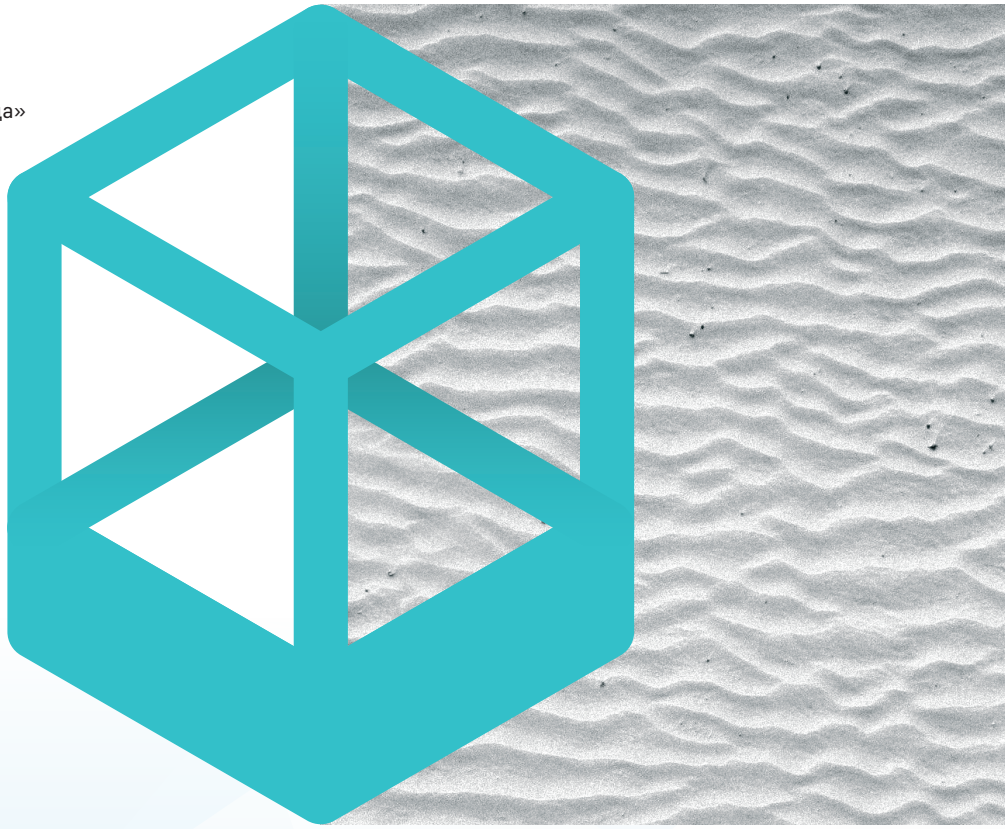
СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

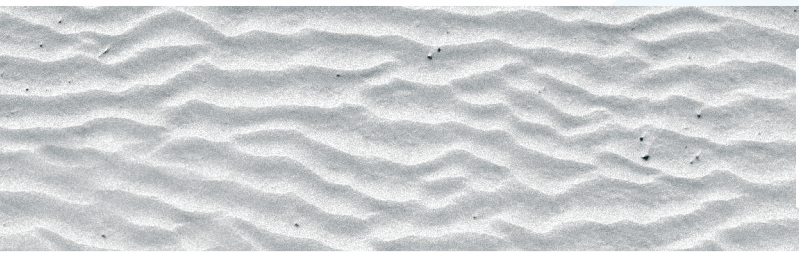
БЕЗОПАСНАЯ СРЕДА / ПЕСОЧНИЦА
DALLAS LOCK SANDBOX

ОБЗОР

Dallas Lock (v. DL80v565.2) «Безопасная среда»



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ



БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Основными задачами, решаемыми «Безопасной средой» Dallas Lock, являются возможность запускать и производить работы с программным обеспечением в изолированной, защищённой среде без внесения изменений в основную ОС и проверка ПО на опасные действия с целью определения степени доверия к такому ПО с формированием отчёта о деятельности программы.

Проверки функционирования ПО в таком окружении (попытки выполнения потенциально опасных действий), исключая возможное вредоносное воздействие, обеспечивают безопасность системного ПО и сохранность пользовательской информации.

Потребность в использовании безопасной среды для запуска приложений обусловлена необходимостью:

- проверить работу ПО без внесения изменений в ОС;
- получить отчёт о потенциальной опасности ПО;
- защитить пользовательские данные от воздействия нежелательного ПО.

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

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

1

БЕЗОПАСНАЯ СРЕДА DALLAS LOCK

Начиная с версии СЗИ НСД Dallas Lock 8.0.565.2, реализована возможность запускать стороннее ПО в изолированной, безопасной среде — «песочнице». Настройки режимов работы и параметры безопасной среды реализованы в оболочке администрирования СЗИ НСД Dallas Lock 8.0, а также в оболочке администрирования Сервера безопасности Dallas Lock. В результате запуска стороннего ПО в «песочнице» производится анализ поведения такого приложения в изолированной среде. По результатам анализа реализована возможность автоматического закрытия приложения в случае обнаружения угроз безопасности и информирование пользователя (администратора) о результатах проверки.

1.1 ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА БЕЗОПАСНОЙ СРЕДЫ

Уполномоченному пользователю предоставляется возможность на вкладке СОВ оболочки администрирования СЗИ НСД Dallas Lock 8.0 (пример оболочки администрирования приведён на Рисунке 1) выбрать категорию «Безопасная среда» и перейти к её настройке. В оболочке администрирования возможно включить или отключить «Безопасную среду», а также изменить другие параметры для более тонкой настройки.

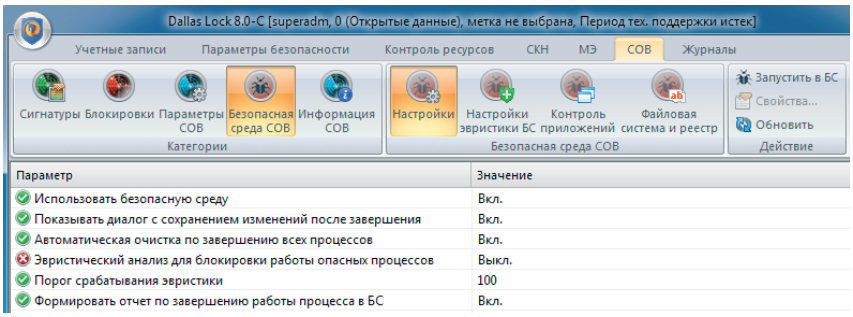


Рисунок 1 — Оболочка администрирования безопасной среды

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.

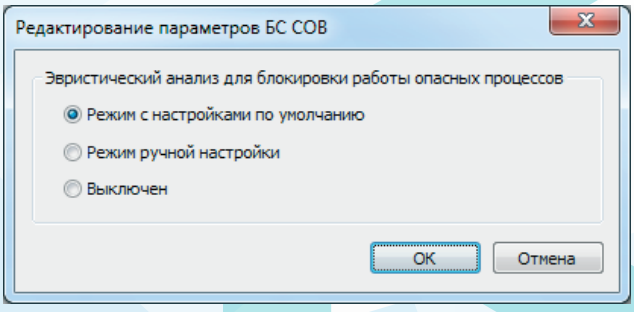


Рисунок 2 — Настройка режима работы эвристического анализа

Для просмотра и изменения политик и других параметров «Безопасной среды» пользователь должен быть указан в значении параметров «СОВ: изменение настроек» и «СОВ: просмотр настроек» категории «Права пользователей» оболочки администрирования СЗИ НСД Dallas Lock 8.0 либо состоять в группе, указанной в данном параметре.

1.2 ЗАПУСК ПО В БЕЗОПАСНОЙ СРЕДЕ

Запуск приложений в «Безопасной среде» возможен в ручном режиме. Запуск в ручном режиме производит пользователь путём нажатия на запускаемом объекте правой кнопкой мыши и вызова контекстного меню, в котором необходимо выбрать соответствующий пункт, либо выбрав программу через меню BlockIcon или через оболочку администрирования СЗИ НСД Dallas Lock 8.0. Подробно варианты запуска пользователем ПО в «Безопасной среде» рассмотрены в главе 2.

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

- обращения ПО к системному реестру и критическим объектам ОС. Критическими являются объекты, удаление, блокирование или модификация которых оказывает влияние на функционирование или безопасность ОС Windows — системные библиотеки, драйверы, файл hosts и т.п.;
- попытки модификации или удаления объектов ПО СЗИ;
- обращения ПО к объектам файловой системы;
- попытки внедрения компонент — подмена и установка сторонних библиотек, установка системных перехватчиков, через которые посторонний код может быть внедрён в другой процесс, оконные перехватчики;
- внедрение в память процесса;
- DDE- и OLE- взаимодействие;
- запросы на завершение и запуск процессов;
- низкоуровневый сетевой доступ и запрет на сетевую активность для запускаемого процесса и дочерних процессов;
- вызов DNS API;
- попытки снятия скриншота экрана, несанкционированного доступа к буферу обмена или перехват нажатия клавиш приложениями.

В случае определения запущенного в «Безопасной среде» приложения как потенциально опасного приложение автоматически завершается. Системой регистрации и учёта происходит фиксация инцидента в «Журнале контроля приложений» с нотификацией пользователя в области системных уведомлений ОС, а также нотификацией администратора информационной безопасности в консоли Сервера безопасности Dallas Lock и по электронной почте.

Администратору информационной безопасности предоставляется возможность делать централизованные настройки через Сервер безопасности Dallas Lock, при этом возможность изменять настройки «Безопасной среды» у неуполномоченных пользователей блокируется.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

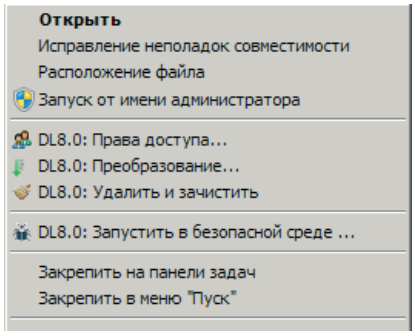
DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

2

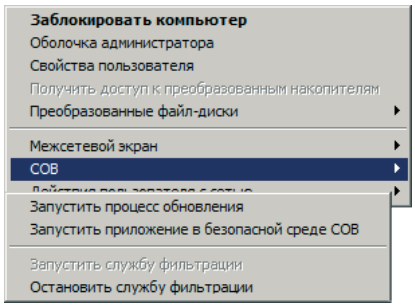
ЗАПУСК ПРИЛОЖЕНИЯ В БЕЗОПАСНОЙ СРЕДЕ



Запуск приложений в «Безопасной среде» СОВ Dallas Lock реализован через контекстное меню, отображаемое после нажатия на нужном файле правой кнопкой мыши. Пример контекстного меню представлен на Рисунке 3.

Рисунок 3 — Пример контекстного меню для запуска приложений в «Безопасной среде»

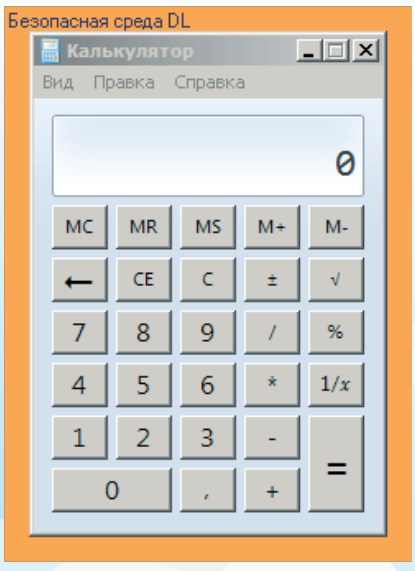
Также запуск приложения в «Безопасной среде» реализован через BlockIcon путём нажатия на нём правой кнопкой мыши, выбора в появившемся меню пункта «СОВ» и далее выбора пункта «Запустить приложение в Безопасной среде СОВ».



После чего появится окно выбора расположения файла, который должен быть запущен в «Безопасной среде» (Рисунок 4).

Рисунок 4 — Запуск приложения в «Безопасной среде» через BlockIcon

Кроме того, запуск приложения возможен из основной формы СЗИ НСД Dallas Lock 8.0 на вкладке СОВ. Необходимо выбрать расположение файла, который должен быть запущен в «Безопасной среде».



Графическая форма приложения, запущенного в «Безопасной среде», выделена цветовой рамкой и подписана (Рисунок 5).

Рисунок 5 — Приложение, запущенное в «Безопасной среде»

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

3

ПАРАМЕТРЫ БЕЗОПАСНОЙ СРЕДЫ

Настройки параметров «Безопасной среды» содержат следующие элементы:

- **Общие настройки «Безопасной среды»** (Рисунок 6):
  - **«Использовать безопасную среду»** — позволяет уполномоченному пользователю включать и отключать «Безопасную среду». Может принимать значения «Вкл.» (по умолчанию) и «Выкл.»;
  - **«Показывать диалог с сохранением изменений после завершения»** — позволяет пользователю отключить сохранение результатов работы процесса, запущенного в «Безопасной среде». Если данный параметр включен, перед сохранением пользователю будет выведено диалоговое окно с предложением сохранить изменения, выполненные завершенным процессом. Может принимать значения «Вкл.» (по умолчанию) и «Выкл.»;
  - **«Автоматическая очистка по завершении всех процессов»** — позволяет пользователю определить будет ли производиться автоматическая очистка временных каталогов от содержимого, созданного процессом или процессами, запущенными в «Безопасной среде». Может принимать значения «Вкл.» (по умолчанию) и «Выкл.»;
  - **«Эвристический анализ для блокировки работы опасных процессов»** — позволяет пользователю разрешить «Безопасной среде» применять эвристический анализ для принудительного завершения работы опасных процессов согласно настройкам эвристического анализа. Может принимать значения «Вкл.» и «Выкл.» (по умолчанию), а также имеет расширенные настройки параметров эвристического анализа;
  - **«Порог срабатывания эвристики»** — позволяет пользователю указать максимальный порог, при достижении которого приложение будет автоматически завершено «Безопасной средой». Может принимать значения от 0 до 1000, по умолчанию — 100;

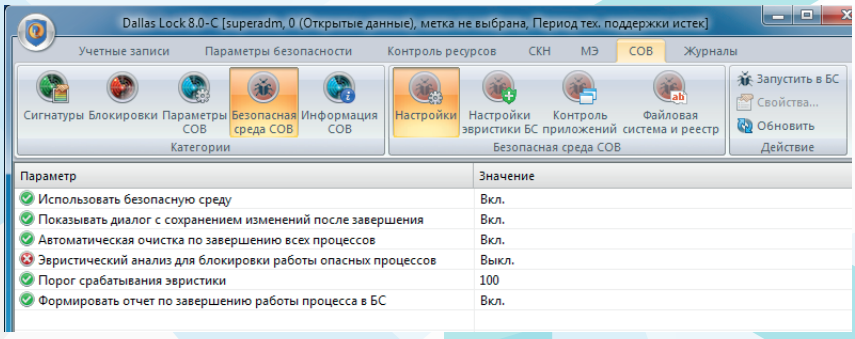


Рисунок 6 — Общие настройки «Безопасной среды»

- **«Формировать отчет по завершении работы процесса в безопасной среде»** — разрешает СЗИ НСД Dallas Lock 8.0 формировать отчет с результатами контроля ПО, запущенного в «Безопасной среде» с уведомлением пользователя. Может принимать значения «Вкл.» (по умолчанию) и «Выкл.»;
- **Контроль приложений** — набор функций, по которым определяется общее поведение «Безопасной среды». Возможно создавать и изменять набор правил для контроля приложений, запускаемых в «Безопасной среде»;
- **Файловая система и реестр** — настройки доступа приложений, работающих в «Безопасной среде», к каталогам и реестру. Данные настройки предназначены для указания пользователем тех областей файловой системы и реестра, которые могут содержать в себе критически важные данные, к которым не следует предоставлять доступ недоверенным приложениям, даже если они запущены в безопасной среде (Рисунок 7).

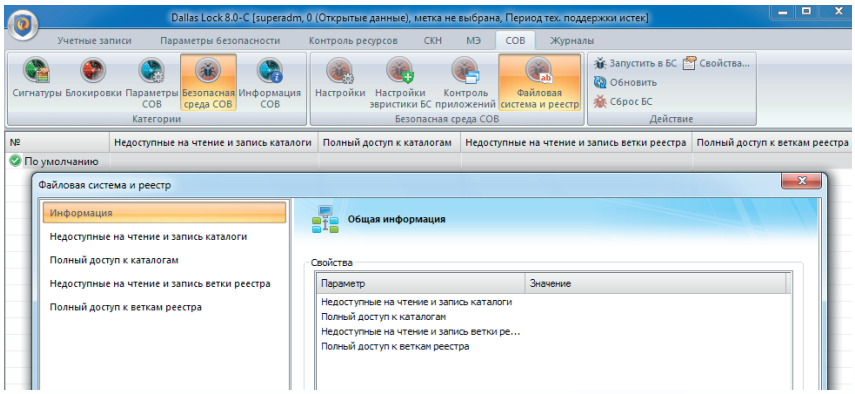


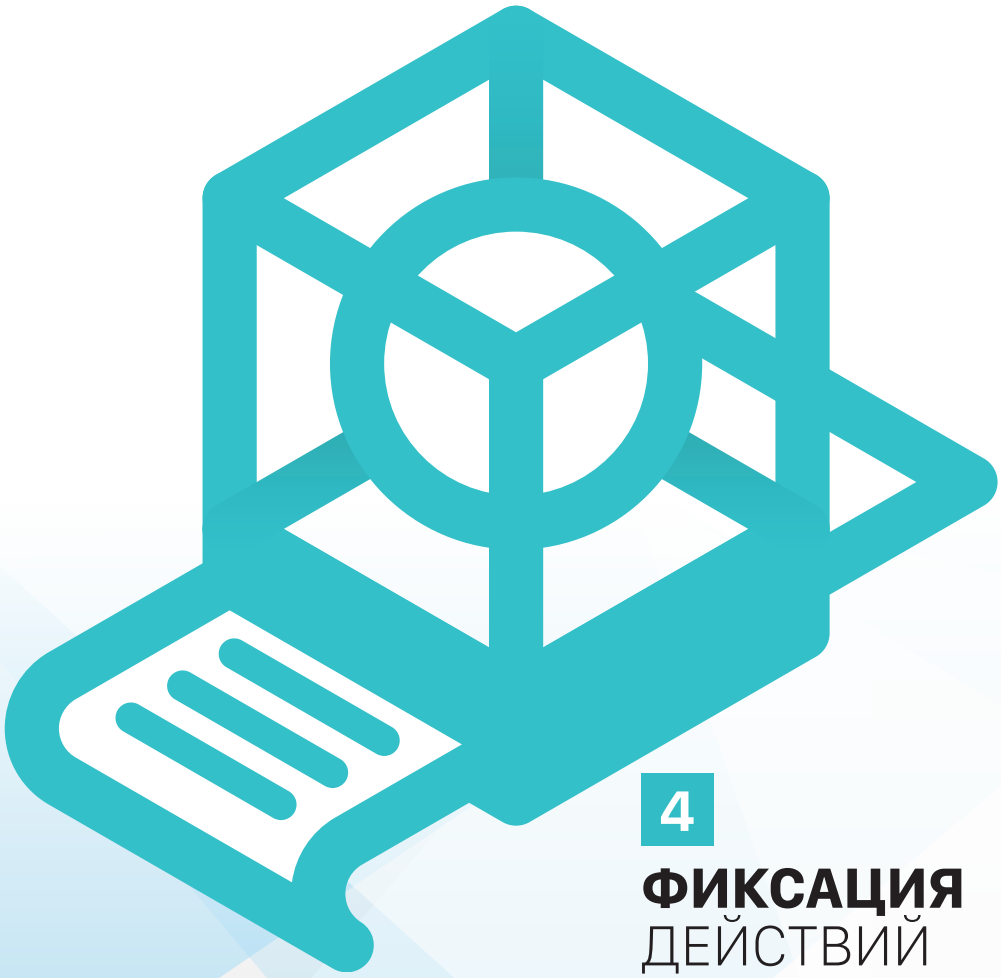
Рисунок 7 — Настройки доступа приложений к файловой системе и реестру

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX



4

ФИКСАЦИЯ ДЕЙСТВИЙ

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, нарушение которого привело к закрытию. На каждое нарушенное правило делается отдельная запись;
- самостоятельное закрытие пользователем приложения, запущенного в «Безопасной среде».

Запись «Журнала контроля приложений» содержит 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 тип атаки (контролируемой функции, из-за которой возникла запись). Поле остается пустым, если запись не связана с конкретной атакой (например, запуск дочернего процесса / запуск пользователем, остановка процесса и т.д.)
Комментарии	При старте процесса в «Безопасной среде» указывается полный путь к процессу и его PID. В остальных случаях поле остается пустым
Процесс	Указывается путь к исполняемому файлу
PID	Указывается уникальный идентификатор процесса
Пользователь	Указывается пользователь, от имени которого был запущен процесс в «Безопасной среде»
id правила	Идентификатор правила, которое было нарушено. ID правила указывается в случае, если запись связана с конкретной атакой
Правило	Наименование правила (причина появления записи), которое было нарушено
Результат	Результат действия «Безопасной среды». Сообщает о попытке вызова функции, которая была запрещена контролем приложений «Безопасной среды», или о срабатывании эвристического анализатора

Кроме того, в «Журнал контроля приложений» заносятся записи согласно настройкам аудита, производимым аналогично настройкам аудита в параметрах СОВ «Контроль приложений». При этом в «Журнал контроля приложений» попадают все действия приложения, запущенного в «Безопасной среде», которые попадают под правила для контроля приложений с пометкой в «Правило», что данное приложение запущено в «Безопасной среде».

4.2 ИНФОРМИРОВАНИЕ ПОЛЬЗОВАТЕЛЯ

После завершения работы приложения в «Безопасной среде» появляется диалоговое окно, представленное на Рисунке 8.

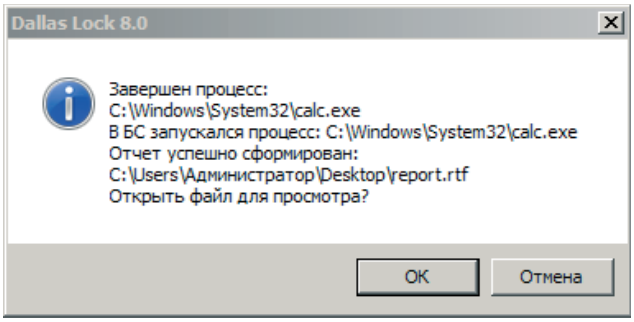


Рисунок 8 — Диалоговое окно с запросом просмотра отчёта

В формируемом «Отчёте о запуске приложения в безопасной среде» в формате RTF представлена информация согласно Таблице 2:

Таблица 2. Информация об отчёте.

Информация об отчете	
Дата построения:	
Имя компьютера:	
Название подразделения:	
Наименование АС:	
Рабочее место:	
Операционная система:	
Версия Dallas Lock:	
Номер лицензии Dallas Lock:	
Максимальное кол-во терминальных сессий:	
Номер системного блока:	

В Таблице 3 представлен пример информации, агрегируемой по итогам работы приложения в «Безопасной среде»:

Таблица 3. Информация о работе приложения в «Безопасной среде».

Имя файла	clt.exe
Путь к файлу	C:***\clt.exe
Идентификатор процесса	3136
Правило контроля приложений БС	По умолчанию
В БС запускался процесс	C:***\clt.exe
Использовать «Безопасную среду»	Вкл.
Показывать диалог с сохранением изменений после завершения	Вкл.
Автоматическая очистка по завершении всех процессов	Вкл.
Эвристический анализ для блокировки работы опасных процессов	Выкл.
Формировать отчет по завершении работы процесса в БС	Вкл.

Контроль приложений		
Правила для контроля приложений	Разрешено/ Запрещено/ Наследуется	Результат (Кол-во вызовов/Не обнаружено)
Взаимодействие с другим процессом посредством отсылки оконных сообщений	Разрешено	2 вызова
Взаимодействие с другим процессом посредством отсылки DDE сообщений	Разрешено	3 вызова
Взаимодействие с другим процессом с помощью OLE объектов	Разрешено	Не обнаружено
Вызов DNS API	Разрешено	Не обнаружено
Вызов функции для отправки ICMP сообщения	Разрешено	4 вызова
Вызов функции для работы с памятью чужого процесса	Разрешено	1 вызов
Вызов функции для создания потока в чужом процессе	Разрешено	1 вызов
Вызов функции потока в чужом процессе	Разрешено	Не обнаружено
Вызов функции DupHandles для работы с объектами чужого процесса	Разрешено	Не обнаружено
Вызов функции SetThreadContext для внедрения в чужой процесс	Разрешено	1 вызов
Вызов функции SetWinEventHook для внедрения dll в чужой процесс	Разрешено	1 вызов
Вызов функции SetWindowsHook для внедрения dll в чужой процесс	Разрешено	1 вызов
Выполнение скриптов через Windows Script Host	Разрешено	Не обнаружено
Выполнение скриптов PowerShell	Разрешено	Не обнаружено
Запуск доверенных (подписанных) дочерних процессов	Разрешено	3 вызова

Продолжение таблицы ▼

Начало таблицы ▲

Запуск драйвера	Разрешено	3 вызова
Запуск не доверенных (не подписанных) дочерних процессов	Разрешено	1 вызов
Запуск службы	Разрешено	Не обнаружено
Запуск cmd (включая пакетные файлы)	Разрешено	Не обнаружено
Изменение файла HOSTS	Разрешено	Не обнаружено
Инсталляция драйвера	Разрешено	4 вызова
Инсталляция службы	Разрешено	Не обнаружено
Использование RAW сокетов	Разрешено	1 вызов
Модификация памяти ядра с помощью привилегий отладки	Разрешено	1 вызов
Перехват нажатия клавиш	Разрешено	Не обнаружено
Получение контекста десктопа или активного окна (возможность снятие скриншота)	Разрешено	Не обнаружено
Право на работу с сетью для дочерних процессов приложения	Разрешено	3 вызова
Управление чужим процессом с помощью отладочного API	Разрешено	209 вызовов
Получение контекста десктопа или активного окна (возможно снятие скриншота)	Разрешено	Не обнаружено
Право на работу с сетью для дочерних процессов приложения	Разрешено	Не обнаружено
Управление чужим процессом с помощью отладочного API	Разрешено	Не обнаружено

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

БЕЗОПАСНАЯ СРЕДА

DALLAS LOCK SANDBOX

5

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Управление политиками «Безопасной среды» доступно на Сервере безопасности Dallas Lock путём применения политик «Безопасной среды» ко всему домену безопасности либо путём подключения к удалённой рабочей станции, входящей в домен безопасности, и произведением локальных настроек. Управление политиками «Безопасной среды» (подкатегория «Настройки») может производиться на уровне групп и подгрупп (Рисунок 9).

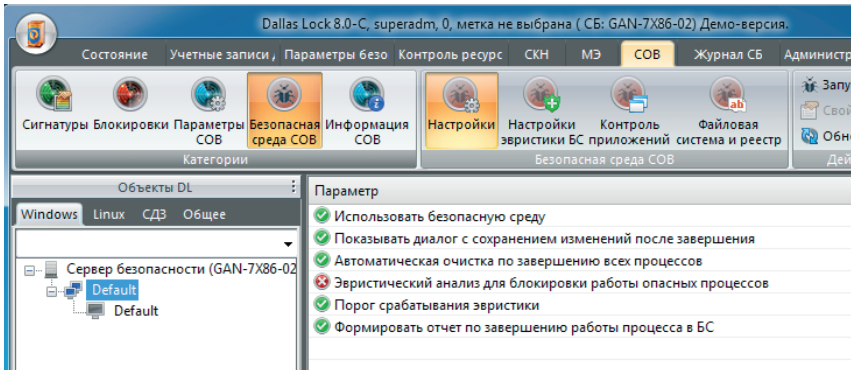


Рисунок 9 — Управление политиками «Безопасной среды» в консоли Сервера безопасности Dallas Lock

Настройки контроля приложений, файловой системы и реестра производятся только на уровне всего домена безопасности (Сервера безопасности Dallas Lock). При попытке настройки данных параметров на уровне групп пользователю выводится соответствующее сообщение (Рисунок 10).

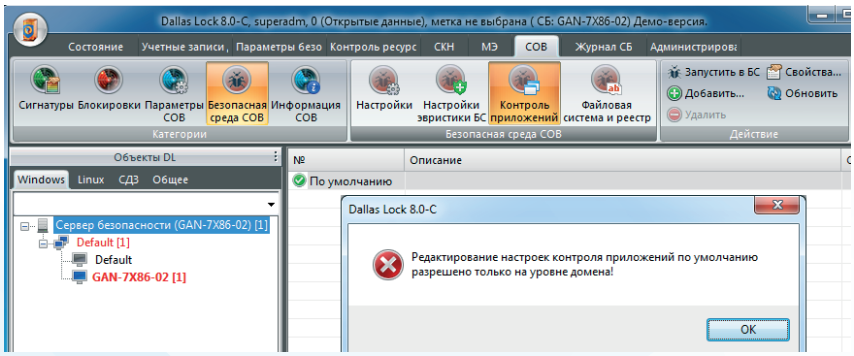


Рисунок 10 — Настройка контроля приложений в «Безопасной среде» доступна только на уровне всего домена безопасности

Настройки контроля приложений существуют также в параметрах СОВ Dallas Lock. Если настройка контроля приложений СОВ запрещает какие-либо действия на уровне всего домена безопасности (Сервера безопасности Dallas Lock), то данные запреты действуют и на контроль приложений «Безопасной среды». Если действия настроек контроля приложений разрешены, то возможно применение запрещающих правил для контроля приложений как на уровне домена безопасности (Сервера безопасности Dallas Lock), так и на уровне пользовательской рабочей станции.

ЗАКЛЮЧЕНИЕ

«Безопасная среда» стала логичным продолжением развития продукта СЗИ НСД Dallas Lock 8.0. Технологии частичной виртуализации позволяют достаточно просто и безопасно запускать приложения, полученные из недоверенных источников. Пользователям предоставлен современный действенный инструмент для защиты данных и приложений. Многолетний опыт разработки СЗИ Dallas Lock позволил реализовать надёжное решение для обеспечения безопасности.

Текущая реализация «песочницы» — это только первый шаг к развитию более широкого спектра функциональности 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.

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

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: