Средство защиты информации Secret Net
Инструкция по настройке механизма замкнутой программной среды

Данный документ содержит описание последовательности действий для настройки использования механизма замкнутой программной среды средства защиты информации Secret Net версий 5.x, 6.x и 7.x. Сведения в данном документе уточняют описание общего порядка настройки механизмов контроля целостности и замкнутой программной среды, которое приводится в эксплуатационной документации на изделие.

Настройка механизма ЗПС выполняется администратором в программе "Контроль программ и данных" (далее — программа управления). Предусмотрены возможности централизованной и локальной настройки механизма. В автономном режиме функционирования СЗИ Secret Net используется только способ локальной настройки. В сетевом режиме настройка может выполняться как локально на защищаемом компьютере, так и централизованно на компьютере (компьютерах) администратора безопасности.

1. Локальная настройка

1. Запустите программу управления в локальном режиме. Для этого выберите элемент "Контроль программ и данных" в списке программ.

2. Сформируйте новую модель данных (фрагмент модели) с настройкой контроля по умолчанию. Для этого выберите команду "Файл | Новая модель данных". В появившемся диалоге настройте параметры для режима замкнутой программной среды:

- отметьте представленные стандартные задачи для ОС и СЗИ;
- оставьте отмеченным поле "Производить подготовку для ЗПС";
- установите отметку в поле "Добавить другие задачи из списка" и нажмите кнопку для выбора задач. В появившемся диалоге выберите в списке элементы, необходимые для работы любого пользователя компьютера. Список содержит установленные на компьютере программы, представленные в меню "Пуск". Для выбора нескольких элементов используйте клавиши <Ctrl> или <Shift>;
- оставьте отмеченным поле "Рассчитывать эталоны"
- если модель данных содержит ранее сконфигурированные объекты, которые нужно сохранить в новой модели — удалите отметку из поля "Предварительная очистка модели данных".

3. Нажмите кнопку "ОК". При появлении диалога запроса на продолжение операции нажмите кнопку "Да". По окончании процесса формирования модели данных в списке заданий появится задание ЗПС, которое будет применяться для всех пользователей группы Users и блокировать запуск программ, не включенных в список ресурсов задания.

4. Для проверки и дополнительной настройки механизма ЗПС включите мягкий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера и в диалоге "Режимы" установите отметки в полях "Режим ЗПС включен" и ""Мягкий" режим".

5. Закройте программу управления с сохранением сделанных изменений и выполните вход в систему с учетными данными пользователя компьютера. В пользовательском сеансе выполните запуск всех приложений, которые необходимы пользователю для исполнения функциональных обязанностей.

6. Завершите сеанс работы пользователя, войдите в систему с учетными данными администратора и снова запустите программу управления.

7. Добавьте в модель данных группы ресурсов, в которых будут представлены ресурсы, необходимые для работы пользователя. Для этого выберите категорию "Группы ресурсов" и в меню выберите команду "Группы ресурсов | Создать группу | По журналу". При появлении диалога для выбора типа ресурсов выберите тип "Загружаемые модули" и нажмите кнопку "ОК". В появившемся диалоге настройки параметров добавления ресурсов укажите в качестве источника журнал Secret Net, настройте параметры интервала времени для анализа событий (укажите время, соответствующее сеансу работы пользователя) и нажмите кнопку "ОК". В списке групп ресурсов появится новая группа ресурсов, сформированная по результатам анализа журнала.

> **Примечание:** В зависимости от установленной версии СЗИ Secret Net в список может быть добавлена группа ресурсов типа "Исполняемые скрипты". В этом случае аналогичным образом можно добавить группу ресурсов, указав этот тип при появлении диалога для выбора типа ресурсов.

8. Проверьте наличие ресурсов в созданных группах. Если группы пустые, это означает, что ранее созданное задание ЗПС полностью обеспечивает возможность работы пользователя. В этом случае перейдите к действию **12**.

9. Создайте новое задание ЗПС, которое будет применяться для пользователя. Для этого выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание". В появившемся диалоге выберите тип задания для ЗПС и нажмите кнопку "OK". В следующем диалоге введите имя и описание задания, после чего нажмите кнопку "OK". Включите созданные группы ресурсов в задание. Для этого вызовите контекстное меню задания и выберите команду "Добавить задачи/группы | Существующие". В появившемся диалоге для выбора объектов выберите созданные группы и нажмите кнопку "OK".

10. Добавьте пользователя в модель данных в качестве субъекта управления и установите связь с созданным заданием. Для этого выберите категорию "Субъекты управления" и в меню "Субъекты управления" выберите команду "Добавить в список". В стандартном диалоге выбора объектов выберите учетную запись пользователя и нажмите кнопку "OK". После этого вызовите контекстное меню добавленного элемента и выберите команду "Добавить задания | Существующие". В появившемся диалоге выберите задание и нажмите кнопку "OK".

11. Выполните процедуру расчета эталонов для ресурсов созданного задания. Для этого вызовите контекстное меню задания и выберите команду "Расчет эталонов". В появившемся диалоге нажмите кнопку "OK". Далее в диалоге запроса на сохранение модели данных нажмите кнопку "Да" и дождитесь завершения процесса расчета.

12. При необходимости выполнить настройку для другого пользователя повторите действия **5**–**11**.

13. Включите жесткий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера и в диалоге "Режимы" удалите отметку из поля ""Мягкий" режим". Сохраните сделанные изменения в программе управления.

2. Централизованная настройка

Если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места — на компьютере с 32-разрядной версией ОС Windows и на компьютере с 64-разрядной версией ОС. В этом случае процедуры централизованной настройки выполняются по отдельности для ОС соответствующей разрядности.

1. Запустите программу управления в централизованном режиме. Для этого выберите элемент "Контроль программ и данных (централизованный режим)" в списке программ.

2. Сформируйте новую модель данных (фрагмент модели) с настройкой контроля по умолчанию. Для этого выберите команду "Файл | Новая модель данных". В появившемся диалоге настройте параметр "Предварительная очистка модели данных" (если модель данных содержит ранее сконфигурированные объекты, которые нужно сохранить в новой модели — удалите отметку из поля) и нажмите кнопку "OK". При появлении диалога запроса на продолжение операции нажмите кнопку "Да" и дождитесь завершения формирования модели данных.

3. Добавьте в модель данных задачи для механизма ЗПС на основе конфигурации ПО данного компьютера. Для этого выберите в меню "Сервис" команду "Генератор задач". В появившемся диалоге настройте параметры:

- в поле "Поиск по" выберите значение "ярлыкам из меню "Пуск" (ЗПС)";
- выберите в списке элементы, необходимые для работы любого пользователя. Список содержит установленные на компьютере программы, представленные в меню "Пуск". Для выбора нескольких элементов используйте клавиши <Ctrl> или <Shift>;
- оставьте отмеченным поле "Помечать выполняемые (для ЗПС)".

4. Нажмите кнопку "OK" и дождитесь завершения формирования задач. По окончании процесса в модель данных добавятся новые задачи, включающие в себя группы ресурсов, но не связанные с вышестоящими объектами (заданиями).

5. Создайте задание ЗПС для включения в него созданных задач. Для этого выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание". В появившемся диалоге выберите тип задания для ЗПС и нажмите кнопку "OK". В следующем диалоге введите имя и описание задания, после чего нажмите кнопку "OK". Включите созданные задачи в задание. Для этого вызовите контекстное меню задания и выберите команду "Добавить задачи/группы | Существующие". В появившемся диалоге для выбора объектов выберите созданные задачи и нажмите кнопку "OK".

6. Добавьте один из защищаемых компьютеров в модель данных в качестве субъекта управления и установите связь с созданным заданием. Для этого выберите категорию "Субъекты управления" и в меню "Субъекты управления" выберите команду "Добавить в список". При появлении диалога для выбора типа субъекта выберите тип "Компьютер" и нажмите кнопку "OK". Далее в диалоге выбора

объектов выберите компьютер и нажмите кнопку "ОК". После этого вызовите контекстное меню добавленного элемента и выберите команду "Добавить задания | Существующие". В появившемся диалоге выберите задание и нажмите кнопку "ОК".

Примечание: В зависимости от установленной версии СЗИ Secret Net в список может быть добавлена группа компьютеров. В этом случае аналогичным образом можно добавить группу компьютеров, указав этот тип при появлении диалога для выбора типа субъектов.

7. Для проверки и дополнительной настройки механизма ЗПС включите мягкий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера или группы (компьютеров) и в диалоге "Режимы" установите отметки в полях "Режимы заданы централизованно", "Режим ЗПС включен" и ""Мягкий" режим". Закройте программу управления с сохранением сделанных изменений.

8. На защищаемом компьютере выполните вход в систему с учетными данными пользователя компьютера. В пользовательском сеансе выполните запуск всех приложений, которые необходимы пользователю для исполнения функциональных обязанностей.

9. Завершите сеанс работы пользователя, войдите в систему с учетными данными администратора и запустите программу просмотра журналов. Загрузите в программу записи журнала Secret Net и экспортируйте в файл формата dvt записи о событиях в период с момента входа пользователя в систему и до завершения сеанса. Скопируйте полученный файл для загрузки на рабочем месте администратора.

10. Запустите программу управления в централизованном режиме и добавьте в модель данных группы ресурсов, в которых будут представлены ресурсы, необходимые для работы на компьютере. Для этого выберите категорию "Группы ресурсов" и в меню выберите команду "Группы ресурсов | Создать группу | По журналу". При появлении диалога для выбора типа ресурсов выберите тип "Загружаемые модули" и нажмите кнопку "ОК". В появившемся диалоге настройки параметров добавления ресурсов укажите в качестве источника файл с сохраненными записями журнала Secret Net, настройте параметры интервала времени для анализа событий (укажите время, соответствующее сеансу работы пользователя) и нажмите кнопку "ОК". В списке групп ресурсов появится новая группа ресурсов, сформированная по результатам анализа журнала.

Примечание: В зависимости от установленной версии СЗИ Secret Net в список можно добавить группу ресурсов типа "Исполняемые скрипты". В этом случае аналогичным образом можно добавить группу ресурсов, указав этот тип при появлении диалога для выбора типа ресурсов.

11. Проверьте наличие ресурсов в созданных группах. Если группы пустые, это означает, что ранее созданное задание ЗПС полностью обеспечивает возможность работы на компьютере. В этом случае перейдите к действию **14**.

12. Создайте новое задание ЗПС, которое будет применяться на защищаемом компьютере (компьютерах). Для этого выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание". В появившемся диалоге выберите тип задания для ЗПС и нажмите кнопку "ОК". В следующем диалоге введите имя и описание задания, после чего нажмите кнопку "ОК". Включите созданные группы ресурсов в задание. Для этого вызовите контекстное меню задания и выберите команду "Добавить задачи/группы | Существующие". В появившемся диалоге для выбора объектов выберите созданные группы и нажмите кнопку "ОК".

13. Установите связь субъекта (субъектов) с созданным заданием. Для этого вызовите контекстное меню субъекта и выберите команду "Добавить задания | Существующие". В появившемся диалоге выберите задание и нажмите кнопку "ОК".

14. При необходимости выполнить настройку для других компьютеров повторите действия **6**–**13**.

15. Включите жесткий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера или группы (компьютеров) и в диалоге "Режимы" удалите отметку из поля ""Мягкий" режим". Сохраните сделанные изменения в программе управления.