Политика по противодействию отмыванию денежных средств и финансированию терроризма (AML/CTF)

ООО «SOLUNEX»

Год 2025

Глава 1. Введение

1.1. Руководство ООО «Solunex» (далее — «Компания») полностью привержено предотвращению финансовых преступлений, отмывания денежных средств и финансирования терроризма (далее — «AML/CTF»).

1.2. Директор(ы) Компании несут ответственность за создание и поддержание эффективной системы оценки и управления рисками AML/CTF, соответствующей характеру и масштабу деятельности Компании, а также за назначение специализированного и обученного персонала для контроля её реализации.

1.3. Для достижения этих целей настоящая Политика разработана с целью установления основных принципов предотвращения отмывания денежных средств и финансирования терроризма.

1.4. Положения настоящего документа основаны на Законе Грузии «О содействии предотвращению отмывания денежных средств и финансирования терроризма» (далее — «Закон»), нормативных актах Службы финансового мониторинга Грузии (далее — «FMS»), нормативных актах и руководящих документах Национального банка Грузии, а также рекомендациях Группы разработки финансовых мер борьбы с отмыванием денег (FATF) и других соответствующих международных организаций, устанавливающих действующие стандарты AML/CTF.

Глава 2. Определения терминов

- Легализация незаконных доходов (отмывание денежных средств) — придание законной формы незаконным и/или необоснованным активам (использование, приобретение, владение, преобразование, передача или иные действия) с целью сокрытия их незаконного происхождения или оказания помощи другому лицу в уклонении от ответственности, а также сокрытие или искажение их истинной природы, источника, местонахождения, размещения, движения, права собственности или иных связанных прав.
- Финансирование терроризма — сбор или предоставление денежных средств или иных активов с заведомым знанием того, что они будут использованы полностью или частично террористом или террористической организацией либо для осуществления террористической деятельности; либо предоставление услуг, убежища, ресурсов или иной материальной поддержки террористу или террористической организации.
- Связанные транзакции — операции, заключённые в разумный период времени или признанные связанными по иным критериям, относящиеся к одному и тому же клиенту.
- Подозрительная транзакция — операция, в отношении которой имеются разумные основания полагать, что она подготовлена, выполнена или осуществлена с

использованием незаконно полученного имущества или доходов от него и/или с целью отмывания денежных средств, либо связана с финансированием терроризма.

- Клиент — лицо, устанавливающее деловые отношения с Компанией или совершающее разовую операцию для использования её услуг.
- Деловые отношения — непрерывные коммерческие или профессиональные отношения между Компанией и клиентом, предполагающие оказание услуг в соответствии с законодательством Грузии.
- Разовая операция — операция (вне рамок деловых отношений), связанная с оказанием услуг Компанией клиенту в соответствии с законодательством Грузии.
- Идентификация — процесс получения идентификационных данных о лице, позволяющих его проверить и отличить от других лиц.
- Верификация — получение информации или документов, позволяющих субъекту отчётности подтвердить точность идентификационных данных лица, а также, в случае бенефициарного владельца, подтвердить его личность.
- Конфиденциальная информация — информация или документы, содержащие профессиональную тайну, коммерческую тайну и/или персональные данные.
- Лицо — физическое лицо, юридическое лицо или незарегистрированное организационное образование.
- Список санкционированных лиц — перечень физических или юридических лиц, в отношении которых введены санкции резолюциями Совета Безопасности ООН, а также США, Великобритании, Европейского союза, России или Беларуси.
- Местонахождение — юрисдикция, страна или территория, в которой лицо зарегистрировано и/или осуществляет деятельность.
- Политически значимое лицо (PEP) — физическое лицо, занимающее высокую государственную или политическую должность (за исключением должностей среднего и низшего уровня), включая:
  a) главу государства, главу правительства, члена правительства (министра), депутата или руководителя государственного учреждения;
  b) члена законодательного органа (парламента);
  c) руководителя политической организации или члена её руководящего органа;
  d) судью Верховного или Конституционного суда либо иного высшего суда;
  e) генерального аудитора, его заместителя или члена аудиторского органа;
  f) члена правления национального (центрального) банка;
  g) посла или руководителя дипломатической миссии;
  h) руководителя вооружённых сил;
  i) руководителя или члена органа управления государственного предприятия;
  j) руководителя, заместителя или члена органа управления международной организации.

- Члены семьи PEP — супруг(а) или лицо, проживающее совместно с PEP, а также родители, дети и супруги детей, проживающие совместно.
- Связанное лицо PEP — физическое лицо, являющееся бенефициарным владельцем юридического лица, траста или иной структуры совместно с PEP, либо имеющее тесные деловые, социальные или политические связи с PEP, либо являющееся бенефициарным владельцем структуры, созданной в интересах PEP.
- Лица со статусом PEP — лица, определённые Компанией как PEP, включая самих PEP, членов их семей и связанных лиц.
- Международная организация — постоянная межправительственная или наднациональная организация.
- Бенефициарный владелец — физическое лицо, которое в конечном итоге владеет или контролирует клиента либо от имени которого проводится операция. Для юридических лиц — лицо, прямо или косвенно владеющее или контролирующее 25% и более долей или голосов либо иным образом осуществляющее контроль.
- Контролирующее лицо юридического лица — физическое лицо, обладающее возможностью оказывать значительное влияние на управление юридическим лицом напрямую или косвенно.
- Юридическое лицо — как резидентные, так и нерезидентные компании, некоммерческие организации и иные организационные образования, включая филиалы и представительства.
- Некоммерческое юридическое лицо — некоммерческая организация частного права (например: НПО, ассоциация, политическая партия, фонд, церковь и др.).
- Траст — доверительная структура, при которой имущество передаётся управляющему для управления в интересах бенефициара или в соответствии с указаниями собственника (включая структуры по Гаагской конвенции 1985 года и аналогичные).
- Юрисдикция высокого риска — юрисдикции, признанные таковыми Президентом Национального банка Грузии.
- Оффшорная зона — юрисдикции, утверждённые как оффшорные Президентом Национального банка Грузии.
- Структура владения/учреждения — цепочка учредителей юридического лица до конечного бенефициара.
- Обоснованное подозрение — совокупность информации или обстоятельств, позволяющая объективному наблюдателю предположить совершение преступления.
- Разумные основания — информация или факты, предоставленные компетентными органами, позволяющие предположить причастность лица к финансированию терроризма или распространению оружия массового уничтожения.

- Подозрение — совокупность фактов или обстоятельств, вызывающих обоснованные сомнения в законности операции.
- Необычная операция — сложная, крупная или нетипичная операция без явной экономической цели.
- Перевод конвертируемого виртуального актива — операция по передаче виртуального актива между адресами распределённого реестра или кошельками через поставщика услуг или финансовое учреждение.
- FMS — Служба финансового мониторинга Грузии.
- RBA — риск-ориентированный подход.
- KYC (Знай своего клиента) — процедуры идентификации и проверки клиентов.
- KYCUB — процедуры идентификации бенефициарного владельца клиента.
- EDD — усиленные меры проверки клиента.
- NBG — Национальный банк Грузии.
- AMLO — сотрудник по AML/комплаенсу Компании.

Примечание: иные термины толкуются в соответствии с законодательством Грузии и нормативными актами.

Глава 3. Оценка и управление рисками отмывания денежных средств и финансирования терроризма

3.1. Компания внедрила процедуры идентификации и оценки рисков AML/CTF и применяет соразмерные меры для управления этими рисками на основе риск-ориентированного подхода.

3.2. Компания установила единый риск-ориентированный подход к оценке клиентов, который включает идентификацию рисков, их анализ, применение соответствующих превентивных мер и разработку эффективной стратегии управления рисками.

3.3. Компания обеспечивает применение риск-ориентированного подхода как к потенциальным клиентам, желающим установить деловые отношения, так и к действующим клиентам, находящимся в рамках постоянных деловых отношений, а также к лицам, осуществляющим разовые операции или сделки.

3.4. Компания устанавливает соответствующие критерии в зависимости от уровня риска, что позволяет эффективно оценивать потенциальные и ожидаемые риски со стороны лиц, заинтересованных в её услугах.

3.5. Компания обеспечивает присвоение соответствующего уровня риска лицам, заинтересованным в её услугах, а также действующим клиентам в соответствии с Политикой оценки рисков клиентов.

3.6. Компания определяет свой организационный уровень допустимого риска AML/CTF, указывая, какие риски отмывания денег/финансирования терроризма она принимает в

соответствии со своими стратегическими целями, а также какие меры контроля или ограничения применяются для управления этими рисками.

3.7. На основе риск-ориентированного подхода трудовые, временные и технологические ресурсы распределяются по приоритетам, обеспечивая усиленный контроль в отношении высоких рисков ML/TF.

3.8. Оценка рисков AML/CTF осуществляется с учётом клиента и бенефициарного владельца, характера их деятельности, юрисдикции их местонахождения и других факторов риска.

3.9. Для клиентов, отраслей бизнеса, юрисдикций, географических зон и каждой группы услуг/продуктов определяются соответствующие уровни риска.

3.10. На основании уровней риска клиенту присваивается категория высокого, среднего или низкого риска.

3.11. Меры управления рисками, применяемые к клиентам, зависят от присвоенного уровня риска. В частности, к клиентам со средним риском применяются стандартные меры, к клиентам с высоким риском — усиленные меры, а к клиентам с низким риском — упрощённые меры.

3.12. Оценка рисков ML/TF, связанных с клиентами, и определение их уровня риска осуществляется до установления деловых отношений, периодически в ходе отношений, а также при возникновении существенных изменений, связанных с клиентом.

3.13. Правила и процедуры оценки риска клиента регулируются настоящей Политикой и Политикой оценки рисков клиентов.

3.14. Внедрение новых технологий, продуктов, услуг или способов их предоставления, а также иных существенных изменений в деловой практике (далее — «новый продукт») допускается только на основании оценки связанных с ними рисков ML/TF.

3.15. Процесс внедрения нового продукта включает оценку связанных рисков, определение необходимых механизмов контроля, процесс управления рисками, стратегию их снижения, оценку остаточного риска и участие всех соответствующих структурных подразделений (как минимум, AMLO, а при необходимости — подразделения информационной безопасности и других).

3.16. До внедрения нового продукта Компания должна обеспечить наличие соответствующих ресурсов, инфраструктуры и процессов для управления рисками.

3.17. Любое существенное изменение характеристик продукта требует повторной оценки. Оценка рисков новых продуктов подлежит документированию.

3.18. Организационный уровень риска определяется в соответствии с «Методологией оценки рисков ML/TF на уровне всей организации», направленной на оценку рисков отмывания денег и финансирования терроризма и совершенствование механизмов их снижения.

3.19. Оценка рисков ML/TF на уровне всей организации проводится каждые два года или, при необходимости, в течение одного месяца после выявления существенного изменения в

профиле рисков Компании (например, изменение организационной структуры, слияние с другой компанией и т.д.). В исключительных случаях (например, по требованию надзорного органа) оценка может проводиться в сроки и с периодичностью, установленными таким органом.

3.20. Результаты оценки рисков ML/TF на уровне всей организации документируются и по запросу предоставляются Национальному банку Грузии.

Глава 4. Контроль международных финансовых санкций

4.1. ООО «Solunex» стремится осуществлять свою деятельность в соответствии с международными и локальными санкциями. Процедура соблюдения и проверки международных финансовых санкций Компании определяет процедуры, руководящие принципы и контрольные механизмы, обеспечивающие соответствие деятельности Компании применимому законодательству и нормативным требованиям в области санкций.

4.2. Управление санкционными рисками включает процессы идентификации, оценки и управления потенциальными рисками нарушения санкций в рамках установленных деловых отношений и выполняемых транзакций.

4.3. Идентификация санкционных рисков включает тщательную проверку профилей клиентов, типов транзакций, блокчейн-адресов, кошельков, видов криптовалют, географического расположения и специфики услуг при установлении деловых отношений или выполнении разовой операции с целью выявления возможных связей с санкционированными лицами или странами.

4.4. Для анализа блокчейна Компания использует специализированное программное обеспечение, которое определяет источник и получателя виртуальных активов в транзакции, анализирует потоки транзакций и выявляет сценарии, указывающие на возможную подозрительную активность.

4.5. Программное обеспечение имеет доступ к спискам санкционированных кошельков и присваивает высокий уровень риска любой транзакции при совпадении, что служит основанием для применения усиленных превентивных мер.

4.6. Принципы, определённые в Процедуре соблюдения и проверки международных финансовых санкций, применяются ко всем транзакциям, операциям, деловым отношениям и разовым операциям.

4.7. Для обеспечения соблюдения международных санкционных требований Компания проверяет всех клиентов и участников транзакций по санкционным спискам, опубликованным Организацией Объединённых Наций, Европейским союзом, Соединёнными Штатами Америки и Соединённым Королевством.

4.8. Компания соблюдает санкционные режимы, введённые против России и Беларуси ЕС, США и Великобританией, в соответствии с Постановлением Национального банка Грузии № 208/04 от 4 августа 2023 года «Правила соблюдения санкционных режимов субъектами отчётности, находящимися под надзором Национального банка Грузии».

4.9. Компания использует автоматизированное программное обеспечение, обеспечивающее автоматическую проверку клиентов по следующим спискам:

1. Консолидированный список Европейского союза
2. Список OFAC (Specially Designated Nationals & Blocked Persons)
3. Список запрещённых лиц (Denied Persons List)
4. Список наиболее разыскиваемых террористов ФБР и лиц, по которым требуется информация
5. Санкционный список Банка Англии
6. HM Treasury
7. Несотрудничающие страны и территории
8. Список PEP
9. Список террористов ЕС
10. Список недобросовестных компаний Всемирного банка
11. Министерство иностранных дел и торговли
12. Санкционные списки, введённые против граждан России и Беларуси в связи с событиями в Украине

4.10. Обеспечение соблюдения санкций включает:

- отказ от установления или продолжения деловых отношений либо выполнения разовых операций, которые могут быть связаны с нарушением санкций;
- внедрение эффективных механизмов контроля для выявления возможных нарушений санкций;
- чёткое определение ответственности за управление санкционными рисками и формирование прозрачной организационной структуры.

4.11. Управление санкционными рисками охватывает идентификацию, оценку и управление потенциальными рисками нарушения санкций для всех деловых отношений и выполняемых операций, включая разовые сделки, в рамках каждой операции.

4.12. Идентификация санкционных рисков включает детальный анализ профилей клиентов, типов транзакций, географических зон и специфики услуг при установлении деловых отношений или выполнении разовых/множественных операций с целью выявления возможных связей с санкционированными лицами, адресами или странами.

4.13. Процесс оценки санкционных рисков является динамичным, регулярно пересматривается и обновляется при существенных изменениях, таких как изменения санкционных режимов, правовых требований или продуктов и услуг Компании.

4.14. Компания внедрила эффективные контрольные механизмы на различных этапах обслуживания клиентов для своевременного выявления и предотвращения возможных нарушений санкций.

4.15. Для соблюдения санкций осуществляется ежедневная автоматическая проверка (каждые 24 часа) действующих клиентов и клиентов, находящихся в текущих деловых отношениях, по санкционным спискам, публикуемым соответствующими органами, с сопоставлением идентификационных данных клиентов с санкционированными лицами.

4.16. Для выявления связей клиентов с санкциями собирается информация обо всех участниках транзакций и источниках виртуальных активов, а также проверяются возможные связи с санкционированными адресами при каждой операции, независимо от её характера (разовая или в рамках деловых отношений).

4.17. При наличии подозрения на нарушение санкционного режима в отношении клиента или его транзакции система автоматически блокирует профиль/счёт клиента (включая электронные кошельки внутри Компании), а также регистрацию/транзакцию. Уведомляется сотрудник по AML, который анализирует информацию и предпринимает соответствующие действия в соответствии с настоящим документом и законодательными требованиями.

4.18. Ответственность за контроль соблюдения санкций возлагается на лицо, ответственное за функционирование системы комплаенса, — сотрудника по AML Компании. Окончательная ответственность за эффективное функционирование системы лежит на директоре Компании.

Глава 5. Превентивные меры

5.1. Основой системы комплаенс-контроля Компании по предотвращению отмывания денежных средств (ML) и финансирования терроризма (TF) является принцип «Знай своего клиента» (KYC).

5.2. Подходы и стандарты KYC регулируются настоящей Политикой и «Политикой KYC и превентивных мер».

5.3. В целях настоящей Политики Компания реализует предусмотренные законодательством превентивные меры, включая:

- идентификацию клиента и проверку его личности с использованием надёжных и независимых источников;
- идентификацию бенефициарного владельца, лица, обладающего полномочиями представительства, а также юридических лиц в структуре собственности, и принятие разумных мер по их проверке;
- определение цели и предполагаемого характера деловых отношений;
- оценку рисков ML/TF, связанных с лицом при разовой операции или в рамках деловых отношений, и присвоение соответствующего уровня риска;
- мониторинг деловых отношений.

5.4. Превентивные меры являются обязательными в следующих случаях:

- установление деловых отношений;
- проведение разовой операции;
- независимо от суммы — если услуга предоставляется юридическому лицу или индивидуальному предпринимателю;
- если сумма разовой операции с конвертируемыми виртуальными активами превышает 3000 лари, 1000 евро/долларов США, либо совокупный объём связанных операций превышает эти значения;
- при наличии сомнений в достоверности идентификационных данных клиента или соблюдении требований законодательства;
- если сумма операции не превышает указанных лимитов, после идентификации/верификации фиксируются следующие данные:
    - полное имя;
    - личный идентификационный номер (при наличии);
    - дата рождения;
    - дата выдачи и срок действия удостоверяющего документа.

5.5. Превентивные меры применяются в соответствии с уровнем риска клиента до установления деловых отношений или проведения операции, а также периодически в процессе сотрудничества или при изменении существенных обстоятельств.

5.6. Анонимное или фиктивное обслуживание клиентов строго запрещено.

5.7. Для клиентов с высоким уровнем риска применяются усиленные меры, включая:

- получение дополнительной информации о клиенте/бенефициаре (деятельность, источники доходов, активов, репутация и др.);
- получение информации о характере деловых отношений и транзакций;
- получение разрешения директора на установление или продолжение отношений;
- установление источника средств и виртуальных активов;
- при необходимости — ограничение доступа к продуктам или установление лимитов.

5.8. Усиленный мониторинг включает:

- ежегодное обновление информации о клиенте;
- проверку целей транзакций, участников и источников средств;
- постоянный контроль соответствия заявленных данных фактической деятельности клиента.

5.9. Юрисдикция высокого риска — страна с существенными недостатками в системе AML/CTF.

5.10. Перечень таких юрисдикций утверждается Национальным банком Грузии.

5.11. Усиленные меры применяются, если:

- клиент зарегистрирован в офшорной или высокорисковой юрисдикции;
- клиент является физическим лицом, проживающим в такой юрисдикции;
- основной доход клиента связан с такой юрисдикцией;
- место рождения клиента — юрисдикция высокого риска.

5.12. До установления отношений определяется, является ли клиент или бенефициар политически значимым лицом (PEP), членом семьи или связанным лицом.

5.13. Для PEP применяются усиленные меры:

- обязательное разрешение руководства;
- установление источников средств;
- усиленный мониторинг;
- учёт рисков даже после прекращения публичной функции.

5.14. Лицо сохраняет статус PEP в течение 1 года после окончания должности.

5.15. Для клиентов с низким риском применяются упрощённые меры:

- обновление данных раз в 5 лет;
- определение цели отношений по типу операций;
- упрощённые меры не применяются при подозрении на ML/TF;
- невозможность применения любых мер без идентификации клиента;
- запрещено устанавливать отношения или проводить операции, если:
    - не выполнены меры контроля;
    - есть подозрение, что клиент связан с санкционными списками;
    - Компания не может эффективно управлять рисками;
    - клиент связан с терроризмом;
    - имеются иные основания, предусмотренные политиками Компании;
- действующие отношения подлежат прекращению при наступлении указанных обстоятельств.

Глава 6. Идентификация и верификация клиентов

6.1. До установления деловых отношений или проведения разовой операции необходимо провести идентификацию клиента и проверку его идентификационных данных на основе надёжных и независимых источников.

6.2. Верификация клиента включает идентификацию любого лица, действующего от имени клиента, проверку такого лица на основе надёжных и независимых источников, а также получение должным образом заверенного документа, подтверждающего его полномочия.

6.3. Идентификация, верификация или обновление данных клиента, представителя или бенефициарного владельца могут осуществляться без согласия клиента через системы, интегрированные с электронными базами данных Агентства развития государственных сервисов.

6.4. Перечень идентификационных данных, информации и документов, а также процедуры их проверки, регистрации, хранения и обновления определяются законодательством Грузии.

6.5. Установление или продолжение деловых отношений, а также проведение разовой операции запрещается, если невозможно выполнить идентификацию или верификацию клиента.

6.6. Компания проводит идентификацию и верификацию клиента на основе надёжных и независимых источников до установления деловых отношений или выполнения операции.

6.7. Для физических лиц идентификация проводится на основании оригиналов документов.

6.8. Документ, удостоверяющий личность, должен:

- содержать стандартные реквизиты (номер, дата выдачи и окончания срока действия, защитные элементы и др.);
- не быть существенно повреждённым;
- содержать фотографию владельца;
- быть действительным на момент предъявления.

6.9. Для физических лиц (резидентов и нерезидентов) собираются:

- полное имя;
- дата рождения;
- личный номер (при наличии);
- номер, дата выдачи, страна и орган выдачи, срок действия документа;
- пол;
- гражданство (включая двойное);
- место рождения;

- адрес регистрации;
- фактический адрес проживания.

6.10. Для лиц, проживающих в Абхазии или Цхинвальском регионе:

- имя и фамилия;
- дата рождения;
- личный номер;
- данные нейтрального документа (при наличии);
- пол;
- место рождения;
- адрес.

6.11. Для индивидуальных предпринимателей дополнительно:

- налоговый номер;
- юридический адрес;
- дата регистрации;
- сфера деятельности.

6.12. Верификация проводится по действительным документам, соответствующим гражданству и месту проживания.

6.13. Для лиц из Абхазии/Цхинвальского региона используется нейтральный документ или база данных Агентства госуслуг.

6.14. Для иностранных граждан:

- вид на жительство;
- временное удостоверение личности;
- паспорт;
- иные документы, разрешённые законодательством.

6.15. Для лиц без гражданства:

- вид на жительство;
- временное удостоверение личности или проездной документ.

6.17. Для индивидуальных предпринимателей — граждан Грузии: паспорт, ID-карта, водительское удостоверение или соответствующее свидетельство.

6.18. Для иностранных предпринимателей: вид на жительство, временное удостоверение, паспорт или иные разрешённые документы.

6.19. Компания не обслуживает лиц младше 14 лет.

6.20. Документы должны содержать фотографию (кроме исключений) и быть действительными.

6.21. Если документ не позволяет подтвердить данные, используются другие надёжные источники.

6.22. Компания может получать данные и фотографии из баз Агентства госуслуг без согласия субъекта.

6.23. Для операций до 3000 GEL / 1000 EUR/USD собираются минимум:

- имя и фамилия;
- личный номер (если есть);
- дата рождения;
- номер документа.

6.24. Установление деловых отношений обязательно:

- для юридических лиц и предпринимателей — независимо от суммы;
- для физических лиц — при превышении лимита, включая полную KYC-проверку.

6.25. Для предпринимателей дополнительно:

- идентификационный номер;
- дата регистрации;
- деятельность;
- количество сотрудников;
- юридический и фактический адрес;
- орган регистрации;
- информация о партнёрах (при необходимости).

6.26. Для юридических лиц:

- наименование;
- дата регистрации;
- страна регистрации;
- юридический адрес;

- регистрационные данные;
- организационно-правовая форма;
- фактический адрес.

6.27. Юридические лица должны иметь надлежащие учредительные документы.

6.28. Документы иностранных компаний должны быть легализованы или апостилированы.

6.29. Требования зависят от юрисдикции и формы организации.

6.30. Проверяется структура владения и контроля, включая бенефициаров.

6.31. Идентификация директоров и представителей проводится по общим правилам.

6.32. Бенефициарный владелец определяется через структуру владения.

6.33. Для филиалов собираются данные материнской компании и её представителей.

6.34. Для госорганов, международных организаций и др. собираются основные данные и информация о руководстве.

6.35. Верификация осуществляется на основе официальных выписок и документов.

6.36. Для грузинских компаний — выписки из реестра.

6.37. Для иностранных — документы из соответствующих реестров.

6.38. Документы должны быть актуальными (не старше 12 месяцев).

6.39. При необходимости используются дополнительные источники.

6.40. Для филиалов проводится дополнительная проверка.

6.41. Для организаций — используются публичные или надёжные источники.

6.42. Компания может получать данные без согласия из государственных баз.

6.43. Для незарегистрированных структур:

- название;
- дата создания;
- юридический и фактический адрес;
- налоговый номер (если есть).

6.44. Для представителей таких структур:

- если физлицо — стандартные данные;
- если юрлицо — данные юридического лица.

6.45. Верификация осуществляется по:

- учредительным документам;
- налоговой регистрации (при наличии).

6.46. Документы должны содержать актуальные данные.

6.47. Компания может использовать государственные базы для проверки без согласия клиента.

Глава 7. Идентификация бенефициарного владельца

7.1. При реализации превентивных мер обязательно определяется, идентифицируется, верифицируется и подтверждается личность бенефициарного владельца клиента.

7.2. Бенефициарный владелец — это физическое лицо, являющееся конечным собственником или контролирующим лицом клиента и/или от имени которого осуществляется операция.

7.3. При идентификации бенефициарного владельца юридического лица, незарегистрированной структуры, траста или аналогичной структуры необходимо анализировать структуру владения и контроля клиента. (Компании запрещено регистрировать юридические лица, имеющие форму траста или аналогичной структуры.)

7.4. Бенефициарный владелец — физическое лицо, прямо или косвенно владеющее 25% и более долей или голосов либо осуществляющее конечный контроль.

7.5. Прямое владение — владение 25%+ долей/голосов. Косвенное — владение через контролируемые юридические лица.

7.6. Если бенефициар с долей 25%+ не выявлен, идентификация проводится для лиц с управленческими полномочиями.

7.7. Процедуры регулируются законодательством Грузии и соответствующей политикой.

Глава 8. Определение цели и характера деловых отношений

8.1. Компания собирает и фиксирует:

- сведения о деятельности клиента;
- источники дохода;
- цель отношений и участие третьих лиц;
- планируемое использование услуг;
- ожидаемый объём, тип, частоту, валюту, географию и контрагентов операций.

8.2. До установления отношений и перед каждой операцией проводится проверка клиента по спискам PEP и санкций.

Глава 9. Мониторинг деловых отношений

9.1. Компания осуществляет постоянный мониторинг, включая:

- обновление данных клиента и бенефициара;
- анализ транзакций и их соответствия профилю клиента;
- выявление подозрительных операций.

9.2. Информация регулярно обновляется и пересматривается уровень риска.

9.3. Частота обновления:

- низкий риск — раз в 5 лет;
- средний — раз в 3 года;
- высокий — ежегодно.

9.4. При изменении структуры или представителей обслуживание возможно только после новой проверки.

9.5. Проводится анализ соответствия транзакций данным клиента.

9.6. Необычные операции фиксируются и анализируются.

9.7. Необычная операция — крупная, сложная или нетипичная операция без явной цели.

9.8. Признаки необычной операции:

- превышение ожидаемого объёма;
- необычная структура или частота;
- высокая сложность.

9.9. При необходимости применяется усиленный контроль.

9.10. Результаты документируются и предоставляются регулятору по запросу.

Глава 10. Политически значимые лица (PEP)

10.1. PEP — лицо, занимающее высокую государственную или политическую должность.

10.2. Члены семьи: супруг, родители, дети и др.

10.3. Связанные лица: партнёры, совладельцы и т.д.

10.4. Проверка проводится:

- до установления отношений;
- перед операциями;
- в процессе отношений;

- при обновлении списков.

10.5. Для PEP применяются усиленные меры:

- проверка источника средств;
- согласие директора;
- усиленный мониторинг.

10.6. Статус может выявляться из открытых источников.

10.7. Статус может быть снят после анализа.

10.8. Риски учитываются даже после прекращения должности.

10.9. Усиленные меры действуют 1 год после утраты статуса.

Глава 11. Проверка адресов виртуальных активов

11.1. Проверка проводится:

- для каждой операции;
- при периодическом мониторинге (не реже 1 раза в год).

11.2. Используется автоматизированное ПО для анализа источников активов.

11.3. Высокий риск:

- связи с преступной деятельностью, терроризмом, санкциями;
- даркнет, мошенничество, вымогательство, взломы и др.

11.4. Подозрительные источники:

- ATM, P2P без KYC;
- DeFi, OTC, нелицензированные провайдеры и др.

11.5. Категории риска:

- низкий — до 30%;
- средний — 30–60%;
- высокий — 60–80%;
- недопустимый — более 80%.

11.6. При выявлении высокого риска:

- операция блокируется;
- проводится усиленная проверка;
- принимается решение о предоставлении услуги;

- при необходимости уведомляется FMS;
- пересматривается риск клиента и требуется одобрение директора.