

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)

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

МОСКВА 2026 г.

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

АННОТАЦИЯ

Настоящий документ содержит Руководство пользователя (РП) программного обеспечения ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS - решение для локального управления разрешениями мобильных приложений по доступу к сети, датчикам линейки мобильных устройств IXIUS под управлением ОС IXIOS v13 и выше. Элемент экосистемы IXIUS.

Рассматриваются основные действия по запуску, настройке и использованию, выполняемые пользователем в процессе использования ПО на мобильном устройстве.

Руководство пользователя содержит информацию о корректной эксплуатации, функциям и настройкам системы локального управления разрешениями мобильных приложений по доступу к сети, датчикам, аппаратным функциями мобильных устройств IXIUS.

Документ разработан в соответствии с:

- Техническим решением на разработку программного продукта ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS решением для локального управления разрешениями мобильных приложений по доступу к сети, датчикам, аппаратным функциям для устройств IXIUS.
- ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

Инв. № подл.	Подп. и дата				Взам. инв. №	Инв. № дубл.	Подп. дата
<p>автоматизированные системы. Автоматизированные системы. Термины и определения»;</p> <p>– ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».</p>							
					<div>ПО Центр конфиденциальности IXIUS</div> <div>Лист</div> <div>2</div>		
Изм	Лист	№ докум.	Подп.	Дата			

СОДЕРЖАНИЕ

1	Введение	5
1.1	Область применения документа	5
1.2	Требования к уровню подготовки персонала	5
1.3	Перечень эксплуатационной документации	5
2	ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	6
2.1	Общие сведения о программном обеспечении	6
2.2	Установка ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ	7
3	Основной функционал ПО	8
3.1	Общее описание	8
3.2	Функционал приложения центр безопасности	9
3.2.1	Основной экран приложения	9
3.2.2	Функционал элемента экрана меню	11
3.2.3	Меню настройки - управление доступом к Wi-Fi	12
3.2.4	Управление глобальным уровнем доступа	16
3.2.5	Управление уровнем доступа приложений	18
3.3	Рекомендации пользователям	19
Лист регистрации изменений		21

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата			ПО Центр конфиденциальности IXIUS	Лист
								3
Изм	Лист	№ докум.	Подп.	Дата				

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Определение понятия
Система/ЦЕНТР БЕЗОПАСНОСТ И IXIUS	Решение для локального управления разрешениями мобильных приложений по доступу к сети и датчикам мобильных устройств аппаратными функциями мобильными устройствами IXIUS.
ОС IXIOS v.13	Операционная система для мобильных устройств компании IXI (WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD) на базе исходного кода AOSP.
Линейка мобильных устройств IXIUS	(WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD)
IXIUS	Экосистема IXIUS
IXI	ООО «АЙ ЭКС АЙ ЛАБОРАТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ»
GPS	Global Positioning System - Система глобального позиционирования
GNSS	Global Navigation Satellite System - Глобальная навигационная спутниковая система
SSID	Service Set Identifier - имя сети
BSSID	Basic Service Set Identifier - Физический MAC-адрес передатчика Wi-Fi
ИБ	Информационная безопасность
СТП	Служба технической поддержки
ОС	Операционная система
РП	Руководство пользователя

Име. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	
Изм	Лист	№ докум.	Подп.	Дата	
ПО Центр конфиденциальности IXIUS					Лист
					4

1 ВВЕДЕНИЕ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА

Настоящий документ является руководством пользователя программного обеспечения ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS, специализированного решения для локального управления разрешениями мобильных приложений по доступу к сети, датчикам мобильных устройств IXIUS под управлением ОС IXIOS v13 и выше.

Руководство предназначено для ознакомления с основными возможностями и правилами эксплуатации.

Основные понятия, требования и правила эксплуатации, описание интерфейсов, сведения о ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS рассматриваемые в настоящем руководстве, носят общий характер. Перечень элементов системы может отличаться в зависимости от устройства и версии ОС. Описания, приведенные в данном РП, соответствуют настройкам системы по умолчанию. Изображения элементов системы приведены в качестве примеров, реальные элементы системы могут отличаться.

Под пользователем подразумевается сотрудник, который использует защищенное мобильное устройство, на котором установлено ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS.

1.2 ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ПЕРСОНАЛА

Пользователь должен иметь навыки работы с ОС семейства IXIOS (вне зависимости от архитектуры), опыт работы со стандартными элементами графического интерфейса приложений.

Для предотвращения несанкционированного доступа к системным компонентам пользователям в ОС запрещается установка и запуск встроенных программ отладки.

Пользователям запрещается производить установку нештатных программных средств, позволяющих осуществить несанкционированную модификацию системных компонент.

Пользователи должны использовать приложения из корпоративного репозитория Архива приложений.

Пользователи мобильных устройств с предустановленной системой ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS должны следовать регламентированным корпоративным стандартам информационной безопасности компании.

1.3 ПЕРЕЧЕНЬ ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ

Сведения по подробным настройкам находятся в документации производителя.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата		ПО Центр конфиденциальности IXIUS	Лист 5
Изм	Лист	№ докум.	Подп.	Дата			

2 ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

2.1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ структурная часть экосистемы IXIUS.

Решение для локального управления разрешениями мобильных приложений по доступу к сети и датчикам для мобильных устройств IXIUS (WP23, WP27, C38, P1PRO) под управлением ОС IXIOS v.13 и выше. Состоит из встроенных в мобильную операционную систему IXIOS сервисов, мобильного приложения.

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;
 - GPS / GNSS модуль;
 - Wi-Fi, Bluetooth, NFC;
 - 2G / 3G / 4G LTE / 5G;
- управление доступом к сетевым интерфейсам;
- управление доступом к датчикам и системным сервисам;
- управлением геолокацией;
- контролем внешних подключений и съемных носителей.

Система реализуется как совокупность:

- встроенных сервисов ОС IXIOS;
- сервисов уровня ядра;
- системных драйверов;
- пользовательского мобильного приложения «Центр конфиденциальности».

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.

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

Полностью отечественная разработка. По состоянию на апрель 2026 года не имеет отечественных аналогов! Зарегистрирована в РОСПАТЕНТЕ (Федеральная служба по интеллектуальной собственности).

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

Изм	Лист	№ докум.	Подп.	Дата

2.2 **Установка ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ**

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS, как составная часть экосистемы IXIUS, поставляется Заказчику в комплекте, предустановленной на мобильные устройства IXIUS, в виде приложения и является его неотъемлемой частью. Дистрибутивы ПО отдельно не поставляются и недоступны для получения конечным пользователям.

Установка ПО проводится индивидуально согласно Договора с Заказчиком.

Инв.№ подл.	Подп. и дата				Взам. инв. №				Инв.№ дубл.				Подп. дата			
					ПО Центр конфиденциальности IXIUS										Лист	
															7	
Изм	Лист	№ докум.	Подп.	Дата												

3 ОСНОВНОЙ ФУНКЦИОНАЛ ПО

3.1 ОБЩЕЕ ОПИСАНИЕ

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS обеспечивает управление политиками конфиденциальности и контроль доступа приложений к аппаратным функциям, датчикам и сетевым ресурсам устройства. 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.

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

Приложение является визуальным фронтендом 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.

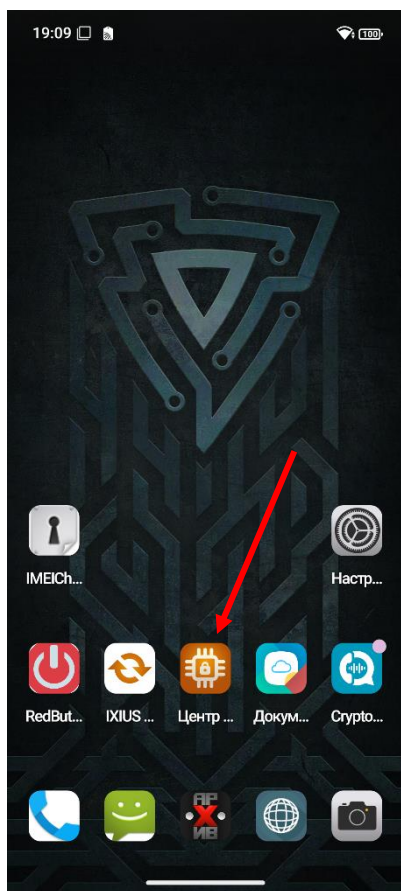
Функционал системы реализует два уровня управления доступом:

- **Глобальный** – отключение, настройка доступа к аппаратным устройствам, интерфейсам связи, внешними подключениями мобильного устройства одномоментно для всех приложений;
- **Локальный** – отключение, 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.

3.2 ФУНКЦИОНАЛ ПРИЛОЖЕНИЯ ЦЕНТР БЕЗОПАСНОСТИ

3.2.1 Основной экран приложения



Использование приложения реализовано для защищенного режима мобильного телефона

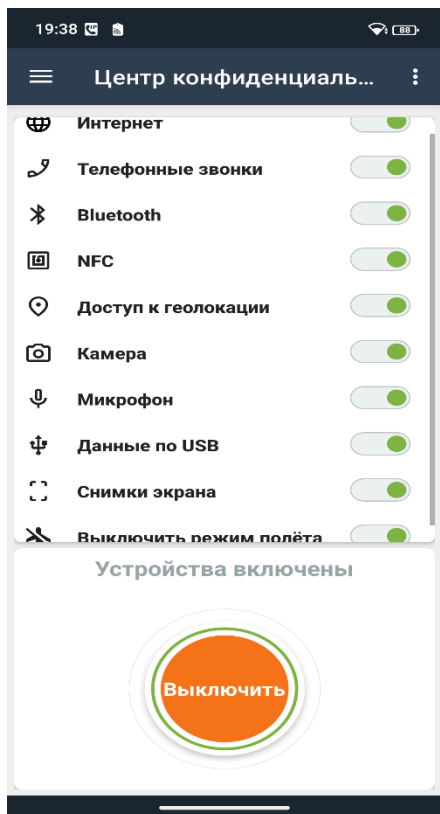
Процесс блокировки, настройки приложений запускается в ручном режиме пользователем в произвольный момент времени.

Основной экран мобильного телефона приведен на рисунке.

Стрелкой показано приложение Центр конфиденциальности.

Приложение также находится в общем экране приложений мобильного устройства.

Для запуска процесса синхронизации необходимо активировать приложение. После активации переходим к основному экрану.



Основной экран включает ряд элементов:

✓ Панель переключателей

(В режиме отключенных расширенных настроек сети)

✓ Кнопка глобального отключения
“Выключить”

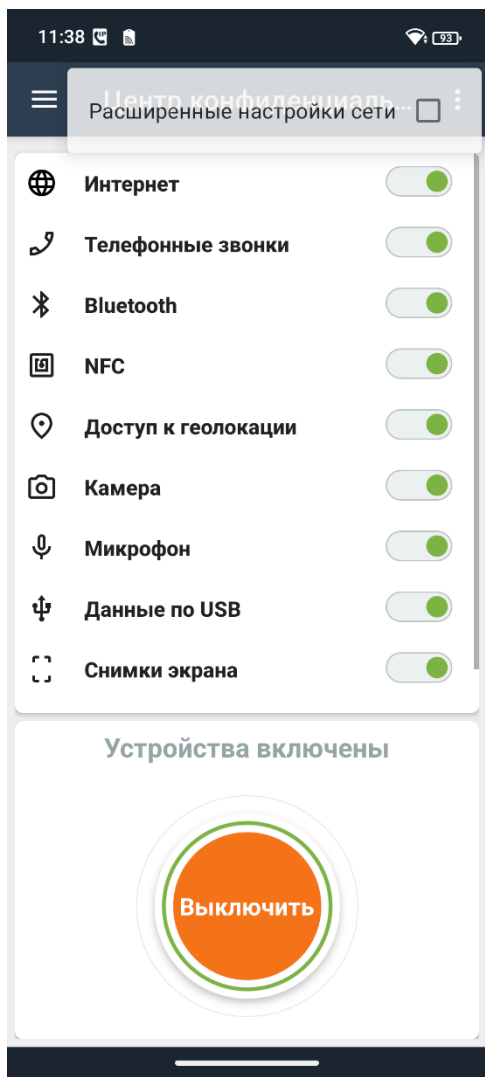
В верхней части экрана расположены элементы управления

✓ В левой части – *четыре черточки* – **меню**

(Элементы меню и функционал рассмотрены далее)

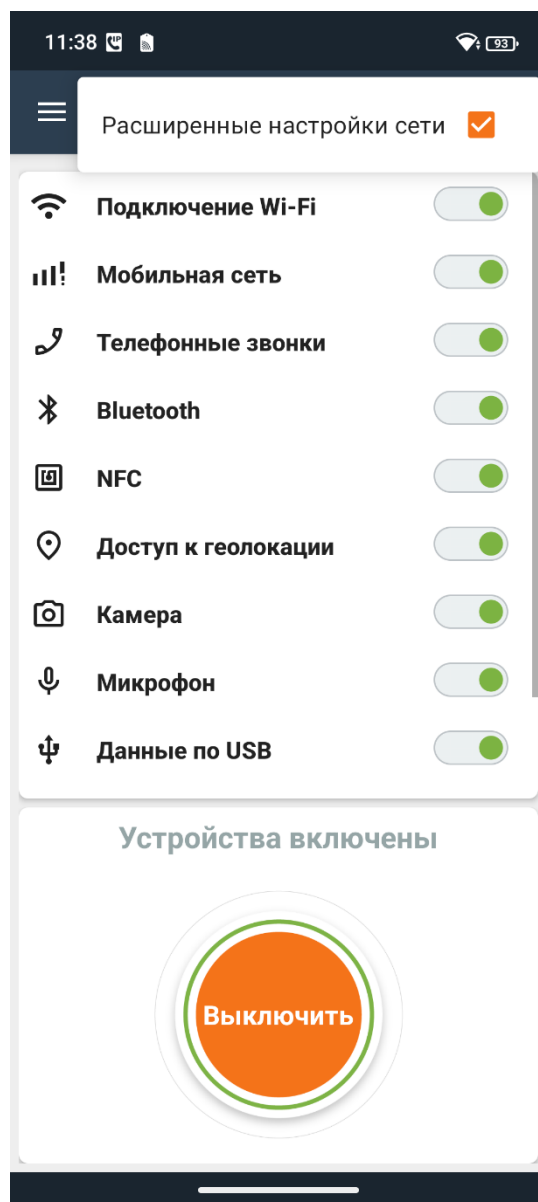
✓ В правой части экрана - *три точки* – управление расширенных настроек

Активация элемента открывает экран функционала дополнительных настроек.



На экране появляется чек-бокс – “Расширенные настройки сети” в состоянии *Неотмеченное*.

Перевод чек-бокса в состояние *Отмеченное* включает в панель управления дополнительные элементы Панели переключателей – *Подключение Wi-Fi* и *Мобильная сеть* и убирает элемент – *Интернет*.



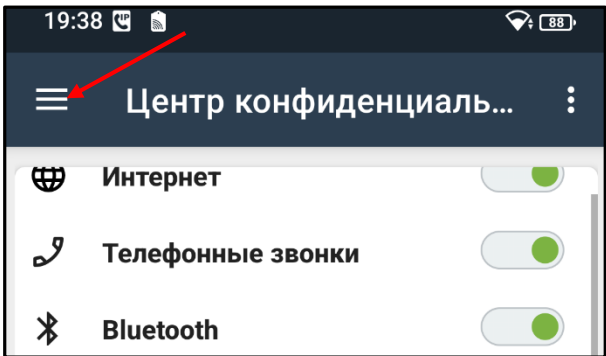
Элементы *Панели переключателей*

- *Снимки экрана;*
- *Выключить режим полета;*

перемещены ниже по экрану и скрыты за элементом *Выключить*.

Для просмотра и использования этих элементов необходимо сместить *Панель переключателей* вверх по экрану

3.2.2 Функционал элемента экрана меню



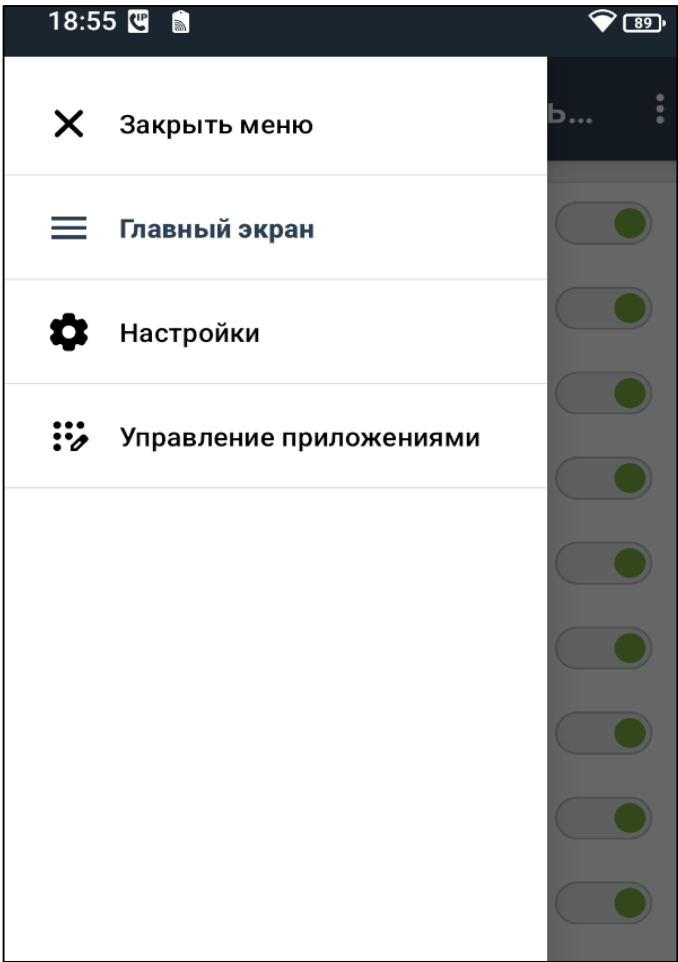
Для перехода к экрану меню необходимо активировать в левой части элемент *четыре полосы*.

Состав элемента меню приведен на следующем рисунке

Экран меню включает элементы со следующим функционалом.

- ✓ *Заккрыть меню*.
- ✓ *Главный экран* – перейти на главный экран.
- ✓ *Настройки* – управление подключением Wi-Fi сетей.
- ✓ *Управление приложениями* – настройки доступа приложений к аппаратным функциям, датчикам и сетевым ресурсам устройства

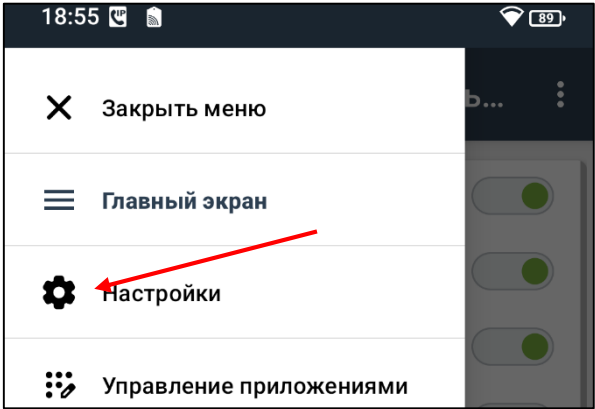
Детально функционал *Настройки* и *Управление* приложениями рассмотрен в отдельных параграфах.



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

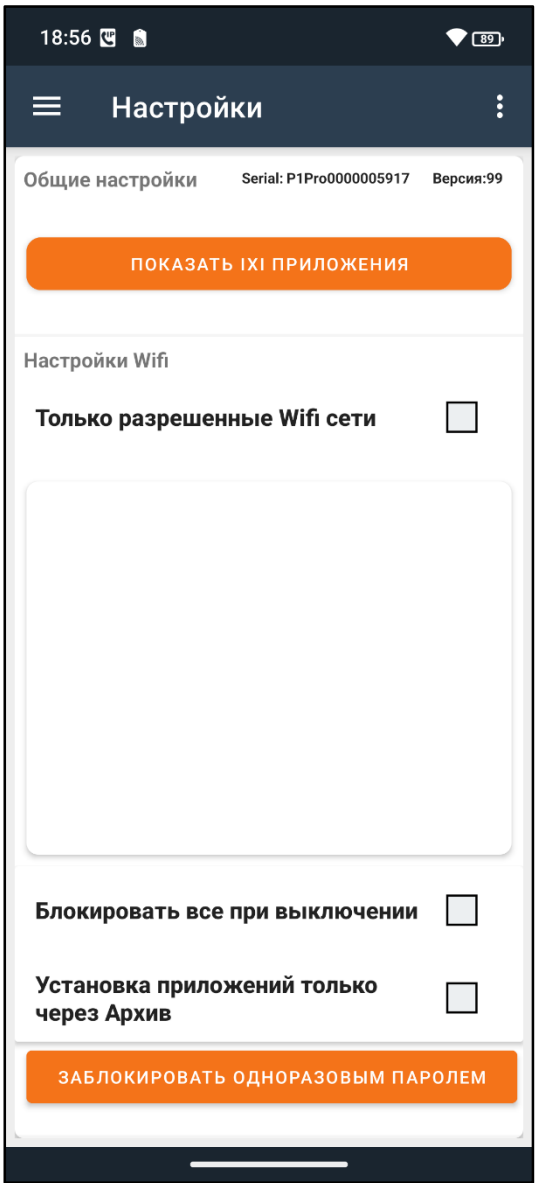
Изм	Лист	№ докум.	Подп.	Дата

3.2.3 Меню настройки - управление доступом к Wi-Fi



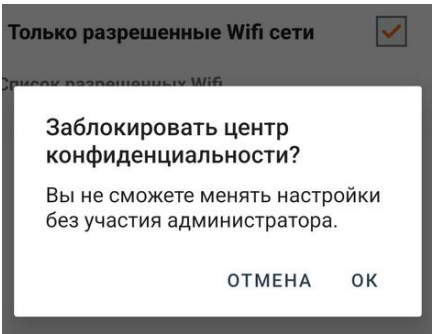
Для перехода к настройкам Wi-Fi необходимо активировать элемент *Настройки*.

Экран *настроек* приведен на следующем рисунке



Экран настроек Wi-Fi включает ряд функциональных элементов:

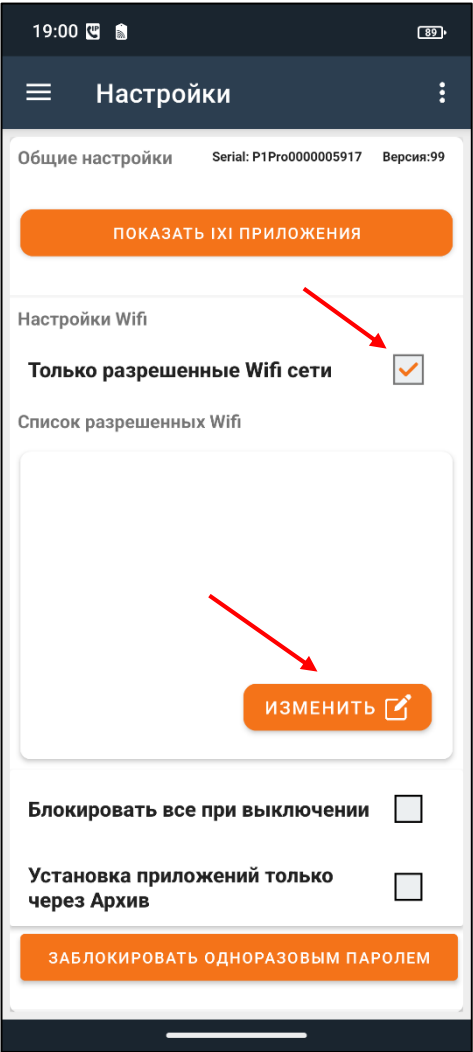
- ✓ ПОКАЗАТЬ/СКРЫТЬ IXI ПРИЛОЖЕНИЯ – переключение активацией элемента. Показывается/скрывается от пользователя приложение CloudSync и Авторизатор.
- ✓ ТОЛЬКО РАЗРЕШЕННЫЕ WI-FI СЕТИ- чек-бокс, состояния Неотмеченное/Отмеченное(галочка). Отмеченное открывает экран настройки Wi-Fi сети.
- ✓ БЛОКИРОВАТЬ ВСЕ ПРИ ВЫКЛЮЧЕНИИ – защита от потенциальных атак на подбор пароля
- ✓ УСТАНОВКА ПРИЛОЖЕНИЙ ТОЛЬКО ЧЕРЕЗ АРХИВ – отметка чек-бокса “галочка” запрещает установку сторонних приложений. Приложения могут быть установлены только из “Архива приложений”
- ✓ ЗАБЛОКИРОВАТЬ ОДНОРАЗОВЫМ ПАРОЛЕМ – позволяет установить одноразовый пароль на изменение настроек. При активации появляется экран для перехода к вводу пароля ОК/ОТМЕНА.



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

Изм	Лист	№ докум.	Подп.	Дата

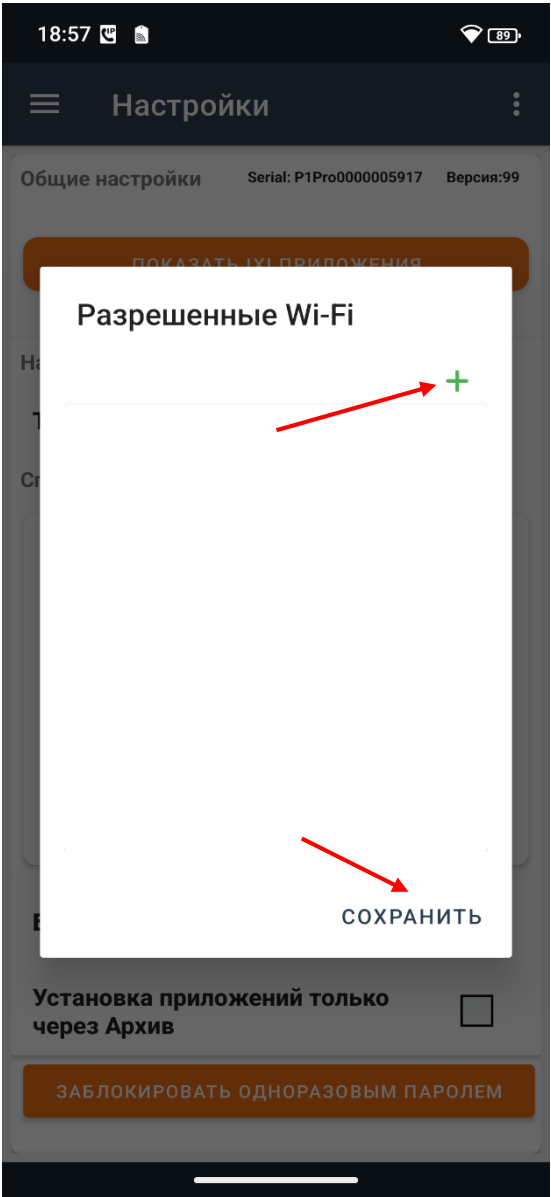
При активации чек-бокса *ТОЛЬКО РАЗРЕШЕННЫЕ Wi-Fi СЕТИ* переходим к экрану:



Отображаются только разрешенные Wi-Fi сети.

Для ввода, корректировки и удаления, разрешенных Wi-Fi сетей необходимо активировать элемент *Изменить*.

Переходим к экрану



Отображаются ранее введенные только разрешенные Wi-Fi сети.

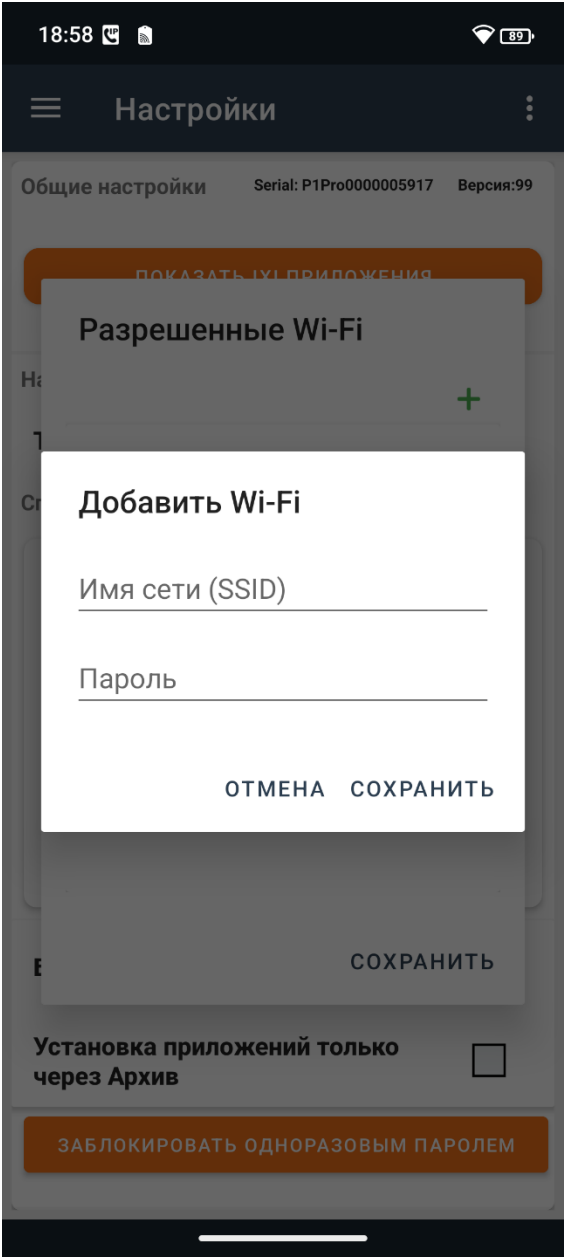
По окончании изменений для их сохранения активируется *СОХРАНИТЬ*.

Для ввода, корректировки и удаления, разрешенных Wi-Fi сетей необходимо активировать элемент +.

Переходим к экрану, показанному ниже

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

Изм	Лист	№ докум.	Подп.	Дата

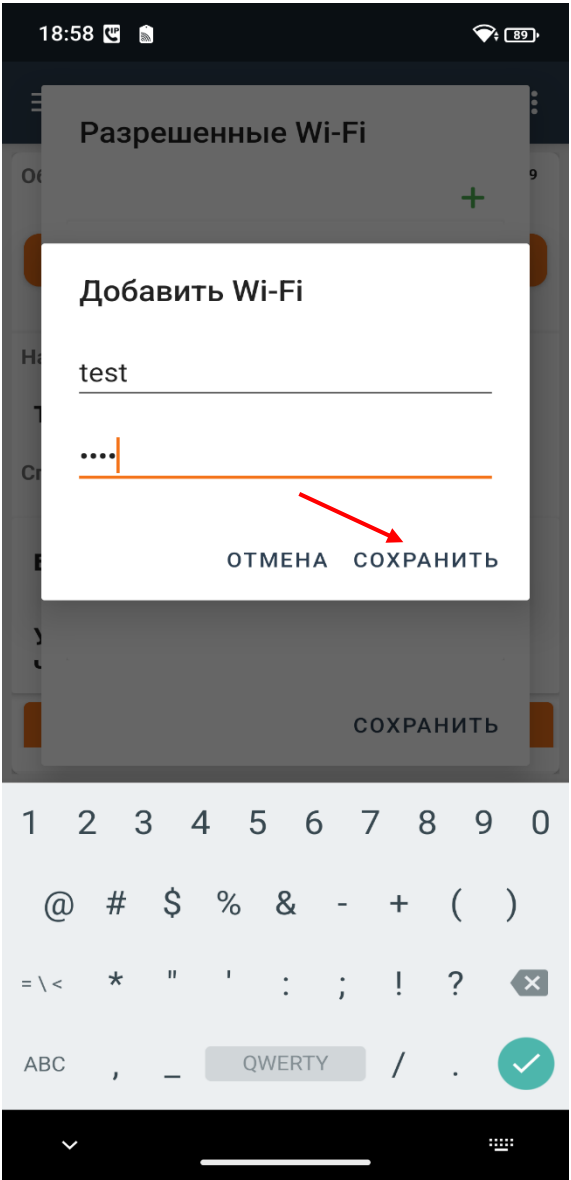


Вводим данные.

Вводится имя сети (SSID)

Пароль

Тестовый пример приведен ниже

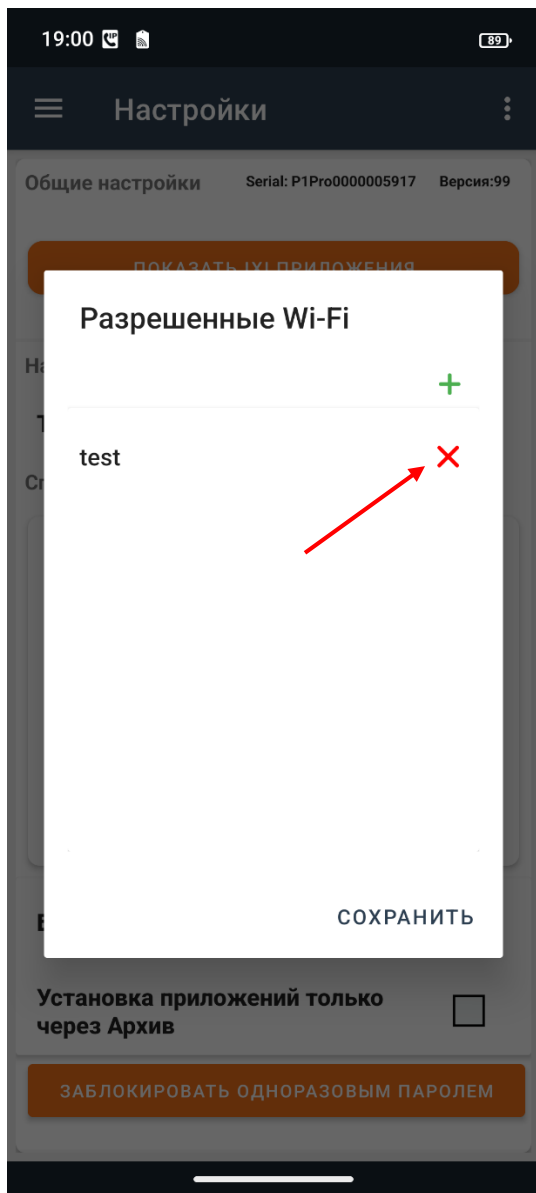


После ввода данных активируем
СОХРАНИТЬ

Переходим к экрану показанному
ниже

Имя № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата

Изм.	Лист	№ докум.	Подп.	Дата



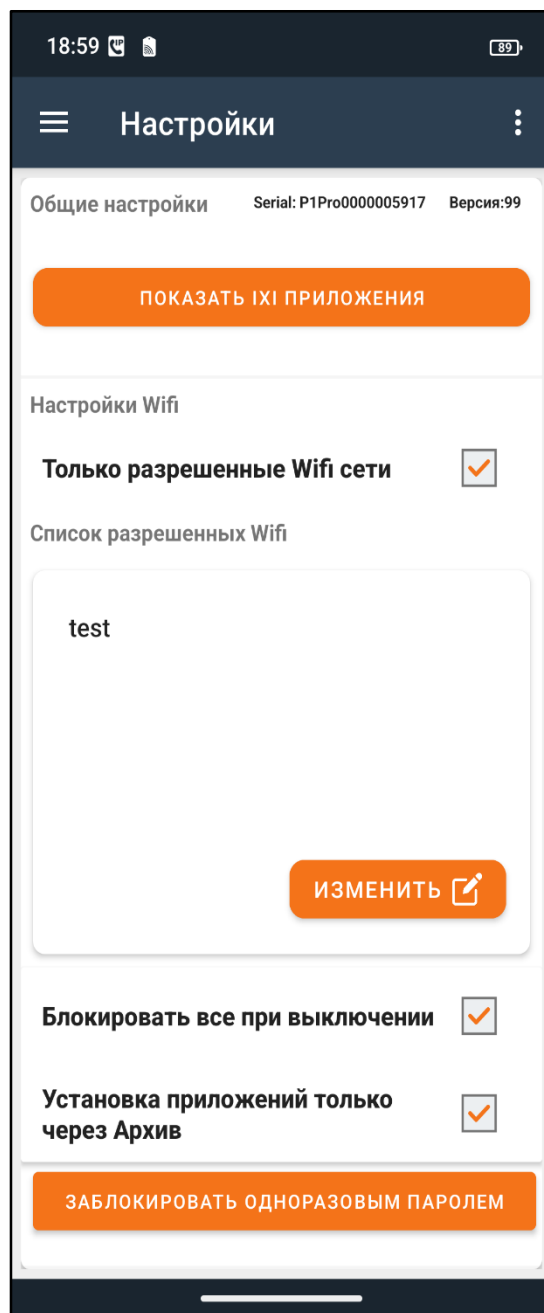
На левом экране отобразилась введенная сеть.

Также отображился элемент удаления сети из списка разрешенных.

Для сохранения проведенных изменений, ввода или удаления сети из списка активируем

СОХРАНИТЬ

Переходим к экрану *Настройки*



Включение опции *Только разрешенные Wi-Fi сети* устанавливает правила подключения:

- Устанавливает жесткую блокировку по SSID/BSSID (уникальное имя/адрес роутера);
- Устройство автоматически пропускает любые публичные точки доступа (метро, кафе и т.д.);
- Разрешенные сети определяются нормами безопасности корпораций, компаний.

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

Изм	Лист	№ докум.	Подп.	Дата

3.2.4 Управление глобальным уровнем доступа

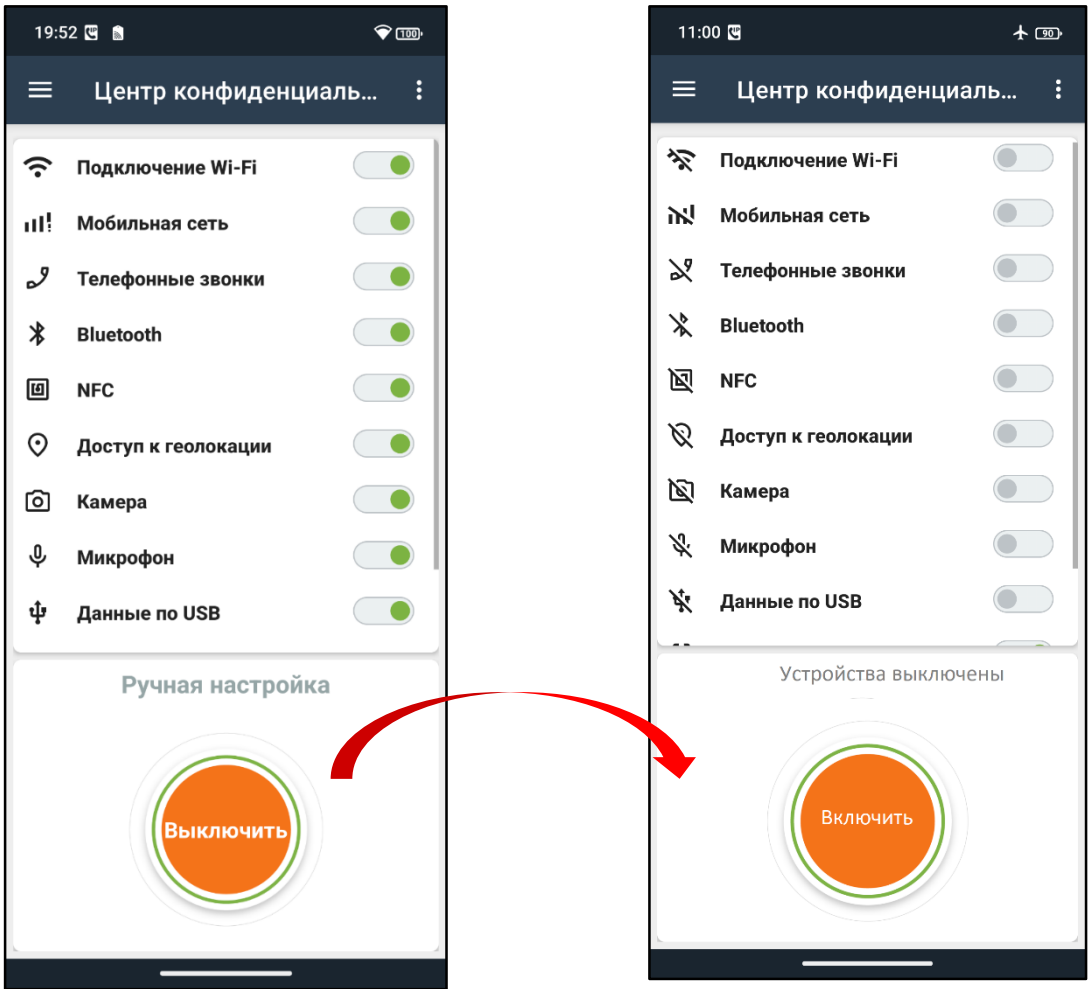
Архитектура Центра конфиденциальности IXIUS реализует принцип эшелонированной защиты: ни одно приложение не может получить доступ к аппаратным ресурсам в обход политик, установленных пользователем или администратором. Гарантия достигается совместной работой всех трёх уровней - от пользовательского интерфейса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

На *глобальном уровне* реализовано отключение, настройка доступа к аппаратным устройствам, интерфейсам связи, внешними подключениями мобильного устройства пользователем/администратором одновременно для всех приложений.

Рассмотрим детально функционал глобального управления доступом. Основной интерфейс управления разрешениями, предоставляющий пользователю единую точку управления всеми аппаратными ресурсами и политиками приложений приведен на рисунке. Реализовано два уровня управления разрешениями *для всех* приложений:

- одномоментное отключение аппаратных ресурсов мобильного устройства;
- гранулированное (выборочное) отключение аппаратных ресурсов.

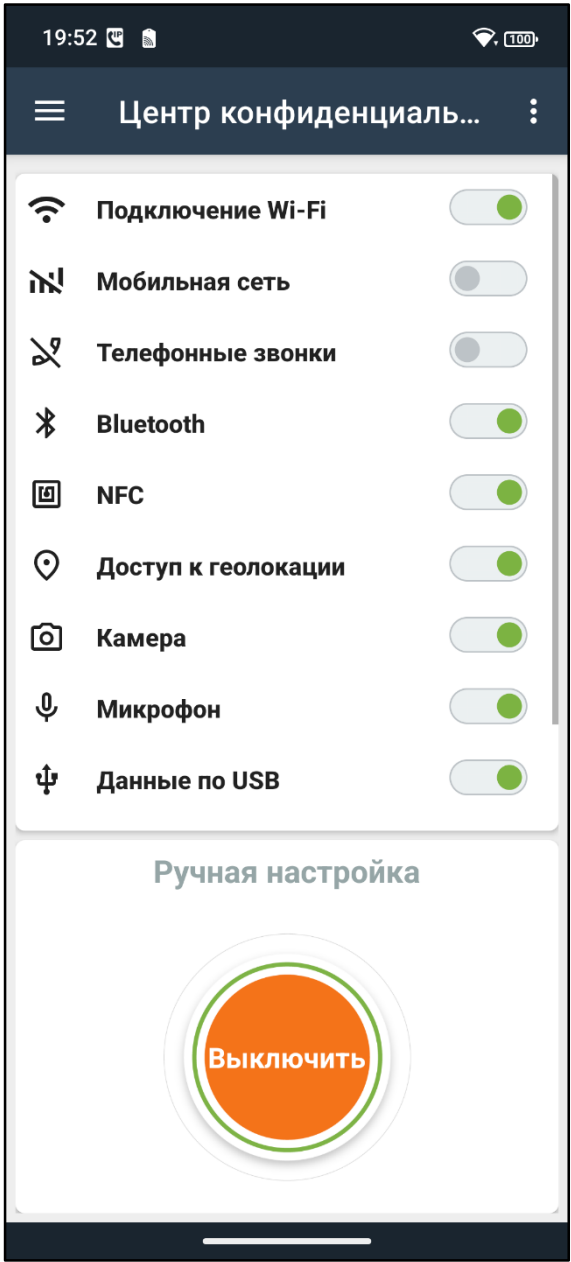
Для одномоментного отключения необходимо активировать элемент интерфейса “**Выключить**”. Результат приведен на правом рисунке.



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

Изм	Лист	№ докум.	Подп.	Дата

Примечание: ряд переключателей (*Снимки экрана, Выключить режим полета*) скрыты за панелями элемента **Выключить, Включить**. Для их просмотра достаточно переместить **Панель переключателей** вверх.



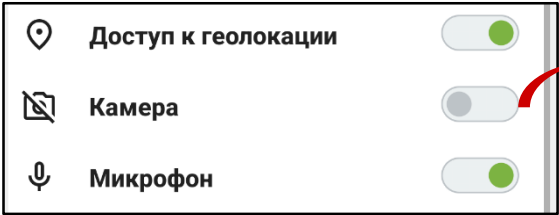
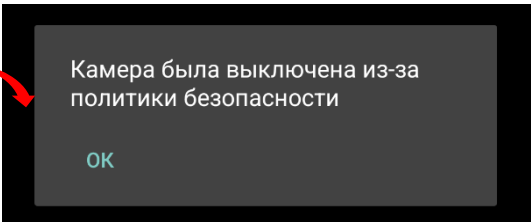
Гранулированное (выборочное) отключение доступа **всех** приложений к отдельным аппаратным ресурсам, реализовано как отключение отдельных элементов на Панели переключателей.

Результаты отключения приведены на рисунке.

Для включения необходимо перевести переключатель в положение “Вкл.”

Примечание:
Отключение доступа к отдельным элементам на **Панели Переключателей** распространяется на **все приложения** мобильного устройства. Изменить право доступа возможно только на Панели переключателей основного экрана. Право управления доступом в этом случае являются привилегированными.

В случае глобальной блокировки аппаратного модуля при обращении к этому модулю приложения, появляется окно предупреждения. Пример для камеры телефона приведен на рисунках.



Подп. и дата	Подп. дата
Изм	Лист
№ докум.	Подп.
Дата	Дата

Изм	Лист	№ докум.	Подп.	Дата
-----	------	----------	-------	------

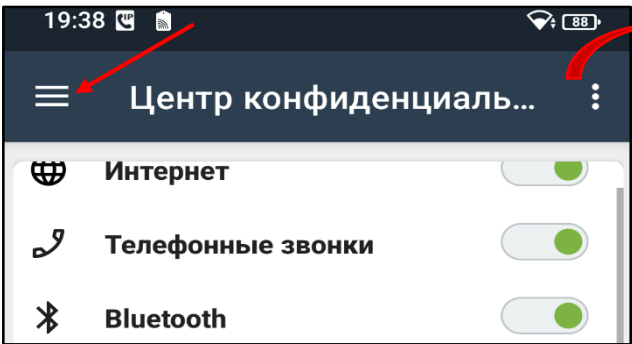
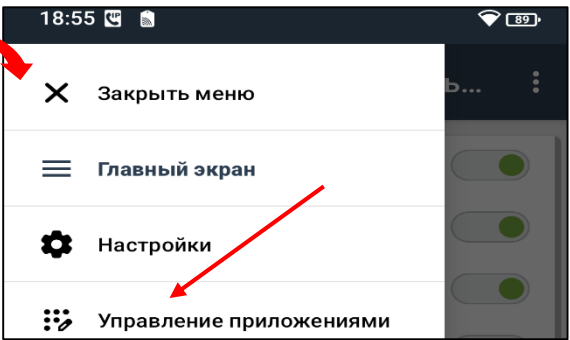
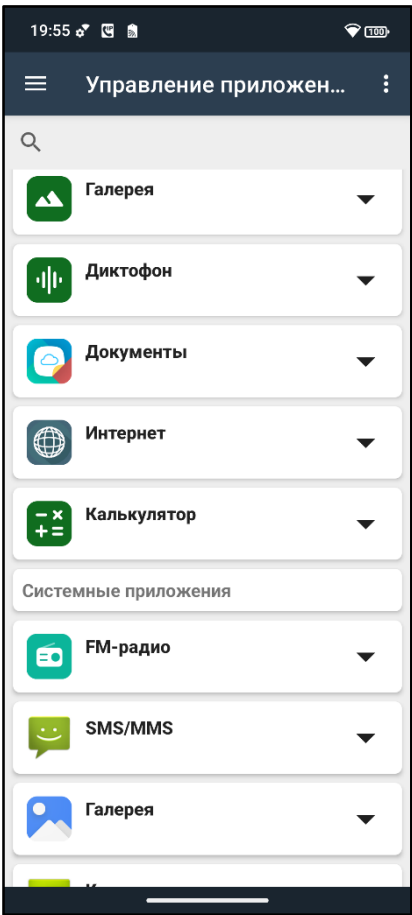
3.2.5 **Управление уровнем доступа приложений**

В системе реализована двухуровневая иерархия управления аппаратными ресурсами:

- Глобальный уровень;
- Уровень приложений.

Настройки доступа на уровне приложений вторичны по отношению к настройкам на глобальном уровне. Если на глобальном уровне на *Панели переключателей* для элемента установлено положение “Выкл.”, то на уровне приложения установка переключателя для элемента в положение “Вкл.” не отменяет блокировку на глобальном уровне.

Рассмотрим детально функционал управления доступом приложений. Для перехода к экрану управления приложениями необходимо использовать элемент меню на главном экране. Активация элемента откроет экран опций меню. Далее – *Управление приложениями*.



Открывается экран *Управление приложениями* - пользовательские приложения.

Справа от названия приложения элемент управления – *Треугольник индикации*.

Активация элемента открывает выпадающий список *Панели переключателей* для данного приложения.

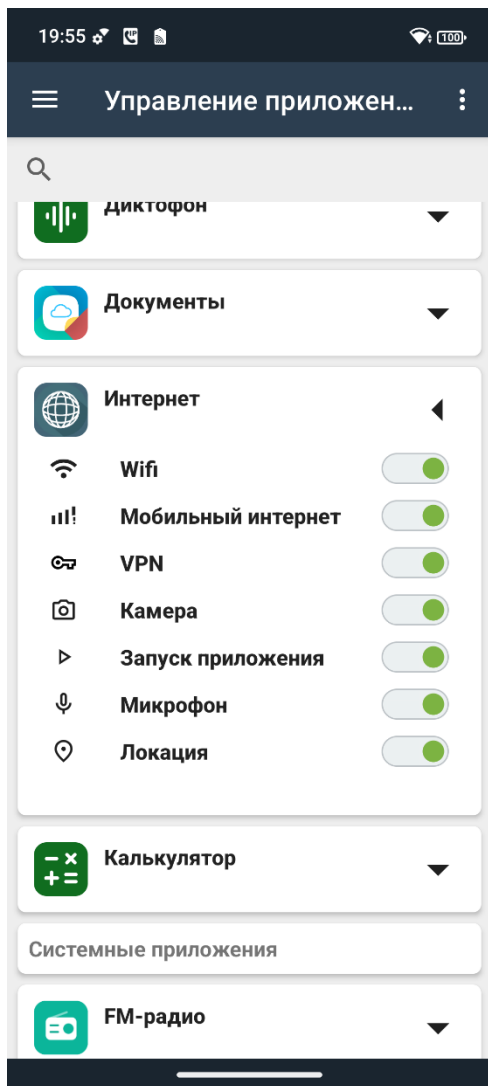
Активируем *Треугольник индикации* для приложения Интернет.

Выпадающий список приведен на рисунке ниже.

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

Изм	Лист	№ докум.	Подп.	Дата

ПО Центр конфиденциальности IXIUS				Лист
				18



Отключение доступа приложения к отдельным аппаратным ресурсам, реализовано как отключение отдельных элементов на Панели переключателей.

Количество элементов на панели в выпадающем списке несколько меньше чем на глобальном уровне.

Схема работы с переключателями интуитивно понятна.

Примечание:

Состояние переключателя доступа на основном экране (глобальном уровне) к отдельным элементам на **Панели Переключателей** распространяется **на все приложения** мобильного устройства.

Изменение состояния переключателя в настройках приложения возможно только в случае если на глобальном уровне элемент находится в положении “Вкл.”

Изменить право доступа возможно только на Панели переключателей основного экрана.

3.3 РЕКОМЕНДАЦИИ ПОЛЬЗОВАТЕЛЯМ

При отключении разрешения использования таких функций, как BlueTooth, NFC и Геолокация, по-отдельности или в составе группы, после повторного включения разрешения не происходит их автоматической активации, требуется активировать соответствующие функции вручную.

Запрет Телефонных звонков так же запрещает набор номера экстренной связи 112.

Блокировку настроек Центра конфиденциальности одноразовым паролем невозможно отменить без помощи Администратора системы, использовать с осторожностью.

По-умолчанию, все приложения имеют свои базовые права доступа, стоит ограничить приложения в правах, которые избыточны для их функций (например, доступ офисного пакета к сети Интернет или проигрывателя видео к геолокации).

Расширенные настройки сетевых разрешений приложений позволяют гибко регулировать их сценарий доступа в сеть. В некоторых случаях важно, чтобы приложение не работало при

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

Изм	Лист	№ докум.	Подп.	Дата	ПО Центр конфиденциальности IXIUS	Лист
						19

использовании VPN, тогда у него отключается переключатель VPN, а в некоторых случаях – наоборот, приложение должно иметь доступ в сеть строго через VPN подключение – тогда отключаются переключатели Wi-Fi и Мобильный интернет.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата					
Изм	Лист	№ докум.	Подп.	Дата	ПО Центр конфиденциальности IXIUS			Лист	
								20	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]

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