Средство защиты информации Secret Net Studio
Комментарии к версии 8.10.18997.0

Данный документ содержит описание новых возможностей СЗИ Secret Net Studio версии 8.10.18997.0 по сравнению с версиями 8.9.18390.00, 8.8.15891.00, 8.7.12011.0, 8.6.8330.0, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации СЗИ Secret Net Studio.

Оглавление

1. Комплект поставки

1.1. Размещение файлов в установочном комплекте

Каталог	Содержимое
\Setup\Server\	дистрибутивы сервера безопасности
\Setup\Console\	дистрибутивы программ 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 8.10.18997.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.10.18997.0 по сравнению с версией 8.9.18390.0.

2.1.1. Общесистемные

1. Обеспечена поддержка Windows 10 версии 22H2, Windows 11 версии 22H2.

2. Обновлен логотип продукта.

2.1.2. Базовая и локальная защита

3. Реализована новая политика механизма защиты входа в систему – "Контроль аутентификации". Политика позволяет использовать модуль входа СЗИ Secret Net Studio наряду с модулями входа других провайдеров либо отключить его и использовать только сторонние модули входа.

4. Реализована совместимость со сторонним провайдером входа ID-Logon.

5. Повышена производительность подсистемы полнодискового шифрования.

6. Оптимизирована работа с централизованным хранилищем AD/LDS.

7. Реализована возможность отправки локальных журналов на сторонний syslog-сервер.

2.1.3. Антивирус и средство обнаружения и предотвращения вторжений

8. В СОВ добавлена база опасных веб-ресурсов от компании "Код Безопасности". База может использоваться отдельно или вместе с базой от компании "Лаборатория Касперского".

2.1.4. Межсетевой экран и авторизация сетевых соединений

9. Для фильтрации сетевого трафика МЭ больше не использует NDIS фильтр (LWF). Вся фильтрация осуществляется средствами современной платформы ОС Windows Filtering Platform (WFP). В результате повышена совместимость со сторонним ПО, расширены возможности обработки сетевого трафика.

2.2. Версия 8.9.18390.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.9.18390.0 по сравнению с версией 8.8.15891.00.

2.2.1. Общесистемные

10. Реализована возможность создания автономного пакета установки для развертывания СЗИ Secret Net Studio.

11. Реализована возможность развертывания СЗИ Secret Net Studio через сервер обновлений. Если не планируется использовать данную функцию, можно отключить обновление дистрибутивов и пакетов исправлений в Сервере обновлений.

2.2.2. Базовая и локальная защита

12. Реализована поддержка аппаратных средств аутентификации RuToken ЭЦП 3.0, RuToken ЭЦП 3.0 NFC, RuToken Lite.

13. Реализована новая политика механизма защиты входа в систему – "Запрет смены пользователя без перезагрузки". При включенном параметре для смены пользователя или завершения сеанса пользователя необходима перезагрузка компьютера.

14. Реализован новый параметр в парольной политике СЗИ Secret Net Studio – "Минимальное число измененных символов нового пароля".

15. Реализована возможность записи нулевого пароля в идентификатор в совместном режиме работы с ПАК "Соболь". Теперь при присвоении пользователю идентификатора необязательно вводить пароль пользователя, совпадающий с паролем для входа в ОС Windows.

16. Реализована защита от подмены VID и PID устройств в механизме контроля устройств.

2.2.3. Антивирус и средство обнаружения и предотвращения вторжений

17. Подсистема антивируса теперь устанавливается без начальных антивирусных баз. Для получения антивирусных баз необходимо настроить получение обновлений.

2.3. Версия 8.8.15891.00

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.8.15891.00 по сравнению с версией 8.7.12011.0.

2.3.1. Общесистемные

18. Secret Net Studio подписан WHQL-сертификатом Microsoft.

19. Обеспечена поддержка Windows 10 версии 21H1, Windows 11, Windows Server 2022.

2.3.2. Базовая и локальная защита

20. Реализована возможность импорта учетных записей доменных пользователей Windows AD в базу Secret Net Studio с помощью утилиты.

21. Реализована поддержка аппаратных средств аутентификации JaCarta PKI/BIO, R301 Foros, Guardant ID 2.0.

22. Исключена поддержка аппаратного средства аутентификации Secret Net Card.

2.3.3. Межсетевой экран и авторизация сетевых соединений

23. Реализована возможность импорта и экспорта правил МЭ с помощью утилиты.

2.3.4. Центр управления

24. Расширена возможность фильтрации табличного вида компьютеров.

25. Реализована возможность копирования в буфер обмена имен компьютеров на панели управления компьютерами.

26. Повышено удобство использования окна редактирования структуры оперативного управления.

2.4. Версия 8.7.12011.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.7.12011.0 по сравнению с версией 8.6.8330.0.

2.4.1. Общесистемные

27. Обеспечена поддержка обновления Windows 10 Spring 2020 Update (2004).

28. Обеспечена поддержка обновления Windows 10 Fall 2020 Update (2010).

29. Обеспечена поддержка Windows 10 Enterprise 2019 LTSC (1809).

30. Реализована усиленная аутентификация через сервер аутентификации при функционировании Secret Net Studio в сетевом режиме. В стандартном режиме аутентификации все компоненты защиты доверяют аутентификации ОС Windows.

31. Доработана схема лицензирования компонентов Secret Net Studio. Активация лицензий осуществляется автоматически посредством обращения к серверу активации с помощью Центра управления либо полуавтоматически через Личный Кабинет.

32. Реализована поддержка использования кумулятивных патчей. Кумулятивный патч для msi-пакета включает в себя все ранее выпущенные и предназначенные для широкого использования патчи данного msi-пакета.

33. Обеспечена возможность пакетного применения патчей (обычных и кумулятивных).

34. Обеспечена возможность централизованного управления лицензиями Secret Net LSP с сервера безопасности Secret Net Studio.

35. Теперь Secret Net Studio выпускается на русском, английском и испанском языках.

2.4.2. Базовая и локальная защита

36. Реализован механизм полнодискового шифрования данных на дисках. Механизм работает на системах с режимом загрузки UEFI. Поддерживается шифрование системных и несистемных разделов жестких дисков со структурой разделов GPT, а также шифрование несистемных разделов жестких дисков со структурой разделов MBR.

37. Обеспечена интеграция клиента Secret Net Studio с модулем обнаружения утечек, разработанным ИСП РАН.

38. Обеспечена интеграция клиента Secret Net Studio с механизмом песочницы стороннего разработчика.

39. Реализована возможность централизованной активации механизма защиты дисков.

40. В программе управления КЦ-ЗПС добавлена возможность расчета контрольных сумм по алгоритму ГОСТ Р 34.11-2012.

41. Реализована возможность экспорта данных механизма "Паспорт ПО" в csv-файл.

42. Реализовано отображение пользователям сообщений о необходимости перезагрузки компьютера при подключении/отключении подсистем и некоторых политик (самозащита, контроль потоков, запрет вторичного входа в систему и др.), требующих перезагрузки.

43. Реализована возможность генерации тревоги в Центре управления при интерактивном отключении защитных подсистем (вне зависимости от наличия защиты от локального администратора).

44. Реализована поддержка входа пользователя в систему по графическому паролю ОС Windows.

45. Реализована поддержка входа пользователя в систему по Windows Live ID.

46. Оптимизирована работа механизма самозащиты в части уменьшения потребления системных ресурсов, ускорения выполнения файловых операций.

47. Реализован детализированный аудит изменения политик. Регистрируются старое и новое значение следующих политик:

- настройки подсистемы затирания данных;
- настройки исключений затирания данных;
- настройки аудита;
- привилегии пользователей;
- настойки журнала;
- настройки секретных ключей;
- настройки паролей;
- список устройств;
- список принтеров;
- настройки входа в систему;
- настройки блокировки;
- настройки полномочного управления доступом;
- названия категорий;
- режим механизма самозащиты.

48. Реализована идентификация действий администратора в системе. В столбце "Пользователь" событий журналов отображается учетная запись пользователя, запустившего административные команды.

49. Реализована передача парольных политик Secret Net Studio, установленных в режиме усиленной аутентификации, в ПАК "Соболь".

2.4.3. Межсетевой экран и авторизация сетевых соединений

50. Обеспечена поддержка авторизации сетевых соединений средствами ОС Windows. Авторизация сетевых соединений осуществляется средствами ОС в том случае, если на клиенте Secret Net Studio включен стандартный режим аутентификации пользователя.

51. Реализована возможность настройки контроля состояния соединений (Stateful Packet Inspection, SPI) через Центр управления. Настройки SPI позволяют включить/отключить отслеживание состояния соединений и блокирование соединений при их несоответствии таблице состояний.

2.4.4. Антивирус и средство обнаружения и предотвращения вторжений

52. Осуществлен переход на драйвер KAV SDK, предоставляемый компанией "Лаборатория Касперского".

53. Обеспечена возможность удаления зажатых активными процессами вредоносных файлов при перезагрузке компьютера.

54. В профилях сканирования антивируса добавлена возможность указания неполных имен расширений файлов, по отношению к которым необходимо осуществлять проверку. Указание неполных имен осуществляется с использованием символов «*» и «?».

55. Реализовано отображение хэш-сумм отправленных в карантин файлов в блоке "Карантин".

56. Механизм почтового антивируса дополнен следующими возможностями:

- поддержка нескольких почтовых ящиков в Microsoft Outlook;
- поиск вирусов во вложенных объектах;
- изменение способа наименования папок с зараженными письмами;
- в случае отсутствия результатов сканирования в течение 1 минуты доступна страница предпросмотра с уведомлением о проблемах в работе почтового антивируса.

57. Реализовано отображение тревоги в системной области панели задач ОС Windows в случае обнаружения вредоносного файла при сканировании по расписанию.

58. Реализовано отображение подробной информации о результатах последнего сканирования в Центре управления на вкладке "Антивирус".

59. Реализована возможность централизованного отката обновлений баз сигнатур антивируса, СОВ и Безопасной среды Secret Net Studio на локальном Сервере обновлений с последующим их откатом на клиенте.

2.4.5. Центр управления

60. Реализован экспорт и импорт списка имен рабочих станций для возможности их подчинения (или вывода из подчинения) серверу безопасности, а также для добавления агентов оперативного управления.

61. Реализовано административное управление сессиями и питанием компьютеров через Центр управления. Доработаны события аудита, отражающие выполнение команд оперативного управления (выключение компьютера, перезагрузка компьютера, завершение сессии пользователя).

2.5. Версия 8.6.8330.0

Данный раздел содержит описание новых возможностей СЗИ Secret Net Studio версии 8.6.8330.0 по сравнению с версией 8.5.5329.0.

2.5.1. Общесистемные

62. Обеспечена поддержка обновления Windows 10 Spring 2019 Update (1903).

63. Обеспечена поддержка обновления Windows 10 Fall 2019 Update (1909).

64. Обеспечена поддержка обновления Windows 10 2004 (20H1).

65. Реализована возможность организации федерации – иерархической структуры лесов доменов безопасности. В федерацию можно добавлять леса доменов безопасности на основе несвязанных лесов доменов Windows AD.

66. Реализована возможность централизованного развертывания СЗИ Secret Net Studio с использованием System Center Configuration Manager 2012, 2016.

67. Реализована работа с терминальными клиентами MS RDP for Mac и ПО тонкого клиента Dell Wyse 5010.

68. Реализована интеграция СЗИ Secret Net Studio с KeyBox.

69. Группа команд Secret Net Studio добавлена в контекстное меню файлов в сторонних файловых менеджерах (Total Commander, Far Manager, FreeCommander, Midnight Commander, Double Commander, XYplorer).

2.5.2. Базовая и локальная защита

70. Доработан механизм самозащиты: реализована защита от локального администратора, обеспечивающая разграничение прав и привилегий между Администратором безопасности и Администратором IT на локальное управление СЗИ Secret Net Studio.

71. Реализована поддержка идентификаторов Guardant ID, Rutoken 2151, Rutoken ЭЦП 2.0 Touch, Rutoken ЭЦП 2.0 Flash Touch, vdToken и смарт-карты Rutoken 2151.

72. Реализована поддержка входа при отключенной политике "Disable Ctrl-Alt-Del".

73. Реализована возможность задания временного интервала блокировки компьютера (в минутах) в случае достижения установленного максимального количества попыток ввода неправильного пароля.

74. В журналах Secret Net Studio для события затирания данных на жестких дисках теперь указывается серийный номер устройства.

75. Реализована работа в совместном режиме с ПАК "Соболь" версии 4.3 в связке с аппаратными средствами аутентификации Guardant ID и ESMART.

76. Реализована возможность сокрытия файлов (в том числе их названий), имеющих метку конфиденциальности выше, чем уровень допуска пользователя и/или текущий уровень сессии пользователя.

77. В механизме "Паспорт ПО" реализован расчет контрольных сумм в соответствии с ГОСТ Р 34.11-2012.

78. В механизме защиты диска реализована возможность создания диска аварийного восстановления на USB-носителе на материнских платах с UEFI.

79. Реализована интеграция модуля входа СЗИ Secret Net Studio с модулем входа ПО Indeed AM.

2.5.3. Межсетевой экран и авторизация сетевых соединений

80. Реализована поддержка сетевого входа на компьютер с компьютера из домена другого леса.

81. Реализована блокировка телеметрии Windows.

2.5.4. Антивирус и средство обнаружения и предотвращения вторжений

82. Повышена производительность антивируса за счет повышения скорости выполнения операции копирования файлов.

83. Реализован клиентский почтовый антивирус, который выполняет фильтрацию вредоносных писем (входящих и исходящих).

84. Расширен перечень настроек профилей сканирования антивируса. Добавлена возможность настройки максимального времени сканирования файлов, параметров сканирования архивов, списка игнорируемых расширений.

85. Реализовано детализированное сканирование по вызову контекстного меню при антивирусной проверке. Теперь пользователю доступна информация о прогрессе выполнения сканирования, продолжительности сканирования, количестве проверенных объектов. По окончании проверки можно ознакомиться с результатами.

86. Реализована возможность работы модуля СОВ на компьютерах с установленным гипервизором.

2.5.5. Центр управления

87. Реализована возможность централизованного управления защищаемыми компьютерами из дочерних лесов доменов безопасности в структуре лесов доменов безопасности, организованной на основе несвязанных лесов доменов Windows AD.

88. Добавлены шаблоны политик для ИСПДн 4 уровня защищенности; ИС Банка России для уровней защиты информации до УЗ-1 включительно; АСУ ТП классов защищенности до К1 включительно; значимых объектов КИИ до 1 категории значимости включительно; ИС, предназначенных для обработки биометрических персональных данных, для стандартного (ЕБС-2) и усиленного (ЕБС-1) уровней защиты информации.

89. Реализовано централизованное управление групповыми политиками подсистемы входа для клиентов с установленным СЗИ Secret Net LSP.

90. Добавлен новый реквизит для учетных записей пользователей – "Тип учетной записи".

91. В журналах Secret Net Studio добавлен столбец с указанием сквозного порядкового номера события.

92. Реализована возможность использования быстрых клавиш для навигации, раскрытия/закрытия узлов дерева, выполнения команд контекстного меню на объекте Контроля устройств.

93. Реализована поддержка групповых операций в Контроле устройств (выбор нескольких устройств в рамках одного класса и назначение параметров контроля/доступа на выбранные устройства).

94. Реализовано автоматическое повторное подключение Центра управления к серверу безопасности, если соединение было разорвано.

95. Изменено отображение компьютеров, удаленных из AD: теперь вместо SID указываются их имена. Восстановление имен по SID выполняется по базе данных сервера аутентификации.

2.5.6. Сервер безопасности

96. Добавлена новая роль для сервера безопасности – шлюз. Шлюз обеспечивает взаимодействие двух серверов безопасности, находящихся в разных и несвязанных лесах доменов безопасности Secret Net Studio.

3. Особенности работы и ограничения

3.1. Базовая и локальная защита

3.1.1. Установка клиента

97. При обновлении Secret Net Studio с версии 8.6 до версии 8.8 в журнале могут регистрироваться ошибки обновления конфигурации агента межсетевого экрана.

98. При обновлении сервера безопасности с более ранних версий продукта до версии 8.7 будет включен режим совместимости для поддержки защищенного соединения между клиентами 8.7 с клиентами более ранних версий продукта. При установке сервера безопасности 8.7 политика режима совместимости по умолчанию будет выключена.

> **Рекомендации:** После обновления всей инфраструктуры Secret Net Studio до версии 8.7 установите значение политики ISAKMPLegacySupport в состояние No с помощью утилиты ScAuthSrvConfig.exe. Для этого на сервере безопасности откройте командную строку и выполните команду:
>
> c:\Program Files\Secret Net Studio\Server\Authentication Server\ScAuthSrvConfig.exe <DOMAIN> /a <administrator> /p <password> /q "set gp ISAKMPLegacySupport 0"
>
> где:
>
> <DOMAIN> - домен безопасности;
>
> <administrator> - имя администратора домена безопасности;
>
> <password> - пароль администратора.
>
> При использовании учетных данных пользователя Secret Net Studio в утилите ScAuthSrvConfig.exe возможно возникновении ошибки "Error: (0x80040505) Bad principal name". В этом случае необходимо выполнить синхронизацию пользователя с базой данных Secret Net Studio. Для этого в программе управления пользователями вызовите контекстное меню пользователя и выберите команду "Синхронизировать с системой защиты".

99. Перед установкой клиента Secret Net Studio необходимо установить пакеты обновлений для ОС, указанные в требованиях к аппаратному и программному обеспечению (см. документ "Secret Net Studio. Руководство администратора. Установка, управление, мониторинг и аудит").

100. 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.

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

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

102. 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).

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

104. 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.

105. 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.

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

107. 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.

108. Если на двух и более серверах создать задание на установку клиента на один и тот же компьютер, то в результате у агента может быть неверно установлен сервер подчинения. Сервером подчинения будет назначен тот сервер, который выполнит задание последним. Получится ситуация, когда агент не сможет подключиться к нужному серверу, так как сервер подчинения, прописанный на стороне агента, не будет соответствовать серверу подчинения, записанному в базе сервера.

Во избежание описанной ситуации нельзя запускать централизованную установку клиента с нескольких серверов одновременно. Необходимо действовать следующим образом:

- определить, какому серверу должен быть подчинен агент. У агента эта информация находится в ключе реестра "\HKEY_LOCAL_MACHINE\SOFTWARE\Infosec\Secret Net 5\LDS\srvName";
- вручную подчинить агент данному серверу;
- если сервер подчинения на агенте выставлен неверно, то необходимо перевести агент в автономный режим, а затем перевести его в сетевой режим с подчинением нужному серверу.

109. При централизованной установке или удалении клиента на компьютерах с серверной ОС автоматическая перезагрузка компьютера по истечении заданного в задании времени ожидания может в некоторых случаях не выполняться.

110. При централизованном удалении клиентов через сервер безопасности в случае потери связи клиента с сервером безопасности возможно отображение ошибки в Центре управления: "Деинсталляция произведена не корректно. Возможно, из-за перезагрузки сервера". Как правило, при этом клиент деинсталлируется в штатном режиме, а оставшуюся учетную запись клиента SNS на сервере безопасности можно удалить в ручном режиме через диалог конфигурирования иерархии управления.

111. 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.

112. 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).

113. 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 Центре 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.

114. Невозможна централизованная установка клиента Secret Net Studio на компьютер под управлением ОС Windows Server 2012 и выше с установленным сервером безопасности, на котором инициировано задание установки.

> **Рекомендации:** Для корректной установки клиента Secret Net Studio отключите Remote UAC Restriction и создайте новое задание на установку. Инструкция по отключению Remote UAC Restriction приведена на сайте Microsoft (https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows).
>
> Также вы можете выполнить установку клиента Secret Net Studio в интерактивном режиме.

115. При повторной централизованной установке пакета исправлений, который ранее уже был установлен, в детальном описании процесса установки может появляться некорректное сообщение об ошибке. При этом установка успешно выполняется.

116. В некоторых случаях служба обновлений ОС может мешать скачиванию дистрибутива Secret Net Studio. Если в момент поступления задания на обновление Secret Net Studio у службы обновлений ОС есть задание на установку/загрузку какого-то обновления, то возможность загрузки обновления Secret Net Studio временно блокируется до тех пор, пока не будет установлено обновление ОС.

3.1.2. Общее

117. 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.

118. 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).

119. 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.

120. При создании криптоконтейнера Secret Net Studio в файловом менеджере Total Commander наряду с основным файлом криптоконтейнера создается дополнительный файл ("Новый SnCrCont.Document") в связи с особенностями данного файлового менеджера.

121. 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*>\...".

122. 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.

123. В системах с медленными каналами связи при обращениях компонентов 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.

124. 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.

125. Secret Net Studio не поддерживает проекцию доменов безопасности из разных лесов безопасности на один и тот же контейнер AD (организационное подразделение или домен). Если это допустить, то возможно некорректное отображение управляемой иерархии.

126. Не допускается создавать в домене Windows AD два леса безопасности Secret Net Studio, которые в дальнейшем будут подчиняться серверу, находящемся в другом лесе безопасности в рамках федерации.

127. Не гарантируется стабильная работа Secret Net Studio с технологией перемещаемых профилей пользователей.

128. С целью дополнительно не нагружать ресурсы компьютера не рекомендуется на контроллер домена устанавливать следующие механизмы Secret Net Studio:

- замкнутая программная среда;
- полномочное управление доступом;
- контроль печати;
- защита дисков и шифрование данных;
- полнодисковое шифрование;
- обнаружение и предотвращение вторжений.

При этом следует исходить из предположения, что на контроллере домена работают только администраторы.

3.1.3. Локальное и централизованное управление

129. 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.

130. 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.

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

131. Если для журнала Secret Net Studio установлен режим очистки вручную и активирована системная настройка "Немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности" — в случае переполнения журнала записями на компьютере будет инициирован системный сбой (BSOD). Для возобновления нормальной работы необходимо загрузить ОС в безопасном режиме, очистить журнал и отключить указанную системную настройку.

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

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

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

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

134. 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.

135. 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.

136. 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.

137. 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).

138. 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.

139. 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.

140. 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".

141. 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").

142. 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 Локального центра управления 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 Локальном центре управления 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.

143. При доступе к содержимому теневого хранилища, выполняется мониторинг запрашиваемых прав доступа и, если клиентское программное обеспечение пытается открыть содержимое теневого

хранилища с правами, допускающими его модификацию или удаление, то такие запросы будут запрещены. Для осуществления доступа к содержимому его следует запрашивать посредством журнала SNS и копировать полученные файловые объекты в удобное для их последующего анализа место. Доступ предоставляется только пользователям, обладающим привилегией просмотра журнала SNS.

144. 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

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

146. 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".

147. В режиме усиленной аутентификации по паролю если пароль пользователя для входа в ОС Windows не синхронизирован с паролем в базе данных Secret Net Studio, то при следующем входе пользователя система предложит процедуру синхронизации паролей.

148. Если при функционировании Secret Net Studio в сетевом режиме и включенной усиленной аутентификации в Windows AD было изменено имя пользователя, для обеспечения входа данного пользователя в систему необходимо в программе "Управление параметрами безопасности пользователей" Secret Net Studio для переименованной (новой) записи вызвать команду "Синхронизировать с системой защиты".

149. 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".

150. При обновлении до версии 8.7 с версий ниже для использования учетных записей Майкрософт необходимо вручную отключить действие стандартной политики "Учетные записи: блокировать учетные записи Майкрософт" (Accounts: Block Microsoft accounts).

151. 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.

152. 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.

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

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

154. При входе в систему по сертификату дополнительно запрашивается пароль пользователя, если в 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.

155. 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.

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

157. При входе в систему под учетной записью Майкрософт (LiveID) вход по идентификатору будет работать только если компьютер введен в домен.

158. Если при включенном механизме контроля потоков, в момент входа в систему под учетной записью Майкрософт (LiveID), отсутствует диалог выбора уровня конфиденциальности текущего сеанса, то необходимо в настройках отключить требование выполнения входа с помощью Windows Hello для учетных записей Майкрософт.

159. Если включен мягкий режим контроля аутентификации, то модуль входа Secret Net Studio позволяет войти в систему по паролю в режиме идентификации пользователя «Только по идентификатору».

160. Если включен мягкий режим контроля аутентификации и на терминальном клиенте не отключен запрос учетных данных, то терминальный вход в систему автоматически выполняется через модуль входа ОС Windows.

3.1.5. Подсистема контроля целостности

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

162. 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>.

163. 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.

164. 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").

165. 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.

166. Не поддерживается расчет эталонных значений для файлов на сетевом диске.

3.1.6. Подсистема замкнутой программной среды

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

168. 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.

169. 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".

170. 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.

171. 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.

172. 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.

173. Механизм контроля скриптов функционирует в полном объеме для браузера Microsoft Edge предыдущего поколения. Для более новых версий Microsoft Edge с движком Chromium работа механизма не обеспечивается.

174. 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.

175. 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).

176. 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").

177. 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.

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

179. 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

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

181. 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.

182. 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).

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

184. 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.

185. 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.

186. Если модель данных содержит более 250000 объектов, при ее сохранении в Центре 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.

187. 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.

188. 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

189. 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.

190. 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.

191. Доступ к файловому объекту осуществляется, исходя из фактического токена потока, выполняющего запрос на доступ. Таким образом, если ОС или приложение использует ограниченный токен доступа, то доступ со стороны подсистемы дискреционного управления доступом может быть не предоставлен из-за отсутствия в токене групп, для которых выданы разрешения.

Примером подобной проблемы может быть запрет доступа из процесса explorer к каталогу, для которого предоставлен доступ системным администраторам при включенном UAC. В эффективном токене будет отсутствовать группа "Администраторы". Решением проблемы может служить предоставление прав доступа на папку для отдельной созданной группы, куда будет добавлен пользователь.

Описанное поведение является особенностью работы операционной системы.

3.1.9. Полномочное управление доступом

192. Большое количество файловых объектов (более 200 тысяч) с уровнями конфиденциальности выше "Неконфиденциально" и/или с метками подсистемы дискреционного управления доступом следует распределять по нескольким рабочим станциям или файловым серверам.

193. 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).

194. 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.

195. 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".

196. 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.

197. 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.

198. 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.

199. 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".

200. 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.

201. 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.

202. 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.

203. 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.

204. 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).

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

206. 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".

207. На компьютере под управлением ОС Windows 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.

208. 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.

209. 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 исклю-

чение 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.

210. 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

211. 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.

212. 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).

213. 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.

214. 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).

215. 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).

216. 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.

217. 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.

218. 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.

219. 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".

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

221. Некоторые приложения могут попытаться произвести печать, минуя виртуальный драйвер принтера. В этом случае произойдет фактический запрет печати (без тревоги). Для решения этой проблемы будет достаточно в приложении, из которого производится печать, в списке принтеров выбрать виртуальный принтер и произвести на него печать.

3.1.11. Контроль устройств

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

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

224. 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.

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

226. 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 из-

менении 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.

227. 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.

228. 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.

229. 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".

230. 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.

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

232. 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.

233.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.

234. 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”.

235. Ряд электронных идентификаторов (например, RuToken ЭЦП Flash 2.0) являются составными устройствами, включающими в себя, кроме электронного идентификатора, еще и устройство хранения. Ряд из них в случае запрета подключения устройства хранения также не будут подключены. Для таких устройств рекомендуется не запрещать подключения устройств хранения, входящих в такое составное устройство, а вместо этого использовать механизм разграничения доступа к устройствам.

236. 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).

237. 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.

238. 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".

239. 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.

240. 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.

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

242. 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.

243. 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.

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

245. 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.

246. 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.

247. 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.

248. 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 КБайт).

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

250. 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.

251. Для сетевых плат и устройств аппаратной поддержки Secret Net Studio во время спящего режима не фиксируется изменение аппаратной конфигурации. Во время работы допускается отклю-

чение и подключение ранее утвержденного адаптера без регистрации событий отключения и подключения.

252. 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".

253. 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.

254. 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.

255. Если в ОС настроена политика "Аудит доступа к объектам" (значение "Определить: Отказ" и/или "Определить: Успех") и при этом в подсистеме контроля устройств СЗИ Secret Net Studio для устройств CD/DVD или Floppy Drive применена политика "Блокировать рабочую станцию при изменении устройства", то при форсированном применении групповых политик ОС и СЗИ Secret Net Studio компьютер будет блокироваться с событием изменения аппаратной конфигурации. Это связано с особенностями работы ОС: при применении указанной выше политики "Аудит доступа к объектам" ОС выполняет отключение и повторное подключение некоторых устройств.

Примечание: Проблема актуальна для СЗИ Secret Net Studio версии 8.5 и выше.

Рекомендации: Во избежание блокировки компьютера при форсированном применении групповых политик ОС предварительно переведите политику "Аудит доступа к объектам" в значение "Не определено".

3.1.12. Подсистема аппаратной поддержки

256. USB-ключи и смарт-карты JaCarta PRO и Jacarta-2 PRO/ГОСТ отображаются в программе управления пользователями как eToken Pro. Это связано с одинаковой элементной базой у данных устройств. В Центре управления (в централизованном и локальном режимах работы) названия этих устройств отображаются правильно.

257. В Secret Net Studio отсутствуют специальные функции смены PIN-кода в USB-ключах и смарт-картах.

Рекомендации: Чтобы сменить PIN-код (пароль) в USB-ключе или смарт-карте, используйте ПО изготовителя устройства.

258. При установке и смене PIN-кода в ПО изготовителя устройств для следующих USB-ключей и смарт-карт необходимо использовать указанные программные модули (апплеты):

- JaCarta PKI/ГОСТ, Jacarta-2 PRO/ГОСТ, Jacarta-2 PRO/ГОСТ SC — апплет PKI;
- JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ — апплет ГОСТ.

259. 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.

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

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

262. Если инициализация идентификатора eToken выполняется средствами 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.

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

264. Идентификаторы (например, USB-ключи), подключенные локально к терминальному серверу с установленным клиентом Secret Net Studio, будут недоступны в терминальной сессии при терминальном подключении с удаленного компьютера, на котором также установлен клиент Secret Net Studio. В этом случае, например, с такого идентификатора нельзя загрузить закрытые ключи для доступа к криптоконтейнерам.

265. На компьютерах с установленным клиентом 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.

266. 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).

267. При инициализации идентификатора Guardant ID средствами Secret Net Studio в окне запроса PIN-кода введите новый PIN-код для данного идентификатора. Таким образом, инициализация идентификатора позволяет сменить его PIN-код.

268. Если на идентификаторах JaCarta установлен пустой PIN-код, то данный идентификатор невозможно присвоить пользователю.

> **Рекомендации:** Для использования идентификаторов JaCarta инициализируйте режим пользователя с помощью ПО изготовителя устройства и установите PIN-код.

3.1.13. Затирание данных

269. Не гарантируется успешная работа механизма 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.

270. Если включен механизм затирания данных, могут возникать задержки при определении впервые подключаемых USB-устройств (например, USB-флеш-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.

271. 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.

272. 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

273. При создании загрузочного диска аварийного восстановления на USB-флеш-накопителе объемом более 4 Гбайт видимый объем диска после форматирования будет ограничен 4 Гбайт. 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.

274. При использовании загрузочного диска аварийного восстановления на компьютерах с режимом загрузки EFI и установленным Secret Net Studio версий 8.5 и 8.6 необходимо отключать функцию Secure Boot.

275. 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.

276. 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-флеш-накопителя может не поддерживаться виртуальной машиной.

277. При загрузке с диска аварийного восстановления не поддерживается работа клавиатуры с интерфейсом PS/2.

278. При удалении СЗИ Secret Net Studio с включенным механизмом защиты дисков загрузчик Secret Net Studio остается в системе. Это не влияет на дальнейшую работу ОС.

279. При восстановлении системы в точку восстановления до установки Secret Net Studio необходимо предварительно расшифровать зашифрованные диски и снять защиту с защищенных дисков, если таковые имеются.

280. При последовательном отключении подсистем защиты диска и полнодискового шифрования выключение последней подсистемы может происходить с задержкой до нескольких минут.

281. Если системный раздел жесткого диска защищен подсистемой защиты дисков, то при выходе из строя загрузчика подсистемы полнодискового шифрования его автоматическое восстановление будет невозможно. В таком случае для восстановления загрузчика необходимо будет отключить защиту системного раздела с помощью диска аварийного восстановления.

3.1.15. Теневое копирование

282. 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).

283. 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.

284. 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.

285. 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%. Secret Net Studio блокирует запись на оптические диски средствами сторонних производителей.

3.1.16. Контроль приложений

286. 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.

287. На компьютере под управлением 64-разрядной версии ОС при запуске пользователем 32-разрядных процессов, для которых указано "запускать только под администратором", в журнале Secret Net Studio может регистрироваться предупреждение. На работоспособности СЗИ и ОС это предупреждение никак не сказывается и связано с особенностью реализации операционной системой повышения прав доступа для таких процессов.

3.1.17. Запрет вторичного входа в систему

288. 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.

289. 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.

290. Для блокирования возможности запуска приложений от имени администратора принудительно изменяется значение стандартного параметра безопасности ОС Windows "Контроль учетных записей: 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.

291. 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.

3.1.18. Самозащита

292. При включенном механизме самозащиты операция восстановления ОС из точки восстановления выполняется с ошибкой. Проблему можно решить, переключив механизм в аварийный режим перед восстановлением.

3.2. Доверенная среда

293. Функционирование ДС на ОС Windows 11 и Widows Server 2022 обеспечивается при установке патча sns88te024.

294. Во время штатного завершения сессии пользователя, перезагрузки или выключения компьютера выполняется принудительная остановка процессов со стороны ОС Windows, которую доверенная среда (ДС) не можем отличить от принудительной остановки процессов злоумышленником. ДС предотвращает завершение процессов, в журнале ДС регистрируется событие попытки завершения, но при этом ОС Windows корректно завершает сессию пользователя или работу компьютера.

295. Описание других особенностей работы, ограничений и рекомендаций содержится в приложении документа "Руководство администратора. Настройка и эксплуатация" из комплекта поставки Secret Net Studio.

3.3. Безопасная среда

296. В связи с особенностями работы файлов, ассоциированных с UPW-приложениями, не поддерживается работа приложений Appx и AppxBundle, которые также известны как приложения магазина Microsoft (UPW, универсальные приложения).

Например, если jpg-файл ассоциирован с приложением "Фотографии" ОС Windows, такой файл не запустится в БС, так как данное приложения является UPW-приложением. В случае, если jpg-файл ассоциирован с любим другим приложением (например, GIMP), данный файл запустится в БС.

3.4. Межсетевой экран и авторизация сетевых соединений

3.4.1. Установка подсистем сетевой защиты

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

298. 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.

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

300. 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.).

301. 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.

302. При обновлении Secret Net Studio с версии 8.5.5329.0 на версию 8.6.8330.0 на компьютере с установленным Kaspersky Endpoint Security версии 11.1.1.126 на этапе обновления подсистемы сетевой защиты может произойти "зависание" системы.

> **Рекомендации:** Для корректного обновления перед запуском процедуры получите статус Windows Defender (в PowerShell введите команду Get-MpComputerStatus).
>
> Если статус получить не удалось, то включите Windows Defender в режиме "Периодическое сканирование". Затем снова получите статус в PowerShell. При получении корректного статуса перезагрузите компьютер и запустите процедуру обновления.

3.4.2. Общее

303. Не поддерживается работа компонентов сетевой защиты на кластерах.

304. 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.

305. 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.

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

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

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

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

310. В безопасном режиме Windows удаление компонентов сетевой защиты завершается ошибкой.

311. При использовании настройки "Требовать защищенное соединение" в исходящих правилах межсетевого экрана необходимо убедиться в том, что на удаленных компьютерах, куда планируются защищенные соединения, развернут компонент сетевой защиты ACC, и выполнены настройки входящих правил доступа для пользователей. Иначе подключения будут неуспешными. Рекомендумое правило межсетевого экрана для удаленных компьютеров: " для входящих соединений запрещен доступ для анонимных пользователей".

3.4.3. Аутентификация

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

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

314. 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.

315. 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).

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

317. Если рабочая станция пользователя запущена, но IP-адрес еще не получен, возможно возникновение ошибки входа на сервере аутентификации.

318. Если администратор выполнил вход в ОС по сертификату и выполнил в программе управления пользователями действия, требующие пароля сервера аутентификации, то при вводе корректного пароля может появиться сообщение "Запрет доступа или неправильный пароль". В этом случае необходимо убедиться, что у администратора задан пароль ОС Windows.

> **Рекомендация:** Если в организации для всех пользователей настроен вход только по сертификату, для управления сервером аутентификации рекомендуется выделить администратора, который сможет выполнить вход в ОС по паролю.

3.4.4. Защищаемый сервер

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

320. 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.

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

322. 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.

323. 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.

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

3.4.5. Прочие особенности

325. 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.

326. 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".

327. 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.

328. При смене имени компьютера, на котором установлен клиент Secret Net Studio с подсистемами сетевой защиты, после перезапуска в Центре управления для межсетевого экрана отображается статус "подсистема не работает в полном объеме". Кроме того, прекращается обновление конфигурации сетевой защиты, и в Центре 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 Центре 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

329. 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).

330. 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.

331. 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 Центре 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).

3.5. Антивирус

3.5.1. Установка подсистемы

332. Для работы антивируса требуется не менее 900 МБайт доступной для ОС оперативной памяти.

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

334. Свободное пространство диска для установки антивируса должно быть не менее 500 МБайт. Такой объем необходим для развертывания антивирусных баз обновлений.

335. 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.

3.5.2. Общее

336. Антивирус (технология ESET) не поддерживается в Secret Net Studio версий 8.7 и выше.

337. Secret Net Studio на серверных ОС не отслеживает наличие сторонних антивирусов. Для корректной работы антивируса Secret Net Studio администратору необходимо при установке продукта удостовериться в отсутствии других антивирусов с движком Лаборатории Касперского.

338. Не поддерживается совместная работа антивируса Secret Net Studio с антивирусными средствами сторонних производителей. Для корректного функционирования может потребоваться дополнительная настройка параметров (см. пункт ниже).

339. 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 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.

340. 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;

* Особенность не относится к антивирусу с технологией ESET.

- 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 Центре управления);
- исключение не действует для буквы виртуального диска, созданного командой SUBST.

341. 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.

342. 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.

343. При отправке почтового сообщения через контекстное меню файла с расширением MSG проверка письма на вирусы не выполняется.

344. При открытии Microsoft Outlook 2013 первое автоматически выбранное письмо не сканируется на вирусы.

345. Если в настройках почтового антивируса установлено значение "Проверять входящие", проверяются все письма, просматриваемые пользователем. Если установлено значение "Проверять исходящие", проверяются отправленные письма.

346. Настройка параметра "Использовать результаты предыдущего сканирования" в профилях сканирования не влияет на работу антивируса.

347. В ОС Windows 10 версии 20H2 и выше, а также во всех версиях ОС Windows 11 при включенной подсистеме антивируса невозможно войти в систему под учетной записью пользователя, не выполнявшего вход в систему до установки Secret Net Studio. Для решения проблемы отключите подсистему Антивируса, войдите в систему новым пользователем и включите подсистему Антивируса.

3.5.3. Карантин

348. При обновлении клиента Secret Net Studio с предыдущих версий на версии 8.6 и выше вся информация о файлах, ранее помещенных в карантин, будет потеряна. После обновления восстановить такие файлы средствами Центра управления будет невозможно.

> **Рекомендации:** Перед выполнением обновления проверьте содержимое карантина на защищаемых компьютерах, восстановите нужные файлы и удалите остальные. Если обновление уже выполнено, восстановить файлы можно с помощью утилиты sns.av_cli.exe с указанием полного пути к файлу (описание работы с утилитой содержится в документе "Руководство администратора. Настройка и эксплуатация").

349. В конфиденциальных сессиях не поддерживается работа с карантином (удаление и восстановление) средствами Локального центра управления. Для восстановления файлов, помещенных в карантин с сетевого ресурса, используется утилита sns.av_cli.

350. В Центре 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.

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

352. 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 sns.av_cli.exe.

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

3.5.4. Защита в режиме реального времени

353. 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.

354. 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.

355. 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.

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

357. 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.

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

3.5.5. Сканирование по расписанию или по требованию

359. 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.

360. 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.

361. 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.

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

3.5.6. Регистрация событий

363. После обновления Secret Net Studio с версии 8.4 на более позднюю у ранее зарегистрированных в журнале Secret Net Studio событий с источником "Antimalware" становится недоступна подробная информация о событии, содержащаяся в поле "Описание".

> **Рекомендации:** Если требуется, изучите информацию о данных событиях перед выполнением обновления.

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

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

3.5.7. Обновление антивирусных баз

366. 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.

3.6. Обнаружение и предотвращение вторжений

367. 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.

368. 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.

3.7. Центр управления

3.7.1. Общее

369. 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 Центра управления необходимо установить русский язык для параметра ОС Windows, определяющего язык программ, не поддерживающих Unicode.

370. При загрузке дистрибутива Secret Net Studio в Центр управления возникает ошибка, если в пути к дистрибутиву имеются символы языка, для которого не установлена локализация.

Рекомендации: Разместите дистрибутив Secret Net Studio в пользовательской папке для временных файлов, содержащей в полном пути символы на языке установленной системы (%TEMP%).

371. При редактировании разрешений в политике устройств в стандартном диалоге ОС Windows для визуализации дескриптора безопасности на закладке "Аудит" задание параметра наследования не поддерживается продуктом SNS. Начиная с Secret Net Studio версии 8.10 кнопка "Наследовать..." будет убрана из графического интерфейса.

3.7.2. Запуск Центра управления

372. Если в параметрах Центра управления 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.

373. Подключение к серверу Центра 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 Центр управления пользователь был добавлен в группу администраторов (не является первичной учетной записью администратора домена Windows).

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

3.7.3. Вывод данных

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

3.7.4. Настройка параметров

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

376. При настройке параметров почтовой рассылки для повышения защищенности рекомендуется в качестве пользователя, от лица которого будет рассылка, указывать отдельно выделенную гостевую учетную запись с минимальным набором привилегий в домене AD.

3.7.5. Работа с журналами

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

378. 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.

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

380. 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.

381. 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.

382. В Локальном центре 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".

383. Для обеспечения пользователю возможности просмотра копий теневого хранилища при просмотре журнала Secret Net Studio необходимо явно предоставить пользователю привилегию "Просмотр журнала системы защиты".

384. При настройке политики отправки журналов на сторонний syslog-сервер отправка журналов производится при каждом изменении параметров политики отправки жирналов, что может привести к дублированию записей на syslog-сервере.

3.8. Сервер безопасности

3.8.1. Установка, обновление, восстановление сервера безопасности

385. 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.

386. 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.

387. Запрещается выполнять восстановление сервера безопасности из любых снимков состояния системы (например, используя диск восстановления ОС Windows или сохраненный образ виртуальной машины). В этом случае происходит откат внутреннего счетчика (USN) централизованного хранилища, что может приводить к нарушениям в работе сервера безопасности. Данная ситуация известна как "USN Rollback" и подробно рассматривается в статье: https://support.microsoft.com/ru-ru/help/875495/how-to-detect-and-recover-from-a-usn-rollback-in-windows-server-2003-w.

388. 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.

389. При установке в домене безопасности сервера безопасности более новой версии, чем версия серверов, уже имеющихся в данном домене, происходит обновление схемы LDS (централизованное хранилище). После этого не рекомендуется устанавливать в данный домен безопасности новые сервера безопасности более старых версий, чем версия установленного сервера.

390. В Secret Net Studio версий 8.0-8.4 и Secret Net версий 7.x при установке сервера безопасности на контроллерах домена AD программа установки создавала служебную учетную запись доменного пользователя SecretNetLDS$ или SecretNetLDS (в зависимости от версии ОС), используемую для запуска служб AD LDS. Эта учетная запись в текущей версии Secret Net Studio не требуется.

Внимание! После обновления ПО серверов безопасности до текущей версии данную учетную запись необходимо в обязательном порядке удалить. Перед выполнением удаления необходимо вначале обновить ПО сервера безопасности на всех без исключения контроллерах домена AD, на которых он функционирует. Затем на одном из контроллеров домена следует запустить на выполнение под учетной записью администратора домена AD утилиту lds_dc_patch.exe с параметром del — lds_dc_patch.exe /del. Утилита размещается в установочном комплекте Secret Net Studio в каталоге Tools\SecurityCode\LdsPasswordChange\.

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

392. 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.

393. 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, управление, мониторинг и аудит".

3.8.2. Взаимодействие с другими компонентами

394. 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).

395. 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 Центр управления.
4. В Центре 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".

396. Возникновение ошибок типа "класс не зарегистрирован" ("class not registered") во время получения журнала или отчета, либо ошибок применения групповых политик "AsyncCallbackApplyPoliciesCommand() Ошибка:Unknown error 0xE06D7363..." 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 комплекта системы Secret Net Studio из каталога \Tools\Microsoft\Prerequisites\.

397. Сертификат сервера безопасности в хранилище объектов централизованного управления должен совпадать с сертификатом, установленным в IIS. При замене сертификата в IIS его необхо-

димо синхронизировать и в хранилище объектов ЦУ. Процедура выполняется в программе генерации сертификатов, входящей в состав ПО сервера безопасности.

398. 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.

399. 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

400. 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.

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

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

402. 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.

3.8.3. Обработка данных

403. 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).

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

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

406. 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".

3.9. Сервер обновлений

407. Если на компьютере, куда планируется установить сервер обновлений, уже установлен клиент Secret Net Studio с включенной защитой от локального администратора, то перед установкой сервера обновлений необходимо отключить защиту от локального администратора и перегрузить компьютер. После установки сервера обновлений снова активируйте защиту.

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