

Система лицензирования и защиты конфигураций платформы 1С:Предприятие 8, версия 3.0

Общие положения

Назначение	1
Совместимость с предыдущими версиями	1
Поддерживаемые режимы платформы 1С:Предприятие 8	2
Поддерживаемые операционные системы	2
Общий принцип работы	2
Ключи защиты.....	4
Состав и структура системы	2

Назначение

Система лицензирования и защиты конфигураций (далее СЛК или СЛК 3.0) представляет из себя программно-аппаратный комплекс и предназначена для защиты от несанкционированного использования авторских конфигураций платформы 1С:Предприятие 8. Использование СЛК позволит разработчикам прикладных решений на базе 1С решить следующие задачи:

- скрыть оригинальный авторский код конфигурации, представляющий "ноу-хау" разработчика;
- запретить использование (запуск и тиражирование) продукта без наличия ключа защиты;
- контролировать количество рабочих мест, используя указанное в ключе защиты количество лицензий;
- наращивать количество лицензий путем установки дополнительных ключей;
- ограничивать пользовательский функционал в зависимости от параметров ключа защиты, значений лицензионных параметров или содержания пользовательской памяти ключа.

Совместимость с предыдущими версиями

СЛК 3.0 является развитием СЛК 2.1 и полностью совместима с ней как по именам экспортируемых функций, так и по форматам данных.

Это означает, что разработчику для перевода конфигурации, использующей СЛК 2.0 / 2.1 на СЛК 3.0 достаточно просто обновить макет компоненты.

Однако, для повышения производительности и надежности работы, рекомендуется изучить документацию / пример защищенной конфигурации и внести в код конфигурации специфичные для СЛК 3.0 изменения.

Также, для создания / изменения файлов данных разработчик может использовать редактор файлов СЛК от предыдущих версий.

Основными отличиями СЛК 3.0 от предыдущих версий являются:

- поддержка работы ОС Linux как на уровне сервера, так и компоненты;
- использование протокола HTTP;
- поддержка интернационализации;
- поддержка работы с неактивированными аппаратных ключами;
- возможность реализации в конфигурации установки и мониторинга лицензий;
- реализация консоли сервера в виде веб-приложения.

Подробнее см. [Отличия от СЛК 2.1](#) и [Таблица отличий от СЛК 2.1](#).

Поддерживаемые режимы платформы 1С:Предприятие 8

СЛК поддерживает работу конфигураций на платформе 1С:Предприятие 8.2 и 8.3 в режимах управляемого и обычного приложения.

Поддерживаются все типы клиента (толстый, тонкий и веб), работа с файловыми ИБ и ИБ, размещенными на сервере приложений или опубликованными на веб-сервере.

Поддерживаемые операционные системы

СЛК поддерживает следующие (как 32-разрядные, так и 64-разрядные) ОС:

- ОС Microsoft Windows XP и выше: XP, Server 2003, Vista, 7, Server 2008 (R2), 8, 8.1, Server 2012 (R2), 10
- ОС Linux на базе Debian: Debian 7.5 и выше, Ubuntu 12.04 и выше
- ОС Linux на базе RedHat: CentOS 6.7 и выше, Fedora 22 и выше

Состав и структура системы

Система состоит из следующих компонентов:

Сервер СЛК

Сервер является основным элементом системы и предназначен для контроля количества лицензий и доступа к ключам защиты, защищенным объектам и лицензионным параметрам.

Сервер СЛК является мини веб-сервером, поэтому для работы ему необходим свободный порт (по умолчанию используется порт **9099**).

Для администрирования, просмотра установленных ключей защиты и текущих соединений используется консоль сервера СЛК, которая реализована в виде веб приложения и доступна по адресу и порту сервера СЛК. Например, на локальном компьютере при использовании стандартного порта адрес консоли будет <http://localhost:9099>.

Подробнее см. [Руководство администратора](#).

Внешняя компонента платформы 1С:Предприятие

Элемент системы, встраиваемый в конфигурацию. Поставляется в виде zip-архива для загрузки в общий макет конфигурации. Этот архив содержит варианты компоненты для всех поддерживаемых СЛК ОС.

Внешняя компонента экспортирует объект, который позволяет запустить систему лицензирования и получить менеджер объектов для доступа к защищенному функционалу, работы лицензионными параметрами и пользовательской памятью ключей защиты и т.д.

Основные действия разработчика по защите конфигурации заключаются именно в подключении компоненты и обращению ее объектам.

Подробнее см. [Руководство разработчика](#), раздел [Подключение](#).

Редактор файлов данных

Редактор файлов данных предназначен для создания файлов, содержащих защищенные объекты и файлов лицензионных параметров. Для работы редактору необходим открытый ключ для конкретной серии ключей, поставляемый в комплекте разработчика.

Подробнее см. [Руководство разработчика](#), раздел [Создание файлов данных](#).

Общий принцип работы

При запуске конфигурации система лицензирования устанавливает соединение с сервером СЛК, который разрешает или запрещает дальнейшую работу в зависимости от наличия ключа защиты и количества свободных лицензий.

Связь с сервером организована по протоколу **HTTP**, поэтому для работы системе необходимо наличие свободного порта (по умолчанию используется порт **9099**).

Система реализует контроль лицензий на стороне сервера, что позволяет существенно упростить использование СЛК в конфигурациях, работающих в тонком и/или веб клиенте и клиент-серверном режиме.

Особенностью подхода является то, что при работе в клиент-серверном режиме (сервер приложений 1С, веб сервер) каждый сеанс информационной базы будет занимать отдельную лицензию. При работе в файловом режиме одну лицензию будут занимать все подключения с одного компьютера (при работе в терминальном режиме одну лицензию будут занимать все подключения с одного терминального клиента).

С целью защиты оригинального авторского кода и экранных форм реализован механизм защиты обработок и отчетов (защищенные объекты). Защищенные объекты исключены из конфигурации и помещены в специальный файл данных, подготовленный разработчиком при помощи редактора файлов данных.

Файлы защищенных объектов рекомендуется включать в конфигурацию в виде общих макетов, но для совместимости с предыдущими версиями СЛК возможно размещать их на сервере СЛК. Также возможно размещение файлов данных в произвольных макетах, например, обработок или отчетов.

При использовании защищенных объектов, разработчик может ограничивать пользовательский функционал в зависимости от параметров ключа, значений лицензионных параметров или содержания пользовательской памяти ключа.

Подробнее см. [Руководство разработчика](#).

Ключи защиты

Ключи защиты – компонент системы, предназначенный для доступа к защищенным объектам и контроля количества лицензий на основе указанного в ключе значения.

Для **каждой защищаемой конфигурации** создается своя, **уникальная, серия ключей**, что делает ключи от одной конфигурации несовместимыми с ключами от других конфигураций.

В рамках серии ключи могут быть **основными** (обычный вариант использования) и **дополнительными** (для расширения функционала и количества лицензий) и **демонстрационными** (временными, для демонстрации возможностей продукта и организации промо-акций).

***Дополнительные** ключи не работают без основного ключа и должны быть установлены на том же компьютере, что и основной ключ.*

***Демонстрационные** ключи не могут быть использованы для увеличения числа лицензий и не могут быть установлены вместе с другими ключами такой же серии.*

Каждый ключ содержит количество лицензий, которое определяет максимально возможное число одновременно занимаемых лицензий. Кроме этого, каждый ключ имеет уникальный серийный номер, присваиваемый при создании ключа.

По виду исполнения ключи могут быть **аппаратными** (USB) или **программными** (привязанные к конфигурации компьютера или неактивированному аппаратному ключу).

Подробнее см. **Ключи защиты**.