

# **МИРАЖ**

Система раннего обнаружения внутренних угроз

## **ДОКУМЕНТАЦИЯ, СОДЕРЖАЩАЯ ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ЭКЗЕМПЛЯРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

## СОДЕРЖАНИЕ

СОДЕРЖАНИЕ .....	2
Обозначения и сокращения.....	3
Термины и определения.....	5
1 Введение .....	6
2 Назначение и условия применения .....	6
2.1 Виды деятельности .....	6
2.2 Программные и аппаратные требования к системе .....	6
3 Состав системы.....	7
4 Функционал системы .....	8
5 Эксплуатация системы .....	9
5.1 Подготовка к работе .....	9
5.2 Использование ИС по назначению.....	9
5.3 Завершение работы Системы .....	11

## Обозначения и сокращения

В настоящем документе применяются следующие сокращения и обозначения, указанные в Таблице 1.

Таблица 1 — Обозначения и сокращения

Сокращение	Расшифровка
2FA	Two-Factor Authentication — двухфакторная аутентификация
AD	Active Directory — служба каталогов Microsoft
API	Application Programming Interface — интерфейс прикладного программирования
CA	Certificate Authority — центр сертификации
CIDR	Classless Inter-Domain Routing — бесклассовая адресация
CSV	Comma-Separated Values — формат табличных данных
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System — система доменных имён
EPS	Events Per Second — количество событий в секунду
FTP	File Transfer Protocol — протокол передачи файлов
HTTP/HTTPS	HyperText Transfer Protocol (Secure)
JSON	JavaScript Object Notation — формат обмена данными
JWT	JSON Web Token — токен аутентификации
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LXD	Linux Containers Daemon — система управления контейнерами
MSSQL	Microsoft SQL Server
mTLS	Mutual TLS — взаимная проверка сертификатов
NTLMv2	NT LAN Manager v2 — протокол аутентификации Windows
PDF	Portable Document Format — формат электронных документов
PKI	Public Key Infrastructure — инфраструктура открытых ключей
RBAC	Role-Based Access Control — управление доступом на основе ролей
RDP	Remote Desktop Protocol — протокол удалённого рабочего стола
REST	Representational State Transfer — архитектурный стиль API
SIEM	Security Information and Event Management
SMB	Server Message Block — протокол файлового доступа Windows
SMTP	Simple Mail Transfer Protocol — протокол отправки почты
SSH	Secure Shell — протокол защищённого удалённого доступа
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TOTP	Time-based One-Time Password — одноразовый пароль
VLAN	Virtual Local Area Network — виртуальная локальная сеть
WinRM	Windows Remote Management — удалённое управление Windows

ZFS	Zettabyte File System — файловая система с поддержкой снимков
VM	Виртуальная машина
ИБ	Информационная безопасность
ИС	Информационная система
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЦПУ	Центральное процессорное устройство (процессор)

## Термины и определения

В настоящем документе применяются термины с соответствующими определениями, указанные в Таблице 2.

Таблица 2 — Термины и определения

Термин	Определение
Ловушка	Поддельный сервер, эмулирующий реальный сетевой сервис и фиксирующий любое обращение как инцидент безопасности
Приманка	Поддельный артефакт (файл, токен), размещённый в инфраструктуре для привлечения атакующего к ловушке
Canary-токен	Уникальный идентификатор (URL), генерирующий событие безопасности при использовании
Control Plane	Центральный компонент управления (VM1): API, база данных, веб-интерфейс
Data Plane	Компонент инфраструктуры ловушек (VM2): LXD-хост с контейнерами
Deception Technology	Технология обмана — метод обнаружения угроз на основе развёртывания ложных активов в сети
Hardware Fingerprint	Аппаратный отпечаток сервера, используемый для привязки лицензии к оборудованию
Heartbeat	Периодический сигнал от ловушки, подтверждающий её работоспособность (каждые 30 секунд)
Lateral Movement	Боковое перемещение — движение атакующего между узлами сети после проникновения
MITRE ATT&CK	Стандартизированная база знаний о тактиках и техниках атакующих
Zero False Positives	Принцип нулевых ложных срабатываний: любое взаимодействие с системой является инцидентом
Контейнер	Изолированная среда исполнения (LXD для ловушек, Docker для сервисов Control Plane)
Сетевой профиль	Конфигурация сети (bridge, VLAN), определяющая сегмент размещения ловушки

## 1 Введение

Программное обеспечение «Мираж» представляет собой платформу раннего обнаружения внутренних угроз информационной безопасности, размещённую на виртуальных машинах в корпоративной сети. Система работает на основе технологии обмана (Deception Technology) и предназначена для выявления несанкционированной активности внутри периметра.

Система предоставляет следующие ключевые возможности:

- развёртывание ловушек, эмулирующих 9 сетевых протоколов (SSH, HTTP, SMB, RDP, FTP, MySQL, PostgreSQL, MSSQL, WinRM);
- создание приманок — файловых артефактов и сапату-токенов, ведущих атакующего к ловушкам;
- сбор и обработку событий безопасности по принципу Zero False Positives;
- автоматический маппинг событий на фреймворк MITRE ATT&CK;
- мониторинг в реальном времени через веб-интерфейс с дашбордом;
- интеграцию с внешними системами (SIEM, Email, Telegram, Webhook, Active Directory);
- ролевое управление доступом (RBAC), аудит действий, лицензирование.

Модульная архитектура системы разделена на два компонента: Control Plane (VM1) — центр управления, API, база данных и веб-интерфейс; Data Plane (VM2) — инфраструктура ловушек на базе LXD-контейнеров. Связь между компонентами осуществляется по защищённому каналу mTLS + JWT.

Доступ к функциям Системы выполняется с использованием веб-интерфейса через браузер. Система поддерживает ролевую модель, благодаря которой каждый пользователь получает доступ только к разрешённым функциям. Система разработана с использованием языков программирования Python и TypeScript.

Целевая аудитория: средний и крупный бизнес с выделенной командой ИБ, государственные организации, компании финансового и промышленного сектора, организации, уже имеющие базовую защиту (SIEM, EDR).

## 2 Назначение и условия применения

### 2.1 Виды деятельности

Система решает задачи обнаружения внутренних угроз в корпоративной сети на основе технологии обмана. Система предназначена для выявления следующих видов угроз:

- инсайдерская активность — сотрудник сканирует сеть или использует найденные приманки;
- скомпрометированные хосты — вредоносное ПО выполняет lateral movement, сканирует подсети;
- АРТ внутри периметра — продвинутые атакующие исследуют сеть после проникновения;
- Red Team / Pentest — пентестеры попадают на ловушки (валидация защиты);
- Ransomware — шифровальщик пытается обращаться к файловым ресурсам ловушек;
- LLMNR/NBT-NS Poisoning — атаки на протоколы резолвинга имён (Responder, Inveigh).

### 2.2 Программные и аппаратные требования к системе

Система размещается на двух виртуальных машинах. Аппаратные требования указаны в Таблице 3.

Таблица 3 — Аппаратные требования

Параметр	Control Plane (VM1)	Data Plane (VM2)
ЦПУ	4 vCPU	8 vCPU
Оперативная память	8 ГБ	16 ГБ
Дисковое пространство	100 ГБ SSD	200 ГБ SSD (ZFS)
Сетевой интерфейс	1 Гбит/с Ethernet	1 Гбит/с Ethernet (+ VLAN)

Требования к программному обеспечению:

- ОС: Ubuntu Server 22.04/24.04 LTS, Debian 11/12, Astra Linux SE 1.7/1.8, РЕД ОС 7.3/8, Альт СП 10, Альт Сервер 10, Альт Виртуализация 10, РОСА ХРОМ Сервер;
- Docker 20.10+ и Docker Compose 2.0+ (VM1);
- LXD 5.x (snap), ZFS для storage pool (VM2);
- браузер: Chrome 90+, Firefox 90+, Safari 14+, Edge 90+.

Требуемые версии ПО для установки на ВМ указаны в Таблице 4.

Таблица 4 — Программные требования к ПО ВМ

Назначение	Наименование и версия	Правообладатель	Лицензия
ПО контейнеризации	Docker Engine Community 20.10+	Docker, Inc.	Apache 2.0
СУБД	PostgreSQL 16.0	The PostgreSQL Global Development Group	PostgreSQL License (вариант MIT)
HTTP-сервер	nginx 1.25+	Nginx, Inc.	BSD 2-clause
Кэш / брокер	Redis 7.0+	Redis Ltd.	BSD 3-clause
Очередь задач	Celery 5.0+	Ask Solem & contributors	BSD 3-clause
Контейнеры ловушек	LXD 5.x	Canonical Ltd.	Apache 2.0
Файловая система	ZFS (OpenZFS)	OpenZFS Project	CDDL

### 3 Состав системы

Программное обеспечение состоит из компонентов, описанных в Таблице 5.

Таблица 5 — Описание компонентов

Название компонента	Описание компонента
СУБД PostgreSQL 16	Используется для постоянного хранения состояния, включает в себя: <ul style="list-style-type: none"> <li>– информацию о пользователях, ролях и учётных записях;</li> <li>– конфигурацию ловушек, приманок и сетевых профилей;</li> <li>– события безопасности (партиционированные по месяцам);</li> <li>– журнал аудита действий пользователей;</li> <li>– настройки интеграций и лицензирования.</li> </ul>
Redis 7	Кэширование данных и обеспечение фоновой обработки:

	<ul style="list-style-type: none"> <li>– кэш сессий и часто запрашиваемых данных;</li> <li>– брокер сообщений для очереди задач Celery;</li> <li>– pub/sub для WebSocket-уведомлений в реальном времени.</li> </ul>
FastAPI Backend	<p>Серверная часть приложения (REST API):</p> <ul style="list-style-type: none"> <li>– обработка HTTP-запросов, аутентификация, авторизация;</li> <li>– бизнес-логика управления ловушками, приманками, событиями;</li> <li>– WebSocket для push-уведомлений;</li> <li>– валидация данных через Pydantic v2.</li> </ul>
Celery Worker	<p>Обработка фоновых задач:</p> <ul style="list-style-type: none"> <li>– развёртывание и удаление ловушек в LXD;</li> <li>– отправка алертов (Email, Telegram, Webhook, SIEM);</li> <li>– экспорт событий.</li> </ul>
Celery Beat	<p>Планировщик периодических задач:</p> <ul style="list-style-type: none"> <li>– проверка heartbeat ловушек (каждые 60 секунд);</li> <li>– создание партиций БД для событий (ежемесячно);</li> <li>– очистка данных согласно retention лицензии;</li> <li>– отправка диагностических отчётов.</li> </ul>
nginx	<p>Веб-сервер и reverse проху:</p> <ul style="list-style-type: none"> <li>– TLS-терминация (порты 80/443);</li> <li>– проксирование запросов к FastAPI Backend;</li> <li>– обслуживание статического контента React UI.</li> </ul>
React UI (Web Application)	<p>Single-page application (SPA), реализующее пользовательский интерфейс для управления Системой через браузер.</p>
Honeypot Agent	<p>Python-скрипт внутри каждого LXD-контейнера:</p> <ul style="list-style-type: none"> <li>– эмуляция сетевых сервисов (SSH, HTTP, SMB, RDP, FTP, MySQL, PostgreSQL, MSSQL, WinRM);</li> <li>– сбор и отправка телеметрии на Control Plane;</li> <li>– локальный буфер событий при недоступности контроллера.</li> </ul>
LXD Host	<p>Система управления контейнерами для изоляции ловушек. Каждая ловушка работает в отдельном непривилегированном контейнере с bridge-подключением к корпоративной сети.</p>

## 4 Функционал системы

В Системе реализованы следующие функции:

- авторизация и аутентификация пользователей (JWT, 2FA TOTP), управление пользователями;
- управление ловушками — создание, развёртывание, запуск, остановка, перезапуск, удаление LXD-контейнеров с эмуляцией 9 сетевых протоколов;

- управление приманками — создание файловых приманок и URL canary-токенов, скачивание для ручного размещения, размещение с использованием AD интеграции;
- управление сетями — создание и настройка сетевых профилей (VLAN/bridge) для размещения ловушек;
- анализ покрытия — контроль охвата сетевых сегментов ловушками (реестр подсетей с классификацией по категории и важности, анализ достижимости, рекомендации по развёртыванию) и охвата пользователей AD приманками (профилирование по ролям, выявление высокоценных целей, статистика и рекомендации по размещению);
- сбор и обработка событий безопасности по принципу Zero False Positives с классификацией по severity;
- автоматический маппинг событий на тактики и техники MITRE ATT&CK;
- мониторинг в реальном времени — дашборд с карточками статистики, timeline, heatmap, top источников, MITRE ATT&CK;
- фильтрация, поиск, подтверждение (acknowledge) и экспорт событий (CSV, JSON, PDF);
- интеграции — настройка каналов оповещения (Email, Telegram, Webhook, SIEM Syslog) и обогащение событий через Active Directory;
- белый список — управление IP/подсетями, исключёнными из мониторинга, с типизацией и сроком действия;
- диагностические отчёты — автоматическая отправка ежедневных/еженедельных отчётов о состоянии системы;
- аудит действий пользователей — полный журнал с экспортом в CSV;
- лицензирование — привязка к hardware fingerprint, поддержка офлайн-активации, ограниченный режим.

## 5 Эксплуатация системы

### 5.1 Подготовка к работе

Для получения доступа к функциям Системы пользователь должен обратиться к администратору Системы для получения учётной записи. Администратор присваивает учётной записи роль, которая определяет доступность функций Системы.

Система реализует ролевую модель со следующими ролями:

- Администратор — полный контроль: все операции, управление пользователями, настройки системы, интеграции, лицензирование;
- Оператор — управление инфраструктурой: CRUD ловушек/приманок/сетей, просмотр событий, экспорт;
- Аналитик — только чтение: просмотр дашборда, событий и активов.

Для доступа к функциям Системы администратор сообщает пользователю: адрес точки входа в Систему (URL), логин (email) и пароль.

### 5.2 Использование ИС по назначению

Использование Системы по назначению выполняется при помощи графического интерфейса, реализуемого через браузер. Для доступа используется IP-адрес, на который установлена Система (порт 443, HTTPS).

Рабочее пространство Системы организовано в виде рабочей области и бокового (главного) меню. Каждая функция содержится в отдельном разделе бокового меню, которые описаны в Таблице 6.

*Таблица 6 — Использование функций Системы через разделы бокового меню*

Пункт меню	Описание / Назначение
Мониторинг (Dashboard)	<p>Главная страница с обзором состояния безопасности:</p> <ul style="list-style-type: none"> <li>– карточки статистики (ловушки, приманки, события, инциденты);</li> <li>– timeline событий, тепловая карта активности;</li> <li>– MITRE ATT&amp;CK — агрегированная статистика тактик;</li> <li>– top источников, последние критические события.</li> </ul>
Ловушки	<p>Управление ловушками (honeypots):</p> <ul style="list-style-type: none"> <li>– просмотр списка с фильтрацией по статусу;</li> <li>– создание ловушки: выбор ОС, сервисов, сети;</li> <li>– действия: запуск, остановка, перезапуск, удаление;</li> <li>– просмотр событий конкретной ловушки.</li> </ul>
Приманки	<p>Управление приманками (breadcrumbs):</p> <ul style="list-style-type: none"> <li>– вкладка Файлы — создание файловых приманок;</li> <li>– вкладка URL Canary — создание canary-токенов;</li> <li>– скачивание приманок для ручного размещения;</li> <li>– отслеживание срабатываний.</li> </ul>
События	<p>Центральный журнал инцидентов:</p> <ul style="list-style-type: none"> <li>– фильтрация по периоду, severity, категории;</li> <li>– полнотекстовый поиск;</li> <li>– детали события: MITRE ATT&amp;CK маппинг, raw data;</li> <li>– подтверждение (acknowledge) событий;</li> <li>– экспорт в CSV, JSON, PDF.</li> </ul>
Сети	<p>Управление сетевыми профилями:</p> <ul style="list-style-type: none"> <li>– создание, редактирование, удаление профилей;</li> <li>– привязка к LXD bridge-интерфейсам Data Plane;</li> <li>– отображение количества ловушек в каждой сети.</li> </ul>
Настройки → Интеграции	<p>Настройка каналов оповещения и экспорта:</p> <ul style="list-style-type: none"> <li>– Email (SMTP), Telegram, Webhook, SIEM (Syslog);</li> <li>– тестирование каждой интеграции.</li> </ul>
Настройки → Диагностика	<p>Настройка автоматической отправки ежедневных и еженедельных отчётов через Telegram/Email.</p>
Настройки → Active Directory	<p>Интеграция с AD/LDAP для обогащения событий данными: hostname, пользователь, отдел, должность.</p>
Настройки → Белый список	<p>Управление исключениями из мониторинга:</p> <ul style="list-style-type: none"> <li>– типы: Инфраструктура, Администрирование, Тестирование, Другое;</li> <li>– указание IP/CIDR, описание, срок действия.</li> </ul>

Настройки → Профиль	Управление личной учётной записью: смена пароля, настройка 2FA (TOTP).
Пользователи (Администратор)	Только для администратора. Управление учётными записями: создание, редактирование, деактивация, назначение ролей.
Аудит (Администратор)	Только для администратора. Просмотр журнала действий пользователей с фильтрацией и экспортом в CSV.
Лицензия (Администратор)	Только для администратора. Просмотр информации о лицензии, загрузка файла лицензии, экспорт hardware fingerprint.

Использование функций является интуитивно понятным. Пользователю доступны подсказки при наведении курсора на объекты пользовательского интерфейса.

### 5.3 Завершение работы Системы

Для завершения работы с Системой пользователь выполняет выход через кнопку «Выход» в боковом меню.

Для безопасного завершения работы серверной части Системы:

1. Убедиться, что все пользователи завершили работу в веб-интерфейсе.
2. Остановить ловушки через веб-интерфейс или дождаться автоматической остановки.
3. Остановить Control Plane (VM1): `docker compose down`.
4. Остановить Data Plane (VM2): остановить LXD-контейнеры, затем выключить VM.

При завершении работы ловушки с активными буферами событий сохраняют данные локально. После повторного запуска буферизованные события автоматически отправляются на Control Plane.