КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

«Защита не «для галочки»: как реализовать меры защиты, чтобы они работали на вас»

?

- Как влияет приказ № 117 ФСТЭК России на подход к защите информации?
- Какие нормативные требования есть для финансового сектора?
- Какие задачи стоят перед объектами КИИ?

Как 117-й приказ ФСТЭК России формулирует требования

117-й приказ описывает защиту **через функции**, а не продукты:

- идентификация и аутентификация
- управление доступом (в т. ч. привилегированным)
- регистрация и анализ событий
- мониторинг ИБ
- защита конечных устройств
- защита сетевого взаимодействия
- управление уязвимостями и обновлениями

Необходима архитектура, а не набор решений

Формальное наличие СЗИ ≠ выполнение требований приказа

Меры 117 приказа, которые закрывает Dallas Lock Linux

Категория мер	Код	Наименование меры	Покрытие
1. Идентификация и аутентификация (ИАФ)	ИАФ.1	Идентификация пользователей	✓ Полностью
	ИАФ.2	Идентификация устройств	✓ Полностью
	ИАФ.3	Аутентификация пользователей	✓ Полностью
	ИАФ.4	Аутентификация устройств	± Частично
2. Управление доступом (УПД)	УПД.1	Реализация модели управления доступом	✓ Полностью
	УПД.2	Разграничение и контроль прав доступа	✓ Полностью
	УПД.3	Управление учётными записями	✓ Полностью
	УПД.4	Ограничение неуспешных попыток доступа	✓ Полностью
	УПД.7	Ограничение числа параллельных сеансов	✓ Полностью
	УПД.8	Блокирование сеанса при неактивности	✓ Полностью
	УПД.9	Контроль действий до идентификации	✓ Полностью
3. Регистрация событий безопасности (РСБ)	РСБ.1	Определение событий безопасности	✓ Полностью
	РСБ.2	Анализ событий безопасности и реагирование	✓ Полностью
	РСБ.3	Генерация временных меток	✓ Полностью
	РСБ.4	Сбор, хранение и защита данных о событиях	✓ Полностью
	РСБ.5	Реагирование на сбои регистрации	± Частично
9. Защита конечных устройств (ЗКУ)	ЗКУ.1	Контроль доступа	✓ Полностью
	ЗКУ.2	Контроль целостности	✓ Полностью
	ЗКУ.3	АВЗ и СОВ на конечных устройствах	± Частично
	ЗКУ.4	Мониторинг процессов и состояния устройства	✓ Полностью
	ЗКУ.5	Контроль трафика на устройстве	✓ Полностью
	ЗКУ.6	Регистрация и реагирование на устройстве	✓ Полностью

Категория мер	Код	Наименование меры	Покрытие
13. Антивирусная защита (АВЗ)	АВЗ.4	Замкнутая программная среда	± Частично
14. Обнаружение вторжений (СОВ)	СОВ.1	Обнаружение вторжений на периметре	± Частично
	СОВ.2	Обнаружение вторжений в сегментах ИС	± Частично
15. Сегментация и МЭ (МСЭ)	МСЭ.1	Сегментация сети	± Частично
	МСЭ.2	Демилитаризованная зона	± Частично
	МСЭ.3	Контроль сетевого доступа и фильтрация	✓ Полностью
17. Защита каналов связи (ЗКС)	ЗКС.1	Защита данных при передаче	± Частично
	ЗКС.2	Контроль атрибутов безопасности	± Частично
	ЗКС.3	Подлинность сетевых соединений	± Частично
	ЗКС.4	Контроль доступа к внешним ресурсам	± Частично

Более детальный перечень мер, которые закрывает Dallas Lock, можно запросить у менеджера Зеон.

Нормативная база для финансового сектора

Банковский сектор переживает масштабное обновление нормативной базы.
Основным документом сейчас является **Положение Банка России № 851-П** (вступило в силу в 2025 году, заменив 683-П).
Основная тематика — это **оценка по ГОСТ Р 57580 — обязательная аттестация.**

Банки обязаны регулярно (раз в 2 года для стандартного уровня, раз в год для повышенного) проводить оценку соответствия требованиям ГОСТ 57580.1. Прикладное ПО, обрабатывающее защищаемую информацию (системы ДБО, ядра АБС), должно пройти **сертификацию** или оценку соответствия по оценочному уровню доверия не ниже ОУД4 для системно значимых банков и не ниже ОУД5 для остальных.

Банки попадают под действие Федерального закона № 152-ФЗ «О персональных данных» (ИСПДн) и Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ).

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Меры по банковскому стандарту, которые закрывает Dallas Lock ГОСТ Р 57580.1- 2017

№	Условное обозначение	Содержание мер системы защиты информации	Уровни защиты информации			СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ, РК, МП)		Dallas Lock Linux	СДЗ Dallas Lock	СДЗ УБ Dallas Lock	СЗИ ВИ Dallas Lock	WAF Dallas Lock
			3	2	1	8.0-К	8.0-С					
Управление учетными записями и правами субъектов логического доступа (УЗП)												
1.	УЗП.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т	✓	✓	✓	✓	✓	✓	✓ * при доступе к веб-
2.	УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	О	О	Т	✓	✓					
3.	УЗП.3	Контроль отсутствия незаблокированных учетных записей: - уволенных работников;	О	О	Т	✓	✓					

№	Условное обозначение	Содержание мер системы защиты информации	Уровни защиты информации			СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ, РК, МП)		Dallas Lock Linux	СДЗ Dallas Lock	СДЗ УБ Dallas Lock	СЗИ ВИ Dallas Lock	WAF Dallas Lock
			3	2	1	8.0-К	8.0-С					
		(владельца ресурса доступа)										
8.	УЗП.8	Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации	О	Т	Т	✓	✓	✓	✓	✓	✓	
9.	УЗП.9	Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа	О	Т	Т	✓	✓	✓	✓	✓	✓	
10.	УЗП.10	Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа	Т	Т	Т	✓	✓	✓	✓	✓	✓	
11.	УЗП.11	Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и	Т	Т	Т	✓	✓	✓	✓	✓	✓	

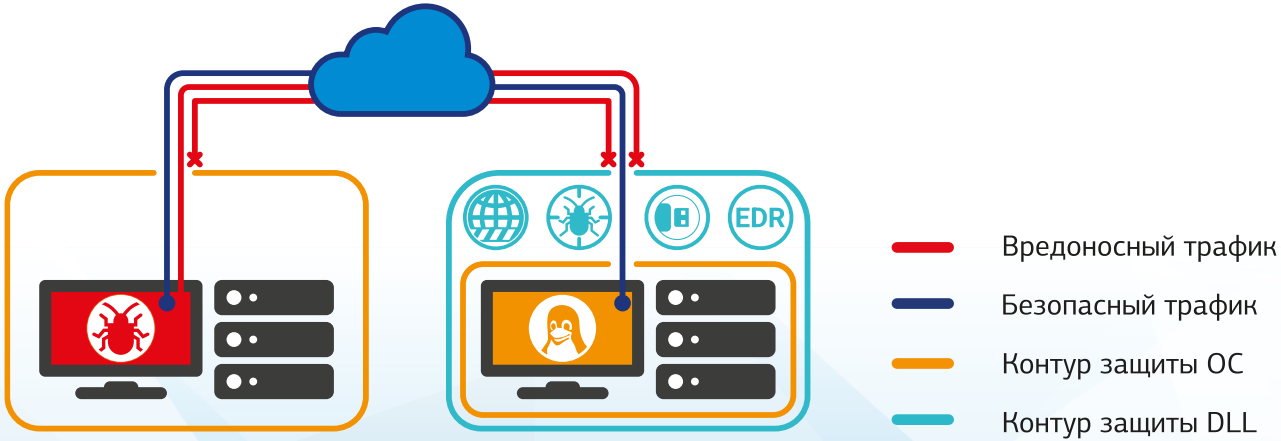
№	Условное обозначение	Содержание мер системы защиты информации	Уровни защиты информации			СЗИ Dallas Lock (НСД, СКН, МЭ, СОВ, РК, МП)		Dallas Lock Linux	СДЗ Dallas Lock	СДЗ УБ Dallas Lock	СЗИ ВИ Dallas Lock	WAF Dallas Lock
			3	2	1	8.0-К	8.0-С					
		осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов										
24.	УЗП.24	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом	Т	Т	Т	✓	✓	✓	✓	✓	✓	
25.	УЗП.25	Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа	Т	Т	Т	✓	✓	✓	✓	✓	✓	
26.	УЗП.26	Регистрация событий защиты информации, связанных с	Н	Т	Т	✓	✓	✓	✓	✓	✓	

Страница 19 из 156

Более детальный перечень мер, которые закрывает Dallas Lock, можно запросить у менеджера Зеон.

Комплексное пакетное предложение с сертифицированными ОС

Сертифицированная операционная система (ОС) – обеспечивает фундамент безопасности, однако этого может быть недостаточно для необходимого уровня защиты. Атаки часто нацелены на каналы обмена данными: сетевой трафик, внешние устройства хранения и файловые ресурсы. Требования регуляторов (ФСТЭК России, ЦБ РФ) предполагают комплексный подход к защите информации, который не может быть обеспечен средствами одной только ОС.



СЗИ Dallas Lock Linux и сертифицированные модули

Сертифицированная СЗИ Dallas Lock Linux позволит обеспечить безопасность рабочих мест и серверов, дополняя меры защиты, реализованные в ОС, поддерживаемыми модулями:

Сертифицированный межсетевой экран Dallas Lock Linux (МЭ) для контроля сетевого трафика. Позволяет осуществлять контроль информационных потоков, блокировать передачу данных, контролировать приложения через создание чёрных и белых списков программ, предоставляет возможность индивидуальной и групповой работы с правилами фильтрации через единый интерфейс.

Сертифицированное средство контроля съёмных машинных носителей информации Dallas Lock Linux (СКН) позволяет управлять списком разрешённых съёмных накопителей, закреплять право подключения накопителей, осуществлять блокировку и разблокировку интерфейсов ввода-вывода, управлять подключением мобильных устройств к компьютеру.

Сертифицированная система обнаружения вторжений Dallas Lock Linux (СОВ) для выявления атак в реальном времени. Позволяет анализировать сетевой трафик и события системы с применением эвристического анализа, применять гибкие сценарии реагирования на угрозы.

Средство обнаружения и реагирования Dallas Lock Linux (СОР/EDR) для оперативного выявления и реагирования на сложные атаки. Позволяет выявлять признаки взлома при помощи механизма обнаружения индикаторов компрометации (IoC), автоматически локализовать инциденты.

Централизованное управление при помощи **Единого центра управления Dallas Lock (ЕЦУ)** доступно для всех модулей Dallas Lock Linux.

Обзор состава решений

ASTRA LINUX

base alt

РЕДОС

- Набор программных решений, разработанных независимыми сторонами
- Подтвержденная технологическая совместимость с сертифицированными и несертифицированными версиями

Сертифицированная редакция ОС

- Система обнаружения и предотвращения вторжений Dallas Lock
- Средство контроля носителей Dallas Lock
- Межсетевой экран Dallas Lock
- COP — Система оперативного реагирования (COP)

Несертифицированная редакция ОС

- СЗИ Dallas Lock Linux
- Система обнаружения и предотвращения вторжений Dallas Lock
- Межсетевой экран Dallas Lock
- Средство контроля носителей Dallas Lock
- COP — Система оперативного реагирования (COP)

Отдельные модули реализуют требуемые меры без конфликта с ОС

- Разграничение и фильтрация сетевого трафика
- Сегментация и изоляция сетевых зон
- Выявление и блокирование сетевых атак
- Контроль и анализ сетевого взаимодействия

- ✓ Обеспечивается реализация мер на разных уровнях ИС в соответствии с приказом № 117
- ✓ Исключается дублирование функций НСД
- ✓ За счет установки отдельных модулей безопасность не избыточна и обеспечивается в соответствии с заданной моделью угроз
- ✓ Упрощается подтверждение соответствия требованиям

Модуль СОР для отечественных ОС



Выявление признаков взлома

- сканирование системы
- управление базой IoC с возможностью добавления пользовательских индикаторов
- регулярное обновление базы индикаторов



Автоматическое реагирование

- блокировка IP-адреса атакующего
- блокировка учетной записи
- блокировка АРМ
- изоляция узла с ограничением сетевой активности
- завершение процесса или отключение АРМ



Защита конечных устройств: МЭ, СОВ, СКН, СОР

- защита на уровне прикладной среды
- контроль сетевых соединений и процессов
- формирование событий для мониторинга



СЗИ ВИ Dallas Lock

Сертифицированная система защиты информации в виртуальных инфраструктурах.

Предназначена для защиты среды виртуализации на базе технологий VMware vSphere, систем управления виртуализацией на базе oVirt (zVirt, РЕД Виртуализация, HOSTVM) и гипервизоров KVM.

vmware ESXi

- VMware 5.5
- VMware 6.0
- VMware 6.5
- VMware 6.7
- VMware 7.0
- VMware 8.0

Microsoft Hyper-V

- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2019
- Microsoft Hyper-V Server 2022

KVM

- oVirt
- CentOS 7.5.1804
- CentOS 8.4.2105
- CentOS Stream 9
- CentOS Linux 8.5 (2111)
- Linux Mint 18.3, 19.3, 20.3, 21.3
- Ubuntu 18.04.2 LTS, 18.04.6 LTS, 20.04.3 LTS, 22.04.4 LTS, 24.04 LTS

Отечественные системы виртуализации

- Виртуализация Astra Linux
- HOSTVM
- zVirt 3.0, 3.1, 3.3, 4.0, 4.1, 4.2
- РЕД Виртуализация 7.3

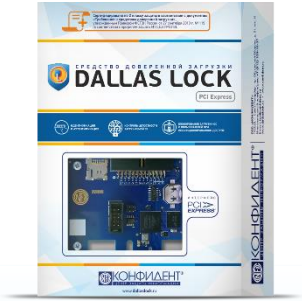
КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

СДЗ Dallas Lock

средство доверенной загрузки Dallas Lock — это два решения, которые блокируют попытки несанкционированной загрузки нештатной операционной системы. Используются для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

СДЗ ПР Dallas Lock

средство доверенной загрузки уровня платы расширения



- Сертификаты ФСТЭК России и МО РФ
- Три форм-фактора (**+ СДЗ USB**)
- Расширен перечень поддерживаемых процессоров, аппаратных платформ и идентификаторов (**в следующей итерации Intel Core Ultra и Kaspersky Thin Client**)
- Дополнен функционал централизованного управления

СДЗ УБ Dallas Lock

средство доверенной загрузки уровня базовой системы ввода-вывода



- Сертификаты ФСТЭК России и МО РФ
- Установка с помощью программатора, что увеличивает процент совместимости
- Расширен перечень поддерживаемых служб каталогов
- Утилита проверки возможности установки СДЗ УБ

Новое изделие СДЗ ПР Dallas Lock (USB/PLS)



KT-600-M-Type A



KT-600-M-PLS



- Доступный и распространенный форм-фактор USB
- Отечественный микроконтроллер «Миландр»
- Часы реального времени (RTC)
- Аппаратный сторожевой таймер (в KT-600M-PLS)

WAF Dallas Lock

Сертифицированный межсетевой экран прикладного уровня, предназначенный для защиты веб-серверов, обслуживающих сайты, веб-службы и веб-приложения, от сетевых атак и нежелательного интернет-трафика.

WAF (Web Application Firewall)

межсетевой экран уровня веб-приложений

UTM (Unified Threat Management)

межсетевой экран уровня логических границ сети и система обнаружения вторжений уровня сети

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

WAF Dallas Lock

Сертифицированный



НЕЙРОННЫЕ СЕТИ

- В WAF Dallas Lock внедрена нейронная сеть для анализа входящего трафика и выявления атак.
- Нейросеть классифицирует запросы по признакам популярных угроз, таких как XSS и SQL Injection.
- Совместная работа нейросети и сигнатурной защиты повышает точность фильтрации и уровень безопасности.



ГРАФ СВЯЗЕЙ

- В WAF Dallas Lock реализовано отслеживание поведения пользователей на защищаемом ресурсе для выявления аномалий.
- Построение гибко настраиваемого графа связей и переходов позволяет точно определять отклонения от нормального поведения.
- Такой механизм снижает количество ложных блокировок и помогает быстро реагировать на атаки в критических ситуациях

ЕЦУ Dallas Lock

центр принятия решений

- Создание иерархической структуры доменов безопасности с наследованием значений параметров безопасности
- Управление СЗИ, находящимися за NAT

Поддержка российских ОС, в том числе сертифицированных ФСТЭК России

ASTRALINUX® common edition · РЕДОС · base alt · ROSA · ASTRA LINUX

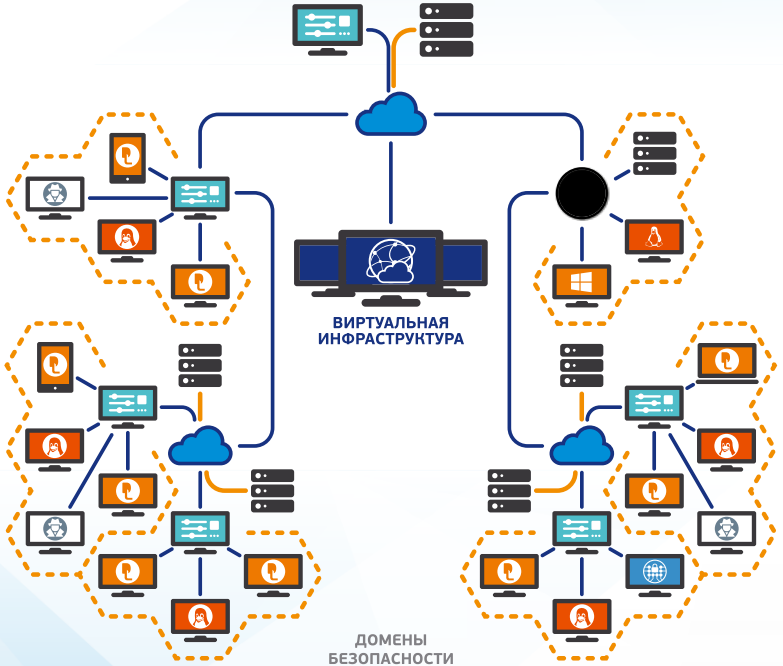
Централизованное управление продуктовой линейкой Dallas Lock

Контроль и управление сетевым оборудованием

- Сканирование сети для обнаружения устройств
- Контроль изменений конфигурации
- Сбор событий по протоколу Syslog

Интеграция со сторонними продуктами

РЕДАДМ · ALD Pro · FreeIPA · SIEM



Агент ЕЦУ



Агент ЕЦУ – это программный компонент, устанавливаемый на клиентские устройства для централизованного сбора информации, управления и администрирования. Он обеспечивает прозрачность и контроль без необходимости установки специализированных средств защиты на всех целевых машинах.



Сбор информации. Системные журналы, версия ОС, IP/MAC-адреса



Мониторинг. Отображение инцидентов безопасности, просмотр состояния АРМ



Отчетность. Формирование отчетов об аппаратном и программном обеспечении



Удаленное подключение. Поддержка подключения к удаленному рабочему столу



Управление. Перезагрузка, выключение, удаление агента



Централизованная установка. Локальная и удаленная установка (Windows/Linux)

Состав изделия NAC Dallas Lock ИК0

Шлюз безопасности WAF (UTM) Dallas Lock

защита от внешних угроз и атак, фильтрация входящего трафика, сегментирование сети, контроль доступа к зонам доверия

Единый центр управления ЕЦУ Dallas Lock

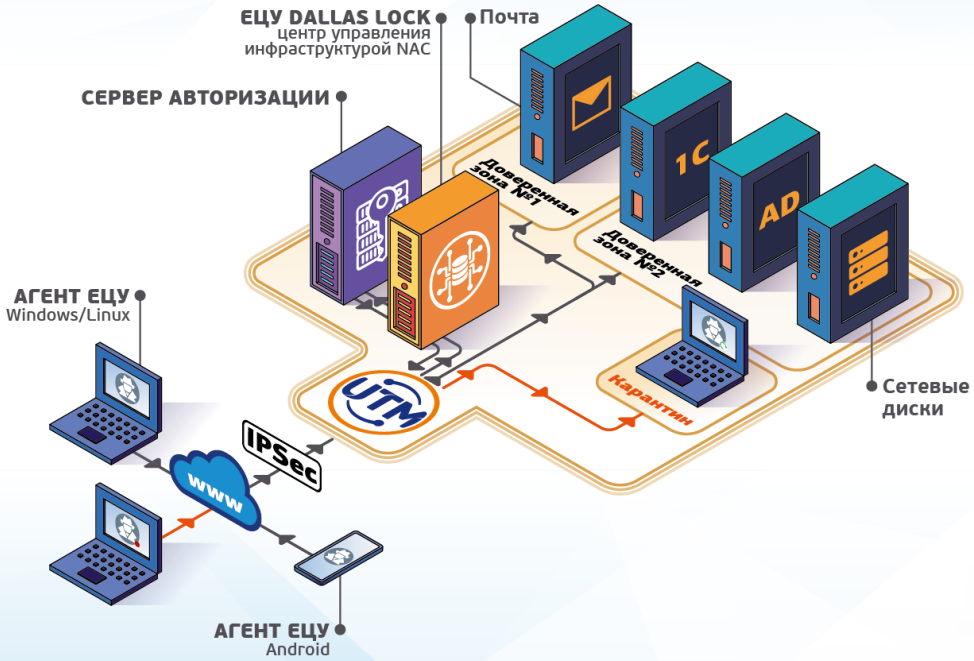
мониторинг и управление работой, регистрация устройств, управление политиками безопасности, журналирование событий

Сервер авторизации NAC Dallas Lock

хранение базы и проверка кредeнталов, авторизация устройств, выделение внутренних ip-адресов

Агенты ЕЦУ + NAC

установка защищённого соединения, формирование отчётов для ЕЦУ



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Основная функциональность NAC Dallas Lock ИК0

Подготовка и настройка инфраструктуры

установка и настройка ЕЦУ, WAF, сервера авторизации
настройка ресурсов и зон доверия в ЕЦУ

Создание нового пользователя / устройства

создание и отправка пользователю профиля сетевого подключения Агента NAC, поддержка Windows, Linux, Android

Авторизация и идентификация пользователя

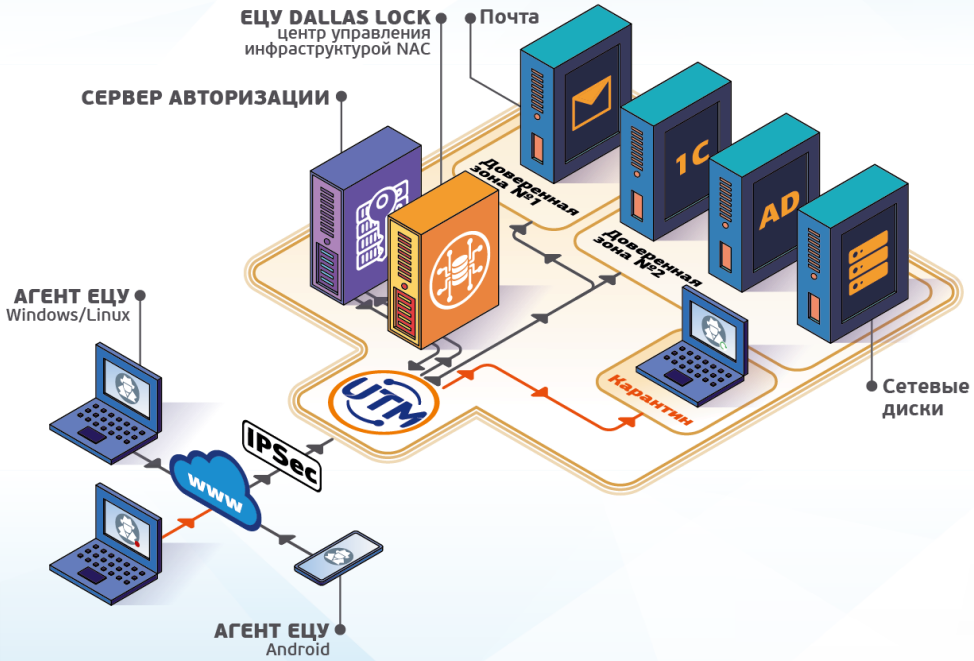
подключение к сетевым ресурсам в один клик
контроль статуса подключенных Агентов

Управление доступом к ресурсам

прекращение доступа пользователя / устройства к ресурсам
изменение зон доверия для групп пользователей

Журналирование действий пользователя

контроль подключений пользователей / устройств
отображение статуса подключенных Агентов



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Предложения для тех, кто находится в процессе импортозамещения

1



Универсальная лицензия даёт право на использование
СЗИ Dallas Lock 8.0-К (для ОС Windows) или СЗИ НСД Dallas Lock Linux
по усмотрению конечного пользователя

2

Расширь возможности сертифицированной ОС :

- возможность приобрети отдельно модули для ОС Linux;
- специальная цена;
- техническая возможность реализована, сертификат ФСТЭК России Q4 2026



3

Трансформируй имеющиеся лицензии DL 8.0 под текущие задачи*:

- перевод на Универсальную лицензию;
- перевод на DL Linux;
- перевод на модули и агент ЕЦУ.

***обращайтесь за индивидуальным подбором решения**