

УТВЕРЖДАЮ
Генеральный директор

Е.В. Ёрхов

«28» мая 2026 г.



ООО «АЙ ЭКС АЙ ЛАБОРАТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

(ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS)

ТЕХНИЧЕСКАЯ АРХИТЕКТУРА

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 технической архитектуры ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS.

ПО Центр конфиденциальности IXIUS – решение для локального управления разрешениями мобильных приложений по доступу к сети и датчикам мобильных устройств аппаратными функциями мобильными устройствами линейки IXIUS (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD). 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. Взаимодействие выстроено таким образом, что политики безопасности определяются на уровне ядра ОС, исключая возможность их обхода сторонним программным обеспечением.

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.

Содержание

1	ВВЕДЕНИЕ	5
1.1	Область применения документа	5
1.2	Требования к уровню подготовки персонала	5
2	ОПИСАНИЕ ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS	6
3	АРХИТЕКТУРА ПО	8
3.1	Основные архитектурные уровни	9
3.1.1	Пользовательский уровень	9
3.1.2	Сервисный уровень IXIOS	10
3.1.3	Уровень контроля доступа	12
3.1.4	Системный уровень	13
3.2	Основные преимущества архитектуры	14
3.3	Интеграция в экосистему IXIUS	15

По дп . да та						ПО ЦЕНТР КОНФИДЕНЦІАЛЬНОСТІ ІХІУС	Лист
Ин в. № ду бл							3
Вз ам . ин в. №							
По дп . и да та							
Ин в. № по дл							
	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 мобильных устройств компании IXI (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD).
IXIUS	Экосистема IXIUS
Линейка мобильных устройств IXIUS	(WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD)
Kernel Security Layer	Ядро ОС IXIOS с расширенными механизмами безопасности, специализированный уровень безопасности, обеспечивающий принудительное исполнение политик безопасности.
Framework Layer	Слой системных сервисов ОС IXIOS.
UID	User Identifier - уникальный номер, который система присваивает каждому зарегистрированному пользователю.
PID	Process Identifier - уникальный цифровой номер каждого запущенного в системе процесса или программы.
eBPF-хуки	Точки привязки в ядре ОС, к которым подключаются программы eBPF. Они позволяют выполнять изолированный код в ответ на события ядра (системные вызовы, сетевые пакеты, выделение памяти) без изменения исходного кода ядра или установки модулей.
eBPF	Extended Berkeley Packet Filter - расширенный фильтр пакетов Беркли
Netfilter	Базовый программный каркас (фреймворк) и механизм внутри ядра ОС, отвечающий за перехват, фильтрацию и модификацию сетевых пакетов.
TCP, UDP, ICMP, RAW	Базовые сетевые протоколы, работающие на транспортном и сетевом уровнях модели TCP/IP.
API	Application Programming Interface - программный интерфейс приложения набор правил, позволяющих разным программам общаться друг с другом
HAL	Hardware Abstraction Layer - слой абстракции оборудования.
LSM	Фреймворк безопасности в ядре ОС, позволяющий использовать различные модели контроля доступа.
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

					ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS		Лист
							4
Изм.	Лист	№ докум.	Подп.	Дата			

1 ВВЕДЕНИЕ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА

В настоящем документе рассматривается описание технической архитектуры 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 разрешениями мобильных приложений по доступу к сети и датчикам мобильных устройств аппаратными функциями.

[illegible]

2 ОПИСАНИЕ ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIUS

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 (WP23, WP27, C38, P1PRO, PIXIUS9, PIXIUS9PRO, PIXIUS9PROFOLD).

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;
- 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».

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

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

6

Изм. Лист № докум. Подп. Дата

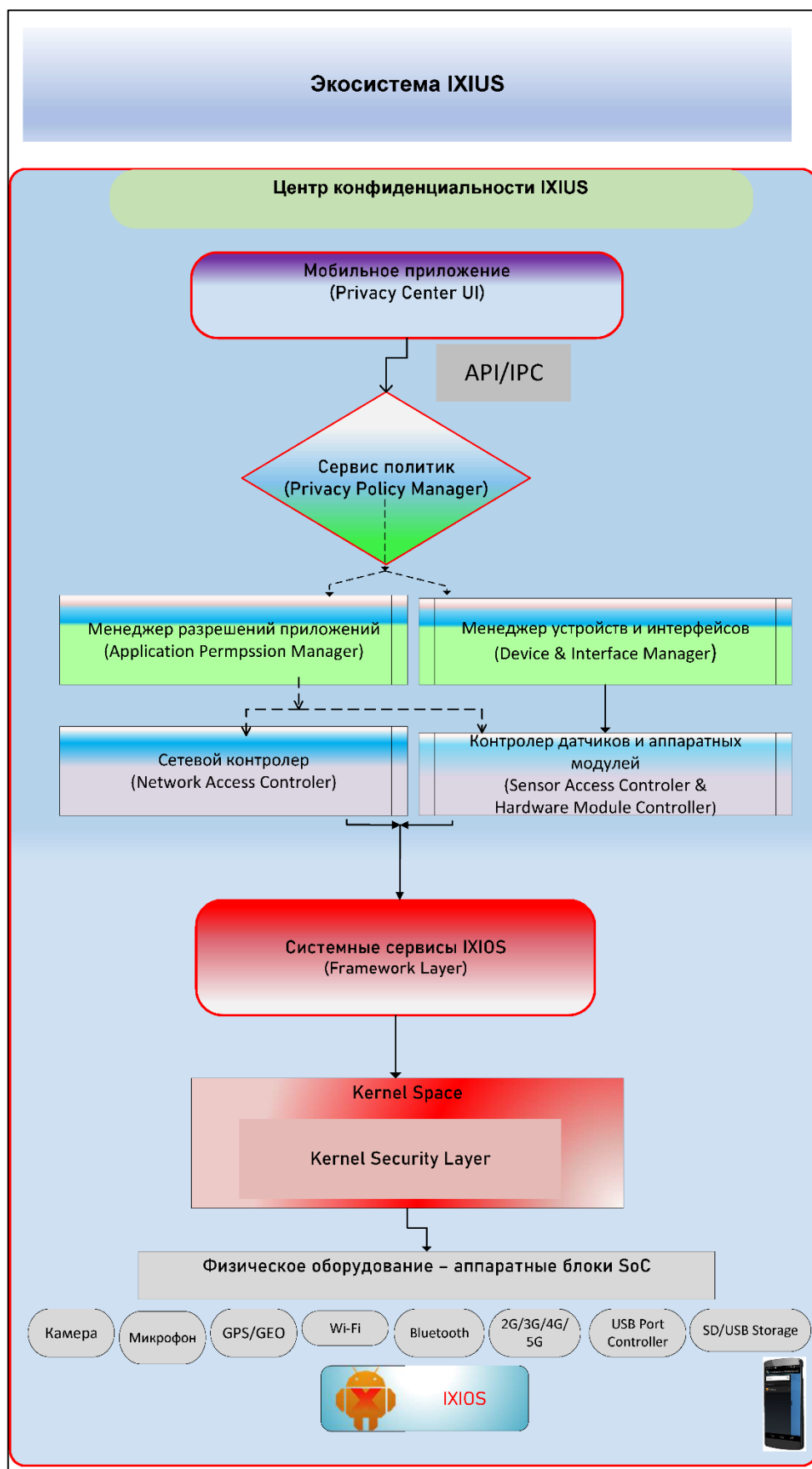
Полностью отечественная разработка. По состоянию на апрель 2026 года не имеет отечественных аналогов! Зарегистрирована в РОСПАТЕНТЕ (Федеральная служба по интеллектуальной собственности).

Свидетельство о государственной регистрации программ для ЭВМ №2025685597 от 25.09.2025г.

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			

3 АРХИТЕКТУРА ПО

Техническая архитектура программного обеспечения приведена на рисунке.



По
дп
·
да
та

Ин
в.
№
ду
бл

Вз
ам
·
ин
в.
№

По
дп
·
и
да
та

Ин
в.
№
по
дл

Архитектура включает четыре уровня с чёткими границами ответственности. Уровни на рисунке выделены цветовой гаммой.

1 уровень – приложение Privacy Center UI

2 уровень – Сервисный уровень, включающий

- Сервис политик (Privacy Politic Manager);
- Менеджер разрешений приложений (Application Permission Manager);
- Менеджер устройств и интерфейсов (Device & Interface Manager);

3 уровень – Уровень контроля доступа, включающий

- Сетевой контролер (Network Access Controler);
- Контролер датчиков (Sensor Access Controller);
- Контролер аппаратных модулей (Hardware Module Controller).

4 уровень – Системный уровень, включающий

- Framework Layer;
- Kernel Security Layer.

Каждый уровень независимо применяет политики = компрометация одного уровня не позволяет обойти нижележащие.

Архитектура обеспечивает полную цепочку гарантированного отключения аппаратных ресурсов на уровне драйверов. Ни один из четырех уровней не является единственной точкой доверия - совместная работа всех слоёв делает систему устойчивой к любым попыткам обхода.

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 четырех уровней - от пользовательского интерфейса до аппаратных блокировок на уровне ядра.

3.1 ОСНОВНЫЕ АРХИТЕКТУРНЫЕ УРОВНИ

3.1.1 ПОЛЬЗОВАТЕЛЬСКИЙ УРОВЕНЬ

Пользовательский уровень включает приложение Центр конфиденциальности – основной интерфейс управления разрешениями, предоставляющий пользователю единую точку управления всеми аппаратными ресурсами и политиками приложений. 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

По
дп
·
да
та

Ин
в.
№
ду
бл

Вз
ам
·
ин
в.
№
По
дп
·
и
да
та

Ин
в.
№
по
дл

ядра и драйверов. Взаимодействует через защищенный API и не осуществляет прямое управление оборудованием. Все команды выполняются через доверенные системные сервисы.

Основные компоненты архитектуры приложения Центр конфиденциальности

- Главная панель (Dashboard). Функционал:
 - отображение состояния оборудования, статуса ключевых аппаратных модулей;
 - управление профилями безопасности приложений
 - временная или постоянная блокировка управления функциями паролем.
- Управление аппаратными функциями (Device Control Panel). Функционал:
 - управление коммуникационными модулями, аппаратными блоками для приема/передачи данных (контроллеры Wi-Fi, Bluetooth, GPS, модемы сотовой связи (2G/3G/4G5G, USB и др.).
- Управление сетевым доступом (Network Control Manager). Функционал:
 - разрешение или блокировка доступа приложений к сети Интернет, локальной сети, беспроводным интерфейсам.

Ключевые особенности:

- интуитивно понятный интерфейс для пользователя;
- все настройки конфиденциальности в одном месте;
- включение/отключение датчиков глобально;
- назначение разрешений для каждого приложения;
- визуальная обратная связь - индикаторы состояния в реальном времени;
- безопасность по умолчанию - новые приложения не имеют доступа ни к чему - пользователь разрешает явно;
- контроль администратора - возможность блокировки изменений (для корпоративных устройств).

3.1.2 СЕРВИСНЫЙ УРОВЕНЬ IXIOS

Сервисный уровень IXIOS включает:

- Сервис политик (Privacy Politic Manager);
- Менеджер разрешений приложений (Application Permission Manager);
- Менеджер устройств и интерфейсов (Device & Interface Manager);
- Сервис политик (Privacy Politic Manager) - системный сервис ОС IXIOS, обеспечивающий централизованное управление, хранение и применение политик конфиденциальности и безопасности устройства. Связующим звено между

По
дп
·
да
та

Ин
в.
№
ДУ
бл

Вз
ам
·
ин
в.
№

По
дп
·
и
да
та

Ин
в.
№
по
дл

ПО ЦЕНТР КОНФИДЕНЦИАЛЬНОСТИ IXIOS

Лист

10

Изм. Лист № докум. Подп. Дата

приложением Центр безопасности, системными сервисами ОС и модулем принудительного контроля на уровне ядра и драйверов.

Основной функционал:

- хранение, валидация и применение политик конфиденциальности;
- маршрутизация запросов разрешений между приложениями и системными менеджерами;

- Менеджер разрешений приложений - системный компонент Центра конфиденциальности IXIUS, предназначенный для контроля и управления доступом приложений к аппаратным функциям устройства, датчикам, системным сервисам и сетевым ресурсам. Отвечающий за пользовательское управление разрешениями для каждого установленного приложения. Предоставляет интерфейс для настройки и отслеживания прав доступа к аппаратным и сетевым ресурсам.

Основной функционал:

- управление разрешениями приложений на доступ к аппаратным функциям устройства;
- контроль доступа к камере, микрофону, геолокации и датчикам;
- управление сетевым доступом отдельных приложений с возможностью отдельной регулировки доступа к Wi-Fi, GSM и VPN, указания разрешённых и запрещённых для подключения Wi-Fi сетей;
- применение индивидуальных и групповых политик безопасности
- передача решений на уровень сервисов ОС, ядра и драйверов для принудительного исполнения.

- Менеджер устройств и интерфейсов - системный компонент Центра конфиденциальности IXIUS, предназначенный для централизованного управления аппаратными устройствами, интерфейсами связи и внешними подключениями мобильного устройства. Реализует гарантированное отключение доступа к аппаратным модулям через системные вызовы и драйверы.

Основной функционал:

- принудительное отключение камеры, микрофона, GPS на аппаратном уровне;
- управление беспроводным интерфейсом, отключение/включение Wi-Fi, Bluetooth, NFC, модема (в т.ч. отдельно: сотовая связь, передача данных);
- контроль USB-порта, блокировка передачи данных;

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

11

Изм. Лист № докум. Подп. Дата

- управление съемными носителями, запрет монтирования SD-карт, контроль доступа к внешним накопителям;

3.1.3 УРОВЕНЬ КОНТРОЛЯ ДОСТУПА

Уровень контроля доступа - исполнительный слой между политиками конфиденциальности и физическим оборудованием. Основные компоненты:

- Сетевой контролер (Network Access Controller):
 - управляет сетевыми соединениями приложений реализует фаервол для отдельных приложений на уровне ядра IXIOS;
 - каждое приложение идентифицируется по UID/PID;
 - правила применяются через eBPF-хуки и Netfilter до установки соединения.
- Контролер датчиков (Sensor Access Controller) - управляет аппаратными модулями и периферийными интерфейсами;
- Контролер аппаратных модулей (Hardware Module Controller) - контроль доступа к камере, микрофону, GPS и другим аппаратным функциям.

Компоненты работают в режиме реального времени и подчиняются командам Менеджера разрешения приложений и Менеджера устройств и интерфейсов.

Ключевой принцип - управление выполняется на уровне ядра и драйверов, что исключает обход средствами пользовательских приложений

Основной функционал:

- 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;
- управление доступом к модулям Wi-Fi, Bluetooth, модем, NFC, USB;
- 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

12

Изм. Лист № докум. Подп. Дата

3.1.4 СИСТЕМНЫЙ УРОВЕНЬ

Системный уровень - базовый уровень архитектуры Центра конфиденциальности IXIUS, обеспечивающий взаимодействие с аппаратными ресурсами устройства и принудительное исполнение политик безопасности на уровне операционной системы. Включает Системные сервисы IXIOS (Framework Layer) и Kernel Security Layer.

- Framework Layer - слой системных сервисов IXIOS, обеспечивающий унифицированный API для управления разрешениями, межпроцессорным взаимодействием, HAL-абстракцией и мониторингом ресурсов.

Основной функционал:

- предоставление API для управления устройствами и системными ресурсами;
- обработка запросов от Privacy Center Manager;
- управление состоянием аппаратных модулей и интерфейсов;
- взаимодействие с драйверами и аппаратным абстрактным уровнем (HAL);
- сбор телеметрии и системных событий;
- журналирование операций и событий безопасности.

- Kernel Security Layer - ядро IXIOS с расширенными механизмами безопасности, специализированный уровень безопасности, обеспечивающий принудительное исполнение политик безопасности.

Основной функционал:

- 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 системного уровня

- разделение ответственности - сервисы пользовательского пространства управляют политиками, ядро - их принудительным применением;
- невозможность обхода - LSM и eBPF срабатывают до вызова драйверов;

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

13

Изм. Лист № докум. Подп. Дата

- 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 |
| 15 |

Лист регистрации изменений

[illegible]

По
дп
.
да
та

Ин
В.
№
ду
бл

Вз
ам
.
ИН
В.
Но

Подп. и дата

Ин
В.
№
по
дл