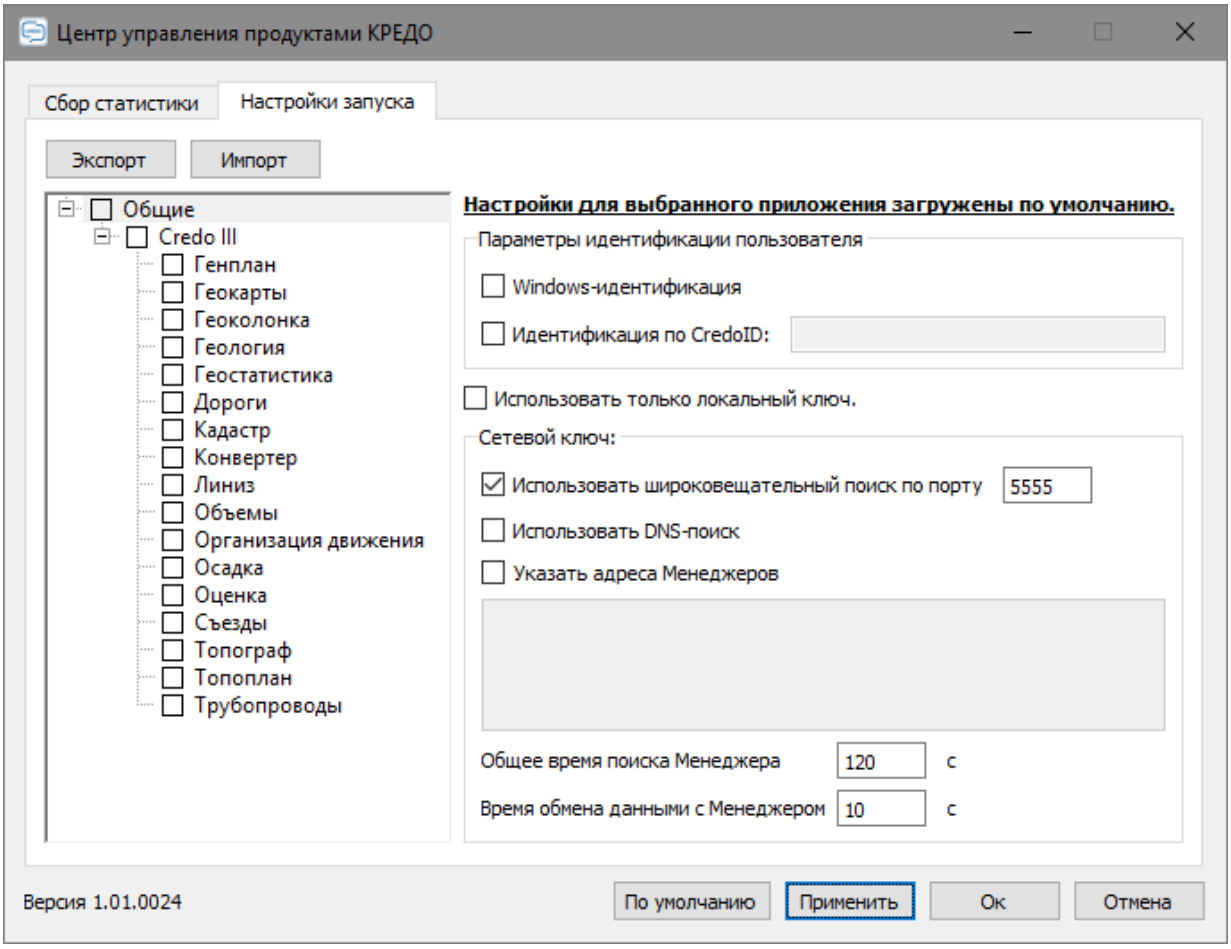
АДАПТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ЭШЕЛОН II К СЕТЕВОМУ ОКРУЖЕНИЮ

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.



Центр управления продуктами КРЕДО

Более тонкую настройку параметров защиты можно произвести с помощью Центра управления продуктами КРЕДО. Вкладка **Настройки запуска** (рисунок) предоставляет графический интерфейс для редактирования настроек всех ПП, установленных на компьютере, значительно расширяя возможности использовавшегося в предыдущих версиях конфигурационного файла *Netech2.ini*.

ВНИМАНИЕ ! При обновлении предыдущих версий защищенных систем конфигурационный файл *Netech2.ini* будет удален. Если в нем были заданы пользовательские настройки, сохраните файл перед обновлением и импортируйте в Центр управления.

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*. В случае отсутствия пользовательских настроек будут использованы 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 компании «Кредо-Диалог». 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 – 120 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 – 10 секунд.

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