

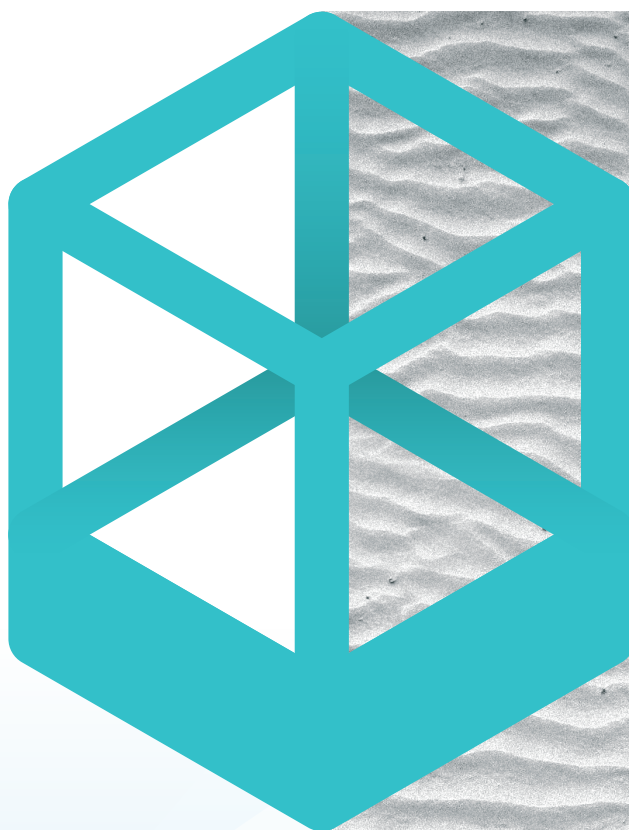


СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА / «ПЕСОЧНИЦА»
DALLAS LOCK SANDBOX

ОБЗОР





ОГЛАВЛЕНИЕ

Введение2

1. БЕЗОПАСНАЯ СРЕДА DALLAS LOCK.....3

1.1 Предварительная настройка Безопасной среды4

1.2 Запуск ПО в Безопасной среде.....5

2. ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ БЕЗОПАСНОЙ СРЕДЫ.....7

3. ПАРАМЕТРЫ БЕЗОПАСНОЙ СРЕДЫ..... 10

4. ФИКСАЦИЯ ДЕЙСТВИЙ 14

4.1 Фиксация действий в подсистеме регистрации и учета..... 15

4.2 Информирование пользователя 16

5. ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ 18

Заключение 20



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.



БЕЗОПАСНАЯ СРЕДА

**DALLAS LOCK
SANDBOX**

ВВЕДЕНИЕ Безопасная среда (БС) Dallas Lock – механизм, предоставляющий пользователю возможность запускать любое стороннее ПО в изолированной среде. Позволяет детально изучить работу ПО и получить подробный отчет в удобном для пользователя виде. Механизм помогает исключить риск негативного воздействия стороннего ПО на инфраструктуру объекта информатизации.

Основные задачи, которые решает Безопасная среда Dallas Lock:

- возможность запускать и производить работы с программным обеспечением в изолированной, защищенной среде без внесения изменений в основную ОС;
- проверка ПО на опасные действия, с целью определения степени доверия к такому ПО;
- формирование отчета о деятельности программы;
- защита пользовательских данных от воздействия нежелательного ПО.

Безопасная среда Dallas Lock (или «песочница») предназначена для защиты пользовательских компьютеров при запуске ПО, полученного из недоверенных источников, повышения общего уровня защищенности домена безопасности, а также реализации требований, установленных Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».



1

**БЕЗОПАСНАЯ СРЕДА
DALLAS LOCK**



Компания «Конфидент» начиная с 2018 года поддерживает механизм Безопасной среды в решении Dallas Lock 8.0. Механизм регулярно обновляется и успешно применяется в ГИС, на значимых объектах КИИ и на других объектах информатизации.

1.1 ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА БЕЗОПАСНОЙ СРЕДЫ

Основные настройки Безопасной среды доступны в оболочке администрирования Dallas Lock 8.0 на вкладке «COB», категория «Безопасная среда COB», подкатегория «Настройки» (рисунок 1).

Параметр «Эвристический анализ для блокировки работы опасных процессов» позволяет в автоматическом режиме завершать работу потенциально опасных приложений. В случае обнаружения угроз безопасности приложение будет автоматически закрыто, а пользователь – немедленно проинформирован. Настройки режимов работы и параметры Безопасной среды доступны в оболочке администрирования Dallas Lock 8.0, а также при централизованном управлении с помощью Консоли Единого центра управления (ЕЦУ) Dallas Lock.

Параметр «Автоматический запуск приложений в БС» позволяет по умолчанию запускать приложения из недоверенных источников в Безопасной среде.

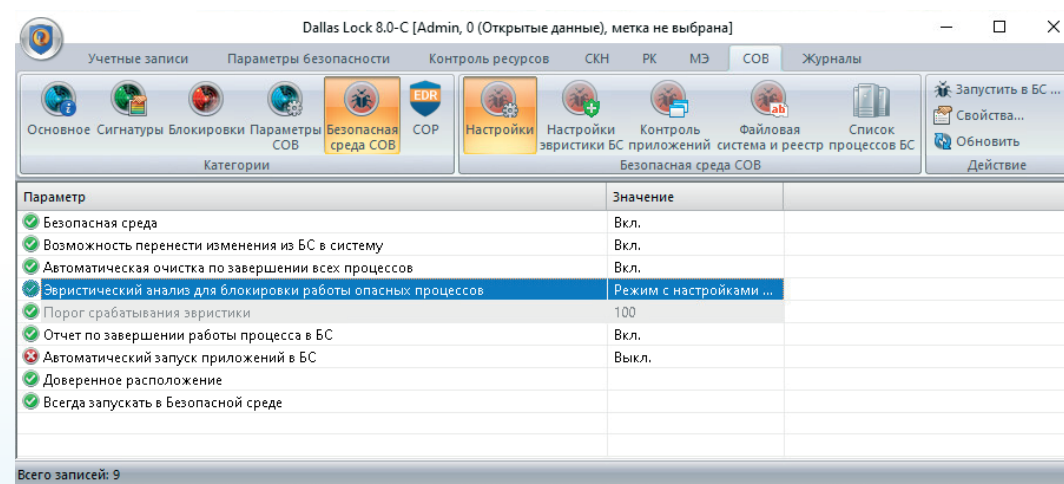


Рисунок 1

Параметру «Эвристический анализ для блокировки работы опасных процессов» (рисунок 2) может быть задано одно из значений автоматического режима определения и завершения потенциально опасных приложений (с настройками весов правил эвристического анализа по умолчанию или ручными настройками). В «Режиме ручной настройки» пользователь самостоятельно определяет весовые коэффициенты и порог срабатывания эвристики. При переключении с «Режима ручной настройки» на «Режим с настройками по умолчанию» будет выведено сообщение о сбросе настроек на значения по умолчанию.

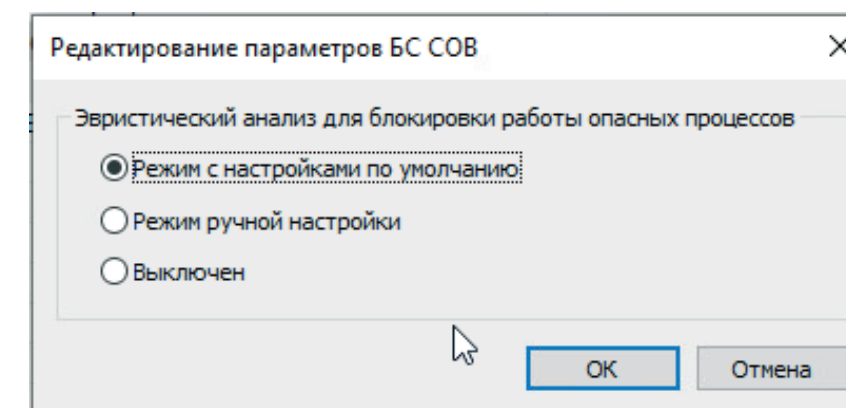


Рисунок 2

Для просмотра и изменения настроек Безопасной среды пользователь должен быть указан в значениях параметров «COB: изменение настроек» и «COB: просмотр настроек» на вкладке «Параметры безопасности», в категории «Права пользователей» оболочки администрирования Dallas Lock 8.0 либо состоять в группе пользователей, указанной в данных параметрах.

1.2 ЗАПУСК ПО В БЕЗОПАСНОЙ СРЕДЕ

Запуск приложений в Безопасной среде возможен в ручном и автоматическом режимах. Запуск в ручном режиме происходит через выбор соответствующего пункта контекстного меню, либо выбором программы через меню BlockIcon на панели задач или через оболочку администрирования Dallas Lock 8.0. Запуск приложения в Безопасной среде в автоматическом режиме производится после включения соответствующего параметра в разделе «Настройки» БС COB. В главе 3 варианты запуска рассмотрены более подробно.

При запуске приложения в Безопасной среде Dallas Lock 8.0 перехватывает вызовы функций от приложений к ОС и отслеживает следующие события:

- обращения ПО к системному реестру и критическим объектам операционной системы. Критическими являются объекты, удаление, блокирование или модификация которых оказывает влияние на функционирование или безопасность ОС Windows — системные библиотеки, драйверы, файл HOSTS и так далее;
- попытки модификации или удаления объектов ПО СЗИ;
- обращения ПО к объектам файловой системы, в том числе прямой доступ к диску;



БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

- попытки внедрения компонент – подмена и установка сторонних библиотек, установка системных перехватчиков, через которые посторонний код может быть внедрен в другой процесс, оконные перехватчики;
- внедрение в память процесса;
- DDE- и OLE-взаимодействие;
- запросы на завершение и запуск процессов;
- низкоуровневый сетевой доступ;
- вызов DNS API;
- попытки снятия скриншота экрана, несанкционированного доступа к буферу обмена или перехват нажатия клавиш приложениями.

В случае определения запущенного в БС COB приложения как потенциально опасного, путем сложения в специализированном счетчике весовых коэффициентов операций, которые указываются в категории «Параметры COB» - «Настройки эвристики», приложение автоматически завершается. Системой регистрации и учета происходит фиксация инцидента в «Журнале контроля приложений» с нотификацией пользователя в системном трее ОС, а также уведомлением администратора информационной безопасности в Консоли ЕЦУ Dallas Lock и по электронной почте.

Только уполномоченный пользователь может выполнять настройки централизованно через Единый центр управления (ЕЦУ) Dallas Lock.



2

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ БЕЗОПАСНОЙ СРЕДЫ



Все настройки Безопасной среды Dallas Lock доступны в оболочке администратора Dallas Lock 8.0 на вкладке «COB», категория «Безопасная среда COB» (рисунок 3). Категория «Безопасная среда COB» содержит следующие подкатегории:

- **Настройки** – общие настройки Безопасной среды;
- **Настройки эвристики БС** – настройки правил эвристики Безопасной среды;
- **Контроль приложений** – набор функций, по которым определяется общее поведение Безопасной среды;
- **Файловая система и реестр** – настройки доступа приложений, работающих в Безопасной среде, к каталогам и реестру;
- **Список процессов БС** – список запущенных в Безопасной среде процессов с указанием их идентификаторов.

Кроме того, реализованы кнопки блока «Действие»:

- **Запустить в БС COB** – произвести запуск выбранного приложения в Безопасной среде;
- **Свойства** – открыть окно свойств выбранного параметра;
- **Обновить** – произвести обновление текущего окна.

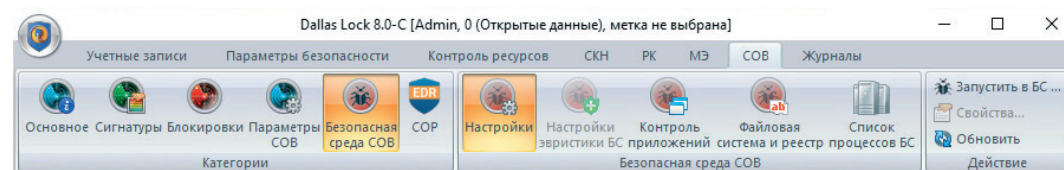


Рисунок 3

Запуск приложения в Безопасной среде COB доступен через контекстное меню, отображаемое после нажатия на нужном файле правой кнопкой мыши. Пример контекстного меню представлен на рисунке 4.

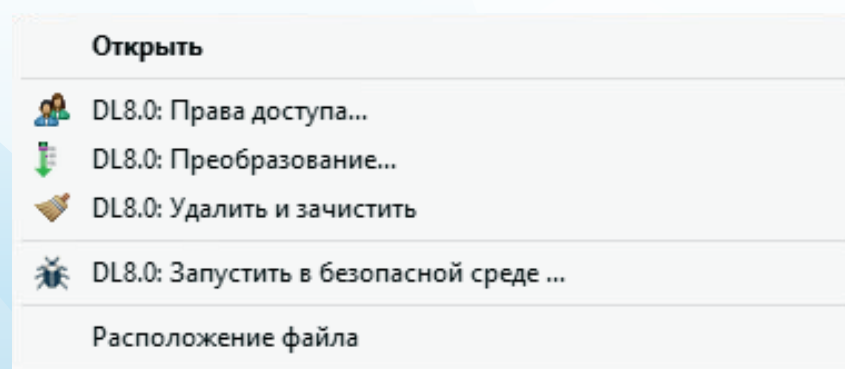


Рисунок 4

Также запустить приложение в Безопасной среде можно через BlockIcon, нажав на него правой кнопкой мыши и выбрав в меню пункт «COB» и далее – пункт «Запустить приложение в Безопасной среде COB».

После чего появится окно выбора расположения файла, который должен быть запущен в Безопасной среде (рисунок 5).

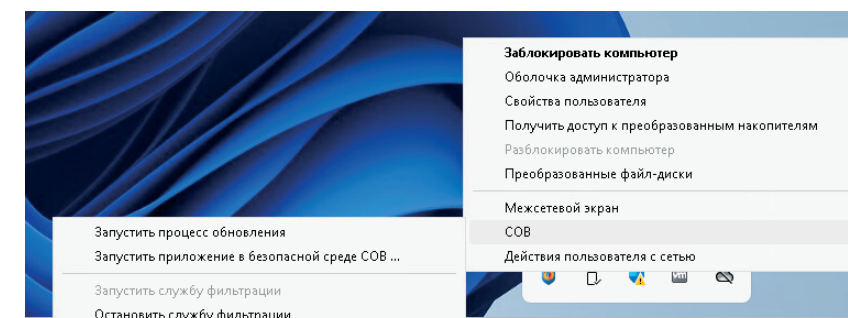


Рисунок 5

Кроме того, запустить приложение в Безопасной среде можно через оболочку администрирования Dallas Lock 8.0. Для этого нужно перейти на вкладку «COB» и выбрать расположение соответствующего файла.

Графическая форма приложения, запущенного в Безопасной среде, выделена цветовой рамкой и подписана. Пример формы представлен на рисунке 6.

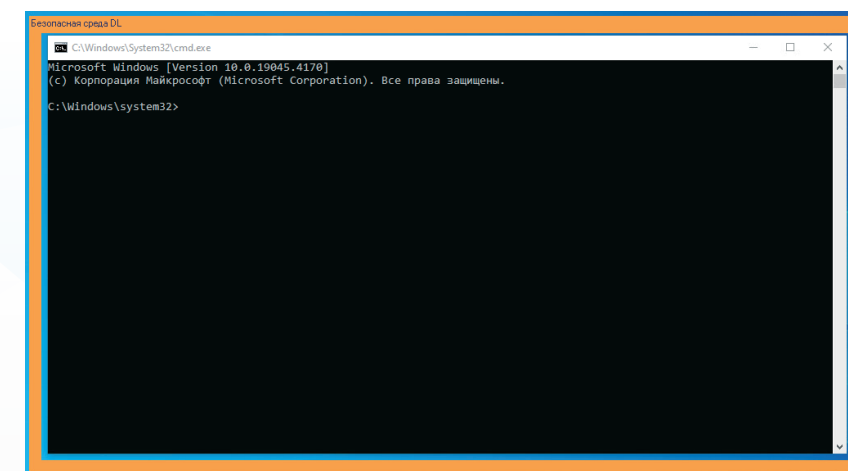


Рисунок 6



БЕЗОПАСНАЯ СРЕДА

**DALLAS LOCK
SANDBOX**



3

**ПАРАМЕТРЫ
БЕЗОПАСНОЙ СРЕДЫ**

Общие настройки Безопасной среды (рисунок 7):

- «Безопасная среда» – позволяет включать и отключать БС.
- «Возможность перенести изменения из БС в систему» – позволяет отключить сохранение результатов работы процесса, запущенного в Безопасной среде.
- «Автоматическая очистка по завершению всех процессов» – данная политика позволяет определить, будет ли производиться автоматическая очистка временных каталогов от содержимого, созданного процессом или процессами, запущенными в Безопасной среде.
- «Эвристический анализ для блокировки работы опасных процессов» – позволяет выбрать режим работы эвристики для автоматического завершения потенциально опасных приложений.
- «Порог срабатывания эвристики» – позволяет указать максимальный порог, при достижении которого приложение будет автоматически завершено Безопасной средой.
- «Отчет по завершении работы процесса в БС» – разрешает Dallas Lock 8.0 формировать отчет с результатами контроля ПО, запущенного в БС с уведомлением пользователя.
- «Автоматический запуск приложений в БС» – позволяет автоматически запускать файлы, полученные из недоверенных источников (скачанные из сети Интернет или скопированные с внешних накопителей), в Безопасной среде.
- «Доверенное расположение» – параметр содержит пути к доверенным директориям. Запуск программ и файлов из этих директорий в автоматическом режиме не производится.
- «Всегда запускать в Безопасной среде» – позволяет добавить приложения, запуск которых будет всегда происходить в Безопасной среде.

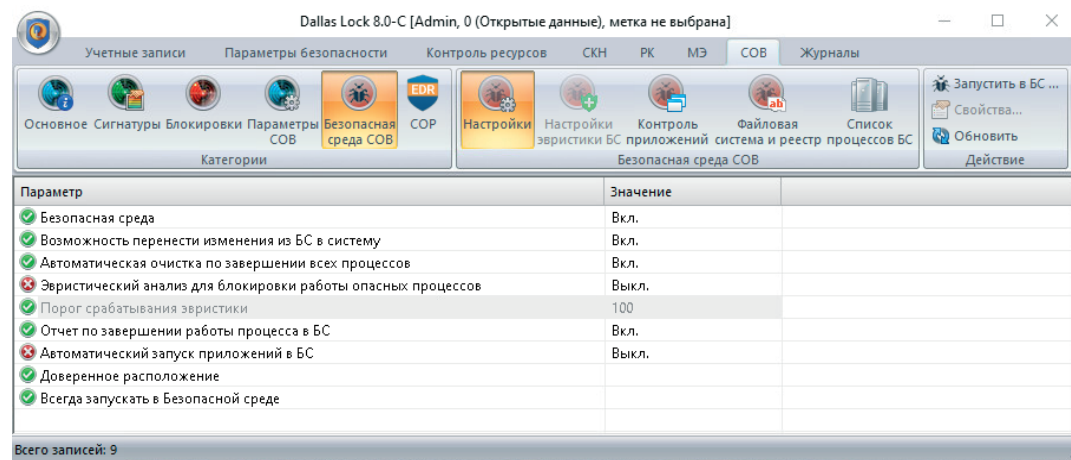


Рисунок 7

Настройки эвристики БС категории «Безопасная среда COB» содержат правила эвристики (рисунок 8). Настройки в данной подкатегории доступны при включённом параметре «Эвристический анализ для блокировки работы опасных процессов» в «Режиме ручных настроек».

Настройки эвристики возможны для следующих правил:

- вызовы различных функций;
- модификация памяти ядра;
- управление чужим процессом с помощью отладочного API;
- инсталляция/запуск драйверов, инсталляция/запуск служб;
- вызов DNS API;
- перехват нажатий клавиш;
- проверка взаимодействий с другими процессами;
- запуск доверенных/не доверенных дочерних процессов;
- право на работу с сетью;
- использование RAW советов;
- изменение файла HOSTS;
- выполнение скриптов через PowerShell и Windows Script Host;
- запуск cmd (командной строки) и прочее.

Для каждой из настроек пользователь может указать следующие значения: «Вес первого срабатывания» и «Вес последующих срабатываний».

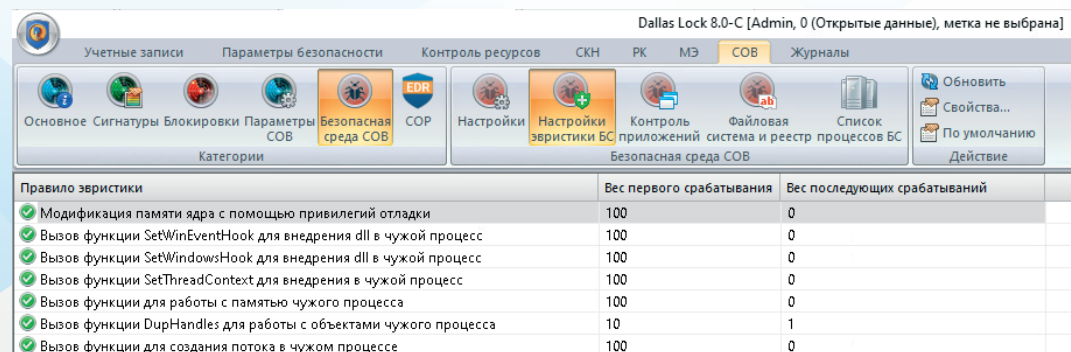


Рисунок 8

Контроль приложений категории «Безопасная среда COB» предназначен для управления правилами Безопасной среды. Содержит настройку «По умолчанию», которая включает в себя набор правил для контроля приложений, запускаемых в Безопасной среде. Необходимо отметить, что если правило COB «Контроль приложений» отмечено как «Запрещено», то общее правило с «Контролем приложений» БС COB будет также запрещено и изменению не подлежит. Если правило COB «Контроль приложений» отмечено как «Разрешено», а в «Контроле приложений» БС COB запрещено, то будет действовать запрещающее правило.

Файловая система и реестр категории «Безопасная среда COB» предназначена для указания пользователем тех областей файловой системы и реестра, которые могут содержать в себе критически важные данные, к которым нельзя предоставлять доступ недоверенным приложениям, даже если они запущены в Безопасной среде (рисунок 9).

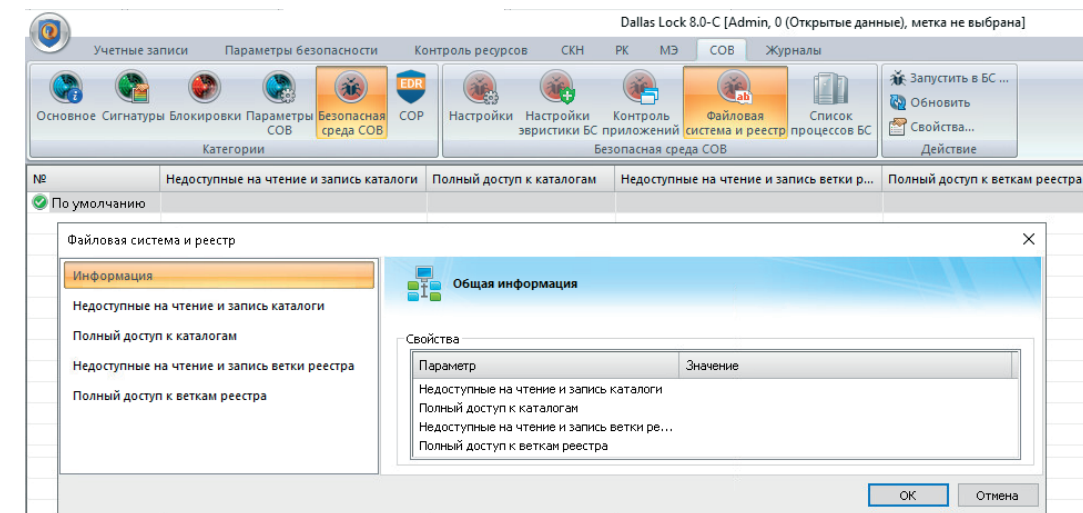


Рисунок 9

Список процессов БС категории «Безопасная среда COB» предназначен для контроля запущенных в Безопасной среде процессов (рисунок 10).

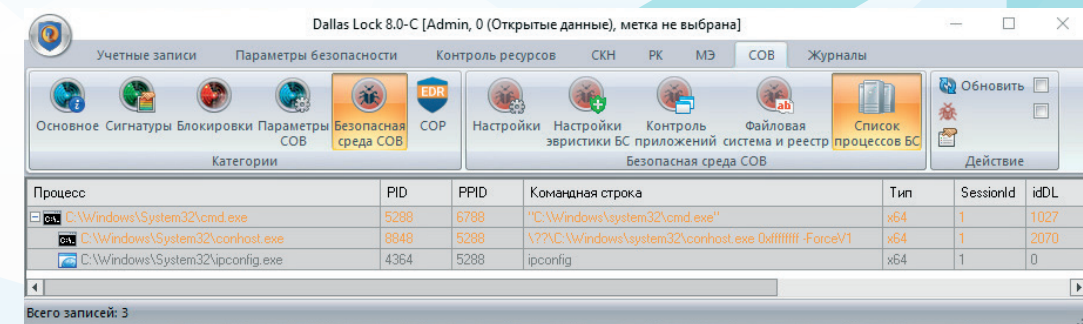


Рисунок 10



БЕЗОПАСНАЯ СРЕДА

**DALLAS LOCK
SANDBOX**

4.1 ФИКСАЦИЯ ДЕЙСТВИЙ В ПОДСИСТЕМЕ РЕГИСТРАЦИИ И УЧЁТА

В «Журнале контроля приложений» фиксируются следующие события:

- Запуск приложения в Безопасной среде;
- Принудительное завершение приложения, с указанием правила или правил, нарушение которых привело к закрытию. Если нарушенных правил фиксируется более чем одно – на каждое нарушенное правило делается отдельная запись;
- Самостоятельное закрытие пользователем приложения, запущенного в БС COB.

Запись «Журнала контроля приложений» содержит следующие элементы, представленные в таблице 1:

Таблица 1. Записи «Журнала контроля приложений»

Наименование класса	Описание
ID	Указывается порядковый номер (идентификатор) события
Время	Указывается время возникновения события безопасности
Тип атаки	Указывается, что процесс был запущен в Безопасной среде
Комментарии	В случае работы с БС COB данное поле не заполняется
Процесс	Указывается путь к исполняемому файлу
PID	Указывается уникальный идентификатор процесса
PID родителя	Указывается уникальный идентификатор родительского процесса
Пользователь	Указывается пользователь, от имени которого был запущен процесс в Безопасной среде
Правило	Наименование правила, которое было нарушено
Результат	Результат действия Безопасной среды. Может принимать следующие значения: • Завершено БС COB • Завершено пользователем

Кроме того, в «Журнал контроля приложений» попадают все действия приложения, запущенного в Безопасной среде.



4

**ФИКСАЦИЯ
ДЕЙСТВИЙ**

4.2

ИНФОРМИРОВАНИЕ
ПОЛЬЗОВАТЕЛЯ

После завершения работы приложения в Безопасной среде вручную или в автоматическом режиме, если параметр «Формировать отчет» имеет значение «Вкл», то появляется окно, представленное на рисунке 11.

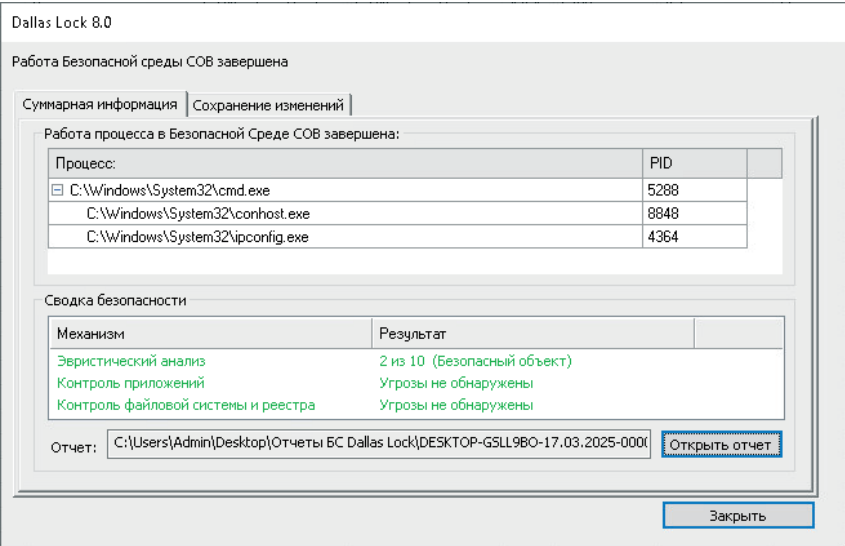


Рисунок 11

В открывшемся окне на вкладке «Суммарная информация» представлена краткая информация о запущенном процессе, а также сводка безопасности, описывающая механизмы работы БС COB и результаты их работы. Внизу окна располагается кнопка «Открыть отчёт», нажав на которую открывается HTML документ с отчётом о работе БС COB.

Пример отчёта Безопасной среды представлен на рисунке 12.

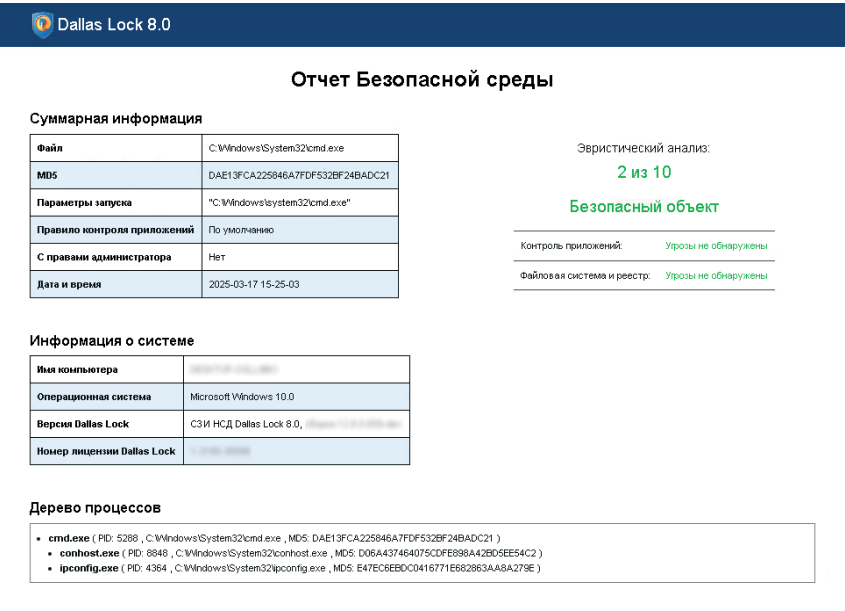


Рисунок 12

На вкладке «Сохранение изменений» в открывшемся по итогам завершения работы БС COB окне пользователь может сохранить файлы из Безопасной среды (рисунок 13).

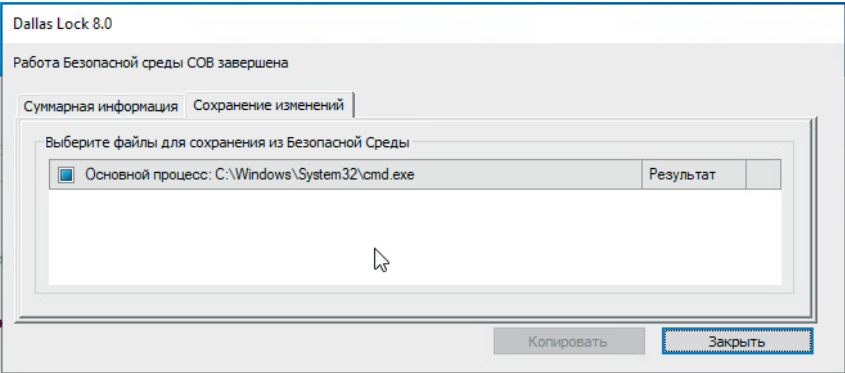


Рисунок 13



БЕЗОПАСНАЯ СРЕДА

**DALLAS LOCK
SANDBOX**

Настройки Безопасной среды можно применить ко всему домену безопасности посредством Консоли ЕЦУ Dallas Lock.

Доступно централизованное управление политиками Безопасной среды в подкатегориях (глава 3):

- Настройки;
- Настройки эвристики БС;
- Контроль приложений;
- Файловая система и реестр.

Централизованное управление в Консоли ЕЦУ Dallas Lock доступно на уровне домена безопасности, группы, АРМ и модуля Dallas Lock 8.0 (рисунок 14).

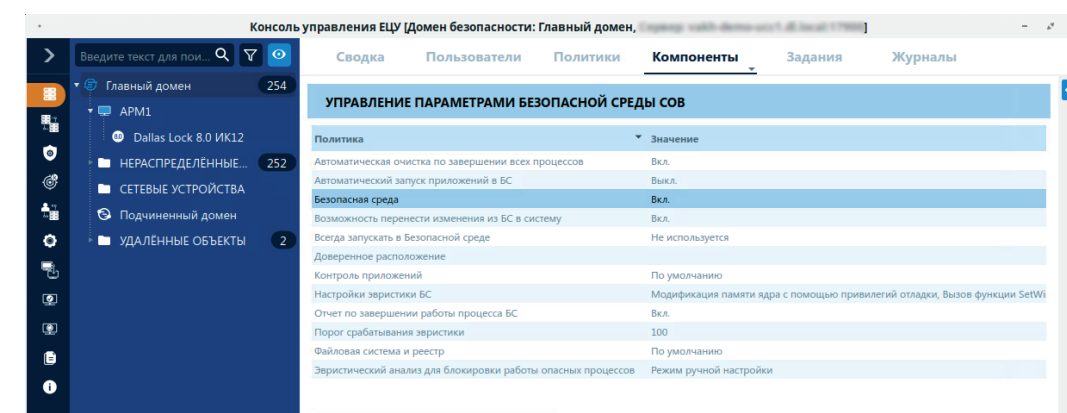


Рисунок 14

5

**ЦЕНТРАЛИЗОВАННОЕ
УПРАВЛЕНИЕ**

ЗАКЛЮЧЕНИЕ

Безопасная среда стала логичным продолжением развития продукта Dallas Lock 8.0. Технологии частичной виртуализации позволяют безопасно запускать приложения, полученные из недоверенных источников (скачанные из сети Интернет или скопированные с внешних накопителей). Пользователям предоставлен эффективный инструмент для защиты данных и приложений. Многолетний опыт разработки Dallas Lock 8.0 позволил реализовать надёжное решение для обеспечения безопасности.

Текущая реализация «песочницы» на протяжении долгого времени предоставляет пользователям Dallas Lock 8.0 широкий спектр функциональных возможностей Безопасной среды. Центр защиты информации ООО «Конфидент» намерен и дальше наращивать эти функции в части более гибкой настройки «песочницы» и автоматизации работы, основанной на реальных сценариях применения продукта.

В новой сертифицированной версии Dallas Lock 8.0 были добавлены функциональные возможности:

- Включение правил МЭ для процессов, запущенных в «Безопасной среде»;
- Автоматический запуск конкретного приложения в «Безопасной среде».



БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK
SANDBOX



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

