеющий свой собственный правовой режим [16].

2.3 Возможные методы борьбы с цифровой коррупцией

В предыдущем подразделе 2.2 рассмотрено понятие отмывания денег в традиционном его понимании, согласно принятым международным стандартам FATF.

Однако, как уже было показано в подразделе 2.1, в современном мире существует использование новых, так называемых цифровых технологий для осуществления коррупционных преступлений.

Поэтому в данном разделе более подробно будет рассмотрен новый феномен под названием цифровая коррупция, а также возможные методы борьбы с ней.

Как считает автор статьи «Противодействие коррупции в условиях цифровизации: возможности, перспективы, риски» Овчинников А.И. вполне реалистичным является использование ИИ для обнаружение конфликта интересов как фактора коррупции.

Применение поисковых систем и программ по типу американского TRM позволяет в некоторых случая обнаруживать «виртуальные следы» и конфликты интересов. В последующем, подготовленные сведения будут направлены в правоохранительные органы для содержания коррупционных признаков [7, с.6].

Исходя из этого, очевидно, что цифровые технологии облегчают процесс отслеживания перемещений коррумпированных функционеров и их капиталов.

В этом роде показателен опыт Китая, где существует межведомственная программа по отслеживанию миграционных путей иммигрировавших за рубеж коррупционеров.

Вошло в практику применение правоохранительными органами ресурсов «больших данных» чтобы производить антикоррупционный контроль за деятельностью должностных лиц.

Из фрагментарных данных при помощи подобного инструмента вырисовывается целостная картина системной коррупционной деятельности. При всем этом возникает возможность автоматического учета сведений статистики значительного числа признаков коррупционных отношений: о конфликте интересов, о появляющихся динамических коррупционных рисках, о статистике коррупционных преступлений в привязке к конкретному размеру полномочий правительственного работника.

Подобные операции приведут к осуществлению объективной оценки коррупционных рисков тех или иных должностей в органах власти с учетом их местоположения, социально-экономических критерий и т.д.

Кроме этого существует также возможность на основе нейросетевого программирования начать попытки моделирования коррупции путем сочетания самоорганизующихся коррупционных схем, предусматривающих последующие начальные значения:

- свод информации уже выработавшихся методик и совершившихся коррупционных прецендентов;
- средство налогооблажения имущества в виде зданий и сооружений;
- ситуация в сфере малого или крупного бизнеса;
- происхождение новых финансово-спекулятивных предприятий;
- постоянный успех у одной и той же политической партии, остающейся у власти продолжительный период и др.

Прогностическая матрица предоставляет различные профили коррупционного риска в зависимости от экономических условий региона, сроков прогноза, политической культуры.

В связи с приведенными аргументами, очевидно, что развитие информационных технологий противодействия коррупции, отдельные проекты их успешного внедрения в передовых странах (США, Китай) позволяет сегодня ставить вопрос о разработке соответствующей концепции развития цифровых технологий по противодействию коррупции.

В целом развитие системы цифровых технологий противодействия коррупции актуализирует вопрос разработки новых криминалистических методов, позволяющих как интерпретировать Big data, выделяя из массивов информации признаки коррупционных отношений, так и определять конкретные параметры, характер данных для сбора и последующей обработки [8, с.8].

Интересным в данном направлении является также исследование ПРООН: «Новые технологии для устойчивого развития: перспективы использования для обеспечения добросовестности, доверия и борьбы с коррупцией».

В указанном исследовании отмечается, что цифровые технологии имеют большие перспективы использования в сфере противодействия коррупции. При этом условно область их применения можно разделить на 2 вектора:

1) использование непосредственно для предупреждения и противодействия коррупционным практикам за счет выявления, анализа, расследования, прогнозирования и мониторинга коррупционных нарушений;

2) использование для косвенного влияния на коррупцию посредством продвижения принципов эффективности, подотчетности и прозрачности в деятельности государственных институтов.

В своей работе авторы согласны, что развитие цифровых технологий создает и новые угрозы, и уязвимости, в том числе коррупционной направленности.

В сравнении с предыдущими данными, приведенными из исследований российских специалистов Овчинникова Н. А. и группы ученых, мы видим, что работа, подготовленная ПРООН, совпадает с мнением, что цифровые технологии могут использоваться для отмывания денег, мошенничества и киберпреступности. Акцент ставиться на том, что применение таких технологий требует соблюдение баланса между регулированием и инновациями, решения этических дилемм, связанных с необходимостью соблюдения прав человека и т.д.

Предлагается рассмотреть насколько эффективно использование цифровых технологий на примере исследования ПРООН [17].

Искусственный интеллект, машинное и глубокое обучение

Ученые отмечают, что кейсов с применением ИИ, как составной части цифровых технологий в борьбе против коррупции относительно немного.

Однако, использование ИИ могло бы позволить значительно упростить механизм выявления, анализа и прогнозирования коррупционных нарушений через:

1) быструю переработку значительных размеров сведений, которое фактически заняло бы у работников компетентных органов много рабочего времени. В таких данных может содержаться потенциальная информация о коррупционных преступлениях;

Примеры так, в Великобритании, использование ИИ позволило следователям проанализировать более 30 млн документов и выбрать релевантные для расследования данные всего за пару месяцев, в то время как «ручная» обработка таких документов заняла бы значительно больше времени;

2) раннего обнаружения аномалий, «красных флажков» и закономерностей, указывающих на вероятные коррупционные нарушения, с достаточно высоким уровнем точности.

Примеры: в Испании исследователи разработали модель на основе нейронных сетей, которая позволяет рассчитывать вероятность коррупционных нарушений в регионах страны и определять условия, способствующие их совершению; соответствующий инструмент может использоваться органами власти для принятия превентивных мер и снижения коррупционных рисков.

А в одном из регионов Чехии были проанализированы общедоступные финансовые и отраслевые данные всех подрядных фирм страны с тем, чтобы предсказать, какие из них имеют связи с политически значимыми лицами; используя методы машинного обучения, исследователи обнаружили, что более 75% фирм с такими связями могут быть точно идентифицированы ИИ;

3) мониторинга соблюдения антикоррупционных стандартов: с одной стороны, ИИ может применяться регулируемыми организациями для того, чтобы привести бизнес-процессы в соответствие с установленными требованиями, с другой – использоваться регулирующими органами для

выявления нарушений требований или преднамеренных попыток мошенничества.

Примеры: Так, израильской компанией Shield FC была создана платформа, основанная на ИИ, обработке естественного языка и возможностях визуализации для автоматизации и организации полного жизненного цикла системы комплаенса в сфере коммуникаций, снижения рисков и повышения эффективности надзора.

Введенная в действие Transparency International Ukraine система Dozorro, основанная на использовании онлайн-мониторинга и набора интеллектуальных инструментов, позволила резко повысить эффективность выявления нарушений в сфере государственных закупок: в период 2016-2018 гг. на основе результатов работы Dozorro были выдвинуты уголовные обвинения в отношении 22 лиц и применены санкции в отношении 79 лиц;

4) снижения влияния человеческого фактора, порождающего дополнительные риски коррупции, за счет передачи ряда функций ИИ.

Вместе с тем, несмотря на очевидные преимущества использования ИИ, существуют также и новые угрозы:

1) ИИ может использоваться в мошеннических и коррупционных схемах;

2) в зависимости от качества используемых данных и заложенных алгоритмов, ИИ может порождать гендерную и расовую дискриминацию; неконтролируемое использование ИИ может приводить к нарушению конфиденциальности данных;

3) сложность алгоритмов ИИ не позволяет точно сказать, как именно выполняется вычисление, приводящее к определенному результату, что неизбежно ведет к непрозрачности процесса, затруднению интерпретации причин принятия тех или иных решений ИИ и, как следствие, снижению доверия к программам, использующим ИИ [17].

Например, в Китае создана экспериментальная система «Zero Trust», которая анализирует данные из более чем 150 баз федеральных и региональных органов власти. Она составляет сложные многоуровневые карты социальных связей должностных лиц и позволяет выявить признаки коррупционных нарушений – например, увеличение банковских сбережений, покупку нового автомобиля или участие в тендере на получение государственного контракта от имени чиновника, членов его семьи или друзей. Однако имеется проблема в части невозможности объяснить используемый системой алгоритм, позволивший прийти к выводу о наличии неправомерной деятельности. Данный факт привел к снижению доверия к данному инструменту, как следствие, многие органы местного самоуправления отказываются от использования «Zero Trust» [17].

Таким образом, авторы в целях минимизации некоторых из указанных рисков предлагают при внедрении технологии ИИ руководствоваться следующими принципами:

1) обеспечивать контроль за работой систем, использующих ИИ, на этапе их проектирования и разработки для устранения системной и случайной предвзятости/дискриминации при принятии решений, а также снижения коррупционных рисков при использовании различных технологий ИИ;

2) инвестировать в создание качественных баз данных, на которых в дальнейшем будет обучаться ИИ;

3) повышать прозрачность и подотчетность работы систем, использующих ИИ, с тем, чтобы обеспечить доверие общества к таким системам [17].

Блокчейн

Сами по себе технологии блокчейна трудно представить в качестве инструмента борьбы с коррупцией, но их текущее использование вселяет надежду на то, что они могут обеспечить открытый процесс отслеживания активов и контроля за государственными контрактами [18].

Обратимся немного к истории, в 2008 году скрытный разработчик, писавший под псевдонимом «Сатоши Накамото», впервые описал биткойн и лежащую в его основе технологию блокчейна [18].

С тех пор цифровая валюта набирала обороты и теперь используется для транзакций по всему миру. Он позволяет переводить законные и незаконные средства и работает так же, как наличные деньги. За исключением того, что никакие банки или границы не препятствуют потоку средств в сфере биткойнов [18].

Официальные биржи, на которых цифровые монеты могут быть конвертированы в фиатные валюты (валюта, стоимость которой обеспечивается государством, которое ее выпускает), регулируются в некоторых странах и подчиняются правилам борьбы с отмыванием денег [18].

Однако в других местах обмен происходит неформально между людьми в закрытых чатах или группах в социальных сетях.

Изначально Биткойн и блокчейн были спроектированы так, чтобы существовать без центрального регулирующего органа. В последнее время интерес к криптовалюте проявляют государственные деятели. Те же учреждения, от которых пытались отказаться цифровые валюты, теперь хотят использовать эту технологию в финансовых целях [18].

В то время как технологии блокчейна предоставляют много возможностей для предотвращения коррупции и содействия прозрачности и добросовестности, они также могут быть использованы не по назначению в личных целях, таких как использование криптовалюты для отмывания денег, незаконных (например, на черном рынке) операций и уклонения от уплаты налогов [18].

Применение криптовалют преступниками для незаконной деятельности на протяжении многих лет привлекало внимание финансовых регуляторов, законодательных органов, правоохранительных органов и средств массовой информации. Некоторые утверждают, что анонимность биткойна способствует отмыванию денег и другим преступлениям [18].

В 2008 году биткойн был представлен как криптовалюта без центрального банка или единого администратора, но управляемая сетью заинтересованных сторон. Биткоины начисляются в результате процесса, известного как «майнинг», и могут быть обменены на продукты, услуги и другие валюты. Это одна из самых известных криптовалют, но она подвержена незаконным транзакциям, отмыванию денег, деятельности на черном рынке и другой коррупционной деятельности [18].

Криптовалюты также были уязвимы для кражи в результате взлома и мошенничества: только в первой половине 2020 года было украдено более 1,4 миллиарда долларов США. В последние годы эта незаконная деятельность привлекла широкое негативное внимание общественности, в том числе со стороны финансовых регуляторов, законодательных органов, правоохранительных органов и СМИ [18].

Блокчейн и технология распределенных реестров - это технологические инновации, питающие биткойн и другие криптовалюты [18].

Другими словами, несмотря на постоянные аргументы за и против криптовалют, они представляют собой лишь одно применение технологий блокчейна, которые также используются в других приложениях, в том числе для смарт-контрактов, управления цепочками поставок и других (как обсуждается в этом исследовании), с широкими преимуществами для повышения прозрачности и целостности [18].

Более того, использование и неправильное использование криптовалют также зависят от правовой и нормативной среды. В некоторых странах существуют положения для обеспечения соблюдения правил «Знай своего клиента» (KYC), которые гарантируют проверку личности клиента во время открытия и ведения счетов для оценки и мониторинга клиентских рисков. Это задумано как способ противодействия от отмывания денег [18].

Как мы видим, блокчейн может расширить возможности людей, которые не имеют достаточных услуг, тем самым помочь решить социальные проблемы.

В 2018 году Национальный исследовательский совет Канады (NRC) начал пилотное внедрение нового блокчейна на основе Ethereum для более открытого управления государственными закупками. Например, канадцы могут получать данные о государственном финансировании с помощью этого смарт-контракта [18].

С помощью технологии блокчейн Индия улучшила процесс отслеживания владения землей, объединив технологию с земельными реестрами. Швейцария улучшает доступ к государственным услугам. А в США электронное голосование на выборах уже идет полным ходом [18].

Все эти процессы тесно связаны со сбором и передачей персональных данных, поэтому в дополнение к преимуществам для всей системы могут возникнуть проблемы, связанные с кражей личных данных, киберпреступностью и мошенничеством [18].

Таким образом, кроме положительных качеств, применение технологий распределенных баз данных сопряжено и с определенными рисками, в том числе [18]:

1) использование технологии блокчейна в целях получения личной выгоды, например, использование криптовалют для отмывания доходов, незаконных сделок и уклонения от уплаты налогов. При этом недобросовестные лица могут пользоваться услугами нерегулируемых криптовалютных бирж или децентрализованных пиринговых сетей (сеть основанная на равноправии участников), которые игнорируют требования по борьбе с отмыванием денег и потому лишают правоохранителей возможности отслеживать такие незаконные транзакции и привлекать соответствующих лиц к ответственности;

2) недостаточная защищенность загружаемой в систему, работающую на основе технологии блокчейна, конфиденциальной информации, которая может быть деанонимизирована, как следствие – возможность использования технологий распределенных баз данных для злоупотребления властью и получения контроля над системой [18].

Для снижения возможных рисков при использовании технологий распределенных баз данных авторы доклада рекомендуют:

– разработать и принять нормативные правовые акты, регулирующие различные аспекты использования указанных технологий, включая вопросы юрисдикции, рисков и ответственности;

– предусмотреть создание и функционирование цифровой инфраструктуры и процессов, обеспечивающих надлежащую работу соответствующих технологий.

Резюмируя тематику блокчейна, в целом, следует отметить, что данная технология все еще далека от того, чтобы быть легко применимой, и масштабируемой как антикоррупционный инструмент.

Потребуются скоординированные усилия, объединяющие все заинтересованные стороны, включая правительство, частный сектор, гражданское общество, технологов и научные круги, для выработки осуществимых политических рекомендаций и руководящих принципов, регулирующих использование технологии блокчейн [17].

Большие данные (Big data)

Проведение анализа больших и сложных массивов данных (Big data) для целей противодействия коррупции может использоваться по двум основным направлениям [17]:

1) для выявления, расследования, мониторинга и аудита подозрительных операций и оценки коррупционных рисков.

Например, анализ Big data применялся журналистами-расследователями при работе с «Панамским Архивом» и «Архивом Пандоры» (в частности, использовались графические платформы, такие как Neo4j и Linkurious) и бразильскими следователями в рамках операции «Автомойка» [17];

Центр по изучению коррупции в Будапеште использует анализ больших данных для мониторинга государственных закупок в странах ЕС, выявляя с его помощью аномальные закономерности, такие как исключительно короткие периоды проведения торгов или необычные результаты (например, отсутствие конкуренции при торгах или неоднократная победа одной и той же организации) [17];

Европейская комиссия разработала программу ARACHNE (в переводе с древнегреческого – «паук»), которая осуществляет перекрестную проверку данных из различных государственных и частных баз данных и позволяет выявлять проекты, подверженные рискам мошенничества, конфликта интересов или иных нарушений [17];

1) для повышения информированности, совершенствования национальной, отраслевой или местной антикоррупционной политики и повышения результативности ее реализации посредством предиктивного анализа и визуализации, способствующих более эффективному принятию решений [17].

Например, в одном из регионов Индии офисом главного министра был запущен дашборд («умная» панель управления, позволяющая отображать данные в реальном времени), который используется для содействия принятию решений на основе фактических данных из различных источников, в том числе полученных от населения по «горячей линии» для регистрации жалоб и предложений, связанных со всеми аспектами функционирования правительства [17].

В данном контексте, как и в предыдущих способах противодействия цифровой коррупции, несмотря на множество возможностей использования анализа Big data для противодействия коррупции, его проведение связано с определенными трудностями, в частности [17]:

1) потребностью в обеспечении контроля за соблюдением конфиденциальности данных и борьбой с неправомерным использованием соответствующей информации.

Пример: скандал вокруг Cambridge Analytica ясно продемонстрировал, как легко персональные данные могут быть извлечены и использованы в политических целях; при этом государственные структуры аккумулируют огромные объемы персональных данных, которые в основном носят конфиденциальный характер, включая данные, связанные с доходами и финансами, медицинские записи, идентификационные сведения и другую политическую или экономическую информацию, а значит, риски утечки и/или деанонимизации таких данных, хранящихся в государственных базах данных, могут иметь еще более существенные последствия [17].

Как отмечают эксперты Независимой антикоррупционной комиссии широкого профиля (Independent Broad-Based Anti-Corruption Commission), действующей в одном из штатов Австралии, несанкционированный доступ к конфиденциальной информации, ее раскрытие и злоупотребление ей со стороны государственных служащих на практике являются ключевыми

факторами, порождающими коррупцию, но часто недооцениваются государством [17];

2) необходимостью понимания и выявления коррупционных рисков – от «захвата государства» до злоупотреблений в сфере регулирования – при обработке больших данных и принятия мер по их минимизации: учитывая влияние результатов анализа Big data на политические процессы, политические решения и законодательные инициативы, недобросовестные лица могут оказывать воздействие на процессы сбора данных и обмена информацией с тем, чтобы получить более выгодные результаты анализа [17];

3) предоставления ресурсов, в том числе человеческих, для проведения анализа и формирования соответствующих навыков, нехватка которых наблюдается во многих странах [17].

Для их преодоления странам предлагается, в частности:

– обеспечивать сбор качественных, надежных и точных используемых для анализа данных компетентными органами;

– повышать квалификацию лиц, проводящих анализ, развивая их аналитический потенциал;

– предусмотреть создание необходимой правовой базы, регулирующей, в том числе, вопросы сбора, хранения и обмена данными, обеспечения их защиты и безопасности;

– принимать меры для ответственного использования данных и соблюдения прав человека при проведении анализа Big data [17].

Используя традиционное программное обеспечение для обработки данных, трудно выявить коррупцию из-за необходимости анализа больших объемов и разнообразия данных. Однако рост объема больших данных привел к появлению новых методов управления данными и интеллектуального анализа данных для предотвращения мошенничества и злоупотреблений в государственном секторе [17].

В этом контексте анализ больших данных в области борьбы с коррупцией, обобщенная в 2018 году общественной организацией U4 (Норвегия), может быть полезна для выявления случаев коррупции, измерения распространенности коррупции, проведения сравнений между организациями или временем и оценки воздействия на коррупцию [17].

Таблица 1 – Анализ Big Data в антикоррупционной работе

ЦЕЛИ АНАЛИЗА	**ОТДЕЛЬНЫЕ ЗАПИСИ ДАННЫХ**	**АНАЛИЗ ПОЛНОГО НАБОРА ДАННЫХ**	**ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА НЕСКОЛЬКО НАБОРОВ ДАННЫХ**
Выявление случаев коррупции	Расследование конкретных лиц, фирм, контрактов и т.д.	Выявление аномальных закономерностей или экстремальных значений	Выявление случаев предоставления услуги за услугу
Измерение распространенности коррупции	Объединение нескольких конкретных расследований	Частота измерения неправильных или подозрительных значений	Измерение частоты ненадлежащих или подозрительных связей
Сравнение между объектами или временем		Сравнение значений между организациями с целью составления рейтингов; или с течением времени с целью оценки тенденций	Сравнение связей между подразделениями с целью составления рейтингов; или с течением времени для оценки тенденций
Оценка воздействия на коррупцию		Сравнение значений между обработанными/необработанными единицами или до/после вмешательства	Сравнение связей между обработанными/необработанными единицами или до/после вмешательства

Примечание – Составлено автором на основании источника [17]

Таким образом, необходимо отметить, что для того, чтобы антикоррупционная аналитика была значимой и эффективной в предотвращении и борьбе с коррупцией, необходимо учитывать несколько факторов: данные хорошего качества, аналитические возможности, соответствующие законы и нормативные акты, доверие к данным, системам и учреждениям.

Чтобы закрепить вышеприведенную информацию о возможностях использования Big data, рассмотрим более детально китайский кейс.

Контролирующие органы КНР, проводящие дисциплинарные расследования, используя платформу больших данных, объединили промышленность, социальное страхование, налоговую службу и другие специализированные данные. Это дает возможность в процессе расследования делать массовое сравнение и анализ, быстро и точно проверять информацию, достоверно определять источник проблемы, что позволило проложить новый современный и качественный технологический путь в борьбе с коррупцией [19, с.3-4].

Возьмем, к примеру, город Харбин. В течение последних лет единое руководство координационной группы по борьбе с коррупцией всеми силами содействовало созданию платформы больших данных, последовательно создавались объекты надзора дисциплинарного расследования, контроль за соблюдением дисциплины, проверка информации о подключении к Интернету и т. д. Всего было создано 11 модулей, которые охватывали 1 169 кадровых работников данного города, 470 000 кадровых партийных работников и государственных служащих всех ступеней, 178 единиц непосредственно городского подчинения и различных уездов (город и пригородные районы), целью которых было создание некоррумпированных правительства и партии. Одновременно происходило объединение ресурсов информационных данных, таких как жилой фонд, промышленность, налоговая служба, медицинское страхование, социальное страхование, коммунальные платежи и пр. Это позволило предоставлять быструю, точную и всестороннюю информацию инспекторам, проводящим расследования по соблюдению дисциплины [19, с.3-4].

В течение пяти лет, с октября 2012 по декабрь 2017 г., контролирующие органы, проводящие дисциплинарные расследования, в Харбине на платформе Big Data провели расследование, а впоследствии и наказали, по 1 669 фактам нарушения партийных Правил восьми пунктов, 2 180 человек попали под следствие, из них 671 «игрок» из партийной власти всех ступеней был отдан под суд [19, с.3-4].

На практическом примере Харбина была продемонстрирована огромная мощь больших данных в борьбе с коррупцией [19, с.3-4].

Как мы видим на примере китайского кейса, данный метод на самом деле является готовым инструментом для противодействия цифровой коррупции.

Борьба с коррупцией с использованием больших данных – это глубокий анализ данных виртуального мира с целью выявления в реальном мире скрытых контактов представителей власти, выявления чиновничьих клик, создаваемых ими с целью извлечения личных выгод; обнаружения случаев коррупции в реальных совокупностях комплексных взаимосвязей.

В эпоху Big Data в сложных социальных сетях информационный след оставляют все, будь то частное лицо или организация: обычную информацию или информацию о передвижениях и местонахождении. Благодаря

проникновению Интернета в мир, популярности социальных сетей пользователи после просмотра страниц оставляют в них электронно-цифровой след (цифровой отпечаток), изучение которого в действительности является изучением взаимосвязей в социальных сетях.

В процессе сбора цифровых данных разнообразная информация сливается воедино, появляется возможность создания виртуального образа личности. Эти электронные следы цифровых данных, или отпечатки, пользователей могут стать ориентиром в борьбе с коррупцией.

В этой борьбе используются технологии управления цифровыми данными, для того чтобы состыковать разнообразные цифровые данные на платформе одной системы, чтобы информационные технологии, технологии дистанционного географического зондирования и органы дисциплинарного контроля и расследования провели перекрещивающееся исследование, а также применяется метод сопоставления цифровых данных, метод совмещения цифровых данных, перекрестного доказательства и другие методы, позволяющие разрешить существующие в цифровых данных пробелы, такие как недостоверность информации, перегруженность или недостаток информации и др.

Таким образом, в море цифровых данных можно выловить ключ к пониманию коррупционных явлений.

Так, основное отличие борьбы с коррупцией с применением Big Data от традиционной заключается в том, что технологии обработки больших данных разбили прежний остров скрываемой коррупционерами информации, наладили взаимосвязь и сообщение между ранее изолированными данными, что позволило более эффективно их использовать.

Например, в процессе выплат минимального социального обеспечения для граждан городов КНР часто встречаются такие коррупционные поступки, как получение пособий от чужого имени, многократное получение пособия одним человеком и т. д. Технология обработки больших данных позволила проанализировать демографические данные и устранить имеющиеся информационные пустоты. В результате под подозрение попали кадровые работники, нарушавшие правила распределения минимального социального обеспечения для граждан [19, с.5-8].

Опыт КНР в борьбе с коррупцией с использованием Big data показывает, что в настоящее время она главным образом применима в следующих пяти областях: письмах и визитах с жалобами в вышестоящие инстанции, привлечении к ответственности за несоблюдение дисциплины, инспекторском предварительном оповещении, народном контроле и открытой информации [19, с.5-8].

Подытоживая сказанное выше, можно констатировать, что в действительности большие данные в последние годы стали настоящим оружием КНР в борьбе с коррупцией.

Однако, нельзя не обратить внимание, что такая технология также легко может нарушить основные права свободных граждан, поэтому в последние

годы Китай активно работает над поиском динамического равновесия между этими аспектами управления на основе законов [19, с.5-8].

Следовательно, чтобы полностью реализовать потенциал новых технологий в обеспечении добросовестности и предотвращении коррупции и других рисков, важно признать ключевые предпосылки их успеха.

К ним относятся уровни цифровой инфраструктуры и прогресс, достигнутый в создании цифрового общества – технически подкованного населения с равным доступом к технологиям и владением ими. Цифровая грамотность, оцифрованные публичные записи, данные и подключение к Интернету - это лишь некоторые из условий, необходимых для применения этих технологий.

В то же время необходимо создать правовую и нормативную базу для предотвращения неправомерного использования и мошенничества, обеспечения конфиденциальности и защиты данных и укрепления доверия.

РЕКОМЕНДАЦИИ

В целях реализации вышеназванных целей в работе ПРООН, которое мы рассмотрели ранее, полагаю целесообразным применить в антикоррупционной деятельности Казахстана технологические рекомендации, предлагаемые ПРООН правительствам стран по созданию благоприятных условий использования и регулирования этих новых технологий таким образом, чтобы поддерживать честность, доверие и противодействие коррупции [16]:

1. Укрепление потенциала правоохранительных, антикоррупционных и надзорных органов для понимания возможностей и рисков, связанных с новыми технологиями в национальной цифровой стратегии. Эта стратегия должна иметь четкие рамки реализации, координации, регулирования, мониторинга и оценки и должна способствовать инновациям и вовлечению, сводя к минимуму потенциальные риски неправильного использования или злоупотреблений. Он также должен реагировать на изменения и инновации в технологии, которые происходят с технологическим прогрессом.

2. Осуществление достаточных инвестиций:

– на пути к развитию общества цифровых знаний и укреплению благоприятной среды, включая содействие доступному цифровому подключению, обеспечение надлежащего уровня цифрового взаимодействия между правительством и обществом и сокращение цифрового разрыва (в том числе между молодыми и пожилыми, мужчинами и женщинами, богатыми и бедными);

– создать цифровую инфраструктуру, необходимую для использования инструментов искусственного интеллекта, технологии блокчейн, анализа больших данных и других новых технологий для антикоррупционной работы. Цифровизация и передача данных являются необходимыми критериями к внедрению новых технологий, но большинство развивающихся стран не имеют необходимого уровня цифровизации и инфраструктуры;

– развивать навыки и аналитические способности, необходимые для внедрения новых технологий для обнаружения, прогнозирования и анализа данных о коррупции;

3. Разработать руководство и процедуры по надлежащему управлению и регулированию использования данных, включая их сбор, хранение, совместное использование, конфиденциальность, безопасность и защиту. Оказывать поддержку учреждениям в стандартизации и сборе данных, от официальной статистики до административных реестров, чтобы сделать их открытыми для надлежащего использования, анализа и мониторинга. Учитывая, что данные лежат в основе преимуществ новых технологий, точность, актуальность и полезность аналитики для совершенствования усилий по борьбе с коррупцией зависят от качества данных.

4. Укреплять цифровое образование и грамотность в обществе, с тем чтобы можно было использовать преимущества технологий во благо, включая укрепление равного доступа населения к технологиям и права собственности на

них. Необходим общегосударственный подход, при котором государственные учреждения работают с частным сектором, а также предоставляют гражданскому обществу и гражданам знания и информацию.

5. Сотрудничать с отраслями промышленности, чтобы обеспечить соблюдение нормативных требований, в то же время позволяя использовать новые технологии с максимальным потенциалом, в том числе в непрерывных экспериментах, инновациях, адаптации и сбоях [17].

Кроме показанных рекомендации международных специалистов, мы считаем целесообразным в первую очередь внести в профильный закон «О противодействии коррупции» определение цифровой коррупции.

Также необходимо будет внести сопутствующие изменения в законы о кибербезопасности, УК и УПК видов мошенничеств реализуемых с помощью криптовалюты.

Если говорить в разрезе каждой цифровой технологии по противодействию коррупции, то в ниже приведенной таблице представлены следующие рекомендации.

Таблица 2 – Краткое изложение выводов и рекомендаций по каждой новой технологии.

Возможности	**Риски и ограничения**	**Рекомендации и моменты, на которые следует обратить внимание**
Технологии искусственного интеллекта (ИИ)		
• Способен анализировать большие объемы данных для выявления сложных взаимосвязей или закономерностей, которые трудно идентифицировать одному человеку;	• Результаты, генерируемые ИИ, и полезность ИИ в значительной степени зависят от конструкции алгоритма и используемых данных;	• Люди должны сначала направлять системы искусственного интеллекта в правильном направлении при их проектировании, разработке и развертывании. Создание эффективного управления и контроля имеет решающее значение для его безопасного и эффективного использования;
• Позволяет властям принимать упреждающие и превентивные меры, выявляя необычные модели или «красные флажки» и прогнозируя коррупционную деятельность;	• Сложность алгоритмов "черного ящика" делает невозможным точное объяснение того, как выполняется вычисление, приводящее к заданному результату;	• Инвестиции в качественные данные имеют решающее значение для получения преимуществ искусственного интеллекта;

Продолжение таблицы 2

• Ускоряет анализ больших объемов данных, что может позволить людям сосредоточиться на тщательном изучении потенциальных коррупционных действий и отслеживать необычные / подозрительные модели	• Процедуры с использованием искусственного интеллекта также могут использоваться для содействия коррупционной деятельности (например, использование методов искусственного интеллекта для мошенничества, манипулирования и других незаконных действий)	
Блокчейн		
• Способен создать прозрачную и подотчетную систему, в которой информация может быть проверена;	• Может быть использовано не по назначению в личных целях, таких как использование криптовалюты для отмывания денег, незаконных операций (например, на черном рынке) и уклонения от уплаты налогов;	• Многим приложениям не хватает надлежащей правовой и нормативной базы для работы, в том числе структуры, которая занимается сложными юрисдикционными вопросами, а также вопросами рисков и ответственности.
• Обеспечивает полную публичную запись изменений, поскольку транзакции и документы, хранящиеся в блокчейне, не могут быть изменены или удалены и защищены от манипуляций и незаконных изменений; • Возможность отслеживать точное движение денег	• Данные, находящиеся в блокчейне, могут содержать конфиденциальную информацию, связанную с личными данными, которая может быть подвержена кибератакам, а также может вызывать опасения по поводу конфиденциальности данных и неправильного использования данных	• Применимость и возможность передачи инструмента на данный момент ограничены, особенно при отсутствии цифровой инфраструктуры и процессов для питания блокчейна. Правительства должны сделать достаточные необходимые инвестиции, чтобы изменить существующие системы и воспользоваться преимуществами блокчейна

Продолжение таблицы 2

Анализ больших данных (Big data)		
• Способен обрабатывать большие объемы и разнообразие данных для выявления моделей подозрительных операций в широком спектре областей и секторов;	• Персональные данные могут быть извлечены и использованы в личных целях;	• Данные хорошего качества и аналитические возможности лежат в основе преимуществ анализа больших данных. Международное сообщество может сыграть важную роль в продвижении открытых данных, в то время как правительства должны инвестировать в сбор качественных данных и обеспечивать, чтобы ответственные национальные учреждения собирали надежные и точные данные;
• Обнаружение в режиме реального времени может помочь агентствам выявлять, пресекать и устранять мошеннические и коррупционные действия;	• Уязвимости в виде конфиденциальности данных, неправильного использования информации, угроз кибербезопасности и мошенничества могут поставить под угрозу общественное доверие;	• Аналитические способности и навыки необходимы для использования преимуществ больших данных и аналитических инструментов. Правительствам и ключевым заинтересованным сторонам следует инвестировать в укрепление внутреннего потенциала и аналитических навыков для внедрения новых технологий;

Продолжение Таблицы 2

• Полезно при оценке коррупционных рисков, что будет фундаментом для принятия мер по их снижению; • Способен содействовать принятию решений, связанных с мониторингом, аудитом и расследованиями, касающимися отдельных операций и организаций; • Способность трансформировать то, как государственные учреждения предоставляют государственные услуги, оценивать эффективность и укреплять надзор и подотчетность	• Политические процессы, регулирующие большие данные и анализ данных, также могут быть подвержены злоупотреблениям. К ним относятся использование собранных данных, политические решения, принимаемые на основе анализа данных, и нормативно-правовая база, направляющая усилия по сбору данных и обмену информацией	• Законы и нормативные акты играют важную роль в регулировании и поощрении прозрачности, подотчетности и открытости в использовании данных, включая их сбор, хранение, обмен, защиту и безопасность; • Ответственное использование данных, основанное на этике, добросовестности и защите прав человека, будет иметь решающее значение для укрепления и поддержания доверия к данным, новым технологиям, системам и учреждениям, управляющим ими

Примечание – Составлено автором на основании источника [17]

ЗАКЛЮЧЕНИЕ

Инновации всегда сопряжены с двумя обещаниями: одно из них открывает огромные возможности для существующих практик, например, делая их более эффективными, инклюзивными или безопасными, а другое связано с потенциальными рисками и проблемами, которые может принести это новое предложение.

Практически во всех областях и секторах технологии способны повышать эффективность и способствовать человеческому прогрессу и устойчивому развитию.

В этом исследовании изложены способы, с помощью которых новые технологии могут быть использованы в качестве эффективных инструментов содействия устойчивому развитию с точки зрения добросовестности, доверия и борьбы с коррупцией. Однако эти преимущества могут быть реализованы только в том случае, если мы предотвратим неправильное использование этих технологий, снизим риски и проблемы, связанные с их использованием, и ликвидируем пробелы, ограничивающие их эффективность.

Как показано в этом исследовании, технология может изменить правила игры в укреплении прозрачности, подотчетности и добросовестности. Однако сложный характер многих новых технологий может создавать риски и уязвимости, включая злоупотребление или неправильное использование технологий в личных целях, отсутствие надлежащих гарантий прав человека и защиты данных, а также растущую цифровую пропасть.

Таким образом, важно признать и устранить существующие риски, ограничения и проблемы, чтобы эффективно использовать преимущества новых технологий для обеспечения добросовестности и борьбы с цифровой коррупцией, а также ускорить усилия по устойчивому развитию.

В этой связи цифровая инфраструктура и эффективное цифровое управление, которые способствуют подотчетности, этике и добросовестности, необходимы для создания устойчивого развития.

Список использованных источников

1 Послание Президента Республики Казахстан Касым-Жомарта Токаева народу Казахстана «Единство народа и системные реформы – прочная основа процветания страны» от 1 сентября 2021 года // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K2100002021. Дата обращения: 15.03.2022 г.

2 Указ Президента Республики Казахстан от 2 февраля 2022 года № 802 «Об утверждении Концепции антикоррупционной политики Республики Казахстан на 2022-2026 годы и внесении изменений в некоторые указы Президента Республики Казахстан» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/U2200000802. Дата обращения: 16.03.2022 г.

3 Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности (Киберщит Казахстана)» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1700000407. Дата обращения: 19.03.2022 г.

4 Definition of Digital corruption. // Информационная платформа по борьбе с коррупцией в образовании. – URL: https://etico.iiep.unesco.org/en/digital-corruption. Дата обращения: 24.03.2022 г.

5 Nurkey A.: Models and methods of digital mechanisms in anti- corruption, their advantages and disadvantages, and applications, 2022 IOP Conf. Ser.: Mater. Sci. Eng. 1216 012015.

6 Santiso C., Hacking corruption in the digital era: How tech is shaping the future of integrity in times of crisis. Agenda for business integrity, May 2020.

7 Овчинников А.И., Противодействие коррупции в условиях цифровизации: возможности, перспективы, риски // Журнал российского права. 2019. – № 11. – С. 158-170.

8 Кравченко А.Г., Овчинников А.И., Мамычев А.Ю. и Воронцов С.А., Использование цифровых технологий в сфере противодействия коррупции // Административное и муниципальное право. – 2020, №6. С.52-63.

9 Постановление Правительства Республики Казахстан «Об утверждении Государственной программы «Цифровой Казахстан» от 12 декабря 2017 года №827 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1700000827. Дата обращения: 25.03.2022 г.

10 Многоликая коррупция: Выявление уязвимых мест на уровне секторов экономики и государственного управления / под ред. Кампоса Э. и Прадхана С.; пер. с англ.-М.: Альпина Паблишер, 2018-551 с.

11 Закон Республики Казахстан от 4 мая 2008 года №31-IV «О ратификации Конвенции Организации Объединенных Наций против коррупции» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z080000031_. Дата обращения: 26.03.2022 г.

12 Агентство Республики Казахстан по финансовому мониторингу. Информация о международном сотрудничестве по финансовому мониторингу // Официальный сайт. – URL: https://www.gov.kz/memleket/entities/afm/activities/813?lang=ru. Дата обращения 22.04.2022 г.

13. Информация о государственном изъятии цифровых активов преступников в Российской Федерации // Информационное агентство «Газета.РУ». – URL: https://www.gazeta.ru/economics/2021/07/07/13710104.shtml. Дата обращения: 28.04.2022 г.

14 Агентство Республики Казахстан по противодействию коррупции, «Национальный доклад о противодействии коррупции в Республике Казахстан» от 24 марта 2022 года.

15 Отчет Transparency International Kazakhstan. Мониторинг состояния коррупции в Казахстане. Под редакцией Шиян О.В., Казахстан, Алматы, 2019.520 с.

16. Информация о повышении налогов на майнинг криптовалют в Казахстане // Информационно-новостной портал «Бизнес Ньюс». – URL: https://www.vedomosti.ru/business/news/2022/02/08/908315-tokaev-poruchil-povisit-nalogi-na-maining, Дата обращения 20.04.2022 г.

17 United Nations Development Programme «New Technologies for Sustainable Development: perspectives on integrity, trust and anti-corruption», One Unlted Natlons Plaza, New York, NY 10017, USA.

18 The U4 Anti-Corruption Resource Centre. Information about the Blockchain as a tool to fight corruption. Case examples and an introduction to technology // Информационно-аналитический портал. – URL: https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption/shortversion. Дата обращения: 10.05.2022 г.

19 Ху Ж., Обеспечение основных прав в борьбе с коррупцией с применением больших данных в КНР: основные законы, риски и пути // Актуальные проблемы экономики и права. 2020. Т. 14, №4. С.814-826.

20 Глисон П. и Готтселиг Г. Органы финансовой разведки. Обзор / Международный Валютный Фонд. – Вашингтон – 2004 г. – 161 с.

ПРИЛОЖЕНИЕ 1

Аналитическая записка

Автор проекта: магистрант Нургалиев Р.А.
Научный руководитель: Сомжурек Б.Ж.,
кандидат исторических наук,
ассоциированный профессор

Идея проекта	**Воздействие цифровой коррупции на мировое сообщество: проблемы и методы борьбы**
Проблемная ситуация (кейс)	Как мы знаем, цифровизация существенно повышает открытость, публичность и прозрачность государственного управления, помогает выявить коррупциогенные связи, различные схемы, но также она способна привести к новым видам коррупции. В настоящее время в Казахстане официально не зафиксированы факты коррупции с использованием цифровых технологий. Однако теоретически такие факты вполне возможны. В данной работе проведено исследование существующих рисков и угрозах так называемой цифровой коррупции. Подготовлены рекомендации о возможных методах борьбы с новыми видами цифровой коррупции
Имеющиеся решения данной проблемы	В нынешнем году принята Концепция антикоррупционной политики Республики Казахстан на 2022-2026 годы, одной из задач которой является применение новых технологий по минимизации коррупционных рисков. В рамках реализации Административного процедурно-процессуального кодекса и концепции «слышащего государства» введена в эксплуатацию информационная система «е-Обращение», которая направлена на обеспечение прозрачности и оптимизацию процессов рассмотрения обращений, повышение сервисного подхода, а также расширение возможностей для аналитики

	К данной платформе подключены все центральные государственные органы и их территориальные подразделения, а также местные исполнительные органы. Зарегистрировано более 186 тысяч пользователей и с момента запуска системы обработано более 667 тысяч обращений. Кроме этого, для обеспечения прозрачности деятельности Агентства, недопущения нарушений прав граждан в служебных помещениях оперативно-следственных подразделений центрального аппарата и территориальных департаментов установлено 466 камер видеонаблюдения с централизацией видеоконтроля. Проект Qujat, являющийся частью централизованной системы конфиденциального делопроизводства, содержит более 55 тысяч учетных сведений по линии оперативно-розыскной деятельности. Он используется для формирования отчетности по делам оперативных проверок по линии Генеральной прокуратуры Преимущества Автоматизация позволила сократить сроки расследования уголовных дел, оптимизировать затраты на оформление материалов, обеспечить онлайн-доступ надзорному органу, усилить ведомственный контроль, а также минимизировать коррупционные риски при назначении экспертиз по уголовным делам. Недостатки Отсутствие концептуальных подходов по развитию цифровых технологий для противодействия новым видам коррупции, а также нет правовой базы в части определения цифровой коррупции
Предлагаемое решение данной проблемы	Компетентным органам следует активно применять ресурсы «больших данных» (Big data) для осуществления антикоррупционного контроля за деятельностью должностных лиц

	Указанный инструмент позволяет из фрагментарных данных получать общую картину системной коррупционной деятельности. При этом появляется возможность автоматизированного учета статистических данных большого количества параметров коррупционных отношений: о конфликте интересов, о возникающих динамических коррупционных рисках, о статистике коррупционных правонарушений в привязке к конкретному объему полномочий государственного служащего Возможности В целом развитие системы цифровых технологий противодействия коррупции позволит разрабатывать новые криминалистические методы, позволяющие как интерпретировать Big data, выделяя из массивов информации признаки коррупционных отношений, так и определять конкретные параметры, характер данных для сбора и последующей обработки. Риски Следует иметь в виду, что цифровизация порождает новые коррупциогенные схемы: от торговли Big data до махинаций с подсчетом голосов или «случайных» программных ошибок и сбоев в смарт-контрактах. Современные преступники разрабатывают специальные технологии, которые используются для «обхода» закона. Следует учитывать, что лица, контролирующие цифровые технологии, попадают в ситуацию, способствующую коррупции, так как обладают уникальными знаниями, компетенциями и навыками, позволяющими обойти программные коды и избежать ответственности
Ожидаемый результат	Применение новых методов для противодействия цифровой коррупции позволит предотвратить системную коррупцию на ранних стадиях и позволит

	исключить их повторение в дальнейшем. Вместе с тем, потребуются скоординированные усилия, объединяющие все заинтересованные стороны, включая правительство, частный сектор, гражданское общество, технологов и научные круги, для выработки осуществимых политических рекомендаций и руководящих принципов, регулирующих использование цифровых технологий. Цифровая инфраструктура и эффективное цифровое управление усилят подотчетность, этику и добросовестность
Литература	1) Послание Президента Республики Казахстан Касым-Жомарта Токаева народу Казахстана «Единство народа и системные реформы – прочная основа процветания страны» от 1 сентября 2021 года // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/K2100002021. Дата обращения: 15.03.2022 г; 2) Указ Президента Республики Казахстан от 2 февраля 2022 года №`802 «Об утверждении Концепции антикоррупционной политики Республики Казахстан на 2022-2026 годы и внесении изменений в некоторые указы Президента Республики Казахстан» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/U2200000802. Дата обращения: 16.03.2022 г.; 3) Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности (Киберщит Казахстана)» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/P1700000407. Дата обращения: 19.03.2022 г.