



# ГЛАВА 5

Четыре уровня абсолютной безопасности  
(Защита данных и GDPR)

# Безопасность на уровне ДНК проекта

Концепция "Security by Design". Почему LINK AI безопасен по своей природе.



## Приоритет №1

Безопасность — это фундамент архитектуры, а не дополнение в конце.



## Изоляция

Проект не имеет доступа к закрытым серверам UDI или внутренним базам Link AS.



## Автономия

Система работает как независимый умный гид по бытовым вопросам лагеря.

### КОММЕНТАРИЙ АРХИТЕКТОРА

*«LINK AI полностью изолирован от госсистем. Это автономный инструмент помощи в быту, спроектированный по принципу "безопасность по умолчанию"».*

# Защита от внешнего доступа

Закрытый контур распространения. Почему приложение невозможно найти в сети извне.

-  **Отсутствие в публичных маркетах:** Ни в App Store, ни в Google Play.
-  **Скрытая инфраструктура:** Ссылка на сервис физически недоступна извне.
-  **Точечная активация:** Доступ открывается только по прибытии человека в лагерь.



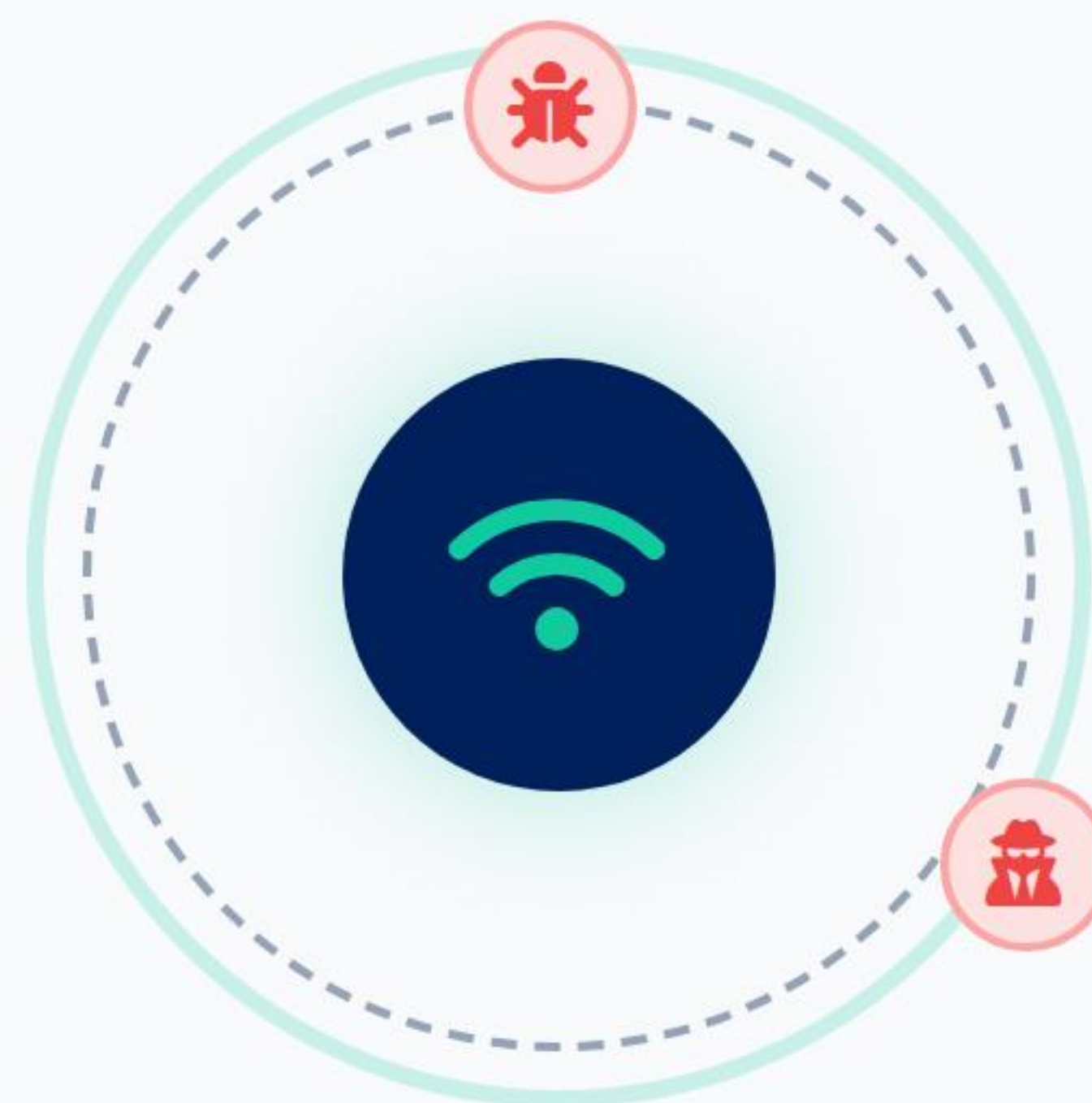
## КОММЕНТАРИЙ АРХИТЕКТОРА

*«Приложение невозможно скачать из интернета. Внешние лица физически не могут получить доступ к платформе — она существует только внутри периметра».*

# Доступ только через Wi-Fi лагеря

Точка входа — Geofencing. Цифровой забор для защиты системы.

- 1 Фильтр IP-адресов:** Прием запросов только от официальных роутеров.
- 2 Активация по QR-коду:** Сканирование на территории моттака.
- 3 Авто-блокировка:** Система отключается при выходе за территорию.



## КОММЕНТАРИЙ АРХИТЕКТОРА

«Вход привязан к IP-адресу лагерного Wi-Fi. Вышел за ворота — система заблокировалась. Это исключает нецелевое использование вне лагеря».

# Принцип «Нет данных — нет утечки»

Уровень 1 — Архитектурный. Абсолютная анонимность пользователя.

- ✓ **Без регистрации:** Нет логинов и паролей.
- ✓ **Без личных документов:** Не требуются ФИО, телефон, DUF-номер.
- ✓ **Без слежки:** Нет доступа к геолокации и камере устройства.



## КОММЕНТАРИЙ АРХИТЕКТОРА

*«Лучший способ защитить данные — не собирать их. Для системы каждый пользователь — анонимный гость. Данных внутри системы нет, украсть их невозможно».*

# Плагин-фильтр персональных данных

Уровень 2 — Программный. Защита пользователя от собственных ошибок.



## Перехват на лету

Проверка текста ДО отправки запроса в нейросеть.



## Умное сканирование

Мгновенное распознавание имен и номеров дел (DUF).



## Мгновенная блокировка

Очистка сообщения за доли секунды без сохранения логов.

### КОММЕНТАРИЙ АРХИТЕКТОРА

*«Я предусмотрел программный щит. Если человек в стрессе случайно напишет свой DUF-номер, скрипт вырежет эти данные до того, как они попадут в ИИ».*

# Механика работы плагина-заглушки

Визуализация алгоритма фильтрации данных в реальном времени.

## Блок ВХОД:

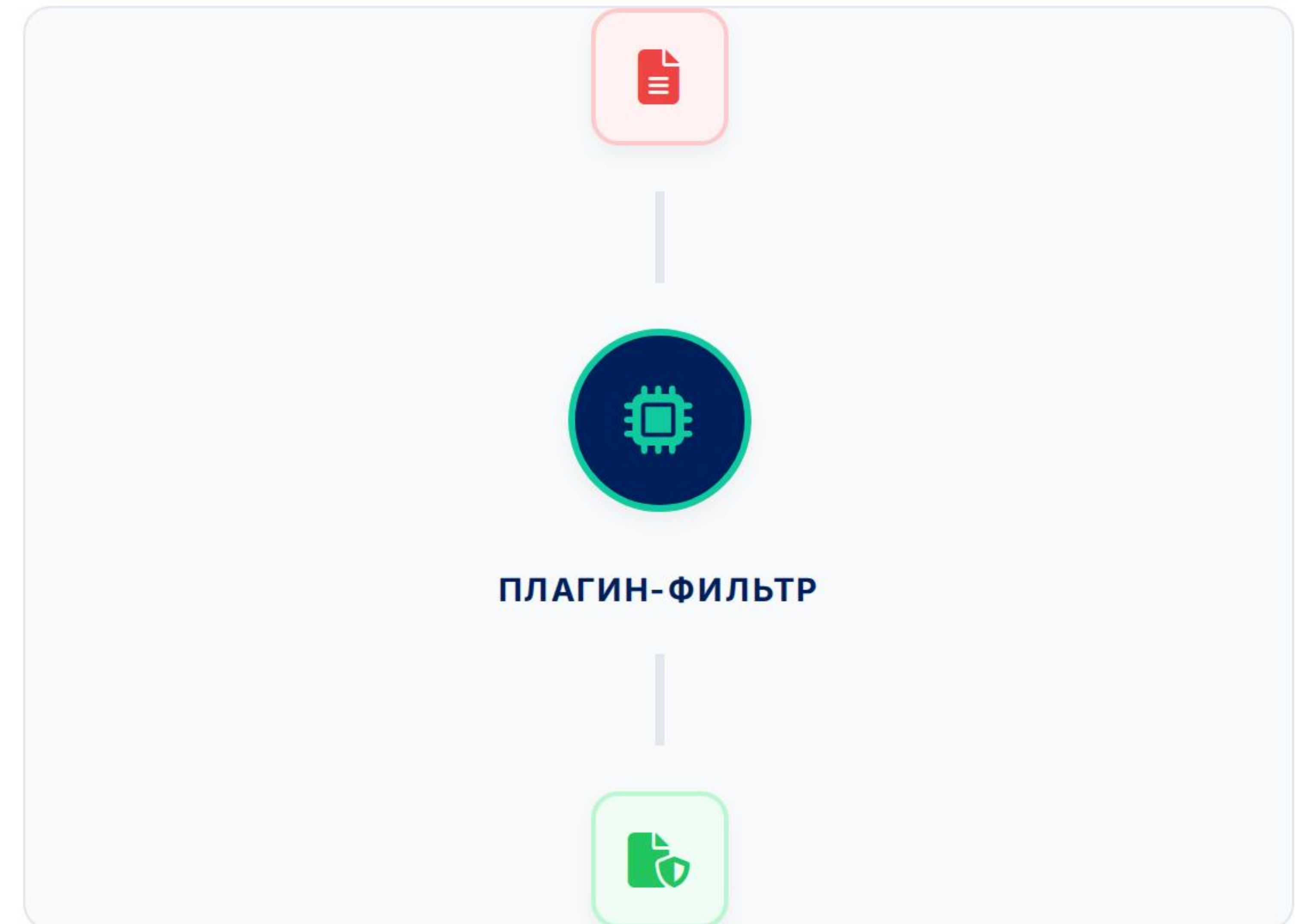
"Я Алекс, мой DUF-номер 12345678901, где забрать белье?"



Авторский Плагин: Удаление личных данных

## Блок ВЫХОД:

"Я [Пользователь], мой номер [Скрыто], где забрать белье?"



## КОММЕНТАРИЙ АРХИТЕКТОРА

«Алгоритм превращает личные данные в обезличенные теги. Нейросеть видит только суть вопроса (постельное белье), что на 100% соответствует требованиям GDPR».

# Коммерческий API корпоративного уровня

Уровень 3 — Юридический. Закрытый контур обработки данных.



## Изолированный канал связи

Инфраструктура построена на базе защищенного Microsoft Azure.



## Официальный договор

Подписанный DPA (Data Processing Agreement) между Microsoft и Link AS.



## Запрет на обучение

Данные зашифрованы и не питают публичные ИИ-модели OpenAI.

### КОММЕНТАРИЙ АРХИТЕКТОРА

*«Мы не используем публичные чат-боты. Работа идет через закрытый коммерческий контур Microsoft, данные юридически защищены от стороннего использования».*

# Сертифицированные норвежские провайдеры

Локализация данных. Физическое хранение данных внутри ЕС/Норвегии.

- ✓ **Свобода выбора хостинга:** Интеграция с любым сертифицированным провайдером Норвегии.
- ✓ **Юридическая чистота:** Гарантированные документы о секретности данных и соответствии GDPR.
- ✓ **Полное сопровождение:** Техническая интеграция под строгим контролем юристов Link AS.



**Data hosted in Norway**

## КОММЕНТАРИЙ АРХИТЕКТОРА

*«Я абсолютно гибок в выборе инфраструктуры. Серверы и хранилища будут расположены строго в юрисдикции Норвегии под контролем вашей компании».*

# Контроль над размещением системы

Уровень 4 — Инфраструктурный. Три варианта интеграции под стандарты ИТ-отдела.



**Демо-режим:** Текущий статус работы платформы для тестов.



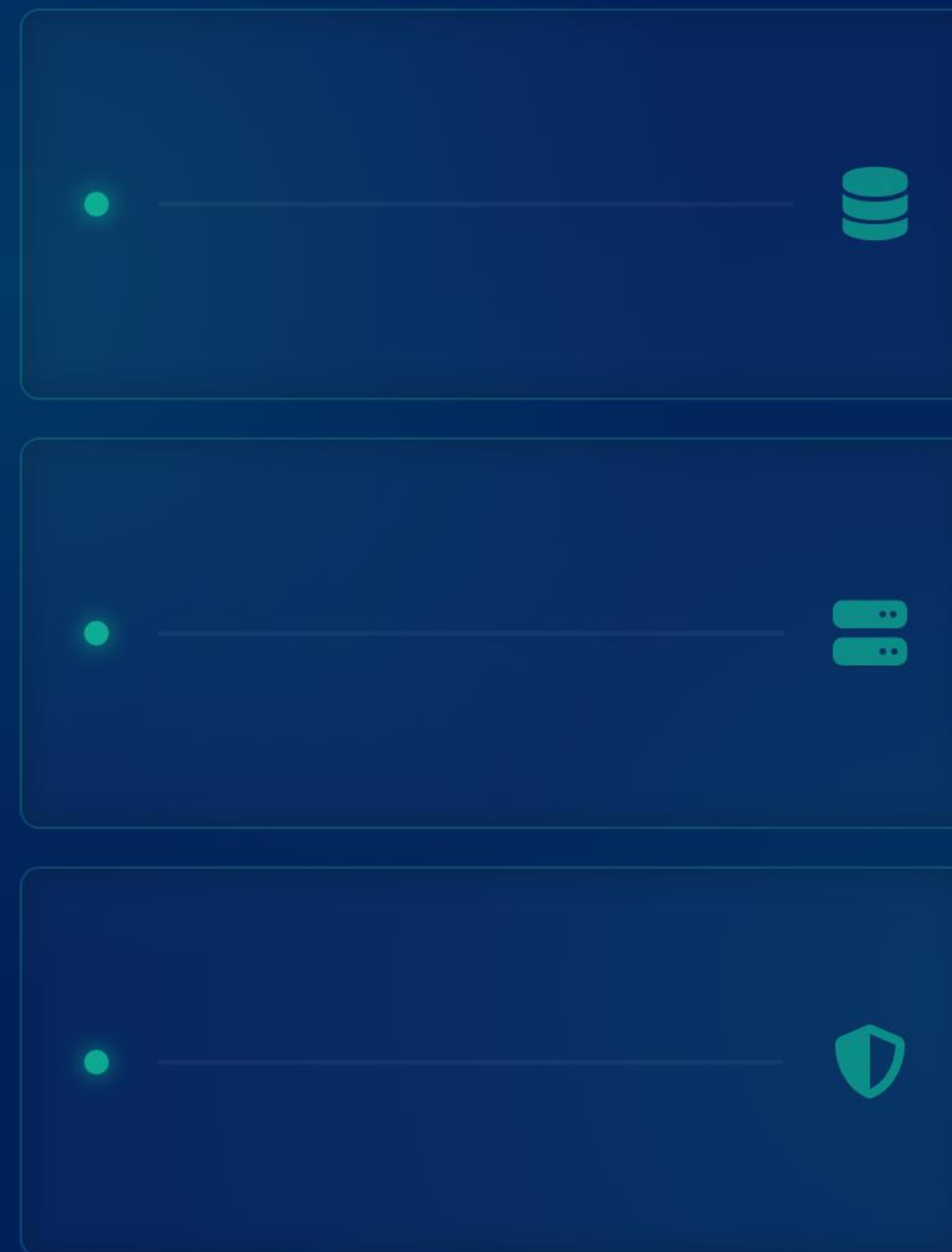
**Вариант А:** Защищенное облако в Норвегии (протоколы SSL/TLS).



**Вариант Б:** Локальный сервер (On-Premises) — полная изоляция внутри периметра Link AS.

## КОММЕНТАРИЙ АРХИТЕКТОРА

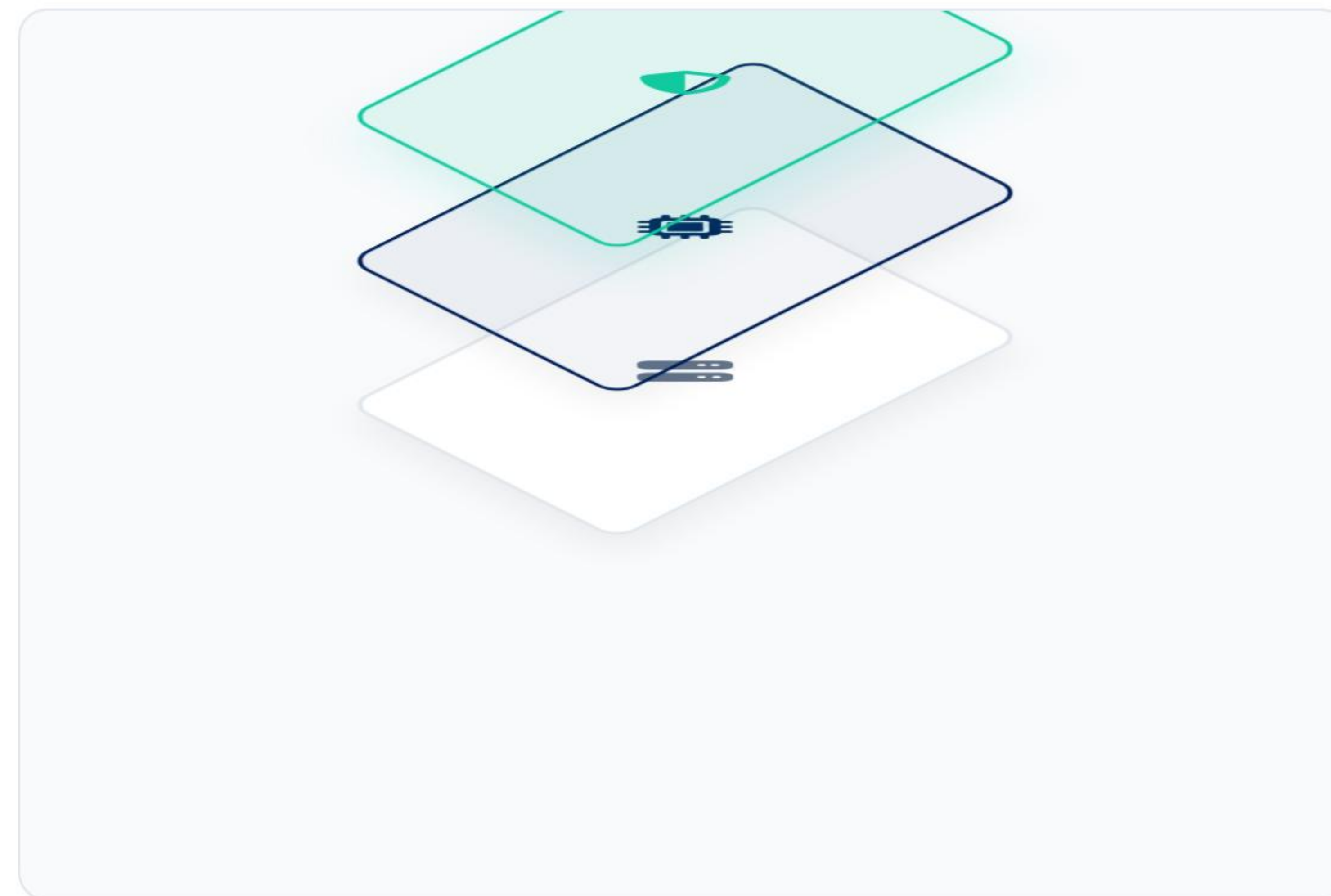
*«Я даю ИТ-специалистам полную свободу выбора. Мы можем перенести проект на ваши внутренние серверы, и тогда данные никогда не покинут периметр Link AS».*



# Эволюция безопасности

Архитектурный конструктор. Прогрессивное масштабирование защиты.

-  **Базовый MVP:** 4 уровней защиты достаточно для безопасной и анонимной помощи.
-  **Модульная архитектура:** Система собирается как безопасный ИТ-конструктор.
-  **Параллельная разработка:** Усиление безопасности синхронно с новыми функциями.



## КОММЕНТАРИЙ АРХИТЕКТОРА

*«Проект — это конструктор. При внедрении новых фич (например, личных кабинетов) протоколы защиты будут разрабатываться параллельно и контролироваться вашим ИТ-департаментом».*