Разработка платформы по управления безопасным доступом и цифровой идентичностью

Сокращённое название – платформа CTfind Security

ОБЩЕЕ ОПИСАНИЕ СИСТЕМЫ

Аннотация

Все термины, которые применяются в данном документе соответствуют определениям, которые даны в Техническом задании на выполнение НИОКР по Договору № 228ГРЦТС10-D5/76576 от 25.05.2022 г.

Документ содержит информацию о назначении Платформы CTfind Security, объектах автоматизации и перечень выполняемых функций.

В документе приведены сведения о структуре системы, назначении её компонентов. Документ содержит сведения о функционировании системы и взаимосвязях компонентов Платформы CTfind Security.

Содержание

Список иллюстраций

Элементы списка иллюстраций не найдены.

1. Назначение системы

1.1. Область применения

Система **CTfind Security** предназначена для автоматизации процессов управления доступом, контроля привилегированных действий, цифровой идентификации и безопасного распределения файлов в среде корпоративной или распределённой ИТ-инфраструктуры. Она применяется в организациях, предъявляющих высокие требования к информационной безопасности, защите критических ресурсов и соблюдению нормативных требований (ФСТЭК, 152-ФЗ, ISO/IEC 27001 и др.).

Система может использоваться в следующих сферах:

- государственные и муниципальные учреждения;
- промышленные и инфраструктурные предприятия;
- телекоммуникационные операторы;
- финтех и банки;
- транспортные и логистические компании.

1.2. Виды автоматизируемой деятельности

Структура CTfind Security обеспечивает автоматизацию следующих направлений деятельности:

- централизованное управление привилегированными учетными записями;
- выдача и отзыв доступов по заявочному принципу;
- идентификация и аутентификация пользователей на основе политик безопасности;
- управление жизненным циклом цифровых идентичностей;
- аудит и контроль действий пользователей в защищаемых системах;
- организация защищённого совместного доступа к файлам;
- интеграция с системами управления ИБ, SIEM, CMDB, IAM.

1.3. Основные функции и задачи

CTfind Security представляет собой модульную платформу, включающую:

- Ядро системы, отвечающее за маршрутизацию данных, базовую авторизацию, журналирование и взаимодействие между модулями;
- Модуль PAM (Privileged Access Management) — управление привилегированным доступом, прокси-доступ, запись и контроль сессий;
- Модуль IDM (Identity Management) — централизованное управление учетными записями и цифровыми идентичностями, самообслуживание, политики жизненного цикла;
- Модуль CFS (Central File Sharing) — безопасный файловый обмен с управлением правами доступа и аудитом действий.

Среди ключевых задач системы:

- повышение прозрачности привилегированного доступа;
- минимизация рисков злоупотребления учетными записями;
- обеспечение соответствия регуляторным требованиям;
- повышение уровня автоматизации процессов ИБ;
- формирование доверенной среды между пользователями, системами и файлами.

2. Структура системы CTfind Security

Система CTfind Security построена по модульному принципу. Ядро системы обеспечивает согласованное функционирование подключаемых модулей, реализующих специализированные функции по управлению доступом, учетными записями и файловым обменом. Такая архитектура позволяет гибко масштабировать систему, подключать новые компоненты, адаптироваться к требованиям заказчика и обеспечивать высокую надежность и безопасность.

Архитектура системы включает:

- Ядро CTfind Security;
- Модуль PAM (Privileged Access Management);
- Модуль IDM (Identity Management);
- Модуль CFS (Central File Sharing).

Все модули взаимодействуют между собой через внутренние API и используют общую систему авторизации, хранения журналов событий и управления пользователями.

2.1. Архитектура системы

Архитектура CTfind Security состоит из следующих уровней:

- Уровень представления (UI Layer)
  Веб-интерфейс для администраторов, аудиторов и пользователей. Предоставляет доступ к заявкам, сессиям, учетным записям, файлам, уведомлениям и настройкам безопасности.
- Прикладной уровень (Application Layer)
  Обрабатывает бизнес-логику: маршрутизация заявок, авторизация сессий, исполнение политик доступа, регистрация действий, управление учетными данными.
- Уровень интеграции (Integration Layer)
  Службы взаимодействия с внешними системами: LDAP/AD, SIEM, корпоративные хранилища, шлюзы и API сторонних решений.
- Сервисный уровень (Service Layer)
  Службы ядра, отвечающие за хранение данных, взаимодействие между модулями, очередь задач, логирование, мониторинг, управление кластерами.

- Хранилище данных (Storage Layer)
  Базы данных и файловые хранилища, используемые для хранения учетных данных, логов, записей сессий, служебной информации и пользовательских файлов.

2.2. Ядро системы

2.2.1 Назначение

Ядро CTfind Security является центральным элементом архитектуры и отвечает за координацию всех операций, поступающих от модулей и пользователей. Оно реализует основные механизмы безопасности, авторизации, межмодульного взаимодействия и мониторинга.

2.2.2 Основные функции ядра

- Централизованная аутентификация и авторизация пользователей;
- Ведение единого реестра учетных записей, ролей и прав доступа;
- Журналирование действий и централизованный аудит;
- Управление очередями задач и событий;
- Обработка заявок на доступ и маршрутизация по политике;
- Поддержка 2FA, политик тайм-аутов, расписаний, геоограничений;
- Мониторинг состояния системы, логирование отказов и инцидентов;
- Обеспечение устойчивой работы модулей через API и событийную шину.

2.2.3 Подсистемы и компоненты ядра

Подсистема	Назначение
Авторизация	Проверка подлинности и контроль прав пользователя

Управление пользователями	Реестр пользователей, ролей и прав
Маршрутизация заявок	Логика обработки запросов на доступ
Событийная шина	Связь между модулями в режиме publish/subscribe
Аудит	Запись действий пользователей и системных событий
API-шлюз	Интерфейс взаимодействия с внешними системами
Управление журналами	Централизованное хранение логов, поддержка форматов SIEM
Мониторинг и алертинг	Контроль работоспособности компонентов и модулей

2.3. Подключаемые модули

Система CTfind Security расширяется с помощью специализированных модулей, реализующих конкретные функции в рамках общей архитектуры управления доступом, идентичностью и безопасным обменом файлами.

Каждый модуль логически и технически интегрируется с ядром системы, использует единые механизмы авторизации, журналирования и управления событиями.

2.3.1 Модуль PAM (Privileged Access Management)

2.3.1.1 Назначение

Модуль PAM (Privileged Access Management) предназначен для централизованного управления привилегированным доступом к критическим ИТ-ресурсам, таким как серверы, сетевое оборудование, базы данных,

системы управления и облачные платформы. Его основная цель — исключение несанкционированного доступа, минимизация рисков утечки конфиденциальной информации и обеспечение полной прозрачности действий администраторов и технических специалистов.

PAM-модуль позволяет компаниям реализовать контроль по принципу Zero Trust, сократить объём постоянных прав, обеспечить временной доступ, автоматизировать согласования и обеспечить запись каждой привилегированной сессии.

2.3.1.2 Основные функции

Модуль реализует следующие функции управления привилегированным доступом:

- Каталог защищаемых ресурсов: ведение реестра серверов, баз данных, сетевых устройств, систем и сервисов, к которым требуется контролируемый доступ;
- Хранилище привилегированных учётных данных (Vault): безопасное централизованное хранение паролей и ключей доступа с многоуровневым шифрованием и ограничением доступа;
- Запрос доступа (Access Request): механизм подачи заявок пользователями на привилегированный доступ с маршрутами согласования по ролям, расписанию или контексту;
- Временный доступ (Just-in-Time Access): выдача временных прав без раскрытия пароля или создания постоянной учетной записи;
- Проксирование сессий (Proxy Access): предоставление доступа к ресурсам через PAM-шлюз без прямого подключения к целевому узлу;
- Запись сессий (Session Recording): видеозапись и логирование всех действий в привилегированной сессии (CLI, RDP, SSH, VNC, веб-доступ);

- Онлайн-мониторинг: возможность администратора подключиться к активной сессии в режиме "просмотр в реальном времени" или остановить её;
- Контроль команд (Command Control): фильтрация и блокировка опасных CLI-команд по белым и чёрным спискам;
- Управление расписаниями и геоограничениями: разрешение доступа только в определённое время, с определённых IP-адресов и устройств;
- Аудит и оповещения: полное журналирование всех действий, уведомления о подозрительной активности или нарушении политики доступа;
- Интеграция с SIEM: экспорт логов, событий и записей сессий в системы управления инцидентами информационной безопасности.

2.3.1.3 Архитектура модуля

PAM-модуль построен по микросервисной архитектуре и взаимодействует с ядром CTfind Security через Kafka (шина событий) и REST API. Основные компоненты модуля:

Компонент	Назначение
PAM Gateway	Шлюз-прокси для создания привилегированных сессий без раскрытия пароля. Поддерживает протоколы: SSH, RDP, VNC, HTTP/HTTPS.
Access Request Engine	Обработка заявок на доступ, маршрутизация по политике, контроль таймеров и 2FA.
Session Recorder	Запись и хранение видео/логов привилегированных сессий, генерация метаданных (команды, окна, действия).
Password Vault	Централизованное хранилище паролей с шифрованием, логированием операций и политиками ротации.
Command Filter Engine	Сервис анализа CLI-команд в режиме реального времени с возможностью блокировки и уведомлений.

Real-Time Monitor	Панель наблюдения за активными сессиями, с возможностью подключиться в режиме "read-only" или "terminate".
Audit Logger	Отправка событий в аудит: начало/конец сессии, команды, ошибки, отклонения от политики.

2.3.1.4 Поддерживаемые сценарии доступа

Модуль поддерживает разнообразные сценарии подключения к ресурсам:

- Jump-to-Server (через PAM Gateway) — пользователь получает доступ через веб-интерфейс или терминальный клиент, при этом его сессия проксируется через PAM Gateway;
- Безраскрытый доступ — пользователь не видит логин/пароль, а инициирует сессию с временным токеном;
- Password Checkout — временная выдача пароля с контролем времени жизни и подтверждением действий;
- Прямое подключение с проверкой — в некоторых случаях возможен доступ с клиента через VPN/SSH, но с авторизацией и контролем со стороны PAM;
- Согласуемый доступ — заявка отправляется на согласование нескольким лицам, доступ открывается только после утверждения.

2.3.1.5 Политики и безопасность

Права на доступ определяются на основе политик, настраиваемых в административной панели.

Политики могут учитывать:

- Роль и подразделение пользователя;
- Тип ресурса и чувствительность данных;
- Геолокацию, IP-адрес, время суток;

- Уровень критичности запроса;
- Требование 2FA или одобрения руководства;

Доступ может предоставляться автоматически или через каскад согласований. Все действия в сессии сопровождаются журналированием и, при необходимости, автоматическими уведомлениями о подозрительной активности.

2.3.1.6 Преимущества внедрения PAM-модуля

- Минимизация человеческого фактора при доступе к критическим системам;
- Исключение необходимости раскрытия паролей;
- Защита от внутреннего злоупотребления привилегиями;
- Соответствие требованиям ФСТЭК, 152-ФЗ, ISO 27001, PCI DSS;
- Возможность последующего форензик-анализа (по видеозаписям и логам);
- Быстрая интеграция с AD, SIEM, DevOps-инфраструктурой.

2.3.2 Модуль IDM (Identity Management)

2.3.2.1 Назначение

Модуль IDM (Identity Management) обеспечивает централизованное управление цифровыми идентичностями пользователей и сервисов в ИТ-инфраструктуре организации. Его основная задача — автоматизация жизненного цикла учетных записей, ролей и прав доступа в соответствии с политиками безопасности, оргструктурой и событиями кадровых процессов.

IDM помогает устранить ручное создание учётных записей, избежать несанкционированного доступа, упростить процессы

подключения/отключения сотрудников и реализовать принципы Zero Trust и Least Privilege.

2.3.2.2 Основные функции

Модуль реализует следующие функции:

- Регистрация и самообслуживание — создание пользователей вручную, по внешним источникам (HR-системы, Excel, API) или через портал самообслуживания;
- Импорт оргструктуры — синхронизация с Active Directory, LDAP, HRMS (1C, SAP, WebSoft, Босс-Кадровик и др.) по расписанию;
- Управление ролями и группами — назначение прав доступа на основе должности, подразделения, проекта, статуса, привязка к ролям RBAC/ABAC;
- Жизненный цикл идентичностей:
  - Приём на работу — автоматическое создание учётной записи, настройка доступа;
  - Перевод — изменение прав доступа, перемещение между группами;
  - Увольнение — отзыв прав, блокировка и удаление учетной записи;
- Автоматическое предоставление и отзыв доступов — через политики Provisioning и правила управления событиями;
- Заявочный процесс (Access Request) — запросы на доступ к ресурсам и ролям с маршрутизацией согласования;
- История и аудит — фиксация всех действий: кто, когда, кому выдал/изменил/удалил доступ;
- Интеграция с внешними системами — IAM, Helpdesk, AD, LDAP, Exchange, GitLab, Jira, Confluence, облачные сервисы;
- Портал сотрудника — личный кабинет с заявками, уведомлениями, доступами, правами, активными ресурсами.

2.3.2.3 Архитектура модуля

Модуль IDM построен на микросервисной архитектуре и включает следующие компоненты:

Компонент	Назначение
Provisioning Engine	Управление жизненным циклом аккаунтов: создание, изменение, деактивация, удаление. Поддерживает шаблоны и правила.
Directory Sync	Двусторонняя синхронизация с AD, LDAP, HR-системами, внешними API.
Access Request Engine	Обработка заявок на доступ к ролям и группам, логика маршрутизации и согласований.
Attribute Engine	Построение логики ABAC: правила доступа на основе атрибутов (например, “если отдел = ‘финансы’, дать роль ‘Просмотр отчётов’”).
Policy Engine	Хранение и применение политик доступа, настройки триггеров, расписаний и правил соответствия.
Audit Logger	Запись всех событий: кто, что, когда, на каком основании получил или потерял доступ.
Self-Service Portal	Веб-интерфейс для сотрудников и администраторов: подача заявок, управление доступом, просмотр истории.

2.3.2.4 Поддерживаемые сценарии использования

IDM охватывает ключевые сценарии управления идентичностями.

Онбординг сотрудников:

- Создание учётной записи в AD, почте, внутренних системах;
- Автоматическая выдача стартового доступа и ролей;
- Уведомление ИТ и руководителя о завершении процедуры.

Изменение должности / переводы:

- Пересмотр и обновление прав;
- Отключение старых и выдача новых ролей;
- Проверка конфликтов доступа и соблюдение SoD (Segregation of Duties).

Увольнение:

- Блокировка и удаление учётных записей по расписанию;
- Отзыв доступов, архивация данных;
- Подпись по чек-листу увольнения.

Самообслуживание:

- Сотрудник может подать заявку на доступ к системе или роли;
- Согласование по иерархии или политике;
- Автоматическая активация и уведомление.

Аудит и отчётность:

- Кто, когда, кому выдал доступ и по какой причине;
- Какие роли активны сейчас, есть ли избыточные права;
- Готовые отчёты по соответствию требованиям (152-ФЗ, 239-ФСТЭК, ISO 27001).

2.3.2.5 Политики и безопасность

Модуль IDM обеспечивает безопасность на уровне процессов и данных:

- ABAC/RBAC политики — гибкая настройка прав по ролям, атрибутам, сценариям;
- SOD (разделение обязанностей) — контроль конфликтующих доступов;
- Верификация сотрудников — подтверждение личности через SSO, 2FA, сертификаты;

- Аудит действий администраторов и сотрудников — полная прослеживаемость;
- Шифрование персональных данных (ПДн) — соблюдение требований 152-ФЗ;
- Таймеры автоматического удаления / блокировки — для временных доступов и подрядчиков.

2.3.2.6 Преимущества внедрения IDM-модуля

- Сокращение времени и ошибок при управлении учетными записями;
- Централизованный контроль над доступами и ролями;
- Повышение прозрачности и ответственности;
- Устранение “забытых” или “висячих” аккаунтов;
- Соответствие нормативным требованиям (ФСТЭК, 152-ФЗ, ISO 27001);
- Увеличение безопасности и производительности ИБ-команд.

2.3.3 Модуль CFS (Central File Sharing)

2.3.3.1 Назначение

Модуль CFS (Central File Sharing) обеспечивает защищённый централизованный доступ к файлам и каталогам внутри организации и за её пределами. Он предназначен для безопасного обмена файлами, контроля за доступом к документам, временной передачи данных и прозрачного журналирования всех операций.

CFS позволяет организациям отказаться от использования небезопасных внешних сервисов (Dropbox, Google Drive, почта и мессенджеры), обеспечивая соответствие требованиям по защите ПДн и корпоративной информации.

2.3.3.2 Основные функции

- Каталог файлов и пространств (Workspaces) — организация доступа к документам по проектам, отделам, ролям, с иерархией и делегированием;
- Гибкое управление правами — разграничение на чтение, редактирование, скачивание, пересылку, загрузку, удаление, с учетом ролей и контекста;
- Временные безопасные ссылки (Secure Link Generator) — выдача внешних ссылок с ограничением по времени, IP, числу загрузок, 2FA;
- Контроль загрузки и скачивания — возможность запретить скачивание файла, разрешив только просмотр (PDF Preview);
- Шифрование файлов при хранении и передаче — на базе AES-256 или ГОСТ по выбору организации;
- Полный аудит всех операций — кто, когда, откуда, с каким результатом загрузил, скачал, удалил или переслал файл;
- Внутренний редактор PDF/Office — возможность редактирования, комментирования и согласования документов без скачивания;
- Подпись файлов (по требованию) — подписание документов сертификатом пользователя через интеграцию с УЦ/СКЗИ;
- Проверка антивирусом и DLP — интеграция с решениями безопасности для фильтрации загружаемых файлов;
- Журналирование и восстановление — версия файлов, откат изменений, корзина, отслеживание истории доступа;
- Интерфейс командной строки и API — поддержка автоматизированной загрузки и выгрузки данных из внешних систем.

2.3.3.3 Архитектура модуля

Модуль CFS состоит из следующих компонентов:

Компонент	Назначение
File Access Engine	Центральный компонент, обрабатывающий запросы на доступ, управление разрешениями, маршрутизацию.
Secure Link Generator	Генератор временных ссылок с параметрами ограничений, подписываемых токенами.
File Storage (MinIO / S3)	Надёжное хранилище с возможностью резервирования, версионирования и шифрования.
Preview & Conversion Engine	Генерация превью, PDF-обложек, скриншотов, водяных знаков.
File Audit Engine	Логирование всех операций, генерация отчётов, экспорт в SIEM.
Web UI & Self-Service	Веб-интерфейс для загрузки, поиска, просмотра, управления и согласования файлов.
API-шлюз	REST API и WebSocket-интерфейс для интеграции с корпоративными системами, ботами, порталами.

2.3.3.4 Поддерживаемые сценарии использования

- Обмен документами внутри проектной команды — по группам, с разграничением на загрузку, чтение, комментирование;
- Внешняя передача файлов контрагенту — выдача временной ссылки, требующей SMS-кода или сертификата;
- Юридическое согласование документов — версия, комментирование, отметки об утверждении, история;
- Автоматизированная выгрузка отчётов — внешние системы выгружают файлы по API, подписывают, загружают в CFS;
- Контроль несанкционированной утечки — запрет скачивания, видимость только в защищённой области предпросмотра;
- Временный доступ партнёру — приглашение по email, доступ к конкретной папке с ограничением по времени.

2.3.3.5 Безопасность и контроль доступа

Модуль CFS реализует гибкую модель защиты:

- Многоуровневая модель прав — права на уровне папки, файла, группы, с возможностью делегирования;
- Срок действия доступа — таймеры на внешние ссылки и внутренние права;
- Фильтрация по IP и локации — запрет доступа извне или вне графика;
- Шифрование на стороне сервера — как при передаче (TLS), так и в хранилище;
- Маскирование и водяные знаки — для ограниченного просмотра без скачивания;
- DLP и антивирусная проверка — интеграция с внешними системами (по API или через промежуточную очередь);
- Аудит — фиксация каждого действия, экспорт событий в SIEM.

2.3.3.6 Преимущества внедрения CFS-модуля

- Исключение теневых ИТ-сервисов (облачных хранилищ, личных почт и мессенджеров);
- Контроль и отслеживание всех действий с корпоративными файлами;
- Упрощение внутреннего и внешнего обмена данными с учётом безопасности;
- Интеграция с электронными подписями и СКЗИ;
- Поддержка корпоративных политик хранения, ротации и удаления;
- Соответствие требованиям 152-ФЗ, 239-ФСТЭК, ISO 27001, DLP-политикам.

3. Описание функционирования системы

Система CTfind Security функционирует как согласованная модульная платформа, в которой ядро обеспечивает координацию всех пользовательских действий, обработку бизнес-логики, реализацию политик доступа, взаимодействие с внешними системами и безопасное выполнение операций. Работа пользователей и администраторов происходит через унифицированный веб-интерфейс, где каждая операция направляется в ядро, а затем делегируется соответствующему модулю (PAM, IDM, CFS) либо обрабатывается напрямую.

3.1. Принципы взаимодействия компонентов

Компоненты CTfind Security взаимодействуют между собой на основе следующих принципов:

- Событийное взаимодействие — компоненты обмениваются сообщениями через внутреннюю шину событий (event bus), обеспечивая масштабируемость и отказоустойчивость;
- REST/GraphQL API — взаимодействие между модулями и внешними системами осуществляется через защищенные программные интерфейсы;
- Очереди задач — обработка заявок и операций происходит асинхронно с помощью очередей (например, Celery, Redis, Kafka);
- Служба авторизации ядра — все запросы пользователей проходят через централизованную проверку прав и токенов доступа.

3.2. Взаимодействие ядра с модулями

Пример взаимодействия:

1. Пользователь подаёт заявку на доступ (через IDM или PAM-интерфейс)

→ Ядро проверяет права пользователя, создаёт заявку и маршрутизирует её на согласование в Access Request Engine.

2. Заявка одобряется

   → Ядро активирует доступ, выдает временный токен или прокси-сессию, запускает PAM Gateway или Provisioning Engine (в зависимости от типа ресурса).

3. Сессия записывается (PAM) или создаётся новая учётная запись (IDM)

   → Ядро логирует событие, передаёт информацию в аудит.

4. Файлы предоставляются во временное использование (CFS)

   → Система создаёт безопасную ссылку, применяет политики удаления по таймеру.

Вся логика маршрутов, сценариев и политик доступа централизованно конфигурируется через административный интерфейс ядра.

3.3. Обработка событий и операций

Каждое действие пользователя (запрос, доступ, редактирование, загрузка файла) формирует событие, обрабатываемое следующими слоями:

- Авторизация - ядро определяет допустимость действия;
- Маршрутизация - запрос направляется в нужный модуль;
- Обработка - модуль выполняет бизнес-логику (например, запись сессии, создание пользователя, выдача файла);
- Аудит - результат действия фиксируется в журнале безопасности;
- Оповещение - при необходимости инициируется уведомление (email, webhook, Telegram и пр.).

3.4. Интеграционные интерфейсы

CTfind Security поддерживает встроенную и внешнюю интеграцию:

Система	Поддерживаемое взаимодействие

Active Directory / LDAP	Синхронизация пользователей и групп, аутентификация
SIEM	Отправка логов и событий (Syslog, JSON, CEF)
HR-системы	Импорт оргструктуры и жизненных событий
Сторонние ИС	Подключение по REST API или webhook
Email / Telegram / Webhook	Оповещение и уведомление пользователей

3.5. Поддержка сценариев безопасности

Система CTfind Security реализует несколько встроенных сценариев обеспечения безопасности:

- Just-in-time доступ — временное предоставление прав с автоматическим отзывом;
- Принцип наименьших привилегий — автоматическая фильтрация разрешений на основе роли, атрибутов и контекста;
- Двухфакторная аутентификация (2FA) — включается при доступе к привилегированным ресурсам или CFS;
- Аудит 100% действий — полная запись операций и сессий;
- Контроль команд — проверка и блокировка критических CLI-команд в PAM;
- Исключение “перехода” между подсистемами без повторной авторизации — SSO внутри платформы.

4. Описание программного обеспечения

Система CTfind Security реализована в виде распределённой модульной платформы, построенной с применением современных веб-технологий и событийной архитектуры. В основе ядра лежит высокопроизводительный backend на Node.js с использованием Apache Kafka в качестве шины обмена сообщениями. Отдельные функциональные сервисы реализованы на Python.

Такой подход обеспечивает масштабируемость, отказоустойчивость и независимость компонент, позволяя развивать систему по микросервисной модели.

4.1. Используемые технологии

CTfind Security использует стек технологий с открытым исходным кодом и промышленными стандартами:

Слой	Технологии
Интерфейс пользователя (UI)	Vue.js (Composition API), TailwindCSS, WebSocket
Ядро системы	Node.js (Express, NestJS), Apache Kafka, TypeScript
Фоновая обработка	Python (FastAPI, Celery)
Хранилища данных	PostgreSQL, MongoDB, MinIO (объектное хранилище)
Аутентификация и безопасность	OAuth2, JWT, OpenID Connect, 2FA, SAML, JaCarta, TLS, ГОСТ-алгоритмы
Контейнеризация и оркестрация	Docker, docker-compose, Helm (Kubernetes-ready)
Мониторинг и логирование	Prometheus, Grafana, Loki, ELK, Sentry
Интеграции	REST API, Webhooks, LDAP/AD, SCIM, SMTP, Telegram API

4.2. Общесистемное ПО

Ядро системы CTfind Security включает следующие программные компоненты:

- Служба авторизации и токенов (Node.js) — централизованная проверка прав, выпуск JWT и OIDC-токенов;
- Менеджер ролей и политик доступа — RBAC/ABAC с централизованным хранилищем;
- Kafka Event Bus — маршрутизация событий и запросов между модулями;
- Service Orchestrator — координация фоновых задач и распределённых сервисов;
- API Gateway — единая точка входа во все интерфейсы (REST/GraphQL);
- Audit Logger — сбор и агрегация событий безопасности;
- Notification Service — шлюз уведомлений по email, Telegram и webhook.

4.3. Специализированное ПО модулей

Модуль	Компоненты	Краткое описание
PAM	PAM Gateway, Session Recorder, CLI Command Control	Управление сессиями и командами, запись видео, прокси-доступ
IDM	Provisioning Engine, Directory Sync, Policy Engine	Жизненный цикл пользователей, политики доступа, синхронизация с AD/LDAP
CFS	File Access Engine, Secure Link Generator, File Audit Engine	Безопасный обмен файлами, журналирование, контроль прав

Модули взаимодействуют с ядром через Kafka и используют общие механизмы авторизации, мониторинга и журналирования.

4.4. Методы и средства разработки

Разработка системы CTfind Security осуществляется с соблюдением принципов CI/CD, code-review и сквозного тестирования. Используемые практики:

- Контроль версий — Git (GitLab/GitHub);
- CI/CD — GitHub Actions, GitLab CI;
- Тестирование — Jest (Node.js), Pytest (Python), Cypress (UI);
- Документирование API — Swagger / OpenAPI;
- Проверка безопасности — Trivy, Snyk, ESLint, Bandit;
- Сборка и развёртывание — Docker, Helm Charts (для Kubernetes или on-premises).

5. Сведения о развертывании и эксплуатации

Система CTfind Security предназначена для гибкого развёртывания в различных инфраструктурных средах, включая корпоративные дата-центры (on-premises), частные и публичные облака, а также в гибридной архитектуре. Благодаря модульной структуре и контейнеризации, система может быть развёрнута поэтапно, в соответствии с приоритетами и задачами информационной безопасности заказчика.

5.1. Поддерживаемые конфигурации

Система поддерживает следующие варианты развертывания:

Вариант	Описание
On-premises	Развёртывание в локальной ИТ-инфраструктуре заказчика. Все компоненты размещаются в изолированной сети и управляются внутренними администраторами. Полный контроль над данными и обновлениями.

Облачное развёртывание (private/public cloud)	Размещение в инфраструктуре заказчика на платформе OpenStack, VMware, Yandex Cloud, VK Cloud, AWS, Azure и др. Возможна аренда управляемого стенда в облаке вендора.
Гибридное развертывание	Комбинация локального ядра с облачными модулями (например, CFS или IDM). Может использоваться для разграничения доступа к чувствительным и вторичным данным.
Тестовая/пилотная установка	Минимальная конфигурация на одном сервере или виртуальной машине. Позволяет оценить функциональность системы без полной интеграции.

Все варианты поддерживают отказоустойчивую архитектуру, масштабирование и миграцию между средами.

5.2. Варианты внедрения

5.2.1 Минимальная конфигурация (Standalone)

- Один сервер;
- Docker Compose;
- PostgreSQL + MinIO + Redis + Kafka (в контейнерах);
- Используется для пилотов, разработки, демо-стендов.

5.2.2 Корпоративная конфигурация (Clustered)

- Модули размещаются на разных узлах;
- Используется Kubernetes или Docker Swarm;
- Kafka, БД и API-шлюз реплицированы;
- Поддержка балансировки, отказоустойчивости и мониторинга.

5.2.3 Облачная / гибридная

- Ядро в защищённой сети (например, в ЦОД или на облачном хостинге);
- Пользовательский интерфейс и уведомления доступны через публичный шлюз;
- Модули PAM/IDM/CFS могут быть размещены в разных зонах ответственности (например, IDM — в HR-контуре, PAM — в ИБ-контуре).

5.3. Аварийное восстановление

CTfind Security реализует встроенные средства восстановления и резервирования:

- Автоматическое резервное копирование баз данных и журналов;
- Поддержка горячего резервирования модулей (active/passive);
- Снятие дампов конфигурации и данных (по расписанию или вручную);
- Встроенные механизмы восстановления состояния после сбоя Kafka или Redis;
- Возможность развёртывания стенда на бэкапных узлах с минимальной задержкой.

5.4. Резервное копирование и обновления

Резервное копирование

- Хранение бэкапов в MinIO, S3, локальном хранилище или внешнем SMB/NFS;
- Поддержка шифрования и контроля целостности резервных копий;
- Возможность восстановления отдельных модулей без остановки всей системы;
- Интеграция с корпоративными системами резервного копирования (Veeam, Bacula и др.).

Обновления

- On-premises: доставка обновлений в виде Docker-образов или Helm-чартов;
- Облако: автоматическая публикация обновлений в репозитории и уведомление администраторов;
- Поддержка миграции схемы БД и rollback при ошибках обновления;
- Возможность обновления поэтапно — сначала ядро, затем модули.

6. Обеспечение безопасности

Система CTfind Security разработана с приоритетом обеспечения информационной безопасности и соответствует лучшим практикам Zero Trust, принципам минимизации прав и требованиям российского законодательства в области защиты информации. Все компоненты системы используют защищённые каналы связи, централизованную модель авторизации и встроенные механизмы аудита.

6.1. Механизмы защиты

CTfind Security реализует многоуровневую модель защиты, включающую:

Категория	Механизмы
Аутентификация	JWT, OAuth2, OpenID Connect, SAML, Kerberos, 2FA, поддержка смарт-карт и токенов JaCarta
Авторизация	Ролевое (RBAC) и атрибутивное (ABAC) управление доступом, политики согласования
Шифрование	TLS 1.2/1.3, ГОСТ-алгоритмы, шифрование резервных копий и хранилищ
Изоляция	Контейнеризация модулей, изоляция сетевых сегментов, доступ по VPN или ZTNA

Журналирование	Полный аудит всех операций, включая команды в CLI-сессиях и работу с файлами
Контроль доступа	Политики временного доступа, гео-ограничения, расписания, доверенные устройства
Сигнатурная защита	Контроль команд и операций с помощью белых/чёрных списков (в PAM)
Мониторинг	Интеграция с SIEM, поведенческий анализ, контроль аномалий входа и действий

6.2. Аудит и журналирование

Система ведёт централизованный аудит всех действий пользователей, администраторов и сервисов.

Что логируется:

- Все действия в интерфейсе (заявки, изменения, загрузки);
- Каждая команда в терминальной сессии (PAM);
- Записи видео-сессий и файловых операций (CFS);
- Входы/выходы, попытки аутентификации, смена паролей;
- Системные события (обновления, сбои, ошибки).

Где хранятся логи:

- Elasticsearch / MongoDB;
- Возможность экспорта в SIEM-системы (CEF, Syslog, JSON);
- Поддержка TTL и архивации;
- Настраиваемая маскировка чувствительных данных (DLP-фильтры).

6.3. Управление правами и доступом

Механизмы предоставления доступа строятся по принципам Just-in-Time и Least Privilege:

- Доступ выдается на ограниченное время по заявке, согласованной с ответственными;
- Возможна автоматическая выдача на основе роли, подразделения и контекста (рабочее время, IP, устройство);
- Отзыв прав при увольнении, блокировке, нарушении политики или по истечении срока;
- Роли можно определять вручную или формировать из атрибутов (например, "DevOps в проекте X").

Права хранятся централизованно в ядре и распространяются в модули при необходимости.

6.4. Криптографическая защита информации

В системе используется криптография как российского, так и международного уровня:

- TLS 1.2/1.3 для всех внешних и внутренних API-запросов;
- ГОСТ Р 34.10/34.11, КриптоПро CSP / VipNet CSP (при необходимости соответствия требованиям ФСТЭК/ФСБ);
- Шифрование паролей, токенов и секретов в хранилище (AES-256, ГОСТ);
- Шифрование резервных копий и записей сессий;
- Хранилища паролей (Vault) с многоступенчатым доступом и логированием всех операций.

Перечень принятых сокращений

Сокращение	Расшифровка
CTfind	Cybersecurity Technologies: Framework for Identity and Network Defense
PAM	Privileged Access Management — управление привилегированными доступами
IDM	Identity Management — управление цифровыми идентичностями
CFS	Central File Sharing — защищённый файловый обмен
RBAC	Role-Based Access Control — ролевое управление доступом
ABAC	Attribute-Based Access Control — атрибутивное управление доступом
2FA	Two-Factor Authentication — двухфакторная аутентификация
SIEM	Security Information and Event Management — система мониторинга ИБ
API	Application Programming Interface — программный интерфейс
JWT	JSON Web Token — формат токена авторизации
SSO	Single Sign-On — единая точка входа
DLP	Data Loss Prevention — предотвращение утечек данных
VPN	Virtual Private Network — виртуальная частная сеть

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

Подпись и дата

Инв. №дубл.

Взам. инв. №

Подпись и дата

Инв. №подл.

						Лист
						34
Изм.	Лист	№ докум.	Подп.	Дата		