Средство защиты информации Secret Net Studio
Комментарии к версии 8.4.2863.0

Данный документ содержит описание новых возможностей СЗИ Secret Net Studio версии 8.4.2863.0 по сравнению с версиями 8.3.31406.0, 8.2.1156.0, 8.1.721.0 и 8.0.647.0, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации СЗИ Secret Net Studio.

Оглавление

1. Комплект поставки

1.1. Размещение файлов на установочном диске

Каталог	Содержимое
\Setup\Server\	дистрибутивы сервера безопасности
\Setup\Console\	дистрибутивы программы управления
\Setup\Client\	дистрибутивы клиента
\Setup\SnCard\	дистрибутивы драйвера средства аппаратной поддержки
\Documentation\	комплект документации
\Tools\	вспомогательные утилиты, программы для установки и настройки ПО

2. Изменения и новые возможности

2.1. Версия 8.4.2863.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.4.2863.0 по сравнению с версией 8.3.1406.0.

2.1.1. Общесистемные

1. Обеспечена совместимость Secret Net Studio с ОС Microsoft Windows Server 2016.

2. Обеспечена совместимость Secret Net Studio с ОС Microsoft Windows 10 April 2018 Update (версия 1803) при условии установки обновлений 8.4.2863.2, 8.4.2863.3, 8.4.2863.4, включенных в установочный комплект Secret Net Studio. Эти обновления устанавливаются автоматически при централизованной и локальной установке клиента Secret Net Studio. После обновления при работе с Secret Net Studio нужно учитывать особенности, описанные в данном документе под номерами 96 и 316.

3. Обеспечена совместимость Secret Net Studio с ОС Microsoft Windows 10 Fall Creators Update (версия 1709).

4. Реализована поддержка для ОС Windows 10 загрузки при включенной в UEFI функции SecureBoot.

5. Из состава Secret Net Studio исключен компонент "Шифрование трафика (VPN клиент)".

6. В состав дистрибутивов Secret Net Studio включены все обновления, выпускавшиеся для Secret Net Studio версий 8.2 и 8.3.

2.1.2. Базовая и локальная защита

7. Изменен механизм обновления клиента Secret Net Studio. Теперь процесс обновления выполняется подобно установке обновлений ОС Windows во время перезагрузки компьютера. Также обновления клиента, размещенные на установочном диске Secret Net Studio, теперь устанавливаются автоматически во время установки клиента, выполняемой как локально, так и с помощью средств централизованного развертывания.

8. Добавлена функция полного затирания внешних носителей и локальных дисков.

9. Выполнена доработка и оптимизация механизма затирания данных. Повышена скорость затирания данных.

10. Реализована поддержка идентификаторов и смарт-карт JaCarta LT, JaCarta 2-ГОСТ, JaCarta 2 PKI/ГОСТ, ESMART GOST D.

11. Реализован механизм синхронизация паролей в RDP-сессиях для случаев, когда пароли в ОС Windows и в Secret Net Studio не совпадают.

12. В состав средств локальной защиты добавлен механизм "Паспорт ПО".

13. Оптимизирована работа клиента Secret Net Studio при загрузке ОС, что позволило повысить скорость загрузки компьютера.

14. Оптимизирована и повышена скорость работы (выполнения операций) механизма контроля целостности.

15. Дополнен и расширен список объектов реестра, устанавливаемых на контроль целостности по умолчанию.

16. Оптимизированы и ускорены проверки перенаправления при входе пользователя в конфиденциальной сессии.

17. Ускорена работа приложений Microsoft Office 2013 и Adobe Acrobat Reader DC в среде с действующими механизмами защиты.

18. Реализована совместимость с технологией персональных виртуальных дисков Personal vDisk Citrix XenDesktop.

2.1.3. Антивирус и средство обнаружения и предотвращения вторжений

19. Разработан новый общий сервер обновлений, позволяющий выполнять обновление и антивирусных баз, и базы решающих правил СОВ.

20. В состав сервера обновлений входит программа управления с графическим интерфейсом, позволяющая управлять обновлениями.

2.1.4. Центр управления

21. Разработана новая панель управления "Дашборд". Панель содержит сведения об общем состоянии защищенности системы и позволяет оперативно отслеживать ряд важных параметров ее работы.

22. Разработан механизм настройки политик безопасности с помощью шаблонов параметров безопасности, позволяющий быстро настроить механизмы защиты за счет тиражирования эталонных наборов параметров.

23. Добавлен функционал, позволяющий централизовано управлять компьютерами под управлением ОС Linux с установленным СЗИ Secret Net LSP версий 1.7 и 1.8.

24. В локальном режиме работы программы управления реализован поиск по данным хранилища теневого копирования с использованием Windows Search.

25. Реализовано наглядное оповещение пользователя при разрыве соединения центра управления с сервером безопасности.

26. Реализовано наглядное оповещение пользователя при длительном отсутствии обновлений антивируса.

27. В панели "Развертывание" добавлена функция централизованного запуска процесса исправления клиентского ПО на защищаемых компьютерах.

28. В панели "Развертывание" добавлено детальное отслеживание состояния процессов установки, обновления, исправления и удаления клиента Secret Net Studio.

29. В панели "Компьютеры" в режиме "Таблица" добавлены функции фильтрации объектов.

30. В фильтре получения тревог (при централизованном управлении) добавлена возможность отображения выборок событий.

31. Повышено удобство работы фильтра отображения событий аудита.

32. В панели "Компьютеры" добавлена возможность выполнять с компьютерами групповые операции, такие как включение и выключение механизмов защиты, отправка команд оперативного управления, принудительное выполнение функционального контроля.

33. Повышено удобство управления карантином антивируса.

34. Повышена скорость запуска программы управления в локальном режиме работы.

35. Параметры политики перенаправления и защиты RDP-сеансов объединены в отдельном разделе политик "Контроль RDP подключений".

36. Добавлена проверка допустимости вводимых значений при настройке параметров антивируса и средства обнаружения и предотвращения вторжений.

37. Повышена устойчивость к переименованию объектов защиты.

2.1.5. Утилиты

38. Разработана утилита миграции, позволяющая перенести данные из СЗИ Secret Net версии 7.6 и выше в Secret Net Studio для сохранения имеющихся настроек групповых политик.

39. В состав дистрибутива Secret Net Studio вновь включена обновленная и доработанная утилита SnDSTool, предназначенная для работы с хранилищем объектов централизованного управления.

2.2. Версия 8.3.1406.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.3.1406.0 по сравнению с версией 8.2.1156.0.

2.2.1. Общесистемные

40. Реализована возможность создания нескольких доменов безопасности в одном контейнере Active Directory (AD). Теперь на базе одного контейнера AD (домена AD или организационного подразделения) можно установить несколько серверов безопасности в режиме создания нового домена безопасности.

41. Обеспечивается частичная совместимость Secret Net Studio и Microsoft Windows 10 Fall Creators Update (версия 1709). Перед проведением обновления Windows 10 до версии 1709 необходимо в Secret Net Studio отключить функцию защиты диска. Эта функция в Windows 10 версии 1709 не поддерживается.

42. Secret Net Studio выпускается теперь на русском и английском языках.

2.2.2. Базовая и локальная защита

43. Добавлена возможность принудительной перезагрузки компьютеров при централизованной установке клиента Secret Net Studio. Теперь в параметрах задания развертывания можно указать интервал времени, по истечении которого будет выполнена автоматическая перезагрузка компьютеров после установки на них заданного ПО.

44. Реализована интеграция с системой Avanpost SSO.

45. Добавлен функционал, позволяющий использовать защищенные носители информации на базе USB-носителей JaCarta SF/ГОСТ.

2.2.3. Антивирус

46. Оптимизирована работа антивируса при загрузке операционной системы компьютера. Теперь загрузка выполняется быстрее.

2.2.4. Сервер безопасности

47. Изменена процедура обновления сервера. Теперь при возникновении ошибки в процессе обновления происходит восстановление сервера безопасности к состоянию до обновления.

2.3. Версия 8.2.1156.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.2.1156.0 по сравнению с версией 8.1.721.0.

2.3.1. Общесистемные

48. Реализована совместимость СЗИ Secret Net Studio и Microsoft Windows 10 Creators Update (версия 1703).

2.3.2. Базовая и локальная защита

49. При попытке пользователя выключить или перезагрузить компьютер во время централизованной установки клиента (а также при централизованном обновлении или удалении) в операционной системе выводится предупреждающее сообщение.

50. Доработаны алгоритмы проверки и удаления патчей для корректного выполнения процедур обновления, исправления и удаления клиента.

51. Реализована возможность установки клиента при наличии установленного СКЗИ "Континент-АП" (все версии до 4.0).

52. Реализована возможность удаления отдельных защитных подсистем клиента, включая программу управления в локальном режиме ("Локальный центр управления").

53. Изменен способ активации административного режима входа в систему. Активация режима осуществляется при нажатии комбинации клавиш <Ctrl>+<Shift>+<Esc>.

54. Реализована поддержка идентификаторов и смарт-карт eToken PRO.

55. Для режима идентификации "Только по идентификатору" оптимизированы процедуры входа в систему и разблокировки при наличии подключенных идентификаторов.

56. Реализовано затирание данных для выбранных файловых объектов по команде "Удалить безвозвратно" в программе Проводник.

57. Реализовано затирание имен удаляемых файлов и каталогов.

58. Реализована поддержка контроля печати для приложений Магазина Windows.

59. В параметрах перенаправления локальных устройств и ресурсов в RDP-подключениях (соответствующие политики групп "Контроль приложений", "Контроль устройств" и "Контроль печати") добавлены дополнительные значения "Определяется политиками Windows" для возможности применения штатных параметров групповых политик Windows.

60. Изменены значения по умолчанию для параметров политик группы "Оповещения о тревогах" (параметр "Фильтр тревог") и группы "Контроль печати" (параметры "Маркировка документов" и Теневое копирование").

61. Доработана процедура начальной настройки механизма замкнутой программной среды при установке и обновлении клиента. В модели данных создается специальное задание ЗПС по умолчанию со списком ресурсов СЗИ. Обновление клиента при включенном механизме ЗПС выполняется без ошибок.

62. Реализована возможность загрузки журнала Secret Net Studio в конфиденциальных сессиях.

63. В программе управления пользователями выполнены доработки для более удобного представления данных: реализованы функции сортировки, поиска объектов и сохранения параметров отображения в следующих сеансах.

64. Реализована возможность доступа к диалоговому окну "Управление Secret Net Studio" в Панели управления из сеанса пользователя. Доступ предоставляется, если в ОС включен механизм управления учетными записями (User Account Control — UAC). Для открытия диалогового окна необходимо указать учетные данные администратора.

65. В программе настройки подсистемы полномочного управления доступом отредактирован и дополнен список приложений, подлежащих настройке (раздел "Вручную / Программы").

66. В утилите экспорта журнала Secret Net Studio (GetEventLog.exe) добавлена возможность экспорта файлов из хранилища теневого копирования.

67. В утилите экспорта и импорта параметров эффективной политики компьютера (SnetPol.exe) реализованы возможности работы с параметрами дополнительных механизмов защиты Secret Net Studio.

2.3.3. Межсетевой экран и авторизация сетевых соединений

68. Добавлен новый тип правил для обеспечения возможности фильтрации сетевого трафика в рамках TCP-соединений (сессий). Данный тип правил позволяет осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода.

2.3.4. Антивирус

69. Реализовано контекстное сканирование выбранных файловых объектов в режиме игнорирования списка исключений. Специальная команда "Проверить на вирусы (игнорировать белый список)" доступна в расширенном контекстном меню каталога или файла для членов локальной группы администраторов. Вызов расширенного контекстного меню осуществляется в программе Проводник при нажатой клавише <Shift>.

70. Реализована возможность использования самораспаковывающихся архивов с обновлениями для антивирусных баз. Файлы доступны для скачивания на серверах обновления антивирусов и на сервере ООО "Код Безопасности".

71. Расширены выводимые сведения об ошибках при обновлении.

72. Оптимизирована работа сканирования в конфиденциальных сессиях.

73. Реализован поиск вирусов в файловых объектах с данными формата reparse point (все объекты, возможные в NTFS: symlink, junction point, mount points).

2.3.5. Шифрование трафика (VPN клиент)

74. Реализован автоматический выбор датчика случайных чисел для использования криптопровайдером. Выбор осуществляется при установке клиента — если на компьютере обнаружен ПАК "Соболь", будет использоваться физический ДСЧ ПАК "Соболь". В противном случае — биологический. При интерактивной установке клиента можно отключить автовыбор и принудительно указать нужный ДСЧ.

2.3.6. Центр управления

75. В локальном режиме работы программы управления реализована возможность смены режима функционирования клиента — из автономного режима в сетевой и наоборот.

76. При отключении отдельных механизмов защиты в программе управления соответствующие подсистемы деактивируются, но не удаляются с компьютера. Кроме подсистемы шифрования трафика — модули этой подсистемы удаляются при отключении механизма.

77. В панели "Развертывание" добавлены средства фильтрации объектов по наличию в названии заданных строк символов.

78. Реализована возможность печати и экспорта сведений о компьютерах, отображаемых в панели "Компьютеры" в режиме "Таблица".

79. Реализована корректная обработка конфликтов при появлении в структуре ОУ "дубликатов" (когда в разных доменах безопасности одного леса присутствуют записи об одном и том же компьютере) или при обнаружении "потерянных" компьютеров (когда объект удален из AD, но запись о нем осталась в структуре ОУ).

2.3.7. Сервер безопасности

80. При установке сервера безопасности в IIS формируется специальный сайт SecretNetStudioSite. Сайт по умолчанию (Default Web Site), необходимый для предыдущих версий сервера безопасности, теперь не используется.

2.4. Версия 8.1.721.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.1.721.0 по сравнению с версией 8.0.647.0.

2.4.1. Общесистемные

81. Реализована поддержка ОС Windows 10.

2.4.2. Антивирус

82. Разработан отдельный компонент антивируса для применения в системах с защитой гостайны.

2.4.3. Центр управления

83. Реализована функциональность детектирования угроз, позволяющая выполнять поиск угроз по событиям из журналов Secret Net Studio и штатных журналов ОС.

3. Особенности работы и ограничения

3.1. Базовая и локальная защита

3.1.1. Установка клиента

84. Перед установкой клиента Secret Net Studio необходимо установить пакеты обновлений для ОС, указанные в требованиях к аппаратному и программному обеспечению (см. документ "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление"). Для централизованной установки клиента на компьютерах под управлением ОС Windows Vista/2008 дополнительно нужно установить следующие распространяемые пакеты компании Microsoft:

- Microsoft C/C++ Runtime для Visual Studio 2013. Для установки можно использовать файлы с установочного диска системы Secret Net Studio, расположенные в каталоге \Tools\Microsoft\Prerequisites: vcredist_x86.exe (для 32- и 64-разрядных версий ОС) и vcredist_x64.exe (для 64-разрядных версий);
- Microsoft .NET Framework 4.5. Для установки можно использовать файлы с установочного диска системы Secret Net Studio, расположенные в каталоге \Tools\Microsoft\Prerequisites: dotNetFx45_Full_x86_x64.exe и dotNetFx45LP_Full_x86_x64ru.exe.

85. Имя домена Active Directory, в котором будут установлены клиенты и другие компоненты Secret Net Studio для сетевого режима, рекомендуется задать без использования символов кириллицы. Также нежелательно использовать буквы любых других алфавитов, отличающиеся от латинских символов. В противном случае компоненты Secret Net Studio могут быть частично или полностью неработоспособны.

86. Для установки компонентов СЗИ из папки на локальном или сетевом диске необходимо скопировать с установочного диска содержимое следующих каталогов (с сохранением их структурной вложенности):

- файлы из корневого каталога диска;
- каталог \Setup;
- каталог \Tools.

87. При первой перезагрузке после установки или обновления выполняется автоматическое утверждение аппаратной конфигурации компьютера. В связи с этим администратор безопасности должен контролировать первую загрузку компьютера после установки, чтобы не допустить регистрацию нежелательных устройств (которые могут быть подключены к компьютеру до загрузки).

88. Установка клиента в сетевом режиме функционирования невозможна при недоступности в сети контроллера домена.

89. При обновлении клиента возможна регистрация ряда ошибок в журнале приложений. Как правило, такие ошибки не являются критическими и никак не влияют на дальнейшую работу системы.

90. Если произошел сбой на стадии установки драйвера виртуального принтера, это может быть связано с повреждением или отсутствием на компьютере системного файла ntprint.inf.

> **Рекомендации:** При возникновении сбоя завершите работу программы установки и проверьте наличие файла ntprint.inf в каталоге \windows\inf. Если файл поврежден или отсутствует, добавьте новый файл, подходящий для данной ОС. Например, скопируйте с компьютера, на котором установлена та же версия ОС соответствующей разрядности.

91. Драйвер средства аппаратной поддержки Secret Net Card устанавливается отдельно от ПО клиента Secret Net Studio.

92. При централизованной установке клиента на компьютер с сервером безопасности установка может завершиться с ошибками. В частности, возможны ситуации, когда компьютер не будет подчинен серверу безопасности.

> **Рекомендации:** Установку клиента на сервере безопасности выполняйте в интерактивном режиме.

93. При централизованной установке нескольких патчей рекомендуется создавать отдельные задания развертывания для каждого патча. Если в одном задании указано несколько патчей, это может привести к ошибкам.

94. После обновления сетевых клиентов с предыдущих версий Secret Net возможна ситуация, когда список ресурсов централизованной задачи "Контроль ресурсов Secret Net Studio" обновляется не на всех компьютерах. В результате списки ресурсов для КЦ и ЗПС могут формироваться некорректно.

> **Рекомендации:** После завершения обновления на всех компьютерах, запустите на рабочем месте администратора программу управления КЦ-ЗПС в централизованном режиме и выполните процедуру отложенного расчета эталонов для любого из заданий, содержащих задачу "Контроль ресурсов Secret Net Studio" (с помощью команды "Отложенный расчет эталонов" в контекстном меню задания).

95. Если выполняется обновление клиента Secret Net версий 6.5 и 7.X с настроенными категориями конфиденциальности ресурсов, при установке клиента Secret Net Studio следует установить подсистему полномочного управления доступом. В этом случае для ресурсов будут сохранены ранее заданные категории конфиденциальности. Если клиент Secret Net Studio был установлен без подсистемы полномочного управления, включить подсистему можно позже в программе управления — однако в этом варианте по умолчанию ранее заданные категории не учитываются. Чтобы применить ранее заданные категории, перед включением подсистемы необходимо в системном реестре компьютера создать ключ HKLM\System\CurrentControlSet\Services\SnFMac\Params.

3.1.2. Общее

96. Если по каким-либо причинам требуется удалить с компьютера обновления, установленные для обеспечения совместимости Secret Net Studio с Windows 10 версии 1803, перед удалением обновления 8.4.2863.4 (например, при выполнении в программе управления команды "Удалить все патчи") отключите дискреционное управление доступом. Удаление данного обновления с включенным дискреционным управлением доступом может привести к нарушениям в работе компьютера.

97. Если доступ к ресурсу запрещен какой-либо защитной подсистемой Secret Net Studio, некоторые программы могут работать некорректно (например, встроенный редактор WordPad). В таких приложениях не осуществляется обработка запрета доступа к ресурсам.

98. При использовании средств ускорения запуска ОС могут возникать ошибки функционального контроля или другие сбои во время загрузки компьютера. Например, при совместном функционировании с ПО RapidBoot Shield, которое установлено на некоторых моделях компьютеров Lenovo.

> **Рекомендации:** Для устранения конфликтов удалите или отключите средство ускорения запуска ОС (дополнительные сведения о ПО RapidBoot Shield приведены на сайте компании Lenovo — см. https://support.lenovo.com/ru/ru/documents/ht075364).

99. При использовании утилиты Userdump компании Microsoft (для создания дампов процессов) возможны сбои при выполнении системой криптографических операций. Для нормальной работы системы защиты необходимо удалить утилиту Userdump после выполнения всех необходимых операций.

100. При регистрации событий защитных подсистем в журнале Secret Net Studio полное имя процесса или файла на локальном диске может быть указано в виде DOS-имени "C:\..." или со сведениями о логическом диске (томе) в формате имени устройства: "\Device\HarddiskVolume<*N*>\...".

101. Если включен режим усиленной защиты доступа к хранилищу объектов централизованного управления (поле "шифровать управляющий сетевой трафик" в списке защитных механизмов окна "Управление СЗИ Secret Net Studio") и при этом в системе не настроена инфраструктура открытых ключей, то средства Secret Net Studio при подключении к хранилищу будут выдавать ошибки "Сервер неработоспособен" или "Клиент затребовал соединение SSL, но сервер не поддерживает таких соединений". В этом случае нужно либо отключить режим усиленной защиты доступа к хранилищу, либо организовать и настроить инфраструктуру открытых ключей.

102. В системах с медленными каналами связи при обращениях компонентов СЗИ Secret Net Studio к хранилищу объектов ЦУ (например, при запуске синхронизации с ЦБД КЦ-ЗПС) может возникать ошибка "Служба не ответила на запрос своевременно". В этом случае для устранения ошибок необходимо увеличить время ожидания ответов на отправленные запросы. Для настройки времени ожидания в системном реестре компьютера в ключе HKLM\Software\Infosec\Secret Net 5 создайте раздел LdapHelper и в нем параметр SearchTimeout типа DWORD. Задайте значение времени в секундах (по умолчанию при отсутствии параметра время ожидания составляет 60 секунд). Значение 0 отменяет ожидание.

103. Если клиент Secret Net Studio установлен без подсистем сетевой защиты (не включены межсетевой экран и авторизация сетевых соединений), при изменении параметров пользователей в программе управления пользователями (например, смена уровня допуска или смена пароля администратором) появляется запрос для ввода учетных данных администратора домена безопасности.

104. В текущей версии некоторые подсистемы Secret Net Studio (дискреционное и полномочное управление доступом, затирание данных) несовместимы с технологией дедупликации данных (data deduplication), используемой в ОС Windows Server 2012. При работе подсистем доступ к преобразованным файлам может блокироваться. Совместимость будет реализована в следующих версиях СЗИ.

3.1.3. Локальное и централизованное управление

105. При запрете использования сетевого интерфейса средствами Secret Net Studio, в списке устройств локальной политики безопасности интерфейс отображается с зачеркнутым названием. Если при этом устройство, соответствующее интерфейсу, остается физически подключенным, нельзя удалять его из списка устройств — иначе будет невозможно дальнейшее использование этого интерфейса в текущей конфигурации. Для восстановления работы сетевого интерфейса потребуется удалить и заново установить драйвер устройства.

Рекомендации: Если в списке устройств сетевой интерфейс отображается с зачеркнутым названием, перед удалением его из списка убедитесь, что устройство отключено.

106. Некоторые параметры пользователя после изменения вступают в силу только при следующем входе пользователя в систему. К таким параметрам относятся:

- привилегии;
- параметры полномочного управления доступом;
- список программ, разрешенных для запуска.

107. После создания доменного пользователя штатными средствами управления Windows требуется некоторое время для синхронизации сделанных в AD изменений с сервером безопасности. Запуск синхронизации выполняется сервером автоматически через каждый час, а также при старте сервера. При входе пользователя в систему до завершения синхронизации возможна некорректная обработка событий входа, если в СЗИ включен режим усиленной аутентификации или действуют механизмы группы сетевой защиты.

Рекомендации: Для создания пользователей рекомендуется использовать программу управления пользователями Secret Net Studio.

108. Если для журнала Secret Net Studio установлен режим очистки вручную и активирована системная настройка "Прекращать работу при переполнении журнала безопасности" — в случае переполнения журнала записями на компьютере будет инициирован системный сбой (BSOD). Для возобновления нормальной работы необходимо войти в систему с правами администратора, очистить журнал и переустановить настройку "Прекращать работу при переполнении журнала безопасности".

Рекомендации: Для журнала Secret Net Studio используйте режим "Затирать события по мере необходимости" (установлен по умолчанию).

109. Если размер журнала Secret Net Studio изменен в сторону уменьшения, изменения вступят в силу только после очистки журнала.

110. Размер журнала системы защиты меняется с шагом 64 Кб. Поэтому в случае, если максимальный размер установлен в 64 или 128 Кб, система будет неверно определять его заполнение на 80%.

Рекомендации: Устанавливайте значение максимального размера журнала не менее 512 Кб (для всех журналов).

111. При загрузке записей журнала Secret Net Studio из файла *.evtx или *.evt в оснастку "Просмотр событий" ("Event Viewer") ОС Windows корректное отображение записей возможно при условии, что пользователь входит в локальную группу администраторов.

112. В сетевом режиме функционирования СЗИ локальный администратор (локальный пользователь, входящий в группу локальных администраторов компьютера) может присвоить локальному пользователю идентификатор, присвоенный до этого доменному пользователю. Это приведет к невозможности использования идентификатора доменным пользователем на данном компьютере.

Примечание: Присвоение локальному пользователю идентификатора доменного пользователя допускается из-за невозможности проверки принадлежности идентификатора в домене под локальной учетной записью.

Рекомендации: Управление параметрами пользователей необходимо осуществлять с правами администратора домена.

113. В сетевом режиме функционирования СЗИ при недоступности контроллера домена невозможна корректная проверка принадлежности идентификатора пользователю.

Рекомендации: Операции управления идентификаторами выполняйте только при доступном контроллере домена.

114. В сетевом режиме функционирования СЗИ не поддерживаются доверительные отношения между доменами, если эти домены не входят в один лес (т. е. у доменов нет общего глобального каталога).

115. В сетевом режиме функционирования СЗИ после удаления идентификатора доменного пользователя выполнять процедуру присвоения этого идентификатора другому пользователю рекомендуется через некоторое время. Пауза необходима для проведения репликации, которая, как правило, занимает (в рамках локальной сети) около 30 секунд.

116. В автономном режиме функционирования СЗИ локальный администратор компьютера не имеет возможности работать со списком доменных пользователей в программе управления пользователями.

Рекомендации: Для управления доменными пользователями выполните вход в систему доменным пользователем, входящим в группу локальных администраторов компьютера.

117. В автономном режиме функционирования СЗИ при попытке добавить доменного пользователя может возникнуть ошибка "Object picker cannot open because no locations from which to choose objects could be found" ("Невозможно открыть Object Picker, поскольку отсутствует то место, где его можно было бы найти"). В большинстве случаев такая ошибка возникает из-за недоступности контроллера домена или некорректной настройки параметров. Например:

- неверно настроен DNS-сервер;
- на компьютере отсутствуют административные общие ресурсы;
- на контроллере домена не запущена служба "Remote Registry".

118. Для корректной работы с параметрами пользователей в группе "Pre-Windows 2000 Compatible Access" должна быть либо группа "Everyone" ("Все"), либо группа "Authenticated Users" ("Прошедшие проверку").

Рекомендации: Если указанные группы не включены в группу "Pre-Windows 2000 Compatible Access", добавьте в нее группу "Authenticated Users" ("Прошедшие проверку").

119. Если в ОС включен механизм управления учетными записями (User Account Control — UAC), система при определенных действиях администратора выдает запросы о предоставлении административных полномочий. В этом режиме возможно проявление следующих особенностей работы с журналами:

- если при запуске программы управления в локальном режиме административные полномочия не предоставлены, запуск программы выполняется, но журнал безопасности будет недоступен для загрузки;
- если привилегия просмотра журнала системы защиты предоставлена только локальной группе администраторов (состояние по умолчанию), в программе управления в локальном режиме могут блокироваться возможности доступа к файлам в хранилище теневого копирования для всех пользователей. В этом случае для обеспечения доступа к хранилищу можно или отключить механизм UAC, или добавить нужных пользователей в список учетных записей с привилегией просмотра журнала системы защиты.

120. При работе с папкой хранилища теневого копирования, открытой из программы управления в локальном режиме, пользователю может быть отказано в открытии XPS-файлов (копии, полученные при печати документов). В этом случае для просмотра содержимого файлов можно копировать их и открывать из другой папки или явно добавить нужных пользователей в список учетных записей с привилегией просмотра журнала системы защиты.

121. Если в пользовательской переменной окружения TEMP задан путь, содержащий длинные имена с пробелами, то при запуске программы редактирования маркеров будет возникать ошибка загрузки XML-файла. Для устранения ошибки задайте в переменной окружения TEMP путь с именем каталога без пробелов.

Примечание: По умолчанию путь в переменной окружения задан в формате 8.3 (короткие имена без пробелов).

3.1.4. Вход в систему

122. При закрытии сессии на терминальном сервере в журнале приложений может регистрироваться ошибка WinLogon "Неверная функция".

123. В режиме усиленной аутентификации по паролю в журнале приложений могут регистрироваться группы ошибок для следующих случаев запрета входа в систему:

- если введено неправильное имя пользователя (пользователь с указанным именем не зарегистрирован в системе) — регистрируются ошибки "Именам пользователей не сопоставлены коды защиты данных";
- если в автономном режиме функционирования СЗИ введено имя доменного пользователя, не добавленного в локальную базу данных Secret Net Studio — регистрируются ошибки "Доменный пользователь не зарегистрирован на компьютере в базе данных Secret Net Studio".

124. В режиме усиленной аутентификации по паролю если пароль пользователя для входа в ОС Windows не синхронизирован с паролем в базе данных Secret Net Studio, при смене пароля самим пользователем новый пароль не будет сохранен в БД Secret Net Studio. Для сохранения нового пароля необходимо выполнить синхронизацию по запросу системы при следующем входе пользователя.

125. После установки СЗИ Secret Net Studio в параметрах безопасности локальной политики принудительно включается действие стандартного параметра "Интерактивный вход в систему: не требовать нажатия Ctrl+Alt+Del".

126. После установки СЗИ Secret Net Studio на компьютер с ОС Windows 8 блокируется возможность использования графических паролей.

127. В СЗИ Secret Net Studio текущей версии не поддерживается вход в систему для учетных записей Майкрософт (Microsoft Live ID account). После установки клиента на компьютер с ОС Windows 8/2012 в параметрах безопасности локальной политики принудительно включается действие стандартной политики "Учетные записи: блокировать учетные записи Майкрософт" (Accounts: Block Microsoft accounts) в режиме "Пользователи не могут добавлять учетные записи Майкрософт и использовать их для входа" (Users can't add or log on with Microsoft accounts). Если вручную отключить действие указанной политики, необходимо учитывать, что возможность выбора учетной записи Майкрософт для входа в систему будет заблокирована из-за особенностей реализации системы защиты. Если на компьютере, не входящем в домен, все учетные записи пользователей преобразованы в учетные записи Майкрософт, вход в систему на этом компьютере будет невозможен.

128. Предусмотрена возможность считывания системой данных из идентификатора, подключенного к считывателю на момент первого локального входа пользователя или при терминальных входах. Функция не действует, если к компьютеру подключены два или более идентификатора. Для активирования функции необходимо в системном реестре компьютера (терминального сервера) создать ключ HKLM\SOFTWARE\Infosec\Secret Net 5\SnLogon (если он отсутствует), в который добавить параметр AutoID типа REG_DWORD с ненулевым значением.

129. На компьютере под управлением ОС Windows 8 и всех последующих версий экран блокировки не отключается автоматически при входе пользователя по идентификатору, в котором отсутствует пароль. Из-за этого приглашение для ввода пароля закрыто экраном. Чтобы ввести пароль пользователя, нужно вручную выполнить действия для отключения экрана блокировки — например, нажать кнопку мыши.

> **Рекомендации:** Режим использования экрана блокировки можно отключить в операционной системе. Для этого в системном реестре создайте ключ HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization (если он отсутствует) и добавьте параметр NoLockScreen типа REG_DWORD со значением 1.

130. При входе в систему по сертификату на некоторых версиях ОС невозможно сменить просроченный пароль пользователя в ОС. Данная особенность не связана с работой СЗИ Secret Net Studio.

> **Рекомендации:** Для смены просроченного пароля выполните вход в систему стандартным способом с вводом учетных данных пользователя.

131. При входе в систему по сертификату дополнительно запрашивается пароль пользователя, если в СЗИ Secret Net Studio включен режим усиленной аутентификации по паролю или включены подсистемы группы сетевой защиты. Во втором варианте при необходимости можно отключить запрос пароля. Для этого в системном реестре создайте ключ HKLM\SOFTWARE\Infosec\Secret Net 5\SnLogon\CPOptions (если он отсутствует) и добавьте параметр DisableTrustAccess типа REG_DWORD со значением 1.

132. В режиме усиленной аутентификации по паролю параметры парольной политики Secret Net Studio действуют независимо от параметров политики паролей Windows. Поэтому возможна ситуация, когда система защиты обязывает пользователя сменить пароль, а политика Windows запрещает эту операцию. В этом случае смену пароля пользователя выполняет администратор.

133. При невозможности входа пользователя из-за рассинхронизации паролей в ОС и СЗИ (например, если пароль был изменен на компьютере без системы защиты) рекомендуется в программе управления пользователями Secret Net Studio сменить пароль пользователя и затем включить стандартный параметр "Требовать смены пароля при следующем входе в систему".

3.1.5. Подсистема контроля целостности

134. Ограничен набор используемых переменных окружения при описании ресурсов. Не поддерживаются произвольные переменные окружения.

135. При запуске программы "Контроль программ и данных" в момент выполнения задания на контроль целостности или в момент выполнения синхронизации система выдает сообщение: "В результате загрузки модели данных произошла ошибка. Идет обработка базы данных контроля целостности". В этом случае дождитесь завершения выполнения процесса, после чего повторите попытку запуска программы или нажмите клавишу <F5>.

136. Чрезмерно большое количество объектов базы данных контроля целостности (от нескольких десятков тысяч) приводит к длительной обработке базы данных при каждой загрузке системы. В этих условиях запуск программы "Контроль программ и данных" следует выполнять через несколько минут после загрузки системы.

137. Если база данных контроля целостности имеет значительный объем, проверка БД во время загрузки компьютера и входа пользователя в систему может занимать длительное время.

Рекомендации: Для ускорения загрузки и входа в систему можно уменьшить объем БД КЦ (например, сократить количество ресурсов, проверяемых методом контроля содержимого по алгоритму "полное совпадение") или изменить для компьютера моменты запуска синхронизации ЦБД и ЛБД КЦ-ЗПС (отключить установленные по умолчанию параметры синхронизации "При загрузке ОС", "При входе" и включить параметр "После входа").

138. При контроле целостности с восстановлением не поддерживается восстановление атрибута ОС "Шифровать атрибут для защиты данных", а также атрибутов доступа (включая атрибут "Время последнего доступа") и категорий конфиденциальности.

139. Не поддерживается расчет эталонных значений для файлов на сетевом диске с длиной имени более 255 символов.

140. При выключении подсистемы шифрования трафика, а также при ее включении, если клиент был установлен без этой подсистемы, — в журнале Secret Net Studio могут регистрироваться события нарушения целостности объектов системного реестра в ключе HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries.

Рекомендации: После включения или выключения подсистемы "Шифрование трафика" выполните процедуру расчета эталонов задания для контроля реестра Windows.

3.1.6. Подсистема замкнутой программной среды

141. Для запуска DOS-программы с помощью ярлыка вызова, пользователю необходимо предоставить разрешение на запуск, как самой программы, так и ярлыка.

142. При вводе сетевого пути с использованием IP-адреса программа "Контроль программ и данных" автоматически преобразует введенный IP-адрес в сетевое имя компьютера. Ввод IP-адресов не поддерживается, поэтому для пользователей отсутствует возможность запуска программ с сетевых ресурсов с указанием IP-адреса сервера.

Рекомендации: В системе следует корректно настроить механизм разрешения имен компьютеров в IP-адреса.

143. По умолчанию подсистема замкнутой программной среды обрабатывает доступ ко всем файлам — независимо от того, являются они исполняемыми файлами или нет.

Рекомендации: Чтобы подсистема отличала исполняемые файлы от других (например, *.txt, *.xml и пр.), необходимо включить режим контроля заголовков исполняемых файлов.

144. В сетевом режиме функционирования СЗИ при необходимости включения замкнутой программной среды на компьютере с установленным сервером безопасности, следует отключить действие механизма ЗПС для учетной записи IWAM_ComputerName. Для этого средствами управления групповых политик предоставьте учетной записи привилегию "Замкнутая программная среда: не действует".

145. При построении списка ресурсов по зависимым модулям в список могут быть включены не все модули. Рекомендуется после построения списка включить "мягкий" режим и скорректировать список разрешенных программ по журналу Secret Net Studio.

146. При использовании сетевого ресурса в сценариях для построения задачи ЗПС необходимо предоставить доступ к данному ресурсу не только пользователям, но и учетной записи Network. В противном случае сценарий для такого сетевого ресурса не будет преобразован в список исполняемых файлов в процессе синхронизации.

147. Механизм контроля скриптов контролирует выполнение сценариев, созданных по технологии Active Scripts. Если приложение использует другую технологию обработки сценариев (например, браузер Mozilla Firefox), в этом приложении перехват сценариев не осуществляется.

148. Из-за особенностей формирования и загрузки сценариев на многих популярных интернет-ресурсах происходит автоматическая модификация одних и тех же сценариев при обращениях к ранее загруженным страницам. Это приводит к невозможности полноценного контроля исполнения сценариев (скриптов) в браузере — поскольку обновляемые сценарии при загрузке страниц воспринимаются как неизвестные, и система регистрирует соответствующие события в журнале.

Рекомендации: Если браузер (например, Internet Explorer) используется для загрузки и просмотра страниц из интернета, включите для исполняемого файла этого процесса функцию исключения контроля скриптов. Для этого отметьте дополнительный параметр "Разрешено выполнять любые скрипты" в диалоге настройки параметров ресурса.

149. Не рекомендуется вручную добавлять в модель данных исполняемый сценарий (скрипт) из wsf-файла. В файле могут быть представлены дополнительные сведения (другие скрипты, ссылки и

пр.), которые не задействуются при исполнении сценария. Поэтому исполнение сценария из wsf-файла может все равно блокироваться системой защиты по причине несоответствия хранящимся сведениям в базе данных. Для таких сценариев следует использовать процедуру добавления ресурсов из журнала (с предварительной настройкой системы для накопления сведений).

150. Из-за особенности реализации стандартного Проводника, запуск файлов *.lnk не регистрируется. При необходимости регистрации запуска lnk-файлов отредактируйте в ключе системного реестра HKLM\System\CurrentControlSet\Services\SnExeQuota\Parameters значение параметра Extensions (по умолчанию установлено значение ".com;.bat;.cmd;.pif").

151. Запуск со сменного носителя некоторых приложений (например, программ установки) может выполняться с особенностями: исполняемый файл со сменного диска копируется во временную папку %USERPROFILE%\....\AppData\Local\Temp\... и запускается непосредственно из этой папки.

152. При запуске приложения с сетевого ресурса в журнале Secret Net Studio могут регистрироваться два идентичных события, относящиеся к запуску приложения.

153. В программе Проводник при наведении курсора на файл программы в журнале будет регистрироваться событие запуска или запрета запуска приложения (в зависимости от того, указано или нет данное приложение в списке разрешенных для запуска).

3.1.7. Централизованное управление КЦ-ЗПС

154. Централизованное управление осуществляется в рамках одного домена безопасности Secret Net Studio.

155. Централизованное управление режимами ЗПС осуществляется на уровне компьютеров и групп компьютеров. Поэтому при необходимости по-разному настроить ЗПС для нескольких пользователей одного компьютера, следует настраивать ЗПС локально.

156. Ресурсы, явно описанные в ЦБД, при установке на контроль остаются в ЛБД и контролируются даже в том случае, если на компьютере не обнаружены соответствующие ресурсы — при контроле будет регистрироваться ошибка отсутствия ресурса. Напротив, ресурсы, описанные через сценарии, не устанавливаются на контроль, если при выполнении сценария они на компьютере не обнаружены (соответственно, эти ресурсы не сохраняются в ЛБД).

157. Если в задаче со сценарием были внесены изменения, после синхронизации регистрируются события удаления задачи и добавления задачи в журнале Secret Net Studio.

158. Если для тиражируемого задания в ЦБД изменить метод контроля и перерасчитать эталоны, то на рабочих станциях новые эталонные значения синхронизируются корректно, но при этом старые значения (рассчитанные по предыдущему методу контроля) не будут удалены из локальной БД.

> **Рекомендации:** При необходимости удаления старых эталонов выполните следующие действия:
>
> 1. Удалите связь задания с субъектом и дождитесь завершения синхронизации.
> 2. Восстановите связь задания с субъектом.

159. Чтобы использовать DNS-псевдоним (alias) вместо настоящего имени компьютера в сценариях для формирования заданий ЗПС, необходимо выполнить регистрацию псевдонима в Active Directory. Регистрация выполняется однократно пользователем с правами администратора домена. Для регистрации введите команду сопоставления имени участника службы (Service Principal Name) в формате: setspn -A HOST/<*псевдоним*>.<*имя_домена*>.ru <*имя_компьютера*>. Например, при использовании в домене testdomain псевдонима th10 для компьютера с именем testws следует ввести команду: setspn -A HOST/th10.testdomain.ru testws. Обработка псевдонима на компьютерах будет выполняться после обновления групповых политик.

160. Если модель данных содержит более 250000 объектов, при ее сохранении в программе управления выдается предупреждающее сообщение. Не рекомендуется хранить в модели количество объектов, превышающее указанное ограничение.

> **Рекомендации:** Для централизованного управления целесообразно использовать сценарии — это уменьшает общее количество объектов модели данных и повышает удобство управления системой.

161. Если в тиражируемом задании контроля целостности используется метод контроля "Содержимое" с алгоритмом "полное совпадение", не рекомендуется включать в задание файлы большого размера. Иначе во время синхронизации возможны задержки из-за необходимости передачи на компьютеры копий этих файлов в качестве эталонов.

162. Если в централизованную модель данных требуется добавить группу ресурсов по журналу, в файле журнала Secret Net Studio должны отсутствовать записи о событиях, источником которых является SnNetworkProtection. Иначе произойдет ошибка при декодировании журнала.

Рекомендации: При создании файла журнала Secret Net Studio выполняйте экспорт записей без событий от источника SnNetworkProtection. Для этого, например, можно выполнить фильтрацию отображаемых записей в программе просмотра. Кроме того, добавление объектов в централизованную модель данных можно выполнять средствами экспорта и импорта (в локальную модель данных добавить нужные ресурсы непосредственно из локального журнала, экспортировать их в файл и затем выполнить импорт из файла в централизованную модель).

3.1.8. Дискреционное управление доступом

163. При установке прав доступа на каталог, к которому предоставлен общий доступ (непосредственно к этому каталогу), необходимо обеспечить возможность просмотра содержимого для системной учетной записи. Для этого разрешение на выполнение должно быть установлено для учетной записи "Система" или для групп, в которую включена данная учетная запись (например, группа "Все"). Иначе механизм дискреционного управления доступом будет блокировать сетевой доступ к этому каталогу для всех пользователей.

164. Если в ОС включен механизм управления учетными записями (UAC), система при определенных действиях пользователя может выдавать запросы на ввод учетных данных пользователя. При выполнении в программе Проводник файловой операции с ресурсом пользователем, у которого недостаточно прав доступа на выполнение данной операции, может появиться запрос системы на ввод учетных данных другого пользователя, обладающего нужными правами. В этом случае при вводе соответствующих учетных данных операция выполняется, но от имени пользователя, чьи учетные данные были введены.

3.1.9. Полномочное управление доступом

165. Регистрация предупреждений, выдаваемых пользователю при доступе к конфиденциальным файлам, повышении категории конфиденциальности файлов и при выводе информации на внешние носители, осуществляется в системном журнале (штатный журнал ОС Windows).

166. Если в ОС включен механизм управления учетными записями (UAC), система при определенных действиях пользователя может выдавать запросы на ввод учетных данных пользователя, обладающего необходимыми правами. При выполнении в программе Проводник файловой операции с конфиденциальным ресурсом пользователем, у которого недостаточно прав на выполнение данной операции (по правилам работы с конфиденциальными ресурсами), может появиться запрос системы на ввод учетных данных другого пользователя, обладающего необходимыми правами. В этом случае при вводе соответствующих учетных данных операция выполняется, но от имени пользователя, чьи учетные данные были введены.

167. Если в системе используется более трех категорий конфиденциальности, рекомендуется на всех компьютерах домена безопасности установить клиента Secret Net Studio текущей версии — для корректной работы подсистем. При наличии компьютеров со старым клиентским ПО, где не поддерживаются дополнительные категории, на этих компьютерах проявляются следующие особенности:

- при входе пользователя с уровнем допуска выше, чем "Строго конфиденциально", — событие "Вход пользователя в систему" не регистрируется совсем или содержит некорректные данные в описании (указывается уровень допуска пользователя "Неконфиденциально");
- работать с программой настройки подсистемы полномочного управления доступом разрешается только пользователям с уровнем допуска "Строго конфиденциально".

168. При отключенном режиме контроля потоков, если в приложении был открыт конфиденциальный документ, печать всех последующих документов в текущем сеансе работы приложения рассматривается как печать конфиденциальной информации (даже если потом были открыты неконфиденциальные документы).

Рекомендации: Для печати неконфиденциального документа закройте приложение и откройте заново, не загружая конфиденциальных документов.

169. В некоторых случаях при открытии конфиденциального файла может быть выдан запрос на повышение уровня конфиденциальности приложения, и при этом в запросе будет указано имя другого файла. Это связано с особенностями работы приложений — могут запрашиваться файлы из списка последних открывавшихся файлов. При согласии на повышение уровня конфиденциальности в журнале будет зафиксировано соответствующее обращение.

170. Для работы при включенном режиме контроля потоков требуется дополнительная настройка параметров, которая осуществляется локально с помощью программы настройки подсистемы полномочного управления доступом. Дополнительную настройку рекомендуется выполнить перед включением режима контроля потоков. Далее в процессе эксплуатации системы программу настройки следует использовать в следующих случаях:

- при увеличении количества используемых категорий конфиденциальности;

- при добавлении нового пользователя или переименовании существующего;
- при установке программ, требующих дополнительной настройки для совместимости с режимом контроля потоков;
- при установке нового принтера;
- при необходимости отключения вывода предупреждающих сообщений системы или регистрации событий обращения к файлам.

171. При включенном режиме контроля потоков для обеспечения необходимого уровня защиты блокируется запуск команд и сетевых подключений с вводом учетных данных пользователя, который не выполнил интерактивный вход в систему. Функция блокировки действует независимо от состояния параметра групповой политики "Вход в систему: Запрет вторичного входа в систему".

172. При работе приложений в конфиденциальных сессиях в журнале Secret Net Studio могут регистрироваться события "Запрет изменения параметров конфиденциальности ресурса" с причиной "Категория файла превышает категорию каталога". Это вызвано особенностями поведения некоторых приложений, которые пытаются записывать информацию в неконфиденциальные каталоги.

173. При включенном режиме контроля потоков не рекомендуется в конфиденциальной сессии выполнять любые административные действия по настройке, управлению, конфигурированию системы (не связанные напрямую с обработкой конфиденциальной информации), даже если система позволяет это сделать. Следующие действия следует выполнять только в неконфиденциальной сессии:

- вход в систему администратора для управления и настройки системы (кроме установки уровней конфиденциальности ресурсов). При настройках системы в конфиденциальной сессии настройки могут либо не сохраниться, либо не выполниться вовсе;
- первый вход в систему нового пользователя или после переименования учетной записи (данное ограничение отслеживается системой автоматически). При первом входе выполняется инициализация профиля пользователя и конфигурирование его параметров;
- конфигурирование и настройка любых приложений пользователем. При конфигурировании в конфиденциальной сессии многие операции могут быть запрещены по полномочным правилам;
- первый запуск какого-либо приложения, с которым пользователь до этого не работал на текущей рабочей станции. Обуславливается тем, что, как правило, при первом запуске приложения происходит его первоначальная настройка под конкретного пользователя;
- первоначальное подключение сетевого диска пользователем. Необходимо для автоматического подключения этого диска при каждом последующем входе пользователя в систему. Если пользователь выполнит процедуру подключения сетевого диска в конфиденциальной сессии, то в следующих сессиях этот диск не будет подключен автоматически.

174. В режиме работы с контролем потоков первый вход пользователя в систему принудительно выполняется в неконфиденциальной сессии. При этом пользователю выводится сообщение вида "Текущий вход является конфигурационным, возможность смены уровня конфиденциальности будет предоставлена при следующем входе". Аналогичное поведение системы может проявиться и позже — например, в случае смены пользователем своего пароля во время входа в систему. В некоторых случаях для входа в конфиденциальной сессии после получения такого сообщения может потребоваться перезагрузка компьютера.

175. В режиме работы с контролем потоков вход пользователя, имеющего перемещаемый профиль в ОС Windows, будет принудительно выполняться в неконфиденциальной сессии (конфигурационный вход). В том же случае, когда часть такого профиля все же хранится локально, пользователь сможет выполнить вход в конфиденциальной сессии, но при этом корректность работы функции перенаправления не гарантируется.

176. Если для устройства записи оптических дисков включен режим теневого копирования, в конфиденциальных сессиях блокируется возможность записи дисков с использованием интерфейса Image Mastering API (IMAPI) — возникает ошибка при записи образа диска в хранилище.

> **Рекомендации:** Для записи оптического диска войдите в систему в неконфиденциальной сессии или осуществляйте запись в формате файловой системы Universal Disk Format (UDF).

177. При работе пользователя в конфиденциальной сессии запрещено удаление любой информации с помещением в Корзину (в том числе неконфиденциальных ресурсов и пустых каталогов).

178. Создание каталогов перенаправления вывода файлов невозможно для каталогов, в которых присутствуют файловые объекты с данными особого формата reparse point и при этом объекты не относятся к типам "символическая ссылка" (symbolic link) или "соединение" (junction). Базовые сведения о применении таких данных приведены на сайте компании Microsoft — см. https://msdn.microsoft.com/en-us/library/aa365503(VS.85).aspx. Если в процессе создания каталогов перенаправления обнаружены файловые объекты неподдерживаемых типов, возникает ошибка: "в директории есть reparse point".

179. На компьютере под управлением ОС Windows Vista/7 по умолчанию действует функция перенаправления вывода общих служебных файлов при создании записок на Рабочем столе (в программах StikyNot или SideBar). Из-за этого имеются следующие особенности работы с записками:

- записки создаются и сохраняются отдельно для каждого уровня сессии пользователя. Например, записки, созданные в строго конфиденциальной сессии, не будут доступны при входе этого же пользователя в конфиденциальной сессии, и наоборот;
- если при завершении сеанса работает приложение "Записки" (на экране отображается хотя бы одна записка), приложение будет работать и в следующем сеансе этого пользователя независимо от уровня конфиденциальности сессии. При этом будут загружены те записки, которые были созданы в сессии с тем же уровнем конфиденциальности.

180. Если на компьютере под управлением ОС Windows 8/10/2012 будут использоваться приложения Магазина Windows, требующие ввода данных учетной записи Майкрософт, перед включением режима контроля потоков выполните запуск этих приложений для сохранения учетных данных.

181. Для режима контроля потоков предусмотрен механизм исключений, позволяющий обеспечить нормальное функционирование приложений, которым требуется доступ к служебным файлам без изменения их категорий конфиденциальности (например, ПО MapInfo). Список исключений хранится в системном реестре компьютера в виде списка значений параметра ProcNotUpFile (тип REG_MULTI_SZ) в ключе HKLM\System\CurrentControlSet\Services\SnFMac\Params. Каждое исключение задается отдельной строкой формата *<путь_к_процессу>*::*<путь_к_файлу>*, где путь к процессу указывается в виде "\Device\Harddisk...*<имя_процесса>*" (например: \Device\HarddiskVolume1\Program Files\MapInfo\Professional\MapInfow.exe), а путь к файлу содержит полный путь в файловой системе (например: C:\WINDOWS\system32\config\software.LOG) или относительный путь с указанием имени файла (например: \system32\config\software.LOG).

Примечание: События категории "Полномочное управление доступом", регистрируемые в журнале Secret Net Studio при попытках доступа к объектам, содержат сведения о путях к процессам и файлам. При формировании списка исключений можно копировать нужные пути из записей журнала.

Рекомендации: Механизм исключений следует использовать только в крайнем случае, когда установлено, что другими способами невозможно обеспечить работоспособность программы в различных сессиях конфиденциальности. Если программа должна использоваться только в сессиях одного уровня конфиденциальности, указывать исключения не требуется. В этом случае выполните настройку программы в сессии с нужным уровнем и не запускайте программу во время работы в сессиях других уровней.

182. При включенной трассировке во время работы в конфиденциальной сессии может регистрироваться большое количество событий тревоги из-за постоянного обращения системы к каталогу с логами. Высокая частота возникновения событий приводит к тому, что оповещение о событиях тревоги не прекращается (пиктограмма Secret Net Studio окрашена красным цветом, мерцает, а команда меню "Сбросить состояние тревоги" недоступна).

Рекомендации: Для каталога с логами создайте каталоги перенаправления.

3.1.10. Контроль печати

183. Список виртуальных принтеров автоматически формируется при включении режима маркировки (стандартная или расширенная обработка) или режима теневого копирования документов. Виртуальные принтеры используются для контроля печати и соответствуют реальным установленным принтерам. Удаление виртуальных принтеров происходит при отключении режимов, при отключении механизма контроля печати или при удалении клиентского ПО СЗИ Secret Net Studio. Если на момент удаления виртуальных принтеров имеются незавершенные задания в очереди печати виртуального принтера, этот виртуальный принтер не будет удален из системы. До следующего формирования списка виртуальных принтеров печать на такой принтер будет невозможна. Чтобы печатать документы на принтере, для которого остался драйвер виртуального принтера, следует вручную удалить этот драйвер, выполнив процедуру удаления виртуального принтера.

Рекомендации: Дождитесь удаления всех заданий в очередях печати виртуальных принтеров перед выполнением любого из следующих действий:

- отключение режимов маркировки и теневого копирования документов;
- отключение механизма контроля печати;
- удаление клиентского ПО СЗИ Secret Net Studio.

184. Если включен режим маркировки (стандартная или расширенная обработка) или режим теневого копирования документов, печать осуществляется только на виртуальные принтеры (реальные принтеры в списке отсутствуют). При печати документа регистрируются 4 события: начало печати документа, начало печати экземпляра документа, успешное завершение печати экземпляра документа, успешное завершение печати документа. Если режимы маркировки и теневого копирования

документов отключены, печать осуществляется на реальный принтер (виртуальных принтеров при этом нет) с регистрацией одного события (разрешения или запрета).

185. Маркировка (добавление грифов) при печати документов выполняется без учета форматирования самих документов. Поэтому при формировании документа для печати с грифом необходимо учитывать области страниц, где будут размещаться фрагменты грифа. Если содержимое документа (например, колонтитул) занимает область вставки грифа, при печати произойдет наложение грифа на эту часть документа.

186. Печать документа с грифом, предусматривающим добавление сведений на оборотной стороне последнего листа, выполняется со следующими особенностями:

- при включенном режиме двусторонней печати (для принтеров с такой возможностью) все страницы документа печатаются на одной стороне листа, а страница грифа со сведениями для оборотной стороны — на обороте последнего листа с использованием автоматической или ручной подачи;
- если включен режим печати двух или более страниц на листе, страница грифа со сведениями для оборотной стороны масштабируется и печатается вместе с остальными страницами документа (не на обороте последнего листа).

187. При включенном режиме маркировки с расширенной обработкой категория конфиденциальности распечатываемого документа определяется следующим образом:

- если документ загружен из файла в приложение MS Word или Excel и не был модифицирован перед печатью — категория конфиденциальности при печати определяется по категории файла;
- во всех остальных случаях категория конфиденциальности документа при печати определяется по уровню процесса, из которого осуществляется печать (при отключенном режиме контроля потоков — процессу присваивается уровень конфиденциальности, равный наивысшей категории конфиденциальности открывавшихся файлов, при включенном режиме контроля потоков — процессу присваивается уровень конфиденциальности сессии).

188. Если включен режим маркировки с расширенной обработкой, не поддерживаются возможности частичной печати документов (печать выделенного фрагмента, области печати, текущей страницы и пр.) за исключением печати указанного списка страниц документа. В стандартных средствах настройки параметров печати неподдерживаемые параметры блокируются. В некоторых приложениях неподдерживаемые параметры печати могут быть доступны для настройки, однако при печати документа такие параметры игнорируются.

189. В некоторых приложениях (например, Microsoft PowerPoint 2010) при включенном режиме маркировки (стандартная или расширенная обработка) или режиме теневого копирования документов при печати может не учитываться количество копий, заданное в диалоге настройки печати в приложении. В таких случаях выполняется печать одного экземпляра документа.

190. При печати грифа заданные значения полей выводятся в объеме, не превышающем отведенное пространство для каждого поля. Перенос строк в длинных значениях полей не осуществляется. Если для поля указано слишком длинное значение (которое не умещается полностью в отведенном пространстве), его правая часть обрезается.

191. Корректное функционирование механизма контроля печати обеспечивается при условии наличия необходимых прав доступа на каталог временных файлов пользователя, заданный переменными окружения %temp% и %tmp%, а также на принтер, используемый для вывода на печать. Если параметры безопасности объектов отличаются от заданных по умолчанию, должны быть предоставлены следующие минимальные права:

- на каталог %temp% (%tmp%) — для системной учетной записи, а также учетной записи текущего пользователя (группы, в которую он включен): "Полный доступ". Чтобы проверить предоставленные права, вызовите диалоговое окно настройки свойств каталога и откройте вкладку "Безопасность". Аналогичным образом следует проверить права на каталог, заданный переменной %tmp%, если он отличается от предыдущего каталога;
- на принтер — для текущего пользователя (группы, в которую он включен): "Печать". Чтобы проверить предоставленные права, в окне "Устройства и принтеры" ("Принтеры и факсы") вызовите диалоговое окно настройки свойств принтера и откройте вкладку "Безопасность".

192. Механизм контроля печати несовместим с принтерами Xerox семейства Phaser 4510. Несовместимость связана с внутренними особенностями функционирования драйверов принтеров указанной серии.

3.1.11. Контроль устройств

193. Если компьютер был заблокирован из-за подключения неразрешенного устройства, после отключения устройства компьютер останется заблокированным до административного снятия блокировки.

194. Дисковод гибких магнитных дисков определяется по настройке в BIOS компьютера — независимо от физического наличия дисковода.

195. Не отслеживаются устройства, подключенные к последовательным и параллельным портам компьютера. Контролируются обращения пользователей к самим портам. В частности, при подключении к параллельному порту ZIP-дисковода, после установки драйверов все дальнейшие обращения через порт выполняются из контекста системы.

> **Рекомендации:** Для исключения возможности использования таких устройств установите запрет работы с портом для всех учетных записей и системы.

196. Для определения параметров сетевых карт используются их драйверы. Поэтому при выключении сетевого подключения будет фиксироваться удаление сетевой карты и наоборот.

197. Если для сетевого интерфейса в политике контроля устройств СЗИ Secret Net Studio включен режим контроля "Подключение устройства разрешено", такой интерфейс будет автоматически подключаться (активизироваться) при поступлении запросов со стороны системы (например, при изменении параметров другого сетевого интерфейса, при загрузке компьютера и др.). Подключение будет происходить даже в том случае, если администратор отключил сетевой интерфейс стандартными средствами ОС.

> **Рекомендации:** Для разграничения доступа к сетевым интерфейсам используйте средства управления СЗИ Secret Net Studio. Если необходимо отключить сетевой интерфейс — включите для него режим контроля "Подключение устройства запрещено" в политике контроля устройств СЗИ Secret Net Studio.

198. В списке устройств политики контроля устройств некоторые сетевые карты могут быть включены в класс, не соответствующий типу сетевого интерфейса. Например, если для адаптера CNET Pro200 PCI Fast Ethernet установлен стандартный драйвер Microsoft, этот сетевой интерфейс будет включен в класс "Беспроводное соединение (WiFi)" (правильный класс — "Соединение Ethernet"). Для исправления ситуации следует установить актуальный драйвер адаптера от производителя.

199. При регистрации доступа к дискам компьютера в записях о таких событиях могут фиксироваться пути вида: K:\SnCP.log\:Docf_ Epgykx0vJecku24w1vbvh5k2Nh:$DATA. Это связано с тем, что программа Проводник делает попытки открывать в файлах альтернативные потоки данных, что регистрирует подсистема разграничения доступа к устройствам.

200. Если для устройства действует режим "Подключение устройства разрешено", при подключении/отключении устройства кроме соответствующих событий может регистрироваться событие "Изменены параметры действующей политики: политика доступа к устройствам".

201. При подключении нового устройства выполняется поиск первых установленных параметров вверх по иерархии списка устройств. Заданные параметры для класса или группы копируются для нового устройства (при этом явно заданные параметры имеют приоритет перед наследуемыми параметрами старших элементов иерархии). Это позволяет на этапе настройки сначала выполнить подключение всех необходимых устройств и разрешить их использование, после чего для соответствующих элементов иерархии можно установить запрет на добавление новых устройств.

202. Для некоторых устройств PCMCIA не отображается информация об устройстве. Как правило это происходит, когда само устройство не содержит необходимой информации.

203. Чтобы обеспечить контроль устройств для шины PCMCIA, в системном реестре должен быть добавлен дополнительный параметр:
HKLM\SYSTEM\CurrentControlSet\Services\Pcmcia\Parameters\IoctlInterface : REG_DWORD : 1.
Данный параметр автоматически создается при установке СЗИ Secret Net Studio.

204.При изменении конфигурации компьютера (а также программной среды - например, при установке, обновлении ПО Secret Net Studio или при обновлении драйверов) при первой загрузке компьютера может возникнуть ошибка функционального контроля на этапе контроля аппаратной конфигурации. Такая ошибка возникает однократно и при следующих загрузках проявляться не будет.

205. Некоторые устройства при подключении могут определяться системой как несколько устройств (далее — составные устройства). Это связано с особенностями реализации контроллеров на данных компьютерах или драйверов устройств. Например, на некоторых моделях компьютеров подключаемые карты памяти MMC/SD определяются еще и как сменные диски и появляются в двух местах списка устройств: в классе "Сменные диски" группы "Локальные устройства" и в группе "Устройства Secure Digital".

> **Рекомендации:** Для корректной настройки составного устройства необходимо выполнить однотипную настройку параметров для всех вариантов его представления в списке устройств. Подробные сведения о работе с составными устройствами содержатся в документе “Руководство администратора. Настройка и эксплуатация. Локальная защита”.

206. При импорте в групповую политику домена или организационного подразделения параметров политик, содержащих список устройств, для всех импортированных групп, классов, моделей и

устройств принудительно включается режим "задать настройки контроля" (даже если он был отключен для элементов списка устройств в экспортируемой политике).

207. Если в групповую политику домена или организационного подразделения импортируется модель устройств и при этом в списке уже есть устройства, относящиеся к такой модели, то эти устройства останутся принадлежащими классу, а не модели. При этом после применения групповой политики на рабочей станции, в локальной политике такие устройства будут включены в модель.

Рекомендации: Если требуется импортировать параметры модели в групповую политику, которая уже содержит устройства этой модели, перед импортом добавьте модель для устройства с помощью команды контекстного меню.

208. Некоторые виды устройств (например, смартфон HTC S710) предоставляют возможность хранить и переносить данные, но в ОС не выступают в качестве диска или переносного носителя — т. е. устройство или его компонент не включается в класс "Хранение данных". При этом в программе Проводник появляется возможность записать файлы на такое устройство. Текущая реализация подсистемы разграничения доступа позволяет только разрешить/запретить подключение таких устройств.

Рекомендации: При необходимости исключить подключение внешних устройств, позволяющих несанкционированно сохранять и переносить данные, запретите подключение устройств (кроме разрешенных) для класса "USB | Прочие".

209. Для работы с группой устройств IEEE1394 необходимо установить обновление Windows6.0-KB953403-x86.msu. Файл с обновлением содержится на дистрибутивном диске Secret Net Studio.

210. При подключении устройства со сменным носителем (CD/DVD) к IEEE 1394 при полном запрете по правам подсистемы разграничения доступа для всех, но разрешенном подключении, в программе Проводник может появиться буква диска. Доступ к носителю при этом получить нельзя.

211. Возможна некорректная ассоциация устройств на шине SD с локальными дисками. Это связано с различиями в версиях драйверов для контроллера SD. Администратор имеет возможность либо запретить, либо разрешить использование шины SD целиком.

212. Игнорируется появление/исчезновение устройств RAS Async adapter, WAN Miniport (PPPOE), WAN Miniport (PPTP) и других подобных. Эти устройства являются программным и не несут угрозу безопасности.

213. При запуске программы со сменного носителя ОС копирует файл во временный каталог пользователя и оттуда производит запуск файла. Подсистема разграничения доступа в этом случае не регистрирует доступ на исполнение к файлу со сменного носителя.

214. При установленном запрете доступа на исполнение для подключаемых дисков (подсистемой разграничения доступа) действие "Open(O)" в программе Проводник будет вызывать ошибку "Нет доступа". Причина заключается в том, что при выполнении данного действия программа Проводник осуществляет попытку открыть на исполнение файл autorun.inf. Действия "Open" и "Explore" выполняются корректно.

215. Подсистема контроля устройств не обнаруживает встроенный PCI-модем.

216. Диски, подключаемые по технологии iSCSI, отключаются при выключении компьютера и подключаются снова при его включении. Подсистема контроля устройств отслеживает данные события. Если такое устройство установлено на контроль, при перезагрузке фиксируется изменение аппаратной конфигурации, что может привести к блокировке компьютера (если включен параметр "Блокировать компьютер при изменении устройства").

Рекомендации: Не устанавливайте на контроль диски, взаимодействие с которыми осуществляется по технологии iSCSI.

217. При использовании RAID-массива дисков подсистема контроля устройств контролирует массив как один физический диск. Вследствие этого некоторые внутренние операции с дисками в массиве (например, замена одного из дисков) могут не контролироваться подсистемой.

Примечание: Для большинства RAID-контроллеров предоставляется возможность настройки с помощью собственных программных средств управления. В частности, такими программными средствами можно отключить автоматическое восстановление массива при смене диска (для защиты от подмены). Кроме того, для обеспечения защиты данных следует реализовать соответствующие меры контроля физического доступа к компьютеру с RAID-массивом.

218. Из-за особенностей работы драйверов аппаратного обеспечения в ОС Windows возможны ситуации, когда разрешенные для использования подключенные устройства могут не появляться в системе после перезагрузки. Такое поведение характерно для устройств, подключенных к шине или на некоторых контроллерах шины SecureDigital (например, Texas Instruments). Чтобы устройство появилось в системе после перезагрузки, как правило, достаточно его отключить и подключить заново.

219. После подключения жесткого диска возможно срабатывание контроля аппаратной конфигурации на изменение памяти компьютера. Такое может произойти при использовании некоторых контроллеров (например, IDE Controller Marvell), которые резервируют для своей работы незначительное количество памяти (8 КБ).

220. При выключении подсистемы шифрования трафика, а также при ее включении, если клиент был установлен без этой подсистемы, — после перезагрузки может фиксироваться изменение аппаратной конфигурации.

221. В некоторых случаях в журнале может зарегистрироваться большее количество событий подключения одинаковых устройств, чем количество устройств, отображенных в диалоге утверждения аппаратной конфигурации.

222. Для устройств, подключаемых к шине IEEE1394 во время работы компьютера (динамический контроль), фактом подключения устройства считается команда операционной системы, активирующая устройство. Поэтому, если драйвер не установлен для конкретного устройства, то такой команды не последует, и подсистема контроля устройств не зафиксирует подключение. Кроме того, при запрете подключения в диспетчере устройств будет отображаться подключенное устройство с ошибкой — т. к. устройство неработоспособно.

223. Для сетевых плат и устройств аппаратной поддержки Secret Net Studio во время спящего режима не фиксируется изменение аппаратной конфигурации. Во время работы допускается отключение и подключение ранее утвержденного адаптера без регистрации событий отключения и подключения.

224. Если для сетевого адаптера включен режим контроля "Устройство постоянно подключено к компьютеру" с параметром "Блокировать компьютер при изменении устройства", то при выходе из спящего режима компьютер может быть заблокирован. Это связано с изменением конфигурации сетевых интерфейсов непосредственно при выходе из спящего режима, так как операционная система в некоторых случаях продолжает процесс отключения интерфейсов, после чего снова их подключает. Отследить включение и отключение спящего режима можно по регистрируемым событиям в журнале Secret Net Studio.

> **Рекомендации:** Чтобы отключение сетевого адаптера, связанное с выходом компьютера из спящего режима, не воспринималось системой как изменение аппаратной конфигурации, включите для этого адаптера режим контроля "Подключение устройства разрешено".

225. Из-за особенностей применения параметров контроля для сетевых адаптеров (асинхронность включения и отключения при применении политики) возможны ситуации, когда после перевода сетевого интерфейса из режима контроля "Подключение устройства запрещено" в режим "Устройство постоянно подключено к компьютеру" с параметром "Блокировать компьютер при изменении устройства" — произойдёт блокировка компьютера.

> **Рекомендации:** Чтобы не произошла блокировка в такой ситуации, при переключении режимов сначала отключите параметр "Блокировать компьютер при изменении устройства", примените политику и затем включите действие параметра.

226. Если в ОС включен механизм управления учетными записями (User Account Control — UAC), не действуют права доступа к устройствам, заданные для группы локальных администраторов. Если доступ к устройству разрешен только для группы локальных администраторов — доступ будет блокироваться для всех пользователей, включая и администраторов. Такое поведение является следствием работы механизма управления учетными записями UAC.

> **Рекомендации:** Для предоставления прав доступа к устройствам используйте любые другие учетные записи.

3.1.12. Подсистема аппаратной поддержки

227. Для работы с идентификаторами eToken PRO необходимо использовать ПО Единый клиент JaCarta версии 2.9.x. В состав установочного комплекта Secret Net Studio добавлен дистрибутив ПО Единый клиент JaCarta версии 2.9.0.1531.

228. В СЗИ Secret Net Studio отсутствуют специальные функции смены PIN-кода в USB-ключе.

> **Рекомендации:** Чтобы сменить PIN-код (пароль) в USB-ключе, используйте соответствующее ПО.

229. Если в памяти электронного идентификатора содержался пароль, превышающий 16 символов, при его замене паролем меньшей длины, в памяти идентификатора останется структура, необходимая для хранения пароля прежней длины. Это может привести к дефициту памяти идентификатора.

> **Рекомендации:** В случае дефицита памяти идентификатора по указанной выше причине, необходимо выполнить инициализацию идентификатора или заново выполнить процедуру присвоения идентификатора пользователю.

230. Если для сменного носителя ни разу не выполнялась процедура присвоения, в диалоге предъявления идентификатора этот носитель будет отображаться без номера.

231. Работу с USB-ключами (Rutoken, JaCarta или eToken) обеспечивает системная служба "Смарт-карты" (ScardSvr.exe). Если эта служба не запущена, использование USB-ключей невозможно.

232. Если инициализация идентификатора eToken выполняется средствами СЗИ Secret Net Studio, из идентификатора удаляются только данные Secret Net Studio и ПАК "Соболь". Полная очистка

памяти идентификатора не осуществляется. Для форматирования с очисткой памяти идентификатора необходимо выполнить процедуру его инициализации с помощью ПО eToken PKI Client.

233. При нестабильном функционировании идентификаторов Rutoken рекомендуется обновить их драйверы на версии, размещенные на диске комплекта поставки в каталоге \Tools\Tokens\RuToken\.

234. На компьютерах с установленным ПО СЗИ Secret Net Studio для использования USB-ключей или смарт-карт при удаленном подключении рекомендуется отключать режим "Смарт-карты" в параметрах подключения (в разделе выбора локальных устройств и ресурсов). Иначе в терминальных сессиях возможны сбои выполнения операций разблокировки компьютера или управления идентификаторами.

235. При использовании для терминального входа идентификатора ESMART возможна длительная задержка обработки идентификатора, приводящая к сбою процесса входа.

> **Рекомендации:** Чтобы обеспечить корректный вход в систему, можно увеличить время ожидания завершения операций при терминальном входе. Для этого в ключе системного реестра HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp создайте параметр LogonTimeout типа REG_DWORD со значением 120 (соответствует двум минутам). Данный параметр может не действовать в некоторых конфигурациях — например, в ОС Windows Server 2008 R2 при определенных условиях требуется специальное исправление от компании Microsoft (см. http://support.microsoft.com/kb/2617878/en-us).

3.1.13. Затирание данных

236. Не гарантируется успешная работа механизм затирания данных с объектами файловой системы UDF (Universal Disk Format). Из-за особенностей реализации файловой системы UDF механизм затирания данных получает ложную информацию о количестве жестких ссылок файлового объекта, если тот имеет альтернативные потоки данных. В результате операция уничтожения данных не выполняется.

237. Если включен механизм затирания данных, могут возникать задержки при определении впервые подключаемых USB-устройств (например, USB Flash-накопитель). Определение устройства может завершиться через несколько минут после его подключения. При этом все следующие подключения того же устройства будут выполняться без лишних затрат времени. Причина задержек — особенности протоколирования установки устройств Plug and Play в операционной системе. При установке драйвера устройства ОС многократно выполняет кеширование и перезапись системного файла логирования (до тысячи циклов и более), что увеличивает суммарное время обработки операций механизмом затирания.

> **Рекомендации:** Для сокращения времени можно изменить уровень логирования операций ОС, включив режим записи только ошибок и предупреждений. Для этого в системном реестре создайте параметр LogLevel типа REG_DWORD (если он отсутствует) в ключе HKLM\Software\Microsoft\Windows\CurrentVersion\Setup и задайте этому параметру шестнадцатиричное значение 0x00002020. Подробные сведения о назначении и использовании параметра см. http://msdn.microsoft.com/en-us/library/windows/hardware/ff550845(v=vs.85).aspx.

238. Механизм затирания данных по умолчанию не действует для файлов на диске с файловой системой ReFS (доступна с версии Windows Server 2012), если для диска, папки или самого файла включен дополнительный параметр проверки целостности (Integrity streams). Это связано с особенностями методики записи таких файлов — данные всегда записываются на новое место дискового пространства. Чтобы включить действие механизма затирания независимо от параметра проверки целостности, в ключе системного реестра HKLM\SYSTEM\CurrentControlSet\services\SnEraser\Parameters создайте параметр DisableReFsIntegrityStream типа REG_DWORD с любым значением и перезагрузите компьютер. После этого драйвер механизма затирания при обращении к файлам будет сбрасывать их атрибуты проверки целостности, чтобы обеспечить затирание и предотвратить появление остаточных данных.

239. По умолчанию при затирании оперативной памяти пропускаются зафиксированные страницы (locked pages). Это позволяет обеспечить функционирование приложений и драйверов, которые продолжают использовать зафиксированные страницы памяти на момент завершения процесса — например, ПО Citrix, DebugView. При необходимости можно включить затирание зафиксированных страниц памяти. Для этого в ключе системного реестра HKLM\SYSTEM\CurrentControlSet\Services\SnWiper создайте параметр WipeLockedPages типа REG_DWORD со значением 1.

3.1.14. Подсистема защиты локальных дисков

240. При создании загрузочного диска аварийного восстановления на USB-Flash-накопителе объемом более 4 Гб видимый объем диска после форматирования будет ограничен 4 Гб. В дальнейшем, если носитель не будет нужен в качестве диска аварийного восстановления (например, при отключении механизма защиты дисков), можно вернуть его исходный объем путем переформатирования стандартными средствами ОС.

241. При использовании диска аварийного восстановления на системе, загружающейся с GPT-диска, не происходит удаление и отключение загрузчика Secret Net Studio. Если этот загрузчик будет блокировать загрузку, его можно отключить в UEFI Setup, выбрав в качестве основного загрузчик Windows.

242. Механизм защиты дисков не поддерживает 32-разрядные UEFI-системы с загрузкой с GPT-диска.

243. При использовании механизма защиты дисков для виртуальной машины рекомендуется создавать загрузочный диск аварийного восстановления на компакт-диске или в виде образа компакт-диска. Возможность загрузки с USB-Flash-накопителя может не поддерживаться виртуальной машиной.

3.1.15. Теневое копирование

244. Если для сменного диска включен режим теневого копирования, реакция подсистемы на попытку записи файла большего размера, чем свободное пространство на диске, зависит от версии ОС и используемой программы. Для такого события в журнале Secret Net Studio может не регистрироваться ошибка записи. Дубликат не поместившегося файла будет либо отсутствовать в хранилище теневого копирования, либо представлен в виде файла урезанного объема (сколько было записано программой на диск до момента переполнения).

245. Если для сменного диска включен режим теневого копирования, в хранилище могут создаваться копии файлов не только при записи на сменный диск, но и при копировании файлов с этого диска в программе Проводник. Это связано с особенностями обработки файлов в данной версии ОС - программа Проводник при копировании открывает исходный файл с правом на запись.

246. В некоторых случаях при включенном режиме теневого копирования для устройства записи оптических дисков может блокироваться операция форматирования чистого компакт-диска в формате файловой системы LFS (Live File System, реализация формата Universal Disk Format). Если форматирование блокируется при отключенном режиме теневого копирования, проверьте наличие предоставленных прав (разрешений) записи для устройства.

247. Система Secret Net Studio контролирует запись информации на оптические диски при условии использования штатных средств операционной системы. Некоторые программы, имеющие функцию записи оптических дисков, используют собственные драйверы управления устройствами. Например: Daemon Tools, Power Archiver Pro, Alcohol 120%. С помощью таких программ пользователи могут осуществлять запись оптических дисков в обход механизма теневого копирования. Для обеспечения гарантированного контроля не устанавливайте на компьютеры ПО сторонних производителей, позволяющее записывать оптические диски (установка ПО разрешается только пользователям, обладающим правами администратора).

3.1.16. Контроль приложений

248. В режиме "аудит пользовательских приложений" (включен по умолчанию) механизма "Контроль приложений" для некоторых процессов в журнале могут регистрироваться только события "Завершение процесса" без предварительной регистрации событий запуска. Например, событие запуска может не регистрироваться для системного процесса rundll32.exe, хотя завершение этого процесса фиксируется в журнале. Данная особенность связана с тем, что запуск таких процессов выполняется от имени системы, а завершение происходит в контексте пользователя. При необходимости регистрации запуска подобных процессов включите режим "аудит пользовательских и системных приложений". При этом нужно учитывать, что указанный режим увеличивает нагрузку на ядро Secret Net Studio и может приводить к переполнению журнала записями о таких событиях.

3.1.17. Запрет вторичного входа в систему

249. При включении режима запрета вторичного входа на компьютере могут блокироваться некоторые административные функции. В частности, данный режим препятствует вводу компьютера в домен, поскольку для этого необходимо ввести учетные данные администратора домена.

250. Имеются следующие особенности применения параметра групповых политик "Вход в систему: Запрет вторичного входа в систему":

- если применение политики происходит при работе компьютера — новое значение параметра начнет действовать со следующей загрузки компьютера;
- в сетевом режиме функционирования СЗИ если в групповой политике параметр был изменен при выключенном компьютере — новое значение параметра начнет действовать со второй (после изменения настройки) загрузки компьютера.

251. Для блокирования возможности запуска приложений от имени администратора принудительно изменяется значение стандартного параметра безопасности ОС Windows "Контроль учетных за-

писей: поведение запроса на повышение прав для обычных пользователей". Данному параметру присваивается значение "Автоматически отклонять запросы на повышение прав".

Рекомендации: Не изменяйте значение указанного параметра (и не задавайте данный параметр в групповых политиках), чтобы исключить возможность выполнения действий с вводом учетных данных пользователя, который не выполнил интерактивный вход в систему.

252. При включенном режиме запрета вторичного входа в журнале Secret Net Studio регистрируются события "Запрет сетевого подключения под другим именем", которые являются результатом попыток открытия сетевых ресурсов от имени пользователя, не выполнившего интерактивный вход в систему. События отказа запуска ПО от имени другого пользователя не регистрируются в журнале Secret Net Studio.

3.2. Межсетевой экран и авторизация сетевых соединений

3.2.1. Установка подсистем сетевой защиты

253. Если в домене включен запрет использования NetBIOS имен, установка подсистем сетевой защиты невозможна на компьютерах с именами длиннее 15 символов.

254. Если в домене не функционирует служба разрешения имен DNS, установка подсистем сетевой защиты может быть прервана с выдачей сообщения об ошибке "2147024638 Время ожидания операции истекло" при попытке обновления информации об агенте на сервере аутентификации. Диагностировать неработоспособность службы DNS можно с помощью следующих стандартных команд ОС:

- ping <*полное_FQDN-имя_компьютера_сервера_безопасности*> — если служба не найдена, команда выполняется с большой задержкой (порядка 10 секунд);
- nslookup <*полное_FQDN-имя_компьютера_сервера_безопасности*> — если служба не найдена, возвращается ошибка из-за превышения времени ожидания ответа DNS-сервера.

255. Во время установки/обновления подсистем сетевой защиты могут прерываться существующие сетевые подключения.

256. Если в операционной системе не настроена поддержка русского языка (в том числе для приложений, не поддерживающих Юникод), подсистемы сетевой защиты могут некорректно обрабатывать объекты с символами кириллицы (имена компьютеров, путь установки и др.).

257. В случае установки на контроллер домена, при перезагрузке компьютера возможно появление сообщений подсистемы аудита о неподписанных пакетах. Сообщения появляются при защите следующих портов контроллера домена: 135 TCP, 139 TCP, 445 TCP, 389 UDP, 88 UDP, NTDS.

3.2.2. Общее

258. Не поддерживается работа компонентов сетевой защиты на кластерах.

259. Не поддерживается работа компонентов сетевой защиты на компьютерах, в именах которых используются только цифры и спецсимволы (например, 2016-1 или 20167).

260. Для корректной работы компонентов сетевой защиты на компьютерах с активной ролью Hyper-V может потребоваться дополнительная настройка параметров сетевых адаптеров. Рекомендации по настройке предоставляются при обращении в службу технической поддержки компании-поставщика.

261. Не рекомендуется совместное использование механизмов сетевой защиты Secret Net Studio с межсетевыми экранами сторонних производителей. Для корректного функционирования может потребоваться дополнительная настройка параметров.

Примечание: При использовании MS Windows Firewall дополнительная настройка параметров не требуется.

262. Механизм авторизации сетевых соединений не поддерживает конфигурацию сети, при которой соединение клиента с защищаемым компьютером осуществляется посредством NAT, VPN или IPSEC.

263. Межсетевой экран не обеспечивает работоспособность с двумя или более сетевыми интерфейсами, соединенными мостом (bridge), а также с сетевыми интерфейсами, сгруппированными в Nic Teaming.

264. События, зарегистрированные механизмами сетевой защиты, могут отображаться в журнале не в хронологическом порядке.

265. После изменения NetBIOS-имени компьютера необходимо выполнить процедуру исправления работоспособности механизмов сетевой защиты с помощью программы управления.

3.2.3. Аутентификация

266. При обращении к защищаемому компьютеру по протоколу FTP с компьютера, на котором запущен брандмауэр Windows, для аутентификации используется учетная запись рабочей станции.

267. Пользователю, аутентифицированному в системе, разрешается доступ к защищаемым компьютерам в течение некоторого времени после отключения или удаления его учетной записи.

268. При смене пароля учетной записи защищаемого сервера (например, после переустановки ПО агента межсетевого экрана или восстановления системы после сбоя) абоненты в течение некоторого времени не смогут устанавливать с этим сервером защищенные соединения.

269. При использовании SMB-соединения возможно появление сообщений аудита об анонимном доступе по протоколу SMB в следующих случаях:

- после выхода компьютера абонента из спящего режима;
- при одновременной работе нескольких пользователей по протоколу SMB (т. к. при этом владение SMB-каналом переходит от одного пользователя к другому).

270. Сетевой трафик от приложения, запущенного в сессии 0 под учетной записью LocalSystem, определяется как системный.

3.2.4. Защищаемый сервер

271. При одновременном срабатывании политик и правил, ограничивающих доступ к защищаемому компьютеру, возможны дублирующие сообщения подсистемы аудита.

272. При смене группы изменения для учетной записи компьютера вступают в действие через несколько часов. Для пользователя изменения вступят в действие во время следующего входа в систему, либо также через несколько часов, если пользователь не выполнял выход и новый вход в систему.

273. При выходе из аварийного режима могут завершиться соединения, установленные абонентами с защищаемыми серверами.

274. При большой нагрузке на компьютере абонента может прерваться существующая ISAKMP-ассоциация между абонентом и защищаемым сервером, в результате чего часть пакетов может отправляться неподписанными до установления новой ассоциации.

275. Если на защищаемом сервере включена проверка подлинности SMB-трафика средствами Windows (обычно на контроллерах домена), то при одновременной работе нескольких пользователей на одном удаленном компьютере с общими папками на этом сервере могут прерываться SMB-подключения.

276. В некоторых случаях, возникающих в силу особенностей маршрутизации и топологии сети, возможно появление сообщений аудита об обнаружении дубликатов сетевых пакетов.

3.2.5. Прочие особенности

277. Если неаутентифицированным пользователям разрешен доступ по протоколу SMB на 445-й и 139-й порты, то при применении прикладных правил не будет учитываться имя пользователя, даже если на удаленном компьютере осуществлен вход от его имени.

278. Правило доступа не действует для заданного исполняемого файла процесса, если сам файл находится на присоединенном сетевом диске. В этом случае необходимо указывать UNC путь в формате "\\<*имя_сервера*>\<*имя_сетевого_каталога*>\<*имя_файла_процесса*>.exe".

279. При подключении к системам хранения данных по протоколам NFS (Network File System) и ISCSI необходимо предоставлять доступ как для учетной записи компьютера, так и для учетной записи пользователя.

280. При смене имени компьютера, на котором установлен клиент Secret Net Studio с подсистемами сетевой защиты, после перезапуска в программе управления для межсетевого экрана отображается статус "подсистема не работает в полном объеме". Кроме того, прекращается обновление конфигурации сетевой защиты, и в программе управления может отображаться старое имя компьютера. Также возможны сбои в работе средства обнаружения вторжений.

Рекомендации: В случае переименования компьютера для возобновления нормальной работы выполните следующие действия.

Если клиент установлен в сетевом режиме функционирования:

1. На рабочем месте администратора в программе управления удалите объект из структуры и затем снова добавьте с подчинением тому же серверу безопасности (СБ).

2. На защищаемом компьютере в командной строке введите команду:
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScAuthChangeRealm.exe" /KDC <*имя_СБ*>

Если клиент установлен в автономном режиме функционирования:

1. На защищаемом компьютере в командной строке последовательно введите команды:
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScLocalCfg.exe NETPROTECTION Reset local
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScLocalCfg.exe NETPROTECTION Reset main

281. При включенном режиме обучения межсетевого экрана и активном соединении абонентского пункта Континент с сервером доступа не применяются блокирующие правила, которые запрещают весь трафик кроме туннеля абонентского пункта (так как в режиме обучения отключаются обычные правила межсетевого экрана).

282. При аварийном завершении работы модуля абонентского пункта Континент ("VPN клиент") не выгружаются созданные для него правила доступа из списка правил межсетевого экрана. Из-за этого, если для пользователя абонентского пункта действует конфигурация, запрещающая весь трафик кроме туннеля абонентского пункта — межсетевой экран может заблокировать все сетевые соединения.

Рекомендации: В случае блокировки соединений можно выполнить операцию кратковременного сброса (удаления) конфигурации межсетевого экрана в драйверах. Действие выполняется с помощью утилиты командной строки ScAuthModCfg.exe, расположенной в подкаталоге \Network Protection каталога установки клиента. Для сброса конфигурации введите команду: ScAuthModCfg.exe /r. После этого до автоматического восстановления конфигурации (от 1 до 6 минут) можно ввести команду ipconfig /renew (для DHCP) и подключиться к серверу доступа АПКШ "Континент" для исправления набора правил.

Примечание: Если применяются динамические IP-адреса (DHCP), для использования защищенного соединения абонентского пункта необходимо создать разрешающее правило для DHCP.

283. На компьютере сервера безопасности при загрузке ОС может возникнуть ошибка 2147218383 во время запуска службы Secret Net Studio Network Protection Management. Из-за этого в программе управления при подключении к агенту выводится статус "Недопустимая операция. Ошибка синхронизации. Повторите запрос", и для подсистем сетевой защиты отображается аварийный режим.

Рекомендации: Запустите вручную службу Secret Net Studio Network Protection Management. Для регулярного запуска службы можно создать задачу в Планировщике заданий Windows. В параметрах задачи задайте следующие параметры:

1. На вкладке "Общие" (General) в разделе "Параметры безопасности" (Security options) укажите используемую учетную запись "Система" (System) и включите режим "Выполнить с наивысшими правами" (Run with highest privileges).

2. На вкладке "Триггеры" (Triggers) создайте новый триггер запуска с параметрами "Начать задачу" (Begin the task), значение "При запуске" (“At startup”) и "Отложить задачу на…" (Delay task for), значение 3 минуты.

3. На вкладке "Действия" (Actions) создайте элемент с параметрами "Действие" (Action), значение "Запуск программы" (“Start a program”); "Программа или сценарий" (Program/script), значение “net.exe” и "Добавить аргументы…" (Add arguments…), значение “start ScConfigServer”.

4. На вкладке "Условия" (Conditions) удалите отметку из поля "Запускать только при питании от электросети" (Start the task only if the computer is on AC power).

3.3. Антивирус

3.3.1. Установка подсистемы

284. Для работы антивируса требуется не менее 900 МБ доступной для ОС оперативной памяти.

285. На некоторых конфигурациях для работы антивируса минимально необходимо 2 ГБ оперативной памяти и использование файла подкачки в ОС*.

286. Свободное пространство диска для установки антивируса должно быть не менее 500 МБ. Такой объем необходим для разворачивания антивирусных баз обновлений.

287. Если в системном каталоге %TEMP% из-за недостатка свободного места невозможно разместить временные файлы (например, для распаковки архивов), может произойти сбой при сканировании.

Рекомендации: Перед установкой антивируса необходимо убедиться, что каталог %TEMP% расположен на диске с достаточно большим свободным пространством.

* Особенность не относится к антивирусу с технологией ESET.

3.3.2. Общее

288. При совместной работе антивируса Secret Net Studio с другими антивирусами, в частности с компонентом ОС "Защитник Windows" (Windows Defender), существенно снижается производительность компьютера. Это может привести к невозможности работы пользователей. Поэтому во время установки антивируса Secret Net Studio на компьютере под управлением ОС Windows Vista/7 "Защитник Windows" выключается, а на ОС Windows 8/10 в этом компоненте отключается режим защиты в реальном времени (отключение происходит после перезагрузки компьютера). Однако в ОС Windows 8/10 "Защитник Windows" может снова включиться из-за применения стандартно настроенных групповых политик Windows или после установки обновлений ОС, затрагивающих работу встроенной антивирусной защиты Windows — например, обновление KB4015217.

> **Рекомендации:** До установки антивируса Secret Net Studio в редакторе групповых политик настройте соответствующие параметры отключения компонента в разделе "Защитник Windows" (название может быть другое в зависимости от версии и языка ОС: Windows Defender или Endpoint Protection). Раздел представлен в группе политик конфигурации компьютера в ветке "Административные шаблоны / Компоненты Windows" (Administrative Templates / Windows Components). Необходимо как минимум включить действие параметра "Отключить Защитник Windows" (название может быть другое в зависимости от версии и языка ОС: Turn off Windows Defender, "Выключить Endpoint Protection" и т. п.). Дополнительно в соответствующих параметрах этого раздела рекомендуется отключить все разрешенные действия для компонента. Параметры должны примениться на компьютерах до установки клиента Secret Net Studio с антивирусом.
>
> Если при установленном антивирусе Secret Net Studio в ОС были установлены обновления, затрагивающие работу встроенной антивирусной защиты Windows, — убедитесь, что параметры отключения компонента "Защитник Windows" остались активны, и перезагрузите компьютер повторно.
>
> **Примечание:** Отключение компонента "Защитник Windows" также может выполняться и через системный реестр. Конфигурация параметров для отключения в ОС Windows 10:
> ключ HKLM\SOFTWARE\Policies\Microsoft\Windows Defender, параметр DisableAntiSpyware типа REG_DWORD со значением 1;
> ключ HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection, параметры DisableBehaviorMonitoring, DisableOnAccessProtection и DisableScanOnRealtimeEnable типа REG_DWORD со значениями 1.

289. Список исключений необходимо формировать с учетом следующих особенностей:

- если диску назначено несколько букв, в списке исключений необходимо указать все;
- если доступ к сетевому ресурсу осуществляется по IP-адресу и по имени компьютера, в списке исключений необходимо указать оба варианта;
- для ресурсов на подключенном сетевом диске необходимо указывать два варианта пути — путь с именем диска и путь в формате Multiple UNC Provider: \Device\Mup\<…> (как он представлен в сведениях в программе управления);
- исключение не действует для буквы виртуального диска, созданного командой SUBST.

290. При проверке сменных носителей могут не действовать исключения для объектов, добавленных в список из карантина. Исключение не учитывается, если при подключении сменного носителя его внутреннее имя в системе не совпадает с указанным в списке исключений — поскольку при новом подключении изменилось имя тома для сменного носителя. Например, когда в пути для исключения задан том HarddiskVolume10, а сменный носитель подключен как HarddiskVolume11.

291. Файлы, расположенные на томе, который подключен в ОС как папка на NTFS-системе, успешно контролируются на наличие вирусов в режиме реального времени (профиль "Постоянная защита"), но при этом при работе с такими томами есть следующие ограничения:

- поиск вирусов в содержимом подключенного тома не выполняется при сканировании корневой папки базового тома или если объектами сканирования являются диски (например, при полном сканировании);
- при контекстном сканировании обнаруженные вирусы не помещаются в карантин;
- при контекстном сканировании не применяется список исключений.

3.3.3. Карантин

292. В конфиденциальных сессиях не поддерживается работа с карантином (просмотр и управление) средствами локальной программы управления. Работайте с карантином только в неконфиденциальных сессиях.

293. В программе управления элементы списка карантина отображаются в формате NT namespace с указанием сведений о логическом диске (томе) в виде: "\Device\HarddiskVolume<*N*>\...". Это обеспечивает унификацию имен файлов на терминальных серверах, когда пути к файлам в виде DOS-имени могут содержать изменяемые части — например, зависящие от имени пользователя.

294. Из карантина автоматически удаляются файлы, хранящиеся более 30 дней. Период хранения можно изменить с помощью утилиты командной строки av_cli.exe.

295. Восстановить файл на сменном носителе, который был помещен в карантин, можно на любом компьютере с установленным компонентом антивируса Secret Net Studio. Восстановление осуществляется с помощью утилиты командной строки av_cli.exe.

> **Примечание:** Например, для восстановления файла Z:\ForVMs.share\vir\AUTORUN\!ITW#184_\!ITW#184.vxe.quarantine введите команду: av_cli.exe -c:restore_file -p:Z:\ForVMs.share\vir\AUTORUN\!ITW#184_\!ITW#184.vxe.quarantine

3.3.4. Защита в режиме реального времени

296. Для профиля "Постоянная защита" не рекомендуется без необходимости включать проверку в максимально полном объеме: "Углубленная эвристика" — включено, "Пропускать архивы" и "Пропускать файлы более … Мб" — отключено. В этих условиях проверка файлов может длиться значительное время и восприниматься пользователем как "зависание" системы.

297. Для файлов на сетевых ресурсах не рекомендуется включать действия "Удалять зараженные файлы" или "Удаляемые файлы поместить в карантин", так как последующий поиск "пропавших" файлов (удаленных или помещенных в карантин) будет возможен только по журналам.

> **Рекомендации:** На компьютерах, которые предоставляют сетевые ресурсы, установите компонент антивируса Secret Net Studio и настройте регулярную проверку локальных носителей.

298. При перемещении файловых объектов внутри одного раздела проверка на вирусы не осуществляется. В этом случае в файловой системе происходит только изменение записей об объектах без физического перемещения содержимого файлов и/или папок.

299. При просмотре файлов в файловом менеджере (например, в программе Проводник) файлы проверяются антивирусом так же, как и при их непосредственном открытии.

300. Если в системе подключен образ диска, который содержит зараженные файлы, при обращении к этому диску в файловом менеджере (например, в программе Проводник) возможны длительные задержки открытия файлов.

301. При включенной трассировке рекомендуется добавить в список исключений каталог с логами. Иначе возможны длительные задержки при загрузке компьютера с регистрацией ошибок функционального контроля.

3.3.5. Сканирование по расписанию или по требованию

302. По умолчанию в системе представлена отдельная постоянная задача по расписанию, применяемая для проверки оперативной памяти (RAM) и основной загрузочной записи физического диска (MBR) через 10 минут после старта сервиса.

303. На компьютере с низкой скоростью выполнения дисковых операций сканирование по расписанию в режиме "После запуска" может существенно увеличить время загрузки ОС.

> **Рекомендации:** На таких компьютерах рекомендуется настраивать сканирование по расписанию в определенное время.

304. При контекстном сканировании CD/DVD-дисков возможно неправильное определение путей к файлам (особенность работы Проводника). Для корректного сканирования не следует одновременно выбирать имеющиеся на диске файлы и файлы, подготовленные для записи на диск.

305. Параметры сканирования методом углубленной эвристики совпадают с параметрами эвристики в обычном режиме*.

3.3.6. Регистрация событий

306. При наличии в имени файла символов процента и цифры (например, %1) возможна некорректная регистрация данных о файле в записи журнала.

307. В регистрируемых событиях сведения об ошибках обновления, связанных с сетевым доступом (https), приводятся на английском языке.

3.3.7. Обновление антивирусных баз

308. Режимы автоматического определения прокси-сервера (direct_connection и system_proxy) могут использоваться при условии предоставления необходимых параметров соединения со стороны серверов DHCP или DNS. В остальных случаях следует использовать режим настройки вручную (custom_settings) с явно указанными параметрами соединения.

* Особенность не относится к антивирусу с технологией ESET.

3.4. Обнаружение и предотвращение вторжений

309. При проведении в сети атак ARP-spoofing детектор Secret Net Studio их успешно обнаруживает. Но в некоторых ситуациях из-за специфики обработки в ОС ARP-трафика возможна подмена реального MAC-адреса фиктивным. Например, при проведении атаки с помощью специализированного ПО Cain & Abel (v4.9.56). Для комплексной защиты от таких атак рекомендуется дополнительно использовать соответствующие средства защиты, имеющиеся на сетевом оборудовании.

310. Если в настройках HTTP анализатора СОВ указать порты, по которым передается **не** HTTP трафик, анализатор может работать некорректно, что может привести к неработоспособности сетевых соединений по этим портам.

3.5. Центр управления

3.5.1. Общее

311. Если на рабочем месте администратора используется ОС Windows с базовым языком, отличным от русского, и установлен русскоязычный вариант компонента "Secret Net Studio — Центр управления", то для корректного отображения интерфейса программы управления необходимо установить русский язык для параметра ОС Windows, определяющего язык программ, не поддерживающих Unicode.

3.5.2. Запуск программы управления

312. Если в параметрах программы каталог для временных файлов указан с использованием переменной окружения (например, %Temp%), имя переменной должно начинаться с символа в верхнем регистре. Иначе возможно возникновение ошибки при запуске программы.

313. Подключение к серверу программы управления на этом же компьютере может блокироваться с ошибкой из-за недостаточных привилегий пользователя при следующих условиях:

- в операционной системе включен механизм управления учетными записями (User Account Control — UAC);
- группой администраторов домена безопасности является стандартная доменная группа администраторов (Domain Admins);
- запустивший программу пользователь был добавлен в группу администраторов (не является первичной учетной записью администратора домена Windows).

Примечание: Ограничение административных прав пользователя является следствием работы механизма UAC.

3.5.3. Вывод данных

314. В некоторых случаях система не может установить тип пользовательской сессии на защищаемом компьютере, и в программе управления отображается значение "не определен".

3.5.4. Настройка параметров

315. При настройке параметров рассылки почтовых уведомлений в поле "От кого" можно указывать только латинские символы, знаки пунктуации и спецсимволы #$|*?!%&+=_-/{}.

3.5.5. Работа с журналами

316. Обновления, обеспечивающие совместимость Secret Net Studio с Windows 10 версии 1803, не полностью восстанавливают работу с журналами Secret Net Studio. Имеются следующие ограничения:

- В программе управления в локальном и централизованном режиме работы даты событий в загруженных внешних журналах Secret Net Studio (ранее сохраненных в формат evtx) будут отображаться как 1970 год, также не будут отображаться названия категорий и описания событий. Для устранения этого ограничения рекомендуется сохранять журналы Secret Net Studio в формате snlog (формат компании "Код Безопасности");
- Так же не будут правильно отображаться журналы Secret Net Studio, сохраненные с помощью утилиты GetEventLog из состава Secret Net Studio.

Примечание: Данные ограничения связаны с ошибкой в пакете обновления Windows 10 версии 1803.

317. В записях журналов имена компьютеров могут отображаться со знаком "$". Наличие или отсутствие знака обуславливается типом учетной записи компьютера: доменная или локальная учетная запись.

318. Описания событий в записях журналов могут быть как на русском, так и на английском языке — в зависимости от локализации операционной системы компьютера, на котором произошло событие.

319. При восстановлении в базе данных записей одного и того же архива происходит дублирование записей (столько раз, сколько выполнялось восстановление).

320. Если изменилось имя агента (из-за переименования компьютера), то при запросе журналов для этого агента, не будут доступны записи, зарегистрированные до переименования. Чтобы отобразить все записи, можно в поле "Компьютер" ввести старое и новое имя агента через запятую. Кроме того, можно получить все записи, отключив применение фильтра по имени компьютера.

321. Для загрузки журналов из больших архивов программе управления может потребоваться значительный объем оперативной памяти. При недостатке оперативной памяти для получения записей из архивов рекомендуется воспользоваться функцией поиска по архивам. Фильтр поиска позволяет указать имя компьютера, типы журналов и событий, время и другие параметры, с помощью которых можно получить относительно небольшую выборку записей для просмотра на компьютерах с ограниченным объемом оперативной памяти.

322. В локальном режиме программы управления при поиске угроз не применяются правила, в которых для поиска указаны параметры в описаниях событий "Параметр: имя пользователя" и "Параметр: код возврата". В частности, не применяется установленное по умолчанию правило поиска "Подбор пароля".

3.6. Сервер безопасности

3.6.1. Установка сервера безопасности

323. Установка сервера невозможна, если в операционной системе включен механизм управления учетными записями (User Account Control — UAC).

> **Пояснение:** Если UAC включен, программа установки предложит отключить этот механизм. После установки ПО механизм можно снова использовать.

324. При установке сервера безопасности в качестве группы администраторов домена безопасности используйте группу, которая не является стандартной доменной группой администраторов. Рекомендуется использовать специально созданную группу пользователей.

325. Особенность обновления предыдущих версий. Если в домене безопасности имеется несколько серверов, процедуру обновления нужно начать с сервера, которому присвоена роль мастера схемы LDS домена безопасности. Обычно роль мастера схемы присвоена первому установленному серверу.

326. При обновлении сервера безопасности предыдущей версии процесс обновления нельзя прерывать и нужно довести до завершения. Если при замене модулей и модификации структур баз данных возникнут ошибки (например, по причинам недостаточных прав доступа или недоступности сервисов), возврат к предыдущему состоянию сервера (до обновления) будет невозможен. В этом случае потребуется либо вручную восстановить сервер предыдущей версии из резервной копии, либо заново установить сервер текущей версии без обновления. Минимально необходимые условия для успешного обновления:

- работоспособное состояние сервера безопасности предыдущей версии;
- наличие прав администратора леса доменов безопасности — при первом обновлении в лесу доменов;
- наличие прав администратора домена безопасности.

327. Если установка сервера безопасности выполняется на контроллере домена, программа установки создает доменного пользователя SecretNetLDS$ с ограниченными правами. Данная учетная запись является служебной и используется для запуска служб AD LDS при функционировании сервера безопасности.

328. При установке сервера безопасности изменяются некоторые параметры IIS (перечень см. в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление"). Восстановление исходных значений данных параметров запрещается.

329. Если установка ПО выполнялась с сетевого диска, то при запуске процедуры восстановления штатным способом (в окне "Установка и удаление программ" или "Программы и компоненты") программе установки потребуется доступ к ресурсу. При недоступности сетевого ресурса на экране появится запрос пути к каталогу с файлами дистрибутива.

330. При установке сервера безопасности с использованием существующей базы данных (оставшейся от ранее удаленного сервера) необходимо корректно указать учетные данные для подключения сервера к БД. Если пользователь указан неправильно (учетной записи с указанным именем в

СУБД не существует), после установки подключение сервера к базе данных будет невозможно. В этом случае необходимо сохранить корректные учетные данные в конфигурационном файле сервера с помощью программы OmsDBPasswordChange.exe. Описание процедуры изменения учетных данных для подключения СБ к серверу СУБД см. в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление".

3.6.2. Взаимодействие с другими компонентами

331. Сетевое соединение с сервером безопасности осуществляется через порт 443 (стандартный порт SSL). На стороне клиента порт выбирается динамически. На стороне сервера возможны следующие конфликты использования портов:

- если функционируют службы обновлений сервера SQL, ПО Apache, Skype, которые используют тот же порт. Сведения о привязке портов к процессам можно получить с помощью команды "netstat –aon";
- если сервер безопасности функционирует на компьютере под управлением ОС Windows Server 2012 R2 с включенным компонентом Work Folders для роли File and Storage Services. В этом случае для обеспечения соединения с сервером или остановите работу службы SyncShareSvc или смените порт, используемый по умолчанию компонентом Work Folders (см. https://blogs.technet.com/b/filecab/archive/2013/10/15/windows-server-2012-r2-resolving-port-conflict-with-iis-websites-and-work-folders.aspx).

332. При выполнении запросов к серверу безопасности возможно возникновение следующих ошибок: 1) 0x80070490 "Элемент не найден" ("Element not found"). 2) 0x00003E3 "Операция ввода/вывода была прервана из-за завершения потока команд или по запросу приложения" ("The I/O operation has been aborted because of either a thread exit or an application request"). Указанные ошибки могут происходить из-за потери сетевого соединения (физический разрыв, низкая пропускная способность) или по причине высокой загруженности компьютеров, на которых установлены и одновременно используются различные компоненты системы Secret Net Studio.

Рекомендации: Для налаживания бесперебойной работы рекомендуется:

1. Не использовать контроллер домена в качестве сервера безопасности.
2. Распределить IIS и сервер СУБД по различным компьютерам.
3. Не запускать на компьютере с сервером безопасности программу управления.
4. В программе управления увеличить значения следующих параметров для сервера безопасности, агентов и самой программы: "Время ожидания разрешения имен DNS", "Время ожидания соединения с сервером", "Время ожидания отправки запроса на сервер", "Время ожидания начала передачи следующего блока", "Время ожидания события для рабочей станции" и "Время ожидания сервером ответа на контрольный запрос".

333. При возникновении ошибок типа "класс не зарегистрирован" ("class not registered") во время получения журнала или отчета, либо ошибок применения групповых политик "AsyncCallbackApplyPoliciesCommand() Ошибка:Unknown error 0xE06D7363..." это может быть связано с отсутствием компонента MS XML Parser нужной версии. Для устранения ошибок установите указанный компонент версии 6.0 или выше. Установку компонента можно выполнить с установочного диска системы Secret Net Studio из каталога \Tools\Microsoft\Prerequisites\.

334. Сертификат сервера безопасности в хранилище объектов централизованного управления должен совпадать с сертификатом, установленным в IIS. При замене сертификата в IIS его необходимо синхронизировать и в хранилище объектов ЦУ. Процедура выполняется в программе генерации сертификатов, входящей в состав ПО сервера безопасности.

335. Для работы сервера безопасности на сервере IIS нельзя использовать несколько рабочих процессов для пула приложений (определяется в оснастке управления IIS) — иначе при соединении с сервером безопасности будет возникать ошибка 0x000005B4. При возникновении данной ошибки проверьте значение параметра "Maximum number of worker processes" в диалоговом окне настройки DefaultAppPool, вкладка Performance, и при необходимости укажите значение 1.

336. При значительной нагрузке на сервер безопасности (порядка 3000 подключенных агентов и более) возможны отказы в обслуживании со стороны сервера IIS, если задано недостаточное значение для параметра appConcurrentRequestLimit. Данный параметр определяет максимальное количество одновременных запросов к IIS.

Рекомендации: Если при попытках соединения с сервером безопасности на клиентах возникает ошибка HTTP 503.2 "Concurrent request limit exceeded", увеличьте значение параметра appConcurrentRequestLimit на сервере IIS. Например, укажите значение 100 000 (по умолчанию 5 000). Для этого в режиме командной строки введите команду: %windir%\System32\inetsrv\appcmd.exe set config /section:serverRuntime /appConcurrentRequestLimit:100000

337. После удаления сервера безопасности все подчиненные ему агенты становятся "свободными" только при наличии в этом же домене безопасности другого сервера. Если удаляется последний сервер

в домене безопасности, данные о подчиненных ему компьютерах удаляются вместе с хранилищем, и эти компьютеры не будут отображаться в структуре в качестве свободных.

338. Для подключения к серверу безопасности компонентов управления (программ управления, агентов, дочерних серверов) требуется доступный DNS-сервер.

> **Рекомендации:** Следите, чтобы в сети всегда был доступен сервер DNS.

339. В некоторых случаях при перезагрузке или выключении компьютера оповещение сервера безопасности об этом не выполняется. Это приводит к невозможности подключения компьютера к серверу безопасности в течение 2–3 минут после предыдущего прекращения работы.

3.6.3. Обработка данных

340. Процедура архивирования журналов зависит от объема данных и может продолжаться до нескольких часов. При интенсивном наполнении журналов рекомендуется достаточно часто выполнять запуск процедуры архивирования (один раз в неделю и чаще).

341. Запрещается удалять права на запись в каталог для хранения временных файлов сервера безопасности (каталог указывается при установке сервера), предоставленные учетной записи "Network Service".

342. Информация о событиях Тревога отправляется получателю почтовой рассылки блоками. В блок попадают события Тревога, произошедшие примерно в одно и тоже время на рабочей станции. Если хотя бы одно из событий подходит под условие отправки почтового уведомления, то получателю отправляется весь блок Тревога.

343. Сервер безопасности использует параметры формата даты и времени, заданные для системной учетной записи. Если параметры изменены для учетной записи пользователя, чтобы их применить на сервере безопасности необходимо выполнить операцию копирования параметров в системную учетную запись. Для копирования параметров текущего пользователя откройте диалоговое окно настройки с помощью ярлыка "Региональные стандарты" в Панели управления, перейдите к диалогу "Дополнительно", нажмите кнопку "Копировать параметры" и в появившемся диалоге установите отметку в поле "Экран приветствия и системные учетные записи".

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	(495) 982-30-20
E-mail:	info@securitycode.ru
Web:	https://www.securitycode.ru