

УТВЕРЖДАЮ
Генеральный директор

Е.В. Ёрхов

«22» июня 2026 г.



ООО «АЙ ЭКС АЙ ЛАБОРАТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

(ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS)

ФУНКЦИОНАЛЬНЫЕ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ

МОСКВА 2026 г.

Име. № подл.	Подп. и дата	Взам. инв. №	Име. № дубл.	Подп. дата

АННОТАЦИЯ

Настоящий документ разработан в рамках исполнения требований Постановления Правительства Российской Федерации от 28.12.2022 N 2461 и содержит описание функциональных и технических характеристик ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS.

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS - встроенное системное решение для локального управления разрешениями мобильных приложений по доступу к сети, датчикам, аппаратными функциям мобильных устройствам линейки IXIUS (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD), работающих под управлением ОС IXIOS v.13 и выше (отечественная сборка на базе открытого кода Android, AOSP, без сервисов Google и скрытой телеметрии). Элемент экосистемы IXIUS.

Состоит из встроенных в мобильную операционную систему IXIOS сервисов, мобильного приложения.

Реализует следующий ключевой функционал:

- Управление аппаратными функциями мобильных устройств. Гарантированное отключение/включение (камера, микрофон, GPS, Wi-Fi, Bluetooth, 2/3/4G и т.д.) на уровне ядра ОС.
- Управление датчиками и сетевым доступом на уровне отдельного приложения.
- Контроль съемных носителей, управление USB-портом.
- Управление геолокацией, определение местонахождения устройства.

Центр конфиденциальности позволяет эффективно управлять мобильными ресурсами, минимизировать риски утечки данных и обеспечивать высокий уровень информационной безопасности.

Архитектура Центра конфиденциальности IXIUS представляет собой многоуровневую систему, обеспечивающую изоляцию пользовательских данных и аппаратное управление ресурсами мобильного устройства.

Клиентская часть включает встроенные в операционную систему сервисы и приложение Центр конфиденциальности работающие на мобильных устройствах IXIUS под управлением ОС IXIOS v.13 и выше.

По дп . да та		<ul style="list-style-type: none">• Контроль съемных носителей, управление USB-портом.• Управление геолокацией, определение местонахождения устройства. <p>Центр конфиденциальности позволяет эффективно управлять мобильными ресурсами, минимизировать риски утечки данных и обеспечивать высокий уровень информационной безопасности.</p>				
Ин в. № ду бл		<p>Архитектура Центра конфиденциальности IXIUS представляет собой многоуровневую систему, обеспечивающую изоляцию пользовательских данных и аппаратное управление ресурсами мобильного устройства.</p>				
Вз ам . ин в. №		<p>Клиентская часть включает встроенные в операционную систему сервисы и приложение Центр конфиденциальности работающие на мобильных устройствах IXIUS под управлением ОС IXIOS v.13 и выше.</p>				
По дп . и да та						
Ин в. № по дл						
Изм.	Лист	№ докум.	Подп.	Дата	ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	Лист
						2

ВВЕДЕНИЕ	5
1.1 Область применения документа	5
1.2 Требования к уровню подготовки персонала	5
1.3 Общие сведения о программном обеспечении	5
2 Функциональные характеристики ПО	7
3 Технические характеристики ПО	10
Лист регистрации изменений	12

По дп · да та							
Ин в. № ду бл							
Вз ам · ин в. №							
По дп · и да та							
Ин в. № по дл							
						ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	Лист
							3
Изм.	Лист	№ докум.	Подп.	Дата			

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Определение понятия
Система/ЦЕНТР БЕЗОПАСНОСТИ IXIUS	Решение для локального управления разрешениями мобильных приложений по доступу к сети и датчикам мобильных устройств, аппаратными функциями мобильными устройствами IXIUS.
ОС IXIOS	Операционная система для линейки мобильных устройств компании IXI (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD).
IXIUS	Экосистема IXIUS
Kernel Security Layer	Ядро ОС IXIOS с расширенными механизмами безопасности, специализированный уровень безопасности, обеспечивающий принудительное исполнение политик безопасности.
Линейка мобильных устройств IXIUS	(WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD)
UID	User Identifier - уникальный номер, который система присваивает каждому зарегистрированному пользователю.
eBPF	Extended Berkeley Packet Filter - расширенный фильтр пакетов Беркли
HAL	Hardware Abstraction Layer - слой абстракции оборудования.
LSM	Фреймворк безопасности в ядре ОС, позволяющий использовать различные модели контроля доступа.
AOSP	Android Open Source Project - проект с открытым исходным кодом для создания операционной системы
TEE	Trusted Execution Environment - изолированная и защищенная аппаратными средствами область основного процессора
SOC	Security Operations Center - центр мониторинга безопасности, решает задачи кибербезопасности или аппаратного обеспечения
Netfilter	Базовый программный каркас (фреймворк) и механизм внутри ядра ОС , отвечающий за перехват, фильтрацию и модификацию сетевых пакетов.
ИБ	Информационная безопасность
ОС	Операционная система
ПО	Программное обеспечение
IXI	ООО «АЙ ЭКС АЙ ЛАБОРАТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ»

По
дп
да
та

Ин
в.
№
ду
бл

Вз
ам
ин
в.
№

По
дп
и
да
та

Ин
в.
№
по
дл

Изм.	Лист	№ докум.	Подп.	Дата

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

Лист

4

ВВЕДЕНИЕ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА

В настоящем документе рассматривается описание функциональных и технических характеристик ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS.

1.2 ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПЕРСОНАЛА

Описание рассчитано на специалистов, имеющих навыки работы по разработке и развертыванию мобильных операционных систем, созданию мобильных приложений для операционной системы ОС IXIOS v.13, разбирающихся в схемотехнике мобильных устройств, принципах построения решений для локального управления доступом к сети и датчикам мобильных устройств на уровне драйверов ядра ОС.

1.3 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS структурная часть экосистемы IXIUS, решение для локального управления разрешениями мобильных приложений по доступу к сети датчикам и аппаратным функциям мобильных устройств линейки IXIUS.

Комплексное решение, встроенное в мобильную ОС IXIOS. Обеспечивает гарантированное управление доступом приложений и системы к аппаратным ресурсам на уровне ядра ОС.

Система построена по гибридной многоуровневой архитектуре.

Ключевое отличие архитектуры — перенос механизмов вызова с уровня приложений на уровень ядра и аппаратных драйверов, что обеспечивает высокий уровень доверия и устойчивость к обходу ограничений.

Основной функционал:

- управление разрешениями для каждого установленного приложения;
- быстрые профили (совещание, режим поездки, публичная сеть и т.д.) полное отключение доступа всем приложениям к датчикам, системным сервисам, сетевым интерфейсам;
- гарантированное управление аппаратными функциями на уровне ядра ОС:
 - камера (фронтальная, основная);
 - микрофон, аудиокодек;
 - GPS / GNSS модуль;
 - Wi-Fi, Bluetooth, NFC;
 - 2G / 3G / 4G LTE / 5G;

По дп . да та	
Ин в. № ду бл	
Вз ам . ин в. №	
По дп . и да та	
Ин в. № по дл	

					ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	Лист 5
Изм.	Лист	№ докум.	Подп.	Дата		

2 ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПО

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS является частью экосистемы IXIUS.

В ПО реализован системный подход к контролю приватности, выходящий за рамки стандартных разрешений. Функциональность достигается глубокой интеграцией с операционной системой IXIOS v13 и выше, построенной на «очищенной» от сервисов Google и телеметрии версии AOSP (отечественная сборка на базе открытого кода AOSP).

Функциональная архитектура ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS реализует управление политиками конфиденциальности и контроль доступа приложений к аппаратным функциям, датчикам и сетевым ресурсам мобильных устройств. Запросы пользователей и приложений обрабатываются сервисами ОС, проходят проверку на уровне контроля доступа, ядра и драйверов устройств. Политики безопасности централизованно управляются, сохраняются в защищенном хранилище и принудительно исполняются на уровне ядра ОС и оборудования, обеспечивая невозможность обхода установленных ограничений.

Реализуется принцип эшелонированной защиты: ни одно приложение не может получить доступ к аппаратным ресурсам в обход политик, установленных пользователем или администратором. Гарантия достигается совместной работой всех четырех уровней - от пользовательского интерфейса до аппаратных блокировок на уровне ядра.

Клиентская часть ПО - мобильное приложение Центр конфиденциальности, функционирующие на линейке мобильных устройств IXIUS. под управлением ОС IXIOS v.13 и выше.

Приложение является визуальным фронтом над Сервисом политик (Privacy Politic Manager) и реализует полный цикл управления в режиме реального времени. Является связующим звеном между приложением, системными сервисами ОС и модулем принудительного контроля на уровне ядра и драйверов. Взаимодействует через защищенный API и не осуществляет прямое управление оборудованием. Все команды выполняются через доверенные системные сервисы.

Центр конфиденциальности – основной интерфейс управления, предоставляющий пользователю единую точку управления аппаратными устройствами (камера, микрофон), интерфейсами связи, внешними подключениями мобильного устройства (Wi-Fi, Bluetooth, GPS, 2G/3G/4G5G, USB), сетевым доступом (Интернет, локальная сеть, беспроводные интерфейсы). Реализует гарантированное отключение доступа к аппаратным модулям через системные вызовы и драйверы.

Функционал системы реализует два уровня управления доступом:

По
дп
.
да
та

Ин
в.
№
ду
бл

Вз
ам
.
ин
в.
№

По
дп
.
и
да
та

Ин
в.
№
по
дл

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

Лист

7

Изм. Лист № докум. Подп. Дата

- **Глобальный** – отключение/включение, настройка доступа к аппаратным устройствам, интерфейсам связи, внешними подключениями мобильного устройства одновременно для всех приложений;
- **Локальный** – отключение/включение, настройка доступа к аппаратным устройствам, интерфейсам связи, внешними подключениями мобильного устройства для каждого отдельного приложения.

Установки глобального уровня доступа имеют приоритет, на уровне локального доступа (отдельного приложения) нельзя изменить установленный на глобальном уровне уровень.

Основные функциональные характеристики ПО:

➤ Пользовательский интерфейс

- интуитивно понятный интерфейс для пользователя;
- отображение состояния оборудования, статуса ключевых аппаратных модулей в реальном времени;
- единая панель управления всеми аппаратными ресурсами и политиками приложений как одно моментно для всех приложений, так и выборочно для отдельного приложения;
- принудительное отключение камеры, микрофона, GPS на аппаратном уровне;
- управление беспроводным интерфейсом, отключение/включение Wi-Fi, Bluetooth, NFC, модемы сотовой связи (2G/3G/4G5G);
- контроль USB-порта, блокировка передачи данных;
- запрет монтирования SD-карт, контроль доступа к внешним накопителям;
- настройка и управление сетями Wi-Fi – только разрешенные сети;
- управление сетевым доступом приложений к сети Интернет;

➤ Контроль доступа

- проверка каждого запроса приложения к защищаемым ресурсам;
- фильтрация сетевого доступа по UID приложения, блокировка/разрешение всего сетевого трафика для конкретного приложения;
- блокировка по протоколам – раздельное управление TCP, UDP, ICMP, RAW-сокеты;
- контроль доступа к сети, драйверам датчиков и аппаратным функциям устройств;
- применение пользовательских и корпоративных политик безопасности;
- разрешение, ограничение или блокировка доступа в режиме реального времени;
- передача решений на уровень системных сервисов, ядра и драйверов ОС;
- обеспечение принудительного исполнения политик безопасности независимо от уровня.

По дп · да та	
Ин в. № ду бл	
Вз ам · ин в. №	
По дп · и да та	
Ин в. № по дл	

					ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	Лист
						8
Изм.	Лист	№ докум.	Подп.	Дата		

➤ Системный уровень

- предоставление API для управления устройствами и системными ресурсами;
- управление состоянием аппаратных модулей и интерфейсов;
- взаимодействие с драйверами и аппаратным абстрактным уровнем (HAL);
- сбор телеметрии и системных событий;
- журналирование операций и событий безопасности;
- контроль доступа к аппаратным устройствам и системным ресурсам;
- принудительное применение политик безопасности на уровне ядра и драйверов;
- защита от эскалации привилегий;
- контроль системных вызовов и меж процессного взаимодействия;
- управление доступом к сети, датчикам и аппаратным функциям;
- защита от обхода политик безопасности и повышения привилегий;
- аудит и регистрация событий безопасности;
- обеспечение целостности и доверенного состояния системы.

Ключевые особенности функциональных характеристик

- разделение ответственности - сервисы пользовательского пространства управляют политиками, и их принудительным применением;
- невозможность обхода - LSM и eBPF срабатывают до вызова драйверов;
- производительность - проверка в ядре за микросекунды;
- динамическое применение сетевых и файловых политик без перезагрузки ядра;
- защита коммуникаций - Netlink-канал защищён от подмены, eBPF-карты доступны только на чтение из ядра;
- целостность- политики хранятся в Secure Storage (TEE), подписаны криптографически;

По
дп
·
да
та

Ин
в.
№
ду
бл

Вз
ам
·
ин
в.
№

По
дп
·
и
да
та

Ин
в.
№
по
дл

Изм.	Лист	№ докум.	Подп.	Дата

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

Лист
9

3 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПО

Аппаратная платформа – линейка защищенных мобильных устройств компании IXI (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD) с базовой операционной системой IXIOS v.13 и выше с предустановленным пакетом лицензионных приложений компании IXI.

Базовая операционная систем ОС IXIOS, построенная на «очищенной» от сервисов Google и телеметрии версии AOSP, управляющее аппаратными и программными ресурсами мобильных устройств на платформе Mediatek. Исходные коды AOSP переработаны, сервисы Google (GMS) удалены, добавлены сервисы единой аутентификации для приложений в экосистеме IXIUS, контроль целостности, сервисы, обеспечивающие защиту устройства от анализа, изменён механизм блокировки/разблокировки устройства. Из системы удалены все программные закладки и скрытый функционал производителей SoC (включая MediaTek), связанный со сбором данных пользователей.

Ядро операционной системы модифицировано с использованием техник Linux Kernel Hardening для укрепления безопасности, ограничения доступа к системным ресурсам и защиты от несанкционированного доступа.

В ОС IXIOS применены дополнительные механизмы защиты ядра Linux (kernel hardening) и переработаны политики SELinux.

Ключевое отличие архитектуры ЦЕНТРА КОНФИДЕНЦИАЛЬНОСТИ IXIUS — перенос механизмов вызова с уровня приложений на уровень ядра и аппаратных драйверов, что обеспечивает высокий уровень доверия и устойчивость к обходу ограничений.

Технически реализуется единая точка контроля над аппаратными интерфейсами устройства, позволяя блокировать обращение приложений к датчикам на системном уровне.

При отключении соответствующих функций доступ к аппаратным средствам ограничивается средствами операционной системы, что исключает их использование прикладным программным обеспечением до повторного включения пользователем.

- Модули программного обеспечения разработаны с использованием инструментария:
- Android Studio Narwhal 4 Feature Drop | 2025.1.4 (Лицензия на основе Apache License 2.0);
 - Система контроля версий GIT v.2.43.0 (GPL).

Языки программирования:

- Java 17;

Список используемых библиотек и лицензий:

- OkHttp v.4.9.3 (Лицензия на основе Apache License 2.0);
- Gson v.2.10.1 (Лицензия на основе Apache License 2.0);

По
дп
·
да
та

Ин
в.
№
ДУ
бл

Вз
ам
·
ин
в.
№

По
дп
·
и
да
та

Ин
в.
№
по
дл

Изм.	Лист	№ докум.	Подп.	Дата

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

Лист
10

- AndroidX Core KTX v.1.16.0 (Лицензия на основе Apache License 2.0);
- AndroidX AppCompat v.1.7.1 (Лицензия на основе Apache License 2.0);
- Material Components for Android v.1.12.0 (Лицензия на основе Apache License 2.0);
- AndroidX Navigation UI v.2.9.3 (Лицензия на основе Apache License 2.0);
- AndroidX Navigation Fragment v.2.9.3 (Лицензия на основе Apache License 2.0);
- AndroidX Room Common JVM v.2.8.4 (Лицензия на основе Apache License 2.0);
- AndroidX Room Runtime v.2.8.4 (Лицензия на основе Apache License 2.0);
- AndroidX Room Compiler v.2.8.4 (Лицензия на основе Apache License 2.0);
- JUnit v.4.13.2 (лицензия Eclipse Public License 1.0 (EPL-1.0)).
- AndroidX JUnit v.1.2.1 (Лицензия на основе Apache License 2.0);
- AndroidX Espresso Core v.3.6.1 (Лицензия на основе Apache License 2.0).

[illegible]

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]

По дп . да та	Ин в. № ду бл	Вз ам . ин в. №	По дп . и да та	Ин в. № по дл
------------------------	---------------------------	-----------------------------	-----------------------------	---------------------------