# NỌX — Roadmap

## Introduction

The NỌX system is created for free communication, messaging, and data exchange without intermediaries or centralized servers. It is designed with a priority on privacy and the fundamental absence of data collection. The functionality is available anywhere in the world, regardless of country, social status, or user location.

## Definitions

— User — a participant of the NỌX network, not required to register and not providing personal data.
— Direct Connection — data exchange between devices without a third party or centralized nodes.
— **Deep InCrypting** — an authorial NỌX term meaning a combination of cryptographic methods ensuring not only the protection of content but also the concealment of the very fact of communication.
— Session — a temporary period of interaction, after which data is not preserved.

## Provisions

— No data storage: messages, files, and metadata are not preserved by the system.
— Autonomy: operation without mandatory registration and with the possibility of complete anonymity.
— Resilience of group communication in case of disconnection or loss of internet connectivity.
— Communication invisibility: traffic cannot be intercepted, censored, or used to identify participants.
— The cryptographic methods used (cryptographic primitives) are the basis of the **Deep InCrypting** mechanism.
— Free access: no financial restrictions or subscriptions.

## Goals

1. Ensure secure and stable communication under any conditions, including extreme ones.
2. Build an independent infrastructure resistant to censorship and blocking.
3. Guarantee anonymity and privacy of each participant.
4. Provide universal communication tools accessible anywhere in the world.
5. Maintain simplicity of use without additional equipment.

## Threat Model

The system was developed with the following potential threats in mind:
— Local and global censorship.
— Purposeful collection and analysis of personal data by global services.
— Analysis of interaction data to construct maps of user relations and habits.
— Attempts to block communication channels.
— Local and global internet shutdowns.

# Implementation Stages

## Stage 1 — Fundamental Functionality

— Direct connection between users without a third party or centralized nodes, with resilience for group communication when disconnected or losing internet connectivity.

— Full autonomous operation, excluding any registration.

— Free access to functionality worldwide, regardless of country, social status, or location.

— Support for messaging, file exchange, audio and video communication over available channels.

— P2P audio calls in the form of a “phone call” without a SIM card or phone number.

— Integration of secure and instant key exchange.

— ****Deep InCrypting**** mechanism ensuring communication invisibility and protection against interception.

## Stage 2 — Extended Capabilities

— Dynamic creation and dissolution of protected groups without saving data after a session ends.

— Modular architecture allowing addition/replacement of components without stopping the system.

— Integration of multiprotocol communication channels to improve reliability.

— Extended tools for secure file and media exchange.

— Protected videoconferencing.

## Stage 3 — Strengthening Resilience and Adaptation

— Strengthening resilience to new technical and censorship threats.

— Updating cryptographic methods and the ****Deep InCrypting**** mechanism.

— Proactive adaptation to changing technological and network risks.

## Stage 4 — Ecosystem and Integrations

— API for integration of NỌX with third-party applications and services.

— Support for anonymous payments and microtransactions inside the network.

— Integration with hardware cryptographic keys and secure devices.

— (No data storage: integrations do not alter the core principle of no storage of content or metadata.)

## Stage 5 — Community and Self-Governance

— Creation of a decentralized system of collective governance (DAO).

— Transparent mechanisms for proposals and voting on changes.

— Grant programs for developers and security researchers.

— Open testing and rewards for discovered vulnerabilities.

# Conclusion

We are moving toward an independent, resilient, and globally accessible communication system that preserves freedom of communication even under pressure, blocking, and interception. NỌX is not just a tool, but a space where everyone remains free, and interaction is protected and invisible to those who try to control it.