ПРИКАЗ ФИНАНСОВОГО РЕГУЛЯТОРА НЕО-СИТИ

№ 312

"О требованиях к хранению данных о финансовых транзакциях"

г. Нео-Сити
22 июля 2089 года

В целях обеспечения надлежащего хранения данных о транзакциях (статья 4.3 КЗД) и соблюдения требований финансового мониторинга, Финансовый регулятор Нео-Сити

ПРИКАЗЫВАЕТ:

1. Общие положения

1.1. Настоящий Приказ устанавливает требования к хранению данных о финансовых транзакциях финансовыми организациями, осуществляющими деятельность на территории Нео-Сити.

1.2. Для целей настоящего Приказа:

а) *финансовая организация* — банк, платёжная система, инвестиционная компания, страховая организация и иные лицензированные финансовые посредники;

б) *транзакционные данные* — информация о финансовых операциях в соответствии со статьёй 4.3 КЗД;

в) *клиент* — физическое или юридическое лицо, пользующееся услугами финансовой организации;

г) *операция* — любое действие с денежными средствами или финансовыми инструментами;

д) *подозрительная операция* — операция, имеющая признаки, указывающие на возможное отмывание денег или финансирование терроризма.

1.3. Действие настоящего Приказа распространяется на:

а) банки и небанковские кредитные организации;

б) платёжные системы и операторы электронных денег;

в) инвестиционные и управляющие компании;

г) страховые организации;

д) криптовалютные биржи и обменники;

е) микрофинансовые организации.

2. Категории хранимых данных

2.1. Финансовые организации обязаны хранить следующие категории транзакционных данных:

2.1.1. Идентификационные данные участников:

а) наименование/ФИО плательщика и получателя;

б) идентификационные номера (ИНН, регистрационный номер);

в) реквизиты счетов;

г) адреса регистрации и фактического местонахождения.

2.1.2. Данные об операции:

а) тип операции (перевод, платёж, обмен, снятие, пополнение);

б) сумма и валюта;

в) дата и время совершения;

г) уникальный идентификатор транзакции;

д) назначение платежа.

2.1.3. Технические данные:

а) канал совершения операции (отделение, банкомат, онлайн, мобильное приложение);

б) IP-адрес (для онлайн-операций);

в) идентификатор устройства;

г) геолокация (при наличии согласия);

д) результат проверки безопасности.

2.1.4. Данные о верификации:

а) метод аутентификации клиента;

б) результат проверки личности;

в) документы, использованные для идентификации;

г) результаты скоринга и мониторинга.

2.2. Дополнительно для подозрительных операций хранятся:

а) результаты анализа на предмет отмывания денег;

б) решение о проведении/блокировке операции;

в) информация о направлении сообщения в уполномоченный орган;

г) материалы внутреннего расследования.

3. Сроки хранения данных

3.1. Стандартные сроки хранения транзакционных данных:

а) данные об операциях — 7 лет с даты совершения операции;

б) данные идентификации клиента — 7 лет с даты прекращения отношений с клиентом;

в) технические данные — 5 лет с даты совершения операции;

г) данные о верификации — 7 лет с даты прекращения отношений.

3.2. Увеличенные сроки хранения:

а) данные о подозрительных операциях — 10 лет;

б) данные об операциях, в отношении которых проводилось расследование — до окончания расследования плюс 5 лет;

в) данные об операциях с публичными должностными лицами — 10 лет;

г) данные об операциях на сумму свыше 10,000,000 кредитов — 10 лет.

3.3. Сокращённые сроки хранения (при условии получения разрешения регулятора):

а) агрегированные данные могут заменить детальные записи по истечении 5 лет;

б) технические данные низкорисковых операций — 3 года.

3.4. По истечении срока хранения данные подлежат уничтожению в соответствии с процедурой, установленной разделом 6 настоящего Приказа.

4. Требования к системам хранения

4.1. Системы хранения транзакционных данных должны обеспечивать:

4.1.1. Надёжность:

а) резервное копирование не реже 1 раза в сутки;

б) географически распределённое хранение резервных копий;

в) время восстановления данных — не более 4 часов;

г) сохранность данных при отказе оборудования.

4.1.2. Безопасность:

а) шифрование данных при хранении (AES-256 или эквивалент);

б) шифрование данных при передаче (TLS 1.3 или выше);

в) контроль доступа на основе ролей;

г) многофакторная аутентификация для доступа к данным;

д) защита от несанкционированного изменения.

4.1.3. Доступность:

а) время доступа к актуальным данным (до 1 года) — не более 5 секунд;

б) время доступа к архивным данным — не более 24 часов;

в) возможность полнотекстового поиска;

г) возможность выгрузки данных в стандартных форматах.

4.1.4. Целостность:

а) использование контрольных сумм;

б) ведение журнала изменений;

в) невозможность удаления или изменения данных без авторизации;

г) контроль версий при корректировке данных.

4.2. Данные должны храниться на территории Нео-Сити или на территориях с адекватным уровнем защиты (статья 31 КЗД).

4.3. При использовании облачных сервисов:

а) провайдер должен быть сертифицирован для работы с финансовыми данными;

б) данные должны быть зашифрованы ключами, контролируемыми финансовой организацией;

в) должна быть обеспечена возможность миграции данных;

г) провайдер должен пройти аудит безопасности.

5. Права клиентов

5.1. Клиент имеет право запросить информацию о своих транзакциях в соответствии со статьёй 11 КЗД.

5.2. Финансовая организация предоставляет:

а) выписку по счёту за любой период в пределах срока хранения;

б) детализацию отдельных операций;

в) копии платёжных документов;

г) информацию о получателях/отправителях платежей (в объёме, разрешённом законом).

5.3. Срок предоставления информации:

а) за текущий год — в течение 3 рабочих дней;

б) за предыдущие периоды — в течение 10 рабочих дней;

в) из архивного хранения — в течение 30 рабочих дней.

5.4. Первая выписка за календарный год предоставляется бесплатно. За дополнительные выписки может взиматься плата, не превышающая фактические расходы на подготовку.

5.5. Ограничения права на информацию:

а) финансовая организация вправе не раскрывать информацию о мерах противодействия отмыванию денег;

б) информация может быть ограничена по требованию правоохранительных органов;

в) информация о подозрительных операциях не раскрывается клиенту.

6. Порядок уничтожения данных

6.1. По истечении срока хранения данные подлежат уничтожению.

6.2. Уничтожение осуществляется:

а) автоматически — для данных с истёкшим сроком хранения при отсутствии оснований для продления;

б) по решению уполномоченного лица — при досрочном уничтожении;

в) по требованию регулятора — в исключительных случаях.

6.3. Процедура уничтожения:

а) формирование реестра данных, подлежащих уничтожению;

б) проверка отсутствия оснований для продления хранения;

в) согласование с ответственным лицом;

г) физическое уничтожение или криптографическое стирание;

д) составление акта об уничтожении.

6.4. Методы уничтожения:

а) для электронных носителей — многократная перезапись или физическое уничтожение;

б) для бумажных носителей — измельчение или сжигание;

в) для облачных данных — криптографическое стирание с подтверждением от провайдера.

6.5. Акт об уничтожении содержит:

а) перечень уничтоженных данных (без раскрытия персональных данных);

б) основание для уничтожения;

в) метод уничтожения;

г) дату и время уничтожения;

д) подписи ответственных лиц.

6.6. Акты об уничтожении хранятся в течение 10 лет.

7. Предоставление данных регулятору

7.1. Финансовая организация обязана предоставлять транзакционные данные:

а) по запросу Финансового регулятора — в срок, указанный в запросе, но не менее 3

рабочих дней;

б) по запросу правоохранительных органов — в соответствии с процессуальным законодательством;

в) по запросу налоговых органов — в соответствии с налоговым законодательством;

г) по запросу иностранных регуляторов — через Финансовый регулятор Нео-Сити.

7.2. Регулярная отчётность:

а) сводная информация о количестве и объёме операций — ежемесячно;

б) информация о подозрительных операциях — незамедлительно;

в) статистика по категориям операций — ежеквартально;

г) отчёт о соблюдении требований хранения — ежегодно.

7.3. Формат предоставления данных:

а) электронный формат согласно спецификации регулятора;

б) через защищённый канал связи;

в) с использованием электронной подписи.

8. Ответственность

8.1. За нарушение требований к хранению данных:

а) предупреждение — при первом незначительном нарушении;

б) штраф 500,000-5,000,000 кредитов — при существенных нарушениях;

в) штраф до 1% годового оборота — при систематических нарушениях;

г) приостановление лицензии — при грубых нарушениях.

8.2. За утрату транзакционных данных:

а) штраф 1,000,000 кредитов — при утрате данных за период до 1 года;

б) штраф 5,000,000 кредитов — при утрате данных за период более 1 года;

в) обязанность восстановить данные из альтернативных источников;

г) уведомление затронутых клиентов.

8.3. За несанкционированный доступ к данным:

а) штраф до 3% годового оборота;

б) обязанность уведомить затронутых клиентов и регулятора;

в) компенсация ущерба клиентам.

8.4. За несвоевременное предоставление данных регулятору:

а) штраф 100,000 кредитов за каждый день просрочки;

б) при умышленном уклонении — приостановление лицензии.

8.5. Должностные лица финансовой организации несут персональную ответственность за организацию хранения данных.

9. Аудит и контроль

9.1. Финансовая организация обязана проводить внутренний аудит систем хранения данных не реже 1 раза в год.

9.2. Внутренний аудит включает проверку:

а) соблюдения сроков хранения;

б) полноты хранимых данных;

в) безопасности систем хранения;

г) процедур резервного копирования;

д) процедур уничтожения данных.

9.3. Результаты аудита документируются и хранятся в течение 5 лет.

9.4. Финансовый регулятор вправе проводить проверки систем хранения данных:

а) плановые — не чаще 1 раза в 2 года;

б) внеплановые — при наличии оснований.

9.5. При выявлении нарушений по результатам проверки регулятор выдаёт предписание об устранении в срок до 90 дней.

10. Переходные положения

10.1. Настоящий Приказ вступает в силу с 01 октября 2089 года.

10.2. Финансовые организации обязаны привести системы хранения в соответствие с требованиями до 01 января 2090 года.

10.3. Требования к срокам хранения применяются к операциям, совершённым после вступления Приказа в силу.

10.4. Для операций, совершённых до вступления Приказа в силу, применяются ранее действовавшие сроки хранения.

Председатель Финансового регулятора

В.К. Банкиров

Регистрационный номер: НС-ФР-312/07-22
Опубликован: 28 июля 2089 года