



## NOX — Дорожная карта

### Введение

Система NOX — созданная для бесплатной связи, коммуникации, обмена сообщениями и данными без посредников и централизованных серверов. Система разработана с приоритетом на конфиденциальность и принципиальным отсутствием сбора данных. Функционал доступен в любой точке мира, независимо от страны, социального положения или местонахождения пользователя.

### Определения

- Пользователь — участник сети NOX, не проходящий обязательную регистрацию и не предоставляющий личные данные.
- Связь напрямую — обмен данными между устройствами без участия третьей стороны или централизованных узлов.
- Глубокое инкриптование — авторский термин системы NOX, обозначающий совокупность криптографических методов, обеспечивающих не только защиту содержимого, но и скрытие самого факта коммуникации.
- Сессия — временный период взаимодействия, по завершении которого данные не сохраняются.

### Положения

- Отсутствие хранения данных: переписки, файлы и метаданные не сохраняются системой.
- Автономность: работа без обязательной регистрации и с возможностью полной анонимности.
- Устойчивость групповой связи при отключении или потере интернет-соединения.
- Невидимость коммуникаций: трафик не поддается перехвату, цензуре или идентификации участников.
- Используемые криптографические методы (криптографические примитивы) лежат в основе механизма глубокого инкриптования.
- Бесплатность: доступ без финансовых ограничений или подписок.

### Цели

1. Обеспечить безопасную и стабильную связь в любых условиях, включая экстремальные.
2. Сформировать независимую инфраструктуру, устойчивую к цензуре и блокировкам.
3. Гарантировать анонимность и приватность каждого участника.
4. Предоставить универсальные средства коммуникации, доступные в любой точке мира.
5. Сохранить простоту использования без необходимости дополнительного оборудования.

## Модель угроз

Система разрабатывалась с учетом следующих потенциальных угроз:

- Локальная и глобальная цензура.
- Целенаправленное накопление и анализ личных данных глобальными сервисами.
- Анализ информации о взаимодействиях, позволяющий строить карту связей и привычек пользователей.
- Попытки блокировки каналов связи.
- Локальные и глобальные отключения интернета.

## Этапы реализации

### Этап 1 — Основополагающий функционал

- Связь напрямую между пользователями без участия третьей стороны или централизованных узлов, с устойчивостью для групповой связи при отключении или потере интернет-соединения.
- Полная автономная работа, исключающая любую регистрацию.
- Бесплатный доступ к функционалу в любой точке мира, независимо от страны, социального положения или местонахождения.
- Поддержка обмена сообщениями, файлами, аудио- и видеосвязью по доступным каналам.
- P2P-аудиосвязь в формате «телефонного звонка» без SIM-карты и телефонного номера.
- Интеграция защищённого и моментального обмена ключами.
- Механизм глубокого инкриптования, обеспечивающий невидимость коммуникаций и защиту от перехвата.

### Этап 2 — Расширение возможностей

- Динамическое создание и распад защищённых групп без сохранения данных после завершения сессии.
- Модульная архитектура с возможностью добавления/замены компонентов без остановки системы.
- Интеграция мультипротокольных каналов связи для повышения надёжности.
- Расширенные инструменты для безопасного обмена файлами и медиа.
- Защищённые видеоконференции.

### Этап 3 — Усиление устойчивости и адаптация

- Усиление устойчивости при появлении новых технических и цензурных угроз.
- Актуализация криптографических методов и механизмов глубокого инкриптования.
- Работа на опережение с учетом меняющихся технологических и сетевых рисков.

### Этап 4 — Экосистема и интеграции

- API для интеграции NOX со сторонними приложениями и сервисами.
- Поддержка анонимных платежей и микротранзакций внутри сети.
- Интеграция с аппаратными криптоключами и безопасными устройствами.
- (Без хранения данных: интеграции не изменяют базовый принцип отсутствия сохранения содержимого и метаданных.)

## **Этап 5 — Сообщество и самоуправление**

- Создание децентрализованной системы коллективного управления проектом (DAO).
- Прозрачные механизмы предложений и голосований за изменения.
- Грантовые программы для разработчиков и исследователей безопасности.
- Открытые тесты и вознаграждения за найденные уязвимости.

## **Заключение**

Мы движемся к независимой, устойчивой и глобально доступной системе связи, которая сохраняет свободу коммуникации даже под давлением, блокировками и перехватом. NQX — это не просто инструмент, а пространство, где каждый остаётся свободным, а взаимодействие защищено и невидимо для тех, кто пытается его контролировать.