ТИМ КРЕДО
ИНФОРМАЦИОННОЕ МОДЕЛИРОВАНИЕ ОБЪЕКТОВ ПГС И ТРАНСПОРТА НА ВСЕХ СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА

РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА

2024

Руководство системного администратора

Руководство пользователя (для начинающих) к версии 2025.1.

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

Модули ТИМ 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 модулей ТИМ КРЕДО на отдельном компьютере, так и для контроля используемых лицензий модулей ТИМ 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.

Система защиты Эшелон II способна работать в операционных системах Microsoft Windows и Astra Linux.

Дополнительные компоненты: Редакторы Классификаторов, Символов, Шаблонов, утилиты Миграции данных не требуют отдельной лицензии, однако для своей работы требуют наличия ключа Guardant Code с любой лицензией ТИМ КРЕДО.

При обновлении или приобретении дополнительных лицензий модулей ТИМ 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

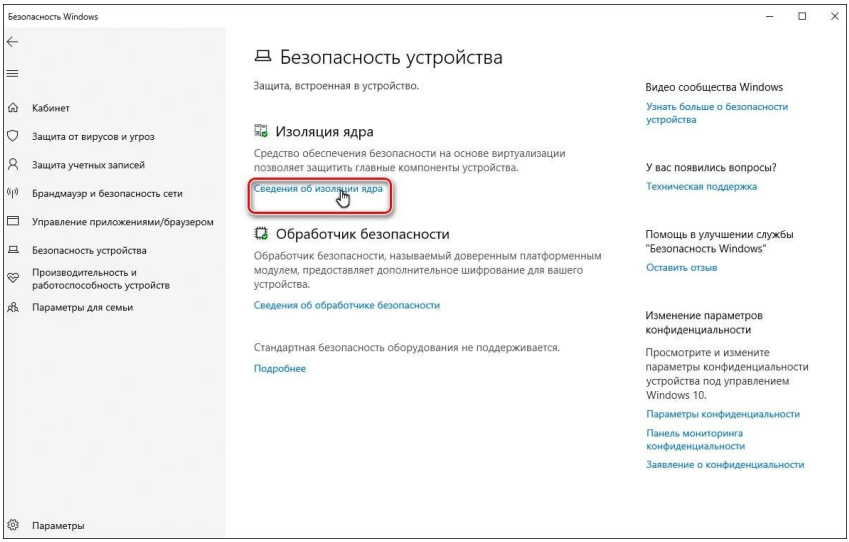
Порядок установки ключа

ВНИМАНИЕ! При установке **Менеджера защиты Эшелон II** устанавливается драйвер Guardant. В Microsoft Windows 11 по умолчанию включена опция «Целостность памяти – Изоляция ядра», которая при установке драйвера Guardant приводит к «синему экрану». Чтобы избежать этой ошибки, нужно до установки отключить данную опцию.

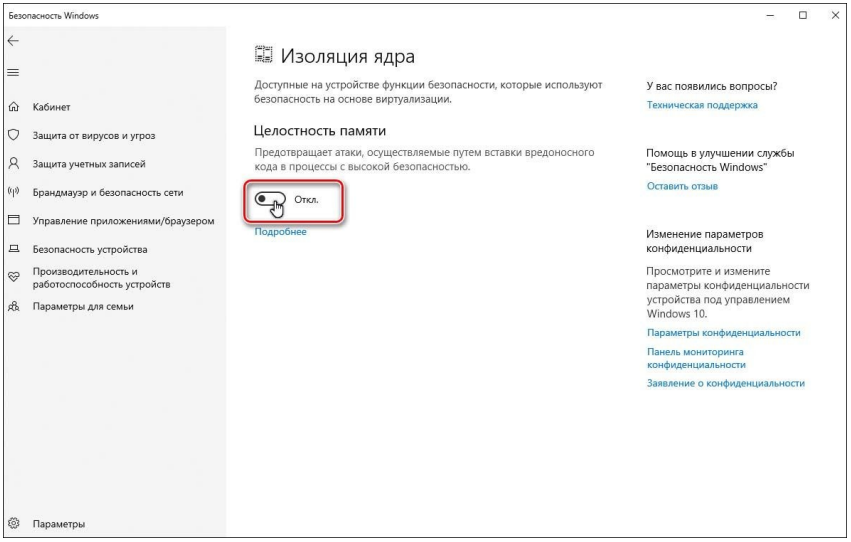
В Microsoft Windows 10 данная опция также может быть включена, поэтому рекомендуется проверить ее до установки Менеджера защиты.

Порядок отключения опции «Целостность памяти – Изоляция ядра»:

1. откройте Центр безопасности Защитника Windows;
2. выберите раздел «Безопасность устройства»;
3. в секции «Изоляция ядра» нажмите ссылку «Сведения об изоляции ядра»:



4. Переведите переключатель «Целостность памяти» в положение «Откл.»:



Порядок установки ключа:

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 защищенный модуль ТИМ КРЕДО функционирует правильно.

ВНИМАНИЕ! Нельзя отсоединять ключ, если он используется защищенными модулями 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 модули 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 модули 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

Электронные ключи защиты содержит информацию о количестве лицензий для определенной версии каждого модуля ТИМ КРЕДО, запуск которого разрешен на данном ключе. При покупке или обновлении модулей ТИМ КРЕДО обмен или приобретение новых ключей защиты не требуется. Пользователь может самостоятельно перепрограммировать ключ с помощью специальной утилиты после того, как получит уведомление от компании «КРЕДО-ДИАЛОГ» или ее регионального представителя о готовности нового состояния ключа. Обычно такие уведомления высылаются по электронной почте.

Инструкция по программированию ключей защиты Guardant Code и Guardant Code Time находится здесь.

Использование системы защиты ЭШЕЛОН II в локальной сети

Количество компьютеров сети, на которых может быть одновременно запущен конкретный модуль ТИМ КРЕДО, ограничено количеством запрограммированных в ключе лицензий для соответствующего модуля. К одному компьютеру может быть подключено несколько ключей защиты, при этом количество лицензий для каждого модуля, 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 каждого модуля ТИМ 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 каждого защищенного модуля 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 модулями и **Менеджером защиты Эшелон II**. Для встроенного брандмауэра операционной системы Windows такая настройка выполняется автоматически во время установки модулей ТИМ КРЕДО и утилит системы защиты Эшелон II.

Адаптация системы защиты ЭШЕЛОН II к сетевому окружению

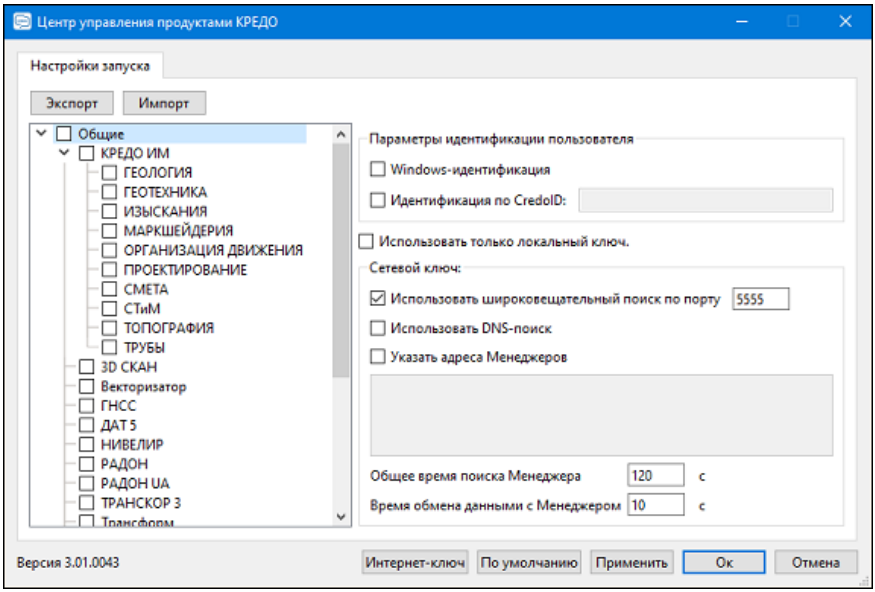
Как правило, для работы системы защиты Эшелон II в локальной сети никаких специальных настроек не требуется. Достаточно установить защищенные модули ТИМ КРЕДО на рабочие станции, выбрать компьютер, к которому будет присоединен ключ защиты, установить на нем **Менеджер защиты Эшелон II** с поддержкой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

Защищенный модуль 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 данного модуля, приложение произведет поиск подходящего ключа в сети. Защищенный модуль будет работать с первым обнаруженным Менеджером, ключ которого имеет соответствующую свободную лицензию.

Настройки запуска модулей ТИМ КРЕДО

Настройка параметров поиска свободной лицензии производится с помощью утилиты **Центр управления продуктами КРЕДО**. Данная утилита предоставляет графический интерфейс для редактирования настроек всех модулей ТИМ КРЕДО.

Центр управления модулями ТИМ КРЕДО позволяет настроить как отдельный защищенный модуль (одновременно 32- и 64-разрядные версии), так и группу модулей (запись *Общие*). Настройки применяются только к тем записям, для которых установлен флаг в дереве в левой части окна Центра управления. Защищенный модуль в первую очередь использует собственные настройки, затем настройки группы и в последнюю очередь - *Общие*. При отсутствии пользовательских настроек используются настройки по умолчанию.



Кнопка **Интернет-ключ** предназначена для быстрой настройки выбранного модуля или группы модулей на получение лицензии через интернет с сервера лицензий ТИМ КРЕДО. Данная кнопка упрощает настройку запуска пользователям временных версий и аренды. При нажатии на кнопку все поля автоматически заполняются необходимыми значениями, остается только ввести или вставить из буфера обмена 32-разрядное значение CredoID, полученное от поставщика модуля ТИМ КРЕДО.

Кнопка **По умолчанию** предназначена для установки всех настроек выбранного модуля или группы модулей в значения по умолчанию, которые позволяют использовать локальный ключ, а в случае его отсутствия либо отсутствия в нем необходимых лицензий - производить автоматический поиск ключей и лицензий в локальной сети. В большинстве случаев набор настроек по умолчанию является оптимальным и не требует модификации.

Кнопка **Экспорт** позволяет сохранить пользовательские настройки для обмена или резервного копирования в формате *credoxml*, а также подготовить информацию обо всех настройках ТИМ 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 защищенного модуля можно настроить следующие параметры (в скобках указаны аналоги в *Netech2.ini* при их наличии):

- Группа **Параметры идентификации пользователя** – указывает защищенному модулю на необходимость предварительной идентификации пользователя для работы с **Менеджером защиты Эшелон II**, который поддерживает механизм управления доступом к лицензиям. Флаг **Windows-идентификация** доступен только в ОС Windows и предписывает отправлять данные учетной записи пользователя Windows или Active Directory, от имени которой запускается модуль (NTLM-авторизация). Флаг **Идентификация по CredoID** позволяет работать с арендованными и временными версиями модулей на серверах ТИМ 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 защищенный модуль 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 защищенному модулю 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 защищенному модулю 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 защищенному модулю 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 защищенный модуль 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 защищенный модуль 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 модулей.

Ведение журнала доступа к лицензиям

На основе журналов можно проводить анализ использования лицензий: частоту и длительность использования, целевое использование в подразделениях, необходимость в дополнительных лицензиях модулей и т. п.

Журнал ведется в текстовом файле (кодировка UTF-8), одна строка соответствует одной операции, поля разделены символом табуляции (\t). Имя файла журнала имеет формат "Echelon-II ГГГГ-ММ-ДД.log". Подробно формат файла журнала описан в справочной системе Эшелон II.

Для активации функции ведения журнала нужно:

- *для Windows*: в разделе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Credo-Dialogue\Echelon-II\Менеджер защиты\Log** создать строковый (*REG_SZ*) параметр **Path**, в котором указать полный путь к директории, в которой будут создаваться файлы журналов. Дополнительно можно ограничить время жизни файлов, после которого служба Менеджера очистит устаревшие файлы: создать числовой (*DWORD*) параметр **Lifetime** в том же разделе и указать срок в днях.
- *для Linux*: в файле

  /etc/Credo-Dialogue/Echelon-II/Менеджер защиты/Log

в параметре **Path** указать полный путь к директории, в которой будут создаваться файлы журналов. Дополнительно можно ограничить время жизни файлов, после которого служба Менеджера очистит устаревшие файлы: задать в параметре **Lifetime** в том же файле срок в днях.

Управление настройками на рабочих местах

Информация в данном разделе актуальна только для операционной системы Microsoft Windows.

В крупных организациях с большим количеством рабочих мест ТИМ 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 модулей, 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 модулей 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 модуля, запущенного на компьютере, доставку их непосредственно к ключу, а также отправку ответов ключа модулю.
- **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.

Перечисленные компоненты Системы защиты Эшелон II существуют в исполнении для операционных систем Microsoft Windows и Astra Linux.

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