ПРОГРАММНЫЙ КОМПЛЕКС
ОБРАБОТКИ ИНЖЕНЕРНЫХ ИЗЫСКАНИЙ, ЦИФРОВОГО
МОДЕЛИРОВАНИЯ МЕСТНОСТИ, ПРОЕКТИРОВАНИЯ
ГЕНПЛАНОВ И АВТОМОБИЛЬНЫХ ДОРОГ

СИСТЕМА ЗАЩИТЫ ЭШЕЛОН II

Продукты КРЕДО с системой защиты Эшелон II

Руководство системного администратора

2020

СИСТЕМА ЗАЩИТЫ ЭШЕЛОН II

Руководство системного администратора.

Восьмая редакция.

support@credo-dialogue.com
training@credo-dialogue.com

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящем документе содержатся инструкции по организации, установке и настройке самой системы защиты Эшелон II.

Документ предназначен для системных администраторов.

За дополнительными сведениями и консультацией обращайтесь в компанию «Кредо-Диалог».

E-mail: support@credo-dialogue.com

Сайт компании: http://www.credo-dialogue.ru

СИСТЕМА ЗАЩИТЫ ЭШЕЛОН II

ОБЩИЕ СВЕДЕНИЯ

Программные продукты КРЕДО защищаются от несанкционированного использования при помощи системы защиты Эшелон II, которая базируется на электронных ключах Guardant Code. Ключи Guardant Code реализованы на современной высокопроизводительной аппаратной платформе с возможностью выполнения произвольного пользовательского кода внутри устройства.

Система защиты Эшелон II может использоваться как для запуска приложений на отдельном компьютере, так и для контроля используемых лицензий программных продуктов КРЕДО в сети предприятия. На каждом компьютере, на котором установлен ключ, необходимо запустить **Менеджер защиты Эшелон II** и при необходимости включить поддержку обслуживания клиентов по сети.

Только для комплекса CREDO III: дополнительные компоненты – редакторы Классификаторов, Символов, Шаблонов, утилиты Миграции данных и Генерации кадастровых запросов не требуют отдельной лицензии, однако для своей работы требуют наличия ключа Guardant Code с любой лицензией КРЕДО.

При обновлении или приобретении дополнительных лицензий систем КРЕДО нет необходимости обменивать или приобретать новый ключ защиты Guardant Code. Устройство может быть дистанционно обновлено с помощью утилиты программирования ключа (см. подраздел «Удаленное программирование ключа защиты»).

ЭЛЕКТРОННЫЕ КЛЮЧИ GUARDANT CODE

ПОРЯДОК УСТАНОВКИ КЛЮЧА

ВНИМАНИЕ ! USB-ключ следует подсоединять к порту только после установки **Менеджера защиты Эшелон II**. Если ключ был подсоединен до установки Менеджера и запустился стандартный мастер установки USB-устройств Windows, то необходимо извлечь ключ из порта и отменить работу мастера.

1. Установите **Менеджер защиты Эшелон II**.
2. Перезагрузите компьютер, если мастер установки потребует этого.
3. Подсоедините ключ Guardant Code к свободному USB-порту. Подключение и отключение может производиться как при включенном компьютере, так и при выключенном.
4. Убедитесь в том, что защищенная система КРЕДО функционирует правильно.

ВНИМАНИЕ ! Нельзя отсоединять ключ, если он используется защищенными приложениями на компьютере или в сети. Система защиты требует постоянного доступа к ключу и может проверять его наличие в произвольные моменты времени. В случае отсоединения ключа ранее запущенные приложения смогут продолжить работу только после восстановления доступа к нему.

ВНИМАНИЕ ! Во избежание потери несохраненных данных нельзя допускать переход компьютера в ждущий режим (standby), если на компьютере запущены защищенные приложения либо **Менеджер защиты Эшелон II** с поддержкой обслуживания клиентов по сети.

ПРАВИЛА ЭКСПЛУАТАЦИИ И ХРАНЕНИЯ

- Оберегайте электронный ключ от механических воздействий (падения, сотрясения, вибрации и т.п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения - все это может привести к выходу ключа из строя.
- Не прилагайте излишних усилий при подсоединении электронного ключа к компьютеру.
- Не разбирайте электронный ключ. Это может привести к поломке его корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие, к ненадежной работе устройства или выходу из строя.
- Допустимая температура окружающего воздуха при хранении, перевозке и работе электронных ключей от +0 до +45 °С. Относительная влажность воздуха от 0 до 100% без конденсата.
- Не используйте электронный ключ, охлажденный при перевозке или хранении до отрицательных температур, прежде чем он прогреется до комнатной температуры.

- Не допускайте попадания на электронный ключ (особенно на разъемы) пыли, грязи, влаги, любых жидкостей и т. п. При засорении разъемов ключа примите меры для их очистки. Для очистки корпуса и разъемов используйте сухую ткань. Использование органических растворителей недопустимо.
- В случае неисправности или неправильного функционирования электронного ключа обращайтесь в службу технической поддержки компании «Кредо-Диалог».

УДАЛЕННОЕ ПРОГРАММИРОВАНИЕ КЛЮЧА

Электронный ключ Guardant Code содержит информацию о количестве лицензий для определенной версии каждой системы КРЕДО, запуск которой разрешен на данном ключе. При покупке или обновлении систем КРЕДО обмен или приобретение новых ключей защиты не требуется. Пользователь может самостоятельно перепрограммировать ключ с помощью специальной утилиты, предварительно получив от компании «Кредо-Диалог» или ее регионального представителя файл нового состояния, для этого необходимо:

1. Сохранить на диске полученный файл программирования ключа.
2. Скачать утилиту программирования ключа.
3. Программирование ключа должно выполняться на том же компьютере, где установлена Система защиты Эшелон II. Перед началом процедуры завершить все приложения, получающие лицензии с программируемого ключа.
4. Вставить в порт компьютера ключ, для которого предназначен файл программирования. Дождаться определения ключа системой (светодиод ключа должен начать гореть постоянно). Если ключ не определится, вставить его в другой порт компьютера, а также убедиться, что подключаемые устройства не блокируются антивирусным или другим программным обеспечением.
5. Запустить утилиту программирования ключа. В открывшемся окне (рис. 1) нажать кнопку **Выбрать**, при этом появится диалог выбора файла, в котором необходимо указать полученный файл программирования ключа. Затем нажать кнопку **Применить**.

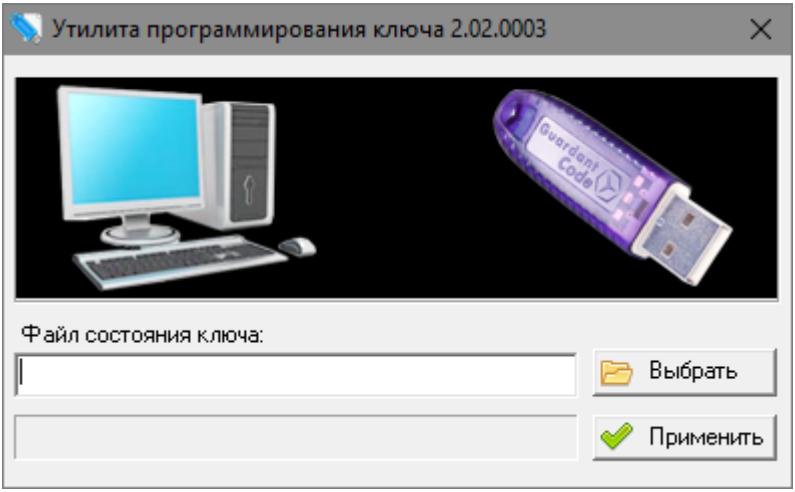

Рис. 1. Утилита программирования ключа

6. Дождаться завершения процесса программирования ключа (он может занять несколько минут). Появится сообщение о результате операции.
7. Обновленный в процессе программирования ключа файл и скриншот сообщения о результате операции необходимо отправить по электронной почте на адрес key@credo-dialogue.com.

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ЭШЕЛОН II В ЛОКАЛЬНОЙ СЕТИ

Количество компьютеров сети, на которых может быть одновременно запущена конкретная система КРЕДО, ограничено количеством запрограммированных в ключе лицензий для соответствующей системы. К одному компьютеру может быть подключено несколько ключей защиты, при этом количество лицензий для каждой системы, запрограммированное в ключах, суммируется. Кроме того, в пределах локальной сети может функционировать несколько **Менеджеров защиты Эшелон II** с включенной поддержкой обслуживания клиентов по сети на разных компьютерах с разными ключами. Общее количество лицензий каждой системы КРЕДО в сети равно сумме лицензий, запрограммированных во всех ключах, обслуживаемых всеми **Менеджерами защиты Эшелон II** в локальной сети.

Система защиты Эшелон II позволяет запускать несколько копий каж-

дого защищенного приложения на одной рабочей станции для одного пользователя, причем всем копиям выделяется единственная лицензия.

ВНИМАНИЕ ! Если на компьютере используется брандмауэр, необходимо настроить его так, чтобы был разрешен обмен информацией между защищенными приложениями и **Менеджером защиты Эшелон II**. Для встроенного брандмауэра операционной системы Windows такая настройка выполняется автоматически во время установки систем КРЕДО и утилит системы защиты Эшелон II.

АДАПТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ЭШЕЛОН II К СЕТЕВОМУ ОКРУЖЕНИЮ

Как правило, для работы системы защиты Эшелон II в локальной сети никаких специальных настроек не требуется. Достаточно установить защищенные системы КРЕДО на рабочие станции, выбрать компьютер, к которому будет присоединен ключ защиты, установить на нем **Менеджер защиты Эшелон II** с поддержкой обслуживания клиентов по сети и вставить ключ. После выполнения этих действий можно приступать к работе.

Защищенная система при запуске сначала пытается обнаружить ключ локально. Если на компьютере не установлен **Менеджер защиты Эшелон II**, или отсутствует ключ, либо на нем нет свободных лицензий для данной системы, приложение произведет поиск подходящего ключа в сети. Защищенная система будет работать с первым обнаруженным Менеджером, ключ которого имеет соответствующую свободную лицензию.

НАСТРОЙКИ ЗАПУСКА ДЛЯ СИСТЕМ:

- КРЕДО РАСЧЕТ ДЕФОРМАЦИЙ 1.02
- КРЕДО ДИСЛОКАЦИЯ 1.2
- КРЕДО МОРФОСТВОР 1.01

Настройку защищенной системы КРЕДО при работе с сетевой защитой можно произвести с помощью конфигурационного файла *Netech2.in*i. Файл *Netech2.ini* должен находиться в той же папке, куда установлена система. Пример файла, содержащего все возможные параметры в виде комментариев, устанавливается вместе с защищенными системами. Для того чтобы получить файл *Netech2.ini*, подходящий для конкретных условий, необходимо удалить символ комментария (;) в строках, содержащих нужные параметры, и задать значения этих параметров.

Параметры файла Netech2.ini

Любой параметр в *Netech2.ini* может отсутствовать или быть закомментирован – в этом случае приложение будет использовать значение по умолчанию.

СЕКЦИЯ [NETWORKPROTOCOLS]

В этой секции задаются общие параметры:

- **LocalOnly:** указывает защищенной системе работать только с локальным **Менеджером защиты Эшелон II**. Возможные значения – 1 (да, работать только с локальным Менеджером) или 0 (нет, используется сетевая защита). Значение по умолчанию – 0.
- **TcpIP:** определяет, необходимо ли использовать протокол TCP/IP для коммуникации с удаленным **Менеджером защиты Эшелон II**. Возможные значения – 1 (да, использовать) или 0 (нет, не использовать). Значение по умолчанию – 1.
- **TcpIPv6:** не используется.

СЕКЦИЯ [TCP/IP]

В этой секции задаются параметры для работы по протоколу TCP/IP:

- **AutoSearch –** указывает защищенной системе, нужно ли произвести автоматический поиск удаленного **Менеджера защиты Эшелон II** по заданным критериям ServerAddress и ServerPort или попытаться подключиться непосредственно к Менеджеру по адресу ServerAddress:ServerPort. Автоматический поиск может использоваться, если адрес Менеджера неизвестен заранее. Возможные значения – 1 (да, произвести поиск) или 0 (нет, не производить). Значение по умолчанию – 1.
- **ServerAddress** – указывает адрес (доменное имя или IP-адрес) компьютера в сети, на котором запущен **Менеджер защиты Эшелон II**. Значение по умолчанию – 255.255.255.255 (адрес для широковещательной рассылки). При этом значении параметра и **AutoSearch**=1 защищенные системы будут производить автоматический поиск **Менеджеров защиты Эшелон II** в сети с помощью широковещательных рассылок.
- **ServerPort** – указывает номер порта, используемого удаленным **Менеджером защиты Эшелон II** для приема запросов при поиске (**AutoSearch**=1) или для приема запросов к ключу (**AutoSearch**=0). Значение по умолчанию – 5555.

- **SessionTimeout** – максимальное время в секундах, в течение которого защищенная система при запуске будет выполнять поиск удаленного **Менеджера защиты Эшелон II**, ключ которого имеет свободную лицензию. Значение по умолчанию – 20 секунд.
- **SendRcvTimeout** – максимальное время в секундах, по истечении которого защищенная система прекратит попытки связаться с удаленным **Менеджером защиты Эшелон II**, предоставившим лицензию. Значение по умолчанию – 7 секунд. По истечении этого срока приложение сообщит, что **Менеджер защиты Эшелон II** не найден, и предложит повторить попытку или завершить работу без сохранения результатов.

НАСТРОЙКИ ЗАПУСКА ДЛЯ ПП КОМПЛЕКСА CREDO III И ПРОЧИХ ПРОГРАММНЫХ ПРОДУКТОВ

Настройка параметров поиска свободной лицензии производится с помощью Центра управления продуктами КРЕДО. Вкладка **Настройки запуска** (рис. 2) предоставляет графический интерфейс для редактирования настроек всех систем КРЕДО, установленных на компьютере, значительно расширяя возможности использовавшегося в предыдущих версиях конфигурационного файла *Netech2.ini*.

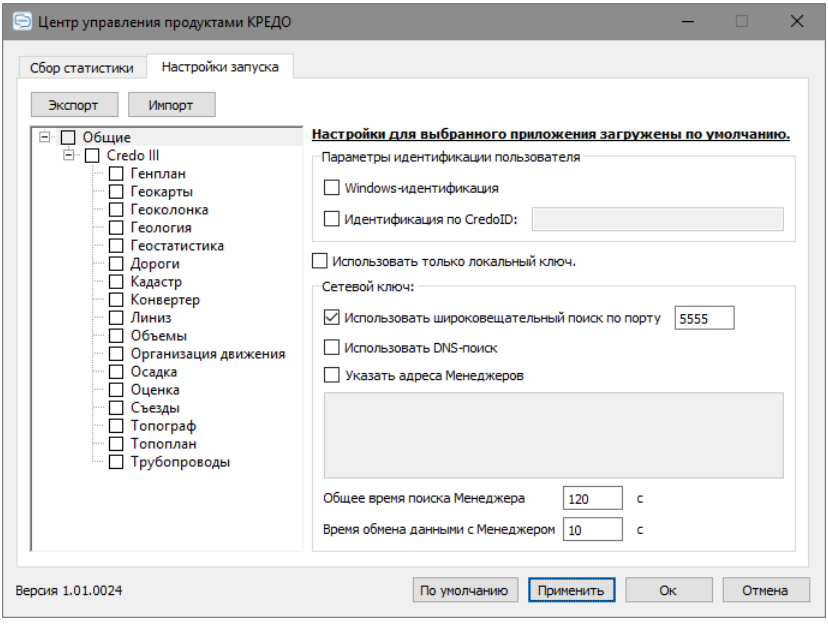

Рис. 2. Центр управления продуктами КРЕДО

Центр управления продуктами КРЕДО позволяет настроить как отдельную защищенную систему (одновременно 32- и 64-разрядные версии), так и все ПП КРЕДО, установленные на компьютере (запись *Общие*). При этом используются только активные записи, напротив которых в списке установлен флаг. Защищенная система в первую очередь использует собственные настройки, затем *Общие*. При отсутствии пользовательских настроек используются настройки по умолчанию.

Для некоторых продуктов (комплекс CREDO III, МАЙНФРЭЙМ, ГЕОСМЕТА) дополнительно используется запись, которая позволяет задать общие настройки для всех приложений группы. Если одновременно заданы настройки для конкретной системы и для группы, то будут использованы настройки конкретной системы.

Кнопка **Экспорт** позволяет сохранить пользовательские настройки для обмена или резервного копирования в формате *credoxml*, а также подготовить информацию обо всех настройках ПП КРЕДО на данном компьютере для отправки в службу технической поддержки в формате *allxml*. Кнопка **Импорт** позволяет загрузить пользовательские настройки из конфигурационного файла *Netech2.ini* или из обменного файла *credoxml*.

Для защищенной системы можно настроить следующие параметры (в скобках указаны аналоги в *Netech2.ini* при их наличии):

- Группа **Параметры идентификации пользователя** – указывает защищенной системе на необходимость предварительной идентификации пользователя для работы с **Менеджером защиты Эшелон II**, который поддерживает механизм управления доступом к лицензиям. Флаг **Windows-идентификация** предписывает отправлять данные учетной записи пользователя Windows или Active Directory, от имени которой запускается приложение (NTLM-авторизация). Флаг **Идентификация по CredoID** позволяет работать с арендованными и временными версиями ПП на серверах КРЕДО. Оба варианта не могут использоваться одновременно. Несоответствие настроек идентификации защищенной системы и Менеджера защиты приведет к ошибке в процессе получения лицензии. По умолчанию оба флага сняты.
- **Использовать только локальный ключ** *(LocalOnly)* – заставляет защищенную систему работать только с локальным **Менеджером защиты Эшелон II**, запуск будет возможен только при наличии установленного на компьютере ключа Guardant Code. По умолчанию флаг снят.
- **Использовать широковещательный поиск по порту** *(ServerPort*

при AutoSearch=1) – указывает защищенной системе произвести автоматический поиск удаленного **Менеджера защиты Эшелон II** с помощью широковещательной рассылки по указанному порту (должен соответствовать порту обслуживания Менеджера по протоколу TCP/IP). По умолчанию флаг установлен, номер порта 5555.

- **Использовать DNS-поиск** – указывает защищенной системе произвести поиск удаленного **Менеджера защиты Эшелон II** по специальным записям в DNS. Для этого используются записи с именем EchMan типа SRV для протокола TCP, например: _echman._tcp.credo-dialogue.local. Поиск происходит в текущем домене. При необходимости можно настроить несколько записей EchMan. Данный вид поиска устраняет недостатки широковещательных рассылок: невозможность обнаружения Менеджеров в других сегментах сети и высокую нагрузку на сеть, создаваемую широковещательными рассылками. По умолчанию флаг снят.
- **Указать адреса Менеджеров** *(ServerAddress:ServerPort при AutoSearch=0)* – указывает защищенной системе адреса удаленных **Менеджеров защиты Эшелон II**, которые должны быть опрошены. Список разделяется символом «точка с запятой» (;), может содержать IP-адреса или доменные имена серверов с указанием номера порта или без него (по умолчанию 5555). По умолчанию флаг снят, список пустой.
- **Общее время поиска Менеджера** *(SessionTimeout)* – задает максимальное время в секундах, в течение которого защищенная система при запуске будет выполнять поиск удаленного **Менеджера защиты Эшелон II**, ключ которого имеет свободную лицензию. Значение по умолчанию – 30 секунд.
- **Время обмена данными с Менеджером** *(SendRecvTimeout)* – задает максимальное время в секундах, по истечении которого защищенная система прекратит попытки связаться с удаленным **Менеджером защиты Эшелон II**, предоставившим свободную лицензию. По истечении этого срока приложение сообщит, что **Менеджер защиты Эшелон II** недоступен, и предложит повторить попытку либо завершить работу без сохранения результатов. Значение по умолчанию – 5 секунд.

ВНИМАНИЕ ! Если один или несколько параметров заданы неверно, то настройки не могут быть сохранены или экспортированы, при этом блокируется переключение на другие записи в списке установленных ПП.

УПРАВЛЕНИЕ НАСТРОЙКАМИ НА РАБОЧИХ МЕСТАХ

В крупных организациях с большим количеством рабочих мест КРЕДО может быть востребовано централизованное управление настройками защиты с помощью групповых политик Active Directory, которые позволяют распространить единообразные наборы настроек на все компьютеры организации или отдельного подразделения. Правильные установки защиты ускоряют запуск ПП, помогают установить различные правила для подразделений, минимизируют обращения за технической поддержкой. При управлении с помощью групповых политик пользователь не сможет редактировать локальные настройки на своем компьютере с помощью Центра управления продуктами КРЕДО.

Все доступные параметры работы защищенных систем могут быть установлены с помощью административного шаблона, для начала его использования можно воспользоваться инструкцией.

КОМПОНЕНТЫ СИСТЕМЫ ЗАЩИТЫ ЭШЕЛОН II

Система защиты Эшелон II включает в себя следующие компоненты:

- **Менеджер защиты Эшелон II** – служба операционной системы, которая обеспечивает приём запросов от защищенного приложения, запущенного на компьютере, доставку их непосредственно к ключу, а также отправку ответов ключа приложению.
- **Утилита управления Менеджером защиты Эшелон II** – вспомогательное приложение, которое позволяет настраивать и контролировать сервис **Менеджера защиты Эшелон II**, установленный на том же компьютере.
- **Монитор защиты Эшелон II** – независимая утилита (может устанавливаться отдельно от других компонентов), позволяет автоматически находить и наблюдать за состоянием всех **Менеджеров защиты Эшелон II**, функционирующих в локальной сети. Дополнительно можно настроить мониторинг любых Менеджеров, для которых известен сетевой адрес.

Подробная информация о функционировании и настройке компонентов приведена в справочной системе.