ИСПОЛЬЗОВАНИЕ КОДА ИДЕНТИФИКАТОРА ЮРИДИЧЕСКИХ ЛИЦ (LEI) НА БЛОКЧЕЙН ДЛЯ СНИЖЕНИЯ РИСКА ОТМЫВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ В ФИНАНСОВЫХ УЧРЕЖДЕНИЯХ

Махмуд Махмудов, *магистрант*
Эстонский университет прикладных наук по предпринимательству, Стратегическое управление предприятием
(Эстония, г. Таллинн)

DOI:10.24412/2500-1000-2022-2-1-167-176

Аннотация. *Обширное применение технологии блокчейн в настоящее время может сыграть ключевую роль в использовании децентрализованной сети в качестве стандартной платформы для размещения базы данных единого и защищенного реестра, с помощью которого финансовые учреждения могут проводить соответствующие меры должной осмотрительности при проверке клиентов и бизнес-транзакций, путем проверки Кодов идентификации юридических лиц (англ. Legal Entity Identifier – LEI), управляемых Глобальным фондом идентификаторов юридических лиц. При правильной реализации это решение можно применять в сетях блокчейн, предлагая дополнительные преимущества контроля качества и подробной бизнес-аналитики. Таким образом, технологии блокчейн теперь могут достичь глобальной стандартизации и признания финансовыми учреждениями по всему миру, предоставляя им преимущество взаимодействия с юридическими лицами, доказавшими свою репутацию, и, следовательно, снижая риск отмывания денежных средств в финансовых учреждениях.*

Ключевые слова: *LEI, блокчейн, противодействие отмыванию денежных средств и финансированию терроризма, оценка риска, управление риском.*

Легализация денежных средств, полученных преступным путем и финансирование терроризма могут нанести ущерб стабильности финансовой системы государства, негативно повлиять на надежность банков и других финансовых учреждений, таких как брокерские и страховые компании. Признаки отмывания денежных средств и неконтролируемый риск-аппетит явились причинами закрытия многих банков по всему миру, включая *European Union Bank, Riggs Bank, Danske Bank AS* и т.д. Эти случаи указывают на то, что риск отмывания денежных средств был реализован в упомянутых финансовых учреждениях, и общий риск вовлечения финансовых учреждений в такие операции высок.

По мере того, как легализация денежных средств, полученных преступным путем, и финансирование терроризма угрожают финансовым и нефинансовым учреждениям, и обществу в целом, возрастает сложность и необходимость разработки технологий для предотвращения и выявления финансовых преступлений. Ключевыми особенностями и основными инструментами решения этой проблемы являются, соответственно, знания (осведомленность) сотрудников финансовых организаций и информационные технологии. Автор считает, что механизмы внутреннего контроля в финансовых учреждениях должны постоянно развиваться для возможности своевременного выявления рисков, связанных с легализацией доходов, полученных преступным путем, и обеспечения экономической безопасности конкретного финансового учреждения. В данной статье рассматриваются риски легализации денежных средств, возникающие при установлении взаимоотношений между финансовыми учреждениями и потенциальными клиентами, а также при мониторинге текущего портфеля клиентов. Важную роль в выявлении такого рода рисков, помимо специалиста (отдела) внутреннего контроля (комплаенс-контроля), играет технологическая база, которой специалисты

пользуются для идентификации клиентов. Исходя из этого, автор предлагает определить роль и значение использования глобального реестра юридических лиц (далее – Глобальный индекс LEI), построенного на децентрализованной платформе и содержащего данные обо всех юридических лицах, которым были выданы Коды идентификации юридических лиц (далее – Коды LEI или LEI) (англ. *Legal Entity Identifier* – LEI). При наличии доступа к такому реестру финансовые учреждения смогут проводить соответствующую комплексную проверку в реальном времени, снижая риск отмывания денежных средств в финансовых учреждениях, путем сравнения и верификации актуальной информации, содержащейся в реестре.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать правовые акты и рекомендации в данной области;

- выявить виды рисков и факторы риска финансовых учреждений в сфере противодействия легализации доходов, полученных преступным путем и финансирования терроризма (далее – ПОД/ФТ) при проведении комплексных мероприятий;

- определить роль Кодов LEI в снижении риска отмывания денежных средств и финансирования терроризма (далее – ОД/ФТ), и важность имплементации их реестра на децентрализованной платформе.

Теоретической и методологической основой исследования послужили положения и выводы по решению проблем управления рисками в сфере ПОД/ФТ, содержащиеся в Руководстве по подготовке к сертификационному экзамену Ассоциации сертифицированных специалистов по предотвращению отмывания денежных средств (ACAMS). Характер поставленных задач и системный подход к их решению определили использование в работе следующих методов исследования: анализ, синтез, обобщение и другие общенаучные методы. Правовую основу проведения оценки рисков ОД/ФТ составляют:

1. Международные стандарты по противодействию отмыванию денежных средств, финансированию терроризма и финансированию распространения оружия массового уничтожения Группы разработки финансовых мер борьбы с отмыванием денег ФАТФ (далее – Рекомендации ФАТФ) (ред. от октября 2021).

2. Федеральный закон от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ред. от 21.12.2021) (далее – Федеральный закон N 115-ФЗ).

3. Приказ Росфинмониторинга от 08.05.2009 N 103 «Об утверждении Рекомендаций по разработке критериев выявления и определению признаков необычных сделок» (далее – Приказ Росфинмониторинга N 103).

4. Приказ Росфинмониторинга от 22.11.2018 N 366 «Об утверждении требований к идентификации клиентов, представителей клиента, выгодоприобретателей или бенефициарных владельцев, в том числе с учетом степени (уровня) риска совершения операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма» (далее – Приказ Росфинмониторинга N 366).

5. Закон Эстонии о предотвращении отмывания денежных средств и финансирования терроризма RT I, 17.11.2017, 2 (ред. от 01.01.2022) (далее – Закон Эстонии о ПОД/ФТ).

6. Рекомендации/инструкции Финансовой инспекции Эстонии, изложенные решением № 1.1-7/172 в документе «Организационное решение для кредитно-финансовых организаций и меры профилактики и препятствия отмыванию денежных средств и финансированию терроризма» от 26.11.2018 (далее – Рекомендации Финансовой инспекции Эстонии).

Юридические аспекты и рекомендации

Мы живем в эпоху ужесточения международного контроля за отмыванием денежных средств и финансированием терроризма. Группа разработки финансовых мер борьбы с отмыванием денег ФАТФ (англ. *Financial Action Task Force on Money*

Laundering – FATF) – межправительственная организация, созданная в 1989 году, которая провела ряд исследований по типологиям отмывания денежных средств и продемонстрировала, что сама процедура отмывания денежный средств может быть осуществлено практически с помощью любого средства, финансового учреждения или бизнеса [1]. Ключевым элементом усилий ФАТФ является издание подробного списка международных стандартов по противодействию отмыванию денежных средств, финансированию терроризма и финансированию распространения оружия массового уничтожения, изложенного в виде 40 рекомендаций ФАТФ, принятых на пленарном заседании ФАТФ в феврале 2012 г. Росфинмониторинг также руководствуется стандартами, изложенными в Рекомендациях ФАТФ, и называет их «основополагающим документом, устанавливающим комплексную и последовательную структуру мер, которые странам следует применять для противодействия отмыванию денег и финансирования терроризма, а также финансированию распространения оружия массового уничтожения» [2]. Следование стандартам ФАТФ обеспечивает, среди прочего, выявление рисков и разработку соответствующей политики, прозрачность юридических лиц и образований в сочетании с международным сотрудничеством. В Рекомендациях Росфинмониторинга (код критерия 1304) также предписано относить к необычным сделки клиентов, не выполняющих Рекомендации ФАТФ, либо использующих счета в банках, зарегистрированных в государстве, не выполняющим Рекомендации ФАТФ [3].

На саммите в Лос-Кабосе в июне 2012 г. [4] лидеры Большой двадцатки G20 одобрили отчет Совета по финансовой стабильности (англ. *Financial Stability Board* – FSB), именуемый как «Глобальный идентификатор юридического лица для финансовых рынков» [5] и призвали к глобальному принятию LEI для поддержки органов власти и участников рынка в выявлении и управлении финансовыми рисками [6]. Более подробное описание LEI приведено далее по тексту.

Деятельность финансовых учреждений является одной из основных в мировой экономике и наиболее чувствительна к внешним изменениям. Создание и поддержание эффективной программы ПОД/ФТ является обязательной частью устава любого финансового учреждения. Как указано в (1) §14 Закона Эстонии о ПОД/ФТ: «Обязанное лицо устанавливает правила и процедуры, которые позволяют эффективно уменьшать и управлять, среди прочего, рисками, связанными с отмыванием денежных средств и финансированием терроризма» [7]. Более того, в соответствии с 10-й рекомендацией ФАТФ меры должной осмотрительности и надлежащей проверки клиента должны быть приняты при «идентификации клиента и проверке личности этого клиента с использованием надежных, независимых исходных документов, данных или информации» [8]. При этом, необходима идентификация бенефициарного владельца и принятие разумных мер для проверки его личности, поскольку финансовое учреждение должно знать, кто является бенефициарным владельцем каждого конкретного клиента – юридического лица.

Риск-ориентированный подход является одной из основных рекомендаций ФАТФ. Подход основан на выявлении риска, как указано выше, и оценке риска отмывания денежных средств в финансовом учреждении, что помогает определить уровень риска клиента, а также способствует выявлению клиентов с высоким риском отмывания денежных средств. Риск-ориентированный подход позволяет предотвратить использование финансового учреждения в целях отмывания денежных средств, о чем также свидетельствует необходимость его применения в соответствии с п. 4 статьи 9.1. Федерального закона N 115-ФЗ [9].

Факторы риска финансовых учреждений

В соответствии с п. 25 Приказа Росфинмониторинга N 366 финансовые учреждения в составе правил внутреннего контроля обязаны разработать программу оценки степени (уровня) риска соверше-

ния клиентом операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма [10]. В программу оценки риска необходимо включить методику оценки и присвоения клиенту степени (уровня) риска до приема на обслуживание клиента и в ходе его обслуживания, в которой рекомендуется предусмотреть классификацию рисков по категориям. О категоризации рисков также говорится в §13 Закона Эстонии о ПОД/ФТ [7], при этом в обоих случаях предусматривается следующая минимальная категоризация:

- риски, связанные со странами и отдельными географическими территориями (географические риски);
- риски, связанные клиентами (клиентские риски);
- риски, связанные с продуктами, услугами, операциями (сделками) или
- каналами поставок, совершаемыми клиентом (операционные риски).

Управление рисками предусматривает принятие мер по снижению рисков ОД/ФТ и смягчению их возможных последствий. Согласно информации Базельского комитета по банковскому надзору [11] и в соответствии с Рекомендациями Финансовой инспекции Эстонии [12], в контексте ПОД/ФТ бизнес-подразделения (например, фронт-офис финансовых учреждений, отдел работы с клиентами) являются первой линией защиты и ответственны за выявление, оценку и контроль рисков. Они должны знать и выполнять политику и процедуры того или иного финансового учреждения, и им должны быть выделены достаточные ресурсы для эффективного выполнения этой задачи. Вторая линия защиты включает главного офицера, отвечающего за ПОД/ФТ, функцию комплаенса, а также человеческие ресурсы или технологии. Третья линия защиты обеспечивается функцией внутреннего аудита. Таким образом, финансовые учреждения должны внедрить свой инструмент оценки риска в соответствии с соответствующим риск-аппетитом и использовать его при идентификации клиентов и проведении мер должной осмотрительности. Пример инструмента оценки рисков финансового учреждения представлен в таблице 1.

Таблица 1. Реальный пример инструмента оценки риска, используемого финансовыми учреждениями

Фактор риска	**Тип**	**Уровень риска**	**Значимость риска**	**Удельный вес**
Тип клиента	Общество с ограниченной ответственностью	Высокий риск	8	0.1
Индустрия клиента	Финансовые услуги / регулируемые	Низкий риск	3	0.15
Взаимоотношения с клиентом	Новый клиент, недавно зарегистрированный <1 года, не имевший до этого счетов в банке	Высокий риск	10	0.1
Юрисдикция клиента	Российская Федерация	Средний риск	4.6	0.2
Юрисдикция бенефициара	Российская Федерация	Средний риск	4.6	0.25
Ежемесячный оборот	5 000 000 рублей <	Высокий риск	7	0.2
Итого				1
	Всего:	Средний риск	**5.72**	Рейтинг риска

Источник: Составлено автором на основании данных, предоставленных финансовым учреждением

Согласно исследованию GLEIF, проведенному в 2018 году, чтобы точно идентифицировать клиентские организации с самыми новыми данными, финансовые учреждения, как правило, используют различные идентификаторы для перекрестных проверок. В среднем они используют 4 разных идентификатора внутри компании, но около трети из них используют 5 или более идентификаторов [13]. GLEIF также предупреждает в своем исследовании о том, что финансовые учреждения используют несколько идентификаторов для перекрестной проверки, но это создает трудности, поскольку один и тот же идентификатор может быть связан с несколькими объектами (49%), а разные идентификаторы могут относиться к одному и тому же объекту (47%). Только две трети финансовых учреждений считают, что они владеют точной информацией о клиентах. В отношении менее трети клиентов имеется уверенность, что они сообщат о существенных изменениях в своем юридическом лице, поэтому бремя проведения регулярных проверок остается «лежать» на учреждении. Эти факты свидетельствуют о реальных проблемах, с которыми сталкиваются финансовые учреждения при взаимодействии со своими клиентами, и на это необходимо обратить особое внимание, поскольку они являются факторами, препятствующими нормальной работе ответственных сотрудников при использовании риск-ориентированного подхода для снижения риска использование финансового учреждения в целях отмывания денежных средств.

Определение LEI

Система LEI была разработана Большой двадцаткой G20 в 2012 году в ответ на неспособность финансовых учреждений осуществлять идентификацию юридических лиц для отслеживания их финансовых операций в различных национальных юрисдикциях. В настоящее время Регулятивно-надзорный комитет LEI ROC представляет собой коалицию финансовых регуляторов и центральных банков по всему миру, которая поощряет расширение LEI. Код LEI представляет собой 20-значный буквенно-цифровой код, основанный на стандарте ISO 17442, который был разработан Международной организацией по стандартизации (ISO). LEI подключается к ключевой справочной информации, позволяющей четко и однозначно идентифицировать юридических лиц, участвующих в финансовых операциях [14].

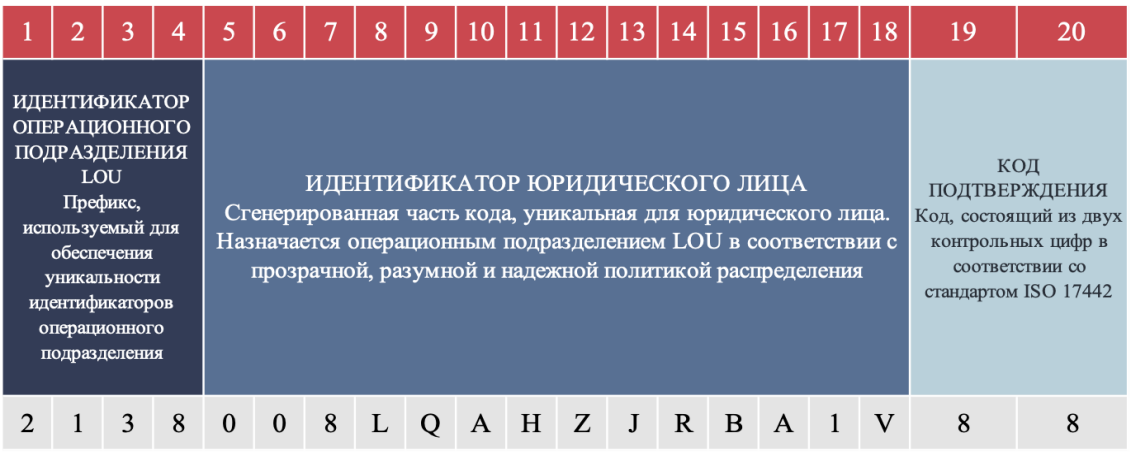

Рис. 1. Значение цифр в Коде LEI

Код LEI определяет минимальные справочные данные, которые должны быть предоставлены для каждого LEI, такие как официальное название юридического лица, указанное в официальных реестрах, зарегистрированный адрес этого юридического лица, страна образования, коды для представления названий стран и их под-

разделений [15]. Информация о дате первого присвоения LEI, дате последнего обновления информации LEI и дате истечения срока действия (если применимо) также хранится в глобальной базе данных. Более того, каждый Код LEI содержит информацию о структуре собственности юридического лица (бенефициары, дочерние и материнские организации) и, следовательно, для каждого конкретного юридического лица, отвечает на вопросы «кто есть кто» и «кто кем владеет» [14]. Каждый Код LEI уникален, выдается разово для конкретного юридического лица и не может быть использован повторно для другого юридического лица. Код LEI не заменяет официальный регистрационный номер юридического лица, находящийся в реестре юридических лиц, который до сих пор используется для идентификации организаций.

Коды LEI связывают юридические лица с ключевой информацией о них. Это позволяет четко и однозначно идентифицировать юридических лиц, например, как участников глобальных финансовых рынков. Данная возможность уже используется для идентификации сторон сделок с производными инструментами EMIR, а благодаря применению регламента EU/2017/105, никакие другие альтернативные коды не могут использоваться при предоставлении уведомления о сделках, совершенных с производными инструментами, начиная с 01.11.2017. Кроме того, с 03.01.2018 Коды LEI уже используются при представлении отчетности организаций. В соответствии с регламентом MiFIR и MiFID II [16], возможности идентификации при помощи LEI также могут быть использованы для расследования злоупотреблений на рынке [17].

Коды LEI глобальны, не имеют границ для актуальной и надежной идентификации юридических лиц и являются единым способом отслеживания юридических лиц по всему миру. С этой точки зрения общедоступный пул данных LEI можно рассматривать как глобальный каталог, реестр, который может значительно повысить прозрачность на глобальном рынке. Такая информация важна для комплаенс-подразделений финансовых учреждений и специалистов по ПОД/ФТ при проведении комплексных проверок в рамках процедур «Знай своего клиента», особенно в тех случаях, когда в качестве клиентов выступают иностранные юридические лица, имеющие сложную и непрозрачную структуру собственности.

Управление системой LEI координируется и поддерживается фондом GLEIF, а регистрация и хранение данных выполняются локальными операционными подразделениями (англ. *Local Operational Units* – LOU), которые, в свою очередь, используют разветвленную структуру регистрационных агентов (англ. *Registration Agents* – RA), получающих заявки от юридических лиц на регистрацию Кодов LEI. Регистрационные агенты проводят комплексную проверку данных заявителя, обработку юридических документов и отправляют заявления в соответствующее операционное подразделение для последующей выдачи Кода LEI заявителю.

Предприятия, предоставляющие финансовые услуги, могут сэкономить время, повысить прозрачность и работать более упорядоченным образом, используя возможности Кода LEI для каждой клиентской организации [18]. В исследовании GLEIF от 2018 г. изучаются проблемы, с которыми сталкивается банковский сектор, когда дело доходит до установления отношений с новыми клиентами. Финансовые учреждения работают в нескольких юрисдикциях и поэтому нуждаются в глобальном стандарте, таком как система LEI, которая предлагает учреждениям единый подход к идентификации юридических лиц, который потенциально может упростить бизнес-процессы [13].

Значение блокчейн для реестра LEI

Как было отмечено выше, фонд GLEIF координирует управление глобальной системой LEI и обслуживает реестр, называемый Глобальным индексом LEI. Однако, в контексте надежности и безопасности, централизованную службу или единый орган управления, обслуживающий реестр,

можно рассматривать как уязвимость и единую точку отказа для всей системы.

В настоящее время существует несколько источников, в которых хранятся данные LEI. В тот момент, когда юридическое лицо регистрируется в системе, либо вносит изменения, часто существует период ожидания, который может занять до нескольких часов, прежде чем обновленная информация отобразится в различных онлайн-инструментах поиска. Учитывая, что по своей природе идентификатор LEI является цифровым продуктом, а все данные хранятся в сети Интернет в различных источниках (на разных серверах), необходимо принять во внимание, что существуют определенные временные лаги, когда информация в таких источниках может не совпадать и быть неактуальной.

Проблемы с качеством данных, связанные с неактуальными кодами LEI, были указаны и обобщены в отчете о ходе работы LEI ROC от 2018 г. [19] с указанием рисков присвоения второго идентификатора LEI одному и тому же юридическому лицу (если, например, изменение имени юридического лица не было своевременно зарегистрировано), путаницы и непрозрачности в отношении сохранившихся идентификаторов LEI в случае слияния юридических лиц, трудности при сверке данных LEI с другими базами данных (например, по разным адресам), отсутствии контроля и оспаривании данных LEI третьими сторонами (поскольку операционные подразделения обычно не могут обновлять запись без согласия юридического лица). Еще одна проблема заключается в том, что в случае, когда идентификатор LEI просрочен, в нем не будут отображены обновления, связанные с юридическим лицом, которому он был присвоен [20]. Указанные риски и потенциальные уязвимости имеют решающее значение для таких реестров, как Глобальный индекс LEI, где информация о юридических лицах должна быть непрерывно доступной, актуальной и подтвержденной, поскольку представители финансовых учреждений должны получать надежную информацию при проведении проверок своих клиентов.

Автор считает, что верным подходом к решению этой проблемы может быть использование технологии распределенного реестра (англ. *Distributed Ledger Technology* – DLT), одним из видов которой является технология блокчейн. Это относительно новая технология для безопасного, децентрализованного и транзакционного обмена данными в большой сети ненадежных участников, без привязки к центральному доверенному органу для записи и подтверждения транзакций. Технология блокчейн создает структуру данных с присущими ей качествами безопасности, основанной на принципах криптографии, децентрализации и консенсуса, которые обеспечивают доверие к транзакциям [21].

Блокчейн имеет три уровня безопасности:

- блокчейн – это распределенная сеть, позволяющая прозрачно хранить данные в неизменном виде;
- блокчейн хранит информацию в цепочке блоков, где каждый последующий блок содержит информацию о предыдущем блоке (значение хеш-функции);
- информация в блокчейне защищена с помощью математических алгоритмов.

Основное отличие реестра, построенного на блокчейне, от реестра, реализованного с помощью обычной базы данных – централизация. В то время как все записи, хранящиеся в обычной базе данных, централизованы, каждый участник блокчейна имеет защищенную копию всех записей и всех изменений сети. Таким образом, каждый пользователь может просмотреть происхождение данных, и, в случае несоответствия, технология блокчейн немедленно выявит и исправит любую недостоверную информацию, поскольку каждый участник сети хранит копию записей. Широкое внедрение технологии блокчейн для обеспечения защиты централизованных баз данных от компрометации является весомым аргументом, чтобы принять решение о целесообразности использования блокчейн для реестра Глобального индекса LEI. Представители GLEIF также заявляют, что интеграция LEI в решения, основанные на цифровых сертификатах и тех-

нологии блокчейн, позволит любому легко подключить все записи, связанные с организацией, и определить «кто кем владеет» [18]. Вместо того, чтобы централизовать данные в одной базе (как это реализовано сейчас), они будут автоматически распределяться по взаимосвязанным узлам, принадлежащим участвующим операционным подразделениям, что обеспечит надежную защиту от возможных атак. Технология блокчейн будет обновлять Глобальный индекс LEI в режиме реального времени подтвержденными данными и отражать релевантную информацию по мере ее изменения с течением времени, сохраняя при этом всю историю произведенных изменений. Любые изменения, сделанные в одной системе, будут регистрироваться и обновляться в других системах в режиме реального времени, а благодаря распределенной сети и защищенным протоколам данных, нет ни единой точки отказа, ни единого органа, контролирующего систему. Обладая указанными преимуществами, блокчейн является идеальной технологией для построения на ней Глобального индекса LEI и в настоящее время GLEIF внедряет свои цифровые проверяемые учетные данные (англ. *Digital Verifiable Credential* – DVC) для проверки этой концепции как в общедоступных (*Ethereum*), так и в частных (*Hyperledger Indy*) блокчейн сетях [22].

Заключение

Проанализировав нормативно-правовые акты и рекомендации в сфере ПОД/ФТ, автор пришел к выводу, что финансовым учреждениям необходимо установить внутренние правила и процедуры, позволяющие эффективно снижать и управлять рисками, связанными с ОД/ФТ. Меры должной осмотрительности должны проводиться при идентификации клиентов и проверке их личности с использованием надежного и независимого источника. Использование риск-ориентированного подхода – одна из главных рекомендаций ФАТФ, основанная на выявлении и оценке риска отмывания денежных средств в финансовом учреждении. Такой подход помогает определить уровень риска клиентов и выявить клиентов с высокой степенью риска отмывания денежных средств. Финансовые учреждения обязаны подготовить оценку рисков, учитывая как минимум риски, связанные с клиентами (клиентские риски), странами, географическими районами или юрисдикциями (географические риски), каналами поставок, совершаемыми клиентом (операционные риски), а также риски, связанные с продуктами, услугами или транзакциями. Кроме того, финансовые учреждения должны внедрить свой инструмент оценки риска в соответствии с приемлемым в учреждении риск-аппетитом и использовать его при идентификации клиентов и проведении мер должной осмотрительности.

Поскольку существует ряд проблем, связанных с актуальностью и точностью данных, с которыми финансовые учреждения сталкиваются при проверке клиентов, автор считает целесообразным использовать систему идентификаторов юридических лиц LEI, разработанную Большой двадцаткой G20 в 2012 г., в целях снижения реализации рисков ОД/ФТ. Поскольку каждый идентификатор LEI содержит информацию о структуре собственности юридического лица (бенефициары, дочерние и материнские организации) и справочные данные, такие как юридический адрес этого юридического лица, страна регистрации и т.д., систему LEI можно использовать для отслеживания юридических лиц по всему миру, а общедоступный пул данных LEI можно рассматривать как глобальный реестр, который может значительно повысить прозрачность данных участников на глобальном рынке. Однако, реестр LEI, внедренный в централизованную базу данных, сталкивается с рядом проблем, среди которых имеют место быть существенные задержки в обновлении информации, уязвимость к атакам, неактуальность данных – все то, что имеет решающее значение для такого реестра, который предполагается использовать при проверке информации о клиентах для снижения рисков ОД/ФТ.

Изучив преимущества размещения баз данных с использованием технологии распределенного реестра, автор пришел к выводу, что решение по внедрению Глобального индекса LEI с использованием технологии распределенного реестра в сетях блокчейн обеспечит высочайший уровень безопасности, позволит обновлять данные в режиме реального времени и сделает доступной всю историю операций для каждого Кода LEI. Первый подход к реализации указанного решения находится в стадии разработки при участии подрядчиков GLEIF, тестирующих концепцию как в общедоступных (*Ethereum*), так и в частных (*Hyperledger Indy*) блокчейн сетях.

Библиографический список

1. Association of Certified Anti-Money Laundering Specialists (ACAMS) / Study Guide CAMS certification exam. 2019. С. 1.

2. Федеральная служба по финансовому мониторингу / Документы ФАТФ. URL: https://www.fedsfm.ru/documents/international-fatf (дата обращения 09.02.2022).

3. Министерство юстиции Российской Федерации / Приказ Росфинмониторинга от 08.05.2009 № 103 «Об утверждении Рекомендаций по разработке критериев выявления и определению признаков необычных сделок». Опубликован 16.06.2020. URL: https://www.minjust.gov.ru/ru/documents/7896/ (дата обращения 10.02.2022).

4. G20 Leaders Declaration / G20 Los Cabos Mexico, 2012. С. 7-8. URL: https://www.fsb.org/wp-content/uploads/g20_leaders_declaration_los_cabos_2012.pdf (дата обращения 15.12.2021).

5. Financial Stability Board (FSB) / A Global Legal Entity Identifier for Financial Markets. 2012. URL: https://www.fsb.org/wp-content/uploads/r_120608.pdf (дата обращения 15.12.2021).

6. Financial Stability Board (FSB) / Press Release. 2019. С. 1. URL: https://www.fsb.org/wp-content/uploads/R280519-2.pdf (дата обращения 18.12.2021).

7. Riigi Teataja / Money Laundering and Terrorist Financing Prevention Act. 2022. URL: https://www.riigiteataja.ee/en/eli/ee/517112017003/consolide/current (дата обращения 03.01.2022).

8. FATF (2012-2021), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France. URL: www.fatf-gafi.org/recommendations.html (дата обращения 12.02.2022).

9. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». URL: https://www.consultant.ru/document/cons_doc_LAW_32834/0efef65a2bed6cda06070121d233657f3c7a94d6/ (дата обращения 10.02.2022).

10. Федеральная служба по финансовому мониторингу. Приказ Росфинмониторинга от 22.11.2018 N 366 «Об утверждении требований к идентификации клиентов, представителей клиента, выгодоприобретателей или бенефициарных владельцев, в том числе с учетом степени (уровня) риска совершения операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма». URL: https://www.fedsfm.ru/documents/rfm/4163 (дата обращения 11.02.2022).

11. Basel Committee on Banking Supervision. Sound management of risks related to money laundering and financing of terrorism. 2020. С. 5. URL: https://www.bis.org/bcbs/publ/d505.pdf (дата обращения 04.01.2022).

12. Finantsinspektsiooni juhendid. Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks. 2018. URL: https://www.fi.ee/sites/default/files/2018-FI_AML_Soovituslik_juhend.pdf (дата обращения 28.12.2021).

13. Global Legal Entity Identifier Foundation (GLEIF). Know Your Customer (KYC): The Challenges Faced by the Banking Sector When Onboarding New Client Organizations. Research

Findings. 2018. URL: https://www.gleif.org/content/3-lei-solutions/6-lei-in-kyc-a-new-future-for-legal-entity-identification/gleif-research-findings_challenges-onboarding-client-organizations-in-banking-sector_v1.0-final.pdf (дата обращения 05.01.2022).

14. Global Legal Entity Identifier Foundation (GLEIF) / Introducing the Legal Entity Identifier (LEI). URL: https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei (дата обращения 03.01.2022).

15. Global Legal Entity Identifier Foundation (GLEIF) / Level 1 Data: Who is Who. URL: https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-1-data-who-is-who (дата обращения 03.01.2022).

16. European Securities and Markets Authority (ESMA) / MIFID II. 2018. URL: https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir (дата обращения 04.01.2022).

17. European Securities and Markets Authority (ESMA). Briefing. ESMA70-145-238. 2017. URL: https://www.esma.europa.eu/sites/default/files/library/esma70-145-238_lei_briefing_note.pdf (дата обращения 04.01.2022).

18. Global Legal Entity Identifier Foundation (GLEIF) / LEI in KYC: A New Future for Legal Entity Identification. URL: https://www.gleif.org/en/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification (дата обращения 04.01.2022.).

19. Legal Entity Identifier Regulatory Oversight Committee (LEI ROC). The Global LEI System and regulatory uses of the LEI. 2018. C. 9. URL: https://www.leiroc.org/publications/gls/roc_20180502-1.pdf (дата обращения 08.01.2022).

20. Financial Stability Board (FSB). Thematic Review on Implementation of the Legal Entity Identifier. 2019. URL: https://www.fsb.org/wp-content/uploads/P280519-2.pdf (дата обращения 08.01.2022).

21. IBM / Basic Blockchain Security. URL: https://www.ibm.com/topics/blockchain-security (дата обращения 10.01.2022).

22. McKenna K., Piechocki M. (2020) Grafting Blockchains into Enterprise Businesses – The LEI and Digital Verifiable Credentials [Видео]. URL: https://www.youtube.com/watch?v=59pPG_srJmQ&t=708s (дата обращения 12.01.2022).

USING LEGAL ENTITY INDENTIFIER (LEI) ON BLOCKCHAIN FOR REDUCING MONEY LAUNDERING RISKS IN FINANCIAL INSTITUTIONS

Makhmud Makhmudov, *Graduate Student*
Estonian Entrepreneurship University of Applied Sciences Mainor, Enterprise Strategic Management
(Estonia, Tallinn)

Abstract. *The increasing use of blockchain technology nowadays can play a key role for using of decentralized network as a standard database for the unified and secured registry through which financial institutions can conduct relevant customer due diligence measures and business transactions by verifying organizations' Legal Entity Identifier (LEI) codes, self-sovereign identifiers managed by the Global Legal Entity Identifier Foundation (GLEIF). With proper implementation, this solution can be applied on blockchain networks, offering the additional advantage of quality control and detailed business analysis. Thus, by giving financial institutions the benefit of interacting with legal entities that have proven their reputation and, therefore, by reducing the money laundering risk in financial institutions, the blockchain technologies now could reach global standardization and acceptance by financial institutions worldwide.*

Keywords: *LEI, blockchain, anti-money laundering, risk assessment, risk management.*