



ЕДИНЬЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ЕДИНЬЙ **ЦЕНТР УПРАВЛЕНИЯ**
DALLAS LOCK

ОБЗОР





ЕДИНЬЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ОГЛАВЛЕНИЕ

Введение	1
1. Масштабируемость и архитектура	2
Варианты развертывания	3
Совместимость с ОС	3
Интеграция со сторонними продуктами	3
2. Преимущества	4
3. Функциональные возможности	5
Агент ЕЦУ	6
Контроль сетевого оборудования	6
Управление компонентами безопасности	7
Аудит и мониторинг	9
Шаблоны политик и управление доступом	9
4. Основные сценарии применения	10
Заключение	11



Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.



ЕДИНЬЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ВВЕДЕНИЕ

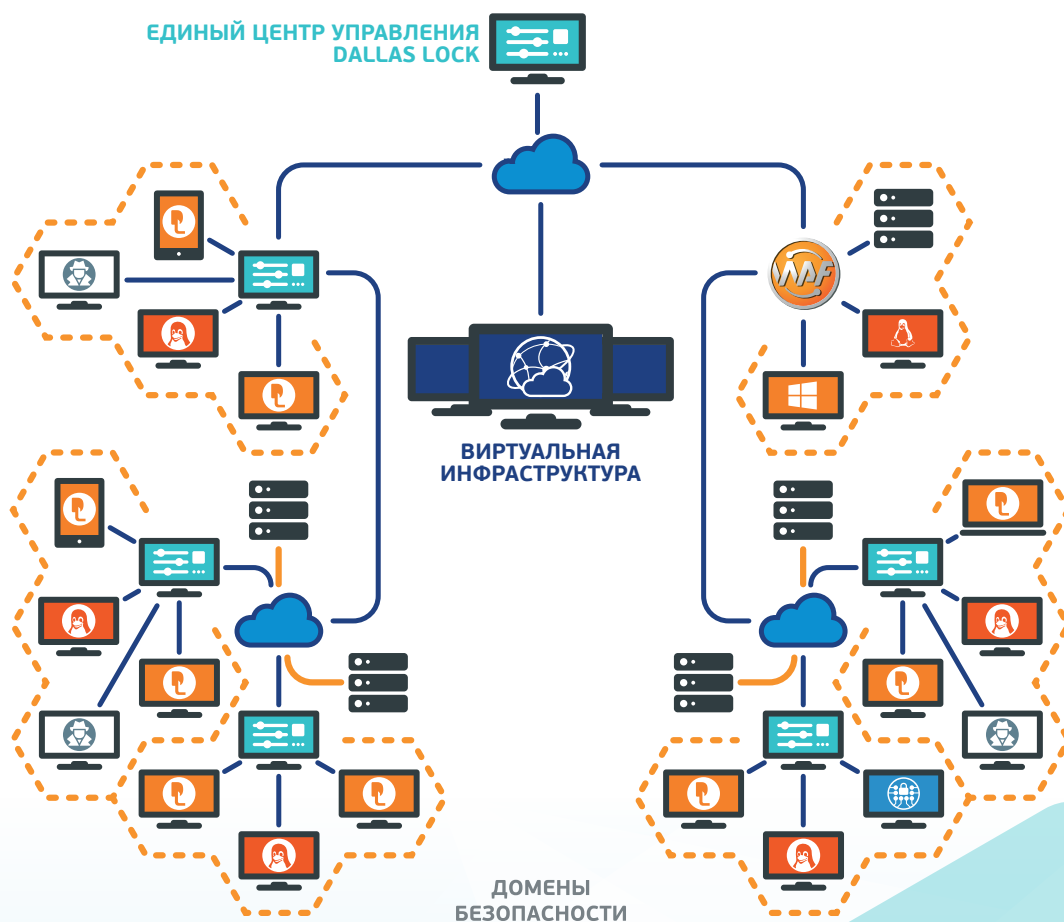
ЕЦУ Dallas Lock (Единый центр управления) представляет собой кроссплатформенное средство централизованного управления, которое работает на сертифицированных российских и международных операционных системах. Решение обеспечивает комплексный контроль всей ИТ-инфраструктуры: рабочих станций, серверов, сетевого оборудования и периферийных устройств.

ЕЦУ Dallas Lock объединяет в одном интерфейсе управление всеми средствами защиты продуктовой линейки Dallas Lock, а также рабочими станциями без установленных СЗИ. Продукт ориентирован на организации любого масштаба: от небольших офисов до крупных территориально распределенных структур с десятками тысяч рабочих мест.



1. МАСШТАБИРУЕМОСТЬ И АРХИТЕКТУРА

Архитектура ЕЦУ Dallas Lock построена на принципе иерархических доменов безопасности. Один сервер ЕЦУ может управлять до 10 000 клиентских модулей. Для более крупной инфраструктуры предусмотрено объединение серверов в кластер и построение дерева доменов безопасности. При количестве защищаемых объектов более 100 шт. использование ЕЦУ Dallas Lock строго обязательно.



Архитектура домена безопасности ЕЦУ Dallas Lock

СРЕДСТВА ЗАЩИТЫ

-  СЗИ DALLAS LOCK 8.0
-  СЗИ DALLAS LOCK LINUX
-  ШЛЮЗ БЕЗОПАСНОСТИ WAF DALLAS LOCK
-  СЗИ ВИ DALLAS LOCK
-  СДЗ DALLAS LOCK (УБ, ПР)

УПРАВЛЯЕМЫЕ ОБЪЕКТЫ

-  АГЕНТ ЕЦУ ОС WINDOWS/LINUX, ANDROID
-  СЕТЕВОЕ ОБОРУДОВАНИЕ
-  ACTIVE DIRECTORY/ LDAP

**ВАРИАНТЫ
РАЗВЕРТЫВАНИЯ**

- **Одиночный сервер ЕЦУ** для небольших и средних организаций (до 10 000 клиентов).
- **Кластер серверов ЕЦУ** для повышения отказоустойчивости и распределения нагрузки с репликацией конфигурации между серверами.
- **Дерево доменов безопасности** для территориально распределенных организаций. Родительский домен управляет подчиненными, каждый уровень может иметь собственные политики безопасности.

**СОВМЕСТИМОСТЬ
С ОС**

ЕЦУ Dallas Lock работает на ОС семейств Windows и Linux, в том числе на:

- Microsoft Windows Server 2012 R2, 2016, 2019, 2022, 2025;
- Astra Linux Special Edition (релиз «Смоленск»);
- Альт Рабочая Станция, Альт Сервер, Альт 8 СП Сервер 10;
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- ROSA FRESH DESKTOP 12;
- МСВСфера АРМ 9.

**ИНТЕГРАЦИЯ
СО СТОРОННИМИ
ПРОДУКТАМИ**

- Антивирус Kaspersky: запуск сканирования, обновление, получение журналов.
- SIEM-системы: передача событий безопасности.
- Службы каталогов: Active Directory, FreeIPA, Samba, ALD Pro, РЕД АДМ.
- Сертифицированная СУБД Jatoba для хранения данных.



2. ПРЕИМУЩЕСТВА

- **Единая точка управления всей системой защиты.** Администратор работает в одном интерфейсе с одинаковыми принципами настройки для всех продуктов Dallas Lock.
- **Снижение нагрузки на администраторов ИБ.** Групповые операции, шаблоны политик и автоматизация рутинных задач сокращают время на обслуживание.
- **Готовые шаблоны политик** для требований ФСТЭК России к АС, ГИС, ИСПДн и КИИ (1, 2, 3 категории значимости). Достаточно выбрать шаблон и применить ко всему домену.
- **Кроссплатформенность.** ЕЦУ Dallas Lock работает на Windows и отечественных Linux-дистрибутивах, в том числе сертифицированных ОС.
- **Иерархическая модель** управления с разграничением прав и зон ответственности. Возможность запрета изменения политик на нижестоящих уровнях.
- **Поддержка NAT.** Клиенты за NAT-устройствами подключаются к серверу ЕЦУ без дополнительных сетевых настроек.
- **Централизованная установка и обновление.** Массовое развертывание средств защиты и Агентов ЕЦУ на рабочие станции без физического доступа.



3. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

ЕЦУ Dallas Lock обеспечивает централизованное управление всеми продуктами линейки Dallas Lock. Для каждого управляемого продукта доступны общие возможности:

- Синхронизация политик безопасности между ЕЦУ и управляемыми модулями;
- Управление пользователями и группами на уровне домена безопасности;
- Сбор журналов модулей в единую систему хранения ЕЦУ или внешнюю базу данных;
- Мониторинг состояния модулей: подключение, версия ПО, заполнение журнала;
- Сигнализация об инцидентах безопасности в реальном времени;
- Завершение работы и перезагрузка управляемых модулей.

На схеме ниже представлены уникальные возможности управления каждым продуктом через ЕЦУ.

УПРАВЛЕНИЕ ПРОДУКТАМИ DALLAS LOCK ЧЕРЕЗ ЕЦУ



ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK



СЗИ DALLAS LOCK 8.0 / LINUX

Защита рабочих станций и серверов

- СЗИ DALLAS LOCK 8.0-K / 8.0-C (Windows)
- СЗИ DALLAS LOCK LINUX
- Модули: МЭ, СОВ, СОР, СКН

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ ЧЕРЕЗ ЕЦУ:

- Удаленное развертывание и обновление
- Управление МЭ, СОВ (вкл. песочницу), СОР, СКН
- Проверка целостности объектов
- Сканирование на IoC и уязвимости
- Сигнализация о событиях НСД



СЗИ ВИ DALLAS LOCK

Защита виртуальных инфраструктур

- VMware VSphere (ESXi 5.5-8.0), Hyper-V, KVM
- oVirt, zVirt, РЭД Виртуализация
- HOSTVM, ROSA Virtualization, Альт Виртуализация

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ ЧЕРЕЗ ЕЦУ:

- Задания: получение / применение конфигурации
- Отчет о параметрах безопасности СЗИ ВИ
- Отправка файла лицензии
- Открытие веб-интерфейса администрирования
- Централизованное управление МЭ СЗИ ВИ



СДЗ DALLAS LOCK

Средство доверенной загрузки

- СДЗ ПР (плата расширения)
- СДЗ УБ (уровень BIOS / UEFI)

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ ЧЕРЕЗ ЕЦУ:

- Удаленная авторизация пользователя
- Удаленное управление оболочкой администрирования
- Тестирование функций СДЗ
- Сброс ДВН, очистка журнала
- Настройка аппаратных идентификаторов
- Взаимодействие с агентом ШОС



WAF DALLAS LOCK

Межсетевой экран прикладного уровня

- WAF: защита уровня веб-приложений
- UTM: МЭ уровня логических границ сети

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ ЧЕРЕЗ ЕЦУ:

- Перевод шлюза в режим Master (кластер)
- Сброс временных блокировок
- Аварийный режим (активация / деактивация)
- Обновление базы решающих правил
- Создание / восстановление резервной копии
- Сброс к заводским настройкам
- Применение файла лицензии

АГЕНТ
ЕЦУ

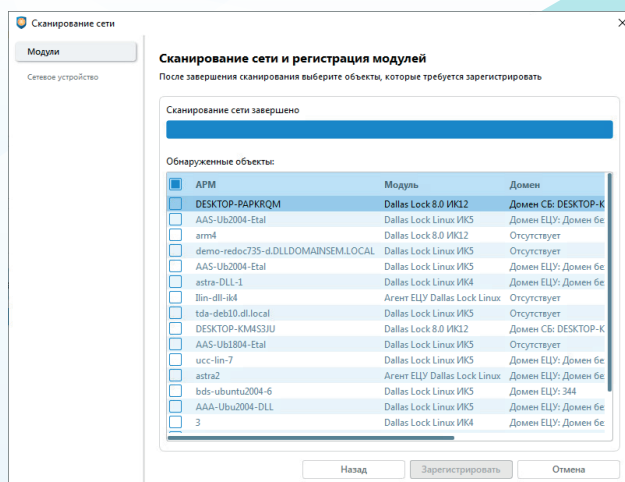
Представляет собой кроссплатформенный модуль для рабочих станций без средств защиты Dallas Lock (Windows и Linux). Обеспечивает прозрачность и контроль без необходимости установки специализированных СЗИ:

- сбор информации: системные журналы, версия ОС, IP/MAC-адреса;
- мониторинг: отображение инцидентов безопасности, просмотр состояния APM;
- отчетность: формирование отчетов об аппаратном и программном обеспечении с возможностью сравнения с эталонными значениями;
- удаленное подключение к рабочему столу пользователя;
- контроль целостности ПО и оборудования на уровне всего домена безопасности;
- удаленное обновление и централизованная установка Агентов ЕЦУ на всех станциях домена.

КОНТРОЛЬ СЕТЕВОГО
ОБОРУДОВАНИЯ

ЕЦУ Dallas Lock обнаруживает активное сетевое оборудование, регистрирует его в дереве домена безопасности и обеспечивает мониторинг конфигурации по протоколам SNMP и SSH, сбор событий по Syslog и контроль изменений параметров с возможностью сравнения текущих и эталонных значений.

Сводка		Конфигурация			
ЭНП					
☐ Показать только отличия					
№	Состояние	Параметр	Эталонное значение	Последнее значение	
1	☒	Описание	RouterOS CHR	RouterOS CHR	
2	☒	Идентификатор вендора	1.3.6.1.4.1.14988.1	1.3.6.1.4.1.14988.1	
3	☒	Контакты	Ø	Ø	
4	☒	Имя узла	MikrotikVM	MikrotikVM	
5	☒	Расположение	Main Office	Main Office	
6	☒	Сетевой уровень сервиса	78	78	
7	☒	Количество сетевых интерфейсов	1	1	
8	☒	Имя интерфейса	ether1	ether-changed	





ЕДИНЬЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

УПРАВЛЕНИЕ КОМПОНЕНТАМИ БЕЗОПАСНОСТИ



ЕЦУ Dallas Lock предоставляет единый интерфейс для настройки и мониторинга ключевых компонентов безопасности на клиентах СЗИ Dallas Lock 8.0 и СЗИ Dallas Lock Linux.

Межсетевой экран (МЭ). Создание, редактирование, активация профилей МЭ, назначение приоритетов. Управление правилами фильтрации трафика, сегментами сети и правилами веб-контроля.

Имя	Статус	Приоритет
Аварийный режим: Автоматическая активация при нарушении КЭ МЭ	не задано	
Аварийный режим: Автоматическая активация при нарушении Агента ВИ со стороны ЦУ	не задано	
Аварийный режим: Автоматическая активация при сбое самотестирования	не задано	
Аварийный режим: Запрет внешнего трафика к гипервизору/СВ	не задано	
Аварийный режим: Запрет трафика между Агентами ВИ и ЦУ	не задано	
Аварийный режим: Запрет трафика между ВМ	не задано	
Белый и черный списки приложений	не задано	
Блокировка протокола QUIC	не задано	
Блокировка адресов	не задано	
Включить уведомление в трей при блокировке соединения	не задано	
Включить фильтрацию	не задано	
Доверенные правила МЭ	не задано	
Использовать безопасный веб-серфинг	не задано	
Максимальный размер http-заголовка	не задано	
Межсетевой экран	не задано	
Отключать GZIP для анализа HTTP трафика	не задано	
Отключать локальные правила МЭ при автопереключении профиля МЭ	не задано	
Отображать сообщение о заблокированном соединении (сайте)	не задано	
Периодичность проверки защищенности системы	не задано	
Протоколирование событий МЭ	не задано	
Протоколирование событий МЭ	не задано	
Режим обучения МЭ	не задано	
Режим работы фильтрации	не задано	



Система обнаружения вторжений (СОВ). Централизованная настройка сигнатур сетевого трафика и индикаторов конфигурации. Контроль запуска приложений и изменений реестра. Просмотр и анализ событий СОВ с возможностью фильтрации по категориям и приоритетам.

УПРАВЛЕНИЕ КОМПОНЕНТОМ СОВ

Сводка СОВ | Общие настройки СОВ | Сигнатуры | Настройки эвристики

Доверенные адреса | Контроль приложений | Контроль реестра

Основная информация

Сигнатуры трафика: **АКТУАЛЬНЫ**

Индикаторы компрометации: **АКТУАЛЬНЫ**

ПАРАМЕТРЫ ОБНОВЛЕНИЯ | Подробнее

Журнал событий

☒ Сигнатуры трафика ☐ Сетевые атаки ☐ Подозрительная активность

Количество запрашиваемых записей: 100 | Параллельно записей

Фильтр по времени: За день | За неделю | За месяц | Период

С: 12.05.2025 3:00 | Применить

По: 12.05.2025 17:52

Дата и время	APM	Тип атаки	Адрес источника	PID	Пользователь	Комментарий
--------------	-----	-----------	-----------------	-----	--------------	-------------



Обнаружение и реагирование (COP). Централизованное управление подсистемой обнаружения и реагирования позволяет:

- управлять базой индикаторов компрометации (IoC), в том числе добавлять пользовательские индикаторы и группировать их для удобной настройки правил реагирования;
- создавать правила автоматического реагирования с выбором действия, включая блокировку процесса, удаление файла и изоляцию узла от сети;
- запускать сканирование системы на обнаружение IoC по требованию или по расписанию, с настройкой области сканирования и автоматической проверкой новых файлов;
- регулярно обновлять базу индикаторов компрометации.



Контроль съемных носителей (СКН). Централизованная настройка правил доступа к съемным машинным носителям информации: разрешение, запрет и ограничение по типу устройства. Ведение реестра доверенных носителей, аудит операций подключения и передачи данных.



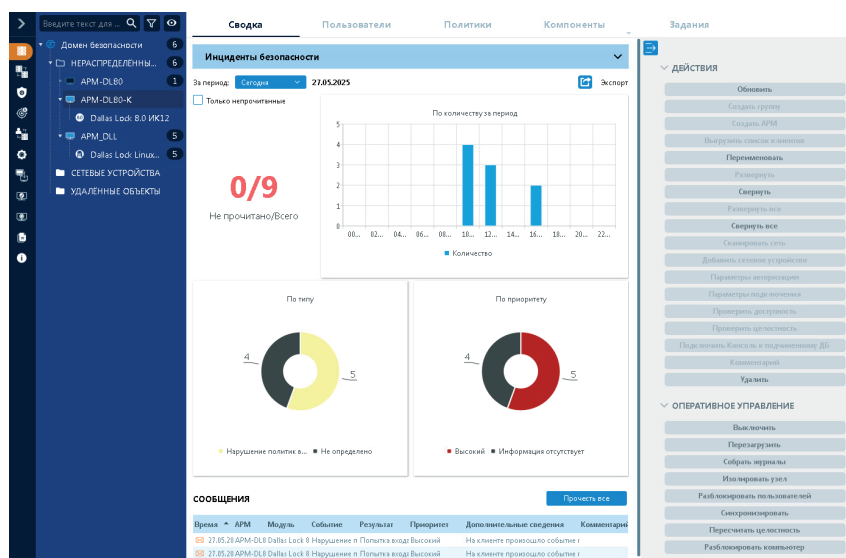
Безопасная среда COB (песочница). Централизованное управление параметрами безопасной среды для клиентов СЗИ Dallas Lock 8.0 и СЗИ Dallas Lock Linux:

- включение/отключение безопасной среды и автоматического запуска приложений;
- настройка правил контроля приложений и эвристического анализа (Dallas Lock 8.0);
- управление профилями изоляции: создание, редактирование, копирование и удаление (Dallas Lock Linux);
- настройка автоматической очистки временных каталогов и доверенного расположения.

АУДИТ
И МОНИТОРИНГ

Подсистема аудита собирает, обрабатывает и визуализирует события безопасности:

- централизованный просмотр журналов с фильтрацией по типу, приоритету и времени;
- графическая панель инцидентов с группировкой по типу и приоритету;
- мониторинг родительских и подчиненных ДБ: отчеты о составе групп пользователей, управление лицензированием, контроль администрирования;
- анализ уязвимостей установленного ПО по Банку данных угроз ФСТЭК России. Формирование отчетов по журналам клиентов СЗИ Dallas Lock 8.0;
- отслеживание последней активной сессии пользователя.



Панель мониторинга инцидентов безопасности

ШАБЛОНЫ ПОЛИТИК
И УПРАВЛЕНИЕ
ДОСТУПОМ

ЕЦУ Dallas Lock содержит предустановленные шаблоны политик безопасности в соответствии с требованиями ФСТЭК России: для АС, ГИС, ИСПДн и КИИ (1, 2, 3 категории значимости). Администратор выбирает шаблон, применяет ко всему домену и при необходимости корректирует параметры.

- Запрет переопределения политик на дочерних уровнях ДБ.
- Блокировка учетных записей при срабатывании правил реагирования с распространением по всему домену.
- Централизованное управление локально заблокированными учетными записями.
- Управление принадлежностью пользователя к объектам дерева ДБ из свойств учетной записи.
- Управление доступом к принтерам: назначение дискреционного и мандатного доступа.
- Распределение квот на управление клиентами между подчиненными ДБ. Один файл лицензии для родительского и подчиненного ДБ.



4. ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ

Обнаружение и регистрация

Сканирование сети для обнаружения средств защиты Dallas Lock, Агентов ЕЦУ и сетевого оборудования. Автоматическое введение под управление ЕЦУ.

Управление политиками безопасности

Централизованное управление учетными записями и политиками безопасности всех средств защиты Dallas Lock из единого интерфейса.

Мониторинг и аудит

Мониторинг событий безопасности на всех уровнях иерархии с визуализацией инцидентов и формированием отчетов.

Инвентаризация и контроль целостности

Сбор отчетов об аппаратном и программном обеспечении. Сравнение с эталонными значениями. Контроль изменений.

Удаленное управление станциями

Подключение к рабочему столу через Агент ЕЦУ. Перезагрузка, выключение, удаление агента.

Развертывание и обновление

Централизованная установка и удаление средств защиты Dallas Lock. Удаленное обновление Агентов ЕЦУ.

Контроль сетевого оборудования

Мониторинг конфигурации активного сетевого оборудования по SNMP/SSH с контролем изменений.

Управление компонентами безопасности

Настройка МЭ, COB, COP, СКН и Безопасной среды COB. Управление модулями СЗИ ВИ, СДЗ и WAF Dallas Lock.

Обнаружение вторжений и реагирование

Настройка COB и COP: сигнатуры, индикаторы компрометации, правила автоматического реагирования.

Соответствие требованиям ФСТЭК

Применение шаблонов политик для АС, ГИС, ИСПДн и КИИ. Запрет переопределения политик на дочерних уровнях.



ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ЗАКЛЮЧЕНИЕ

ЕЦУ Dallas Lock является современным инструментом централизованного управления всей продуктовой линейки Dallas Lock. Продукт обеспечивает комплексный контроль безопасности ИТ-инфраструктуры из единого интерфейса и подходит для организаций любого масштаба.

ЕЦУ Dallas Lock рекомендуется применять в инфраструктурах любого размера, а при количестве защищаемых объектов (рабочие станции, серверы, сетевое оборудование) более 100 шт. его использование строго обязательно.

Для получения подробной информации обратитесь к документу «Инструкция по использованию ЕЦУ Dallas Lock» или запросите бесплатную демо-версию продукта.

ЗАЯВКА НА ДЕМОВЕРСИЮ
ОТСКАНИРУЙТЕ QR-КОД
<https://dallaslock.ru/dlecu-demo>





192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

<http://www.confident.ru/>
<http://www.dallaslock.ru/>
e-mail:

isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда:



www.confident.ru



www.dallaslock.ru



Telegram-канал

