

ПРИКАЗ БЮРО ТЕЛЕКОММУНИКАЦИЙ НЕО-СИТИ

№ 356

"О требованиях к хранению метаданных связи операторами телекоммуникационных услуг"

г. Нео-Сити

15 августа 2089 года

В целях обеспечения безопасности телекоммуникационной инфраструктуры и в соответствии с требованиями раздела V Кодекса о защите данных (статьи 40-43 КЗД), Бюро телекоммуникаций

ПРИКАЗЫВАЕТ:

1. Общие положения

1.1. Настоящий Приказ устанавливает требования к сбору, хранению и обработке метаданных связи операторами телекоммуникационных услуг на территории Нео-Сити.

1.2. Для целей настоящего Приказа:

- а) *оператор связи* — юридическое лицо, имеющее лицензию на оказание услуг связи;
- б) *метаданные связи* — информация о факте, времени, продолжительности, участниках и параметрах сеанса связи, не включающая содержание передаваемых сообщений;
- в) *абонент* — пользователь услуг связи на основании договора с оператором;
- г) *сеанс связи* — установленное соединение для передачи информации;
- д) *идентификатор абонента* — номер телефона, логин, IMSI, IP-адрес или иной уникальный идентификатор.

1.3. Действие настоящего Приказа распространяется на:

- а) операторов фиксированной телефонной связи;
- б) операторов мобильной связи;
- в) интернет-провайдеров;
- г) операторов VoIP-сервисов;
- д) операторов мессенджеров (в части метаданных).

2. Категории хранимых метаданных

2.1. Операторы связи обязаны хранить следующие категории метаданных:

2.1.1. Для телефонной связи:

- а) номера вызывающего и вызываемого абонентов;
- б) дата и время начала и окончания вызова;
- в) продолжительность вызова;
- г) тип вызова (голосовой, видео, факс);
- д) статус вызова (успешный, неуспешный, переадресованный);
- е) идентификатор базовой станции (для мобильной связи);
- ж) IMEI устройства.

2.1.2. Для передачи данных (интернет):

- а) IP-адрес абонента;
- б) время начала и окончания сессии;
- в) объём переданных и полученных данных;
- г) идентификатор точки доступа;
- д) MAC-адрес устройства (при возможности определения);

е) протокол соединения.

2.1.3. Для обмена сообщениями (SMS, MMS):

- а) номера отправителя и получателя;
- б) дата и время отправки;
- в) статус доставки;
- г) размер сообщения (для MMS);
- д) тип сообщения.

2.1.4. Для мессенджеров:

- а) идентификаторы участников;
- б) время отправки и доставки;
- в) тип контента (текст, медиа, голосовое сообщение);
- г) идентификатор группы или чата.

2.2. Запрет на хранение содержания. Операторы связи не вправе хранить содержание сообщений и разговоров, за исключением случаев:

- а) явного согласия абонентов;
- б) решения суда;
- в) собственных голосовых сообщений абонента (голосовая почта).

3. Сроки хранения метаданных

3.1. Стандартные сроки хранения:

- а) метаданные телефонных вызовов — 12 месяцев;
- б) метаданные интернет-сессий — 6 месяцев;
- в) метаданные SMS/MMS — 12 месяцев;
- г) метаданные мессенджеров — 6 месяцев.

3.2. Увеличенные сроки хранения (по запросу правоохранительных органов):

- а) метаданные конкретного абонента — до 3 лет;
- б) метаданные по конкретному инциденту — до окончания расследования.

3.3. Сокращённые сроки хранения (для отдельных категорий):

- а) неуспешные соединения — 3 месяца;
- б) автоматические системные соединения — 1 месяц;
- в) служебные сессии (обновления, синхронизация) — 1 месяц.

3.4. По истечении срока хранения метаданные подлежат автоматическому удалению.

4. Требования к системам хранения

4.1. В соответствии со статьёй 40 КЗД (общие требования безопасности) системы хранения метаданных должны обеспечивать:

4.1.1. Безопасность:

- а) физическую защиту серверов (охрана, контроль доступа, видеонаблюдение);
- б) шифрование данных при хранении;
- в) защиту каналов передачи данных;
- г) сегментацию сетей хранения от публичных сетей;
- д) защиту от DDoS-атак и других киберугроз.

4.1.2. Отказоустойчивость:

- а) резервное копирование не реже 1 раза в сутки;
- б) географически распределённое хранение;
- в) время восстановления — не более 4 часов;
- г) плановая доступность — не менее 99.9%.

4.1.3. Контроль доступа:

- а) ролевая модель доступа;
- б) персональная аутентификация сотрудников;
- в) многофакторная аутентификация для администраторов;
- г) журналирование всех операций доступа.

4.2. В соответствии со статьёй 41 КЗД (конкретные меры безопасности):

- а) применение псевдонимизации метаданных где возможно;
- б) разделение идентификационных данных абонента и метаданных;
- в) регулярная проверка и обновление мер безопасности.

4.3. Системы хранения метаданных размещаются исключительно на территории Нео-Сити.

4.4. Запрещается использование иностранных облачных провайдеров для хранения метаданных связи.

5. Права абонентов

5.1. Абонент имеет право запросить:

- а) детализацию собственных вызовов и сессий;
- б) информацию о хранимых метаданных;
- в) сведения о запросах его метаданных третьими лицами (если это не запрещено).

5.2. Оператор предоставляет детализацию:

- а) за текущий расчётный период — бесплатно через личный кабинет;
- б) за предыдущие периоды (до 12 месяцев) — в течение 5 рабочих дней;
- в) за архивные периоды — в течение 15 рабочих дней.

5.3. Абонент вправе возразить против хранения метаданных сверх установленных сроков, за исключением случаев, когда хранение требуется по закону.

5.4. Ограничения права на информацию:

- а) абонент не вправе получить детализацию другого абонента;
- б) информация о запросах правоохранительных органов может быть ограничена;
- в) корпоративные абоненты получают информацию в соответствии с договором.

6. Предоставление метаданных уполномоченным органам

6.1. Метаданные предоставляются:

- а) правоохранительным органам — по решению суда или в случаях, предусмотренных законом;
- б) органам безопасности — в соответствии с законодательством о безопасности;
- в) Бюро телекоммуникаций — для целей мониторинга и контроля.

6.2. Порядок предоставления:

- а) запрос направляется в письменной форме с указанием правового основания;
- б) оператор проверяет законность запроса;
- в) данные предоставляются в защищённом формате;
- г) факт предоставления документируется.

6.3. Сроки предоставления:

- а) в экстренных случаях (угроза жизни) — незамедлительно;
- б) по решению суда — в срок, указанный в решении;
- в) по иным основаниям — в течение 10 рабочих дней.

6.4. Защита тайны связи. Оператор обязан:

- а) удостовериться в законности запроса;
- б) предоставить только запрошенные данные;
- в) не раскрывать факт запроса абоненту, если это запрещено;
- г) вести учёт всех запросов.

6.5. Оператор вправе отказать в предоставлении данных, если:

- а) запрос не соответствует правовым основаниям;
- б) запрос чрезмерно широк или неопределён;
- в) запрашиваемые данные не хранятся.

7. Уведомление об инцидентах

7.1. В соответствии со статьёй 42 КЗД при утечке метаданных оператор обязан:

- а) уведомить Бюро телекоммуникаций в течение 24 часов;
- б) уведомить Бюро защиты данных в течение 72 часов;
- в) уведомить затронутых абонентов при высоком риске.

7.2. Уведомление содержит:

- а) описание инцидента;
- б) категории и примерное количество затронутых записей;
- в) принятые меры;
- г) контактные данные ответственного лица.

7.3. Оператор ведёт реестр инцидентов безопасности и предоставляет его регулятору по запросу.

7.4. В соответствии со статьёй 42.4 КЗД оператор документирует все инциденты, включая те, которые не требуют уведомления.

8. Защита данных при разработке

8.1. В соответствии со статьёй 43 КЗД (защита данных по умолчанию и при разработке) операторы обязаны:

- а) проектировать системы с учётом требований защиты данных;
- б) применять минимизацию данных по умолчанию;
- в) обеспечивать конфиденциальность на уровне архитектуры;
- г) проводить оценку воздействия на защиту данных.

8.2. При внедрении новых систем хранения метаданных:

- а) проводится оценка рисков;
- б) выполняется тестирование безопасности;
- в) документируются меры защиты;
- г) обеспечивается обучение персонала.

9. Ответственность

9.1. За нарушение требований к хранению метаданных:

- а) штраф 1,000,000-10,000,000 кредитов — за нарушение сроков хранения;
- б) штраф до 3% годового оборота — за утечку метаданных;
- в) приостановление лицензии — за систематические нарушения.

9.2. За незаконное предоставление метаданных:

- а) штраф 5,000,000 кредитов;
- б) уголовная ответственность должностных лиц;
- в) отзыв лицензии при повторном нарушении.

9.3. За отказ предоставить метаданные по законному запросу:

- а) штраф 500,000 кредитов за каждый случай;
- б) принудительное исполнение по решению суда.

9.4. За нарушение требований безопасности:

- а) предписание об устранении — при выявлении уязвимостей;
- б) штраф при неустранении в срок;
- в) ограничение деятельности при критических уязвимостях.

10. Контроль и надзор

10.1. Бюро телекоммуникаций осуществляет контроль за соблюдением требований настоящего Приказа.

10.2. Формы контроля:

- а) плановые проверки — не чаще 1 раза в год;
- б) внеплановые проверки — при наличии оснований;
- в) дистанционный мониторинг — постоянно;
- г) аудит систем безопасности — по согласованию.

10.3. Операторы обязаны:

- а) обеспечивать доступ к системам хранения при проверках;
- б) предоставлять документацию по запросу;
- в) содействовать проведению аудита.

10.4. Результаты проверок документируются. При выявлении нарушений выдаётся предписание об устранении.

11. Переходные положения

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

11.2. Операторы связи обязаны привести системы хранения в соответствие с требованиями до 01 января 2090 года.

11.3. До приведения в соответствие операторы продолжают хранение по ранее действовавшим правилам.

11.4. Бюро публикует технические спецификации форматов данных до 15 сентября 2089 года.

Директор Бюро телекоммуникаций

С.Н. Связев

Регистрационный номер: НС-БТ-356/08-15

Опубликован: 20 августа 2089 года