Средство защиты информации Secret Net Studio
Сведения о совместимости с другими программными средствами

Данный документ содержит сведения о совместимости и особенностях работы СЗИ Secret Net Studio версии 8.10.18997.0 с другими программными средствами при совместном функционировании.

Первая глава документа содержит сведения о совместимости с программными средствами, с которыми проводилось тестирование на совместимость.

Вторая глава документа содержит сведения об известных особенностях работы при совместном использовании СЗИ Secret Net Studio с программными средствами, с которыми не проводилось отдельное тестирование на совместимость.

Оглавление

1. Сведения о совместимости

1.1. Продукты компании "Код безопасности"

1.1.1. Secret Net LSP

1. Обеспечивается возможность централизованного управления с сервера безопасности Secret Net Studio клиентами Secret Net LSP следующих версий:

- 1.11;
- 1.10;
- 1.9.

1.1.2. vGate

2. Обеспечивается совместимость с ПО vGate следующих версий:

- 4.4 (включая Hyper-V) – клиент Secret Net Studio совместим с агентом аутентификации vGate, сервером авторизации, Hyper-V-агентом, vCenter-агентом;
- 4.3 (включая Hyper-V) — клиент Secret Net Studio совместим с агентом аутентификации vGate, сервером авторизации, Hyper-V-агентом, vCenter-агентом.

3. Не поддерживается размещение сервера безопасности Secret Net Studio и сервера авторизации vGate на одном компьютере. Устанавливайте эти компоненты на разных компьютерах.

1.1.3. "Континент"

4. Обеспечивается совместимость с программой управления центра управления сетью АПКШ "Континент" следующих версий:

- 3.9.2;
- 3.9.1.2732.

5. Обеспечивается совместимость с менеджером конфигураций "Континент" следующих версий:

- 4.1;
- 4.

6. Обеспечивается совместимость с СКЗИ "Континент-АП" следующих версий:

- 4.1;
- 3.7.7 исполнение 1 (версия 3.7.7.651).

1.1.4. "Соболь"

7. Обеспечивается совместимость с изделием "Программно-аппаратный комплекс "Соболь" следующих релизов:

- 4.4;
- 4.3 (версия 4.3.352 кода расширения UEFI/BIOS);
- 4.2 (версия 4.2.334 кода расширения UEFI/BIOS);
- 3.1 (версия 3.1.3 кода расширения BIOS);
- 3.0.9 (версия 1.0.227 кода расширения BIOS).

8. Если используется сетевой режим функционирования клиента Secret Net Studio, при инициализации ПАК "Соболь" на компьютерах домена учитывайте следующие требования:

- используйте при регистрации администратора один и тот же идентификатор администратора (или его копию). При этом на первом компьютере регистрация администратора выполняется в режиме первичной регистрации, а на всех остальных — в режиме повторной регистрации;
- для комплексов "Соболь" версий 3.0.9 и 3.1 установите одинаковое значение параметра "Версия криптографической схемы";
- для комплексов "Соболь" версии 4.3 установите для параметра "Версия математических преобразований" значение "1989".

9. После обновления клиента расчет контрольных сумм в программно-аппаратном комплексе "Соболь" выполняется при второй перезагрузке компьютера.

10. При первой перезагрузке после установки платы и ПО ПАК "Соболь" версии 3.0.9 процесс контроля аппаратной конфигурации не обнаружит изменения в аппаратной конфигурации компьютера. После второй перезагрузки устройство будет обнаружено.

11. Централизованные задания КЦ для ПАК "Соболь" отображаются в локальном режиме программы "Контроль программ и данных" даже в том случае, если ПАК не установлен на компьютере или работает в автономном режиме.

12. В автономном режиме функционирования клиента Secret Net Studio если администратор выполнит смену пароля доменного пользователя, этот пользователь не сможет войти в ПАК "Соболь" по новому паролю. Пользователю потребуется войти в ПАК "Соболь" со старым паролем, загрузить систему и самостоятельно сменить свой пароль.

13. При преобразовании журнала ПАК "Соболь" в журнал Secret Net Studio в записях о событиях нарушения целостности в некоторых случаях отсутствуют имена ресурсов.

14. В программе "Контроль программ и данных" перед сохранением любых изменений в заданиях контроля целостности для ПАК "Соболь" необходимо выполнить перерасчет контрольных сумм.

15. После включения режима совместной работы в ПАК "Соболь" выполняется автоматическая очистка содержимого шаблонов контроля целостности.

16. При подключении к работающему компьютеру диска SATA в режиме "горячего включения" (Hot-plug) формирование шаблонов КЦ ПАК "Соболь" для разделов этого диска возможно только после перезагрузки компьютера.

17. При синхронизации настроек Secret Net Studio и ПАК "Соболь" не синхронизируется признак блокировки пользователя в ОС.

18. В совместном режиме с ПАК "Соболь" версии 3.1 можно сформировать задание на контроль целостности только файлов.

19. Контроль целостности ресурсов, в пути которых присутствуют специальные символы (например, знак "®"), не выполняется.

20. Для администратора ПАК "Соболь" не действует режим "Пароль в идентификаторе".

21. Заданный параметр "Максимальный срок действия пароля" не синхронизируется с ПАК "Соболь", так как этот параметр не используется в режиме совместного использования ПАК и Secret Net Studio.

22. Чтобы присвоить пользователю идентификатор администратора ПАК "Соболь", пароль пользователя должен совпадать с паролем администратора ПАК "Соболь".

23. В сетевом режиме функционирования клиента Secret Net Studio если доменному пользователю присвоен идентификатор администратора ПАК "Соболь" — пользователь имеет доступ на администрирование всех ПАК "Соболь" в системе (независимо от того, какие компьютеры перечислены в списке доступных пользователю). При этом сменить свой пароль пользователь может только на тех компьютерах, которые перечислены в списке (при условии наличия на компьютере подключенного ПАК "Соболь").

24. Если в идентификаторе Rutoken S записаны данные Secret Net Studio, то при его предъявлении в ПАК Соболь версии 3.x всегда происходит запрос пользовательского PIN-кода, даже если PIN-код равен значению по умолчанию: 12345678.

1.1.5. "Континент TLS-клиент"

25. Обеспечивается совместимость с СКЗИ "Континент TLS-клиент" следующих версий:

- 2.0.1482.0;

1.1.6. Jinn-Client

26. Обеспечивается совместимость с СКЗИ Jinn-Client версий 1.0.3055, 1.0.3050.3.

27. Если в Secret Net Studio включен механизм замкнутой программной среды, то совместная работа с СКЗИ Jinn-Client обеспечивается при отключенном контроле скриптов.

1.1.7. Континент ZTN Клиент для Windows

28. Обеспечивается совместимость с изделием "Континент ZTN Клиент для Windows".

29. Для совместной работы во включенном режиме контроля потоков необходимо в программе "Настройки подсистемы полномочного управления доступом" создать правила перенаправления для каталогов \appdata\roaming\continentztnclient и \%public%\continentztnclient.

1.2. Антивирусные средства защиты

1.2.1. Общее

30. Не поддерживается совместная работа механизма антивируса Secret Net Studio с антивирусным ПО сторонних производителей. При использовании стороннего антивирусного ПО рекомендуется в настройках антивируса добавлять в исключения каталог установки клиента Secret Net Studio со всеми подкаталогами. Если невозможно отключить проверку всего каталога (из-за политики безопасности и наличия исполняемых модулей) — обязательно укажите подкаталоги \GroupPolicy, \icheck и \etalons. Кроме того, если включена трассировка работы Secret Net Studio, добавьте в исключения для антивируса папку %ProgramData%\Security Code\Secret Net Studio\Logs. В противном случае работа системы существенно замедлится, и могут возникать сбои.

1.2.2. Продукты компании "Лаборатория Касперского"

31. Обеспечивается совместимость с "Kaspersky Endpoint Security для Windows" следующих версий:

- 11.6;
- 10.3.3.304.

32. Совместная работа с "Kaspersky Endpoint Security для Windows" возможна со следующими ограничениями:

- приложение должно быть установлено без модулей шифрования дисков и файлов;
- при совместной работе проявляются задержки в процедуре входа пользователя в систему (на этапе загрузки профиля пользователя), а также при переходах по каталогам на сетевых дисках;
- для успешной установки компонентов сетевой защиты перед установкой клиента Secret Net Studio рекомендуется установить все доступные обновления Kaspersky Endpoint Security.

33. В сетевом режиме функционирования клиента Secret Net Studio если на компьютере установлен компонент Kaspersky Anti-Hacker, в его настройках необходимо либо отключить проверку трафика SSL, либо внести исполняемый файл OmsHost.exe в список доверенных программ и создать правила для портов 443 и 389.

34. Для корректной работы сетевой версии клиента с "Kaspersky Endpoint Security для Windows" версий 11.9 и позже перед установкой клиента необходимо выполнить действия по одному из следующих сценариев:

- В Kaspersky Security Center создайте новую политику и в ее контекстном меню выберите опцию "Изменить параметры политики". В открывшемся окне свойств перейдите в раздел "Общие настройки | Настройки сети" и нажмите кнопку "Доверенные адреса". В открывшемся окне доверенных адресов нажмите кнопку "Добавить" и укажите маску с DNS-именем сервера или домена. Маску также можно добавить локально на компьютере с установленным Kaspersky Endpoint Security, выполнив аналогичную последовательность действий.
- На компьютере с установленным Сервером безопасности откройте Диспетчер служб IIS, выберите сервер и откройте элемент "Сертификаты сервера". В открывшейся панели сертификатов откройте контекстное меню и выберите опцию "Создать самозаверенный сертификат". В окне создания сертификата укажите полное DNS-имя сервера и выберите вариант "Размещение веб-узлов". Далее вызовите контекстное меню сайта SecretNetStudioSite и выберите команду "Изменить привязки". В открывшемся окне нажмите кнопку "Изменить" и в окне изменения выберите созданный самозаверенный сертификат. Откройте программу "Сертификаты", перейдите на вкладку "Сервисы" и нажмите кнопку "Синхронизировать" (потребуются учетные данные администратора домена безопасности). После этого сохраните сертификат на рабочие станции и добавьте его в каталог "Доверенные корневые сертификаты". Добавление можно выполнить с помощью групповых политик: https://learn.microsoft.com/ru-ru/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy.

1.2.3. Продукты компании "Доктор Веб"

35. Обеспечивается совместимость с Dr.Web Enterprise Security Suite следующих версий (с учетом общих рекомендаций для совместной работы с антивирусными средствами защиты):

- 12;

- 11.5.

36. Совместная работа с приложениями "Dr.Web Enterprise Security Suite", "Dr.Web Антивирус" и "Dr.Web Security Space" возможна со следующими ограничениями:

- если включен брандмауэр, перед установкой клиента Secret Net Studio необходимо или отключить брандмауэр, или создать правила разрешения сетевых соединений для LDAP-портов 50000, 50002, 50003. После установки клиента должны быть созданы правила разрешения сетевых соединений для процессов Snichecksrv (порт 21327 и указанные LDAP-порты) и SnHwSrv (порт 21326). Правила можно создать на основе записей в статистике соединений брандмауэра. Также, если в статистике соединений присутствуют записи о попытках соединения со стороны процесса Windows Logon User Interface Host (на ОС Windows 7), необходимо создать правило для этого процесса и соответствующего порта. При отсутствии разрешающих правил могут возникать ошибки и сбои работы системы — например, ошибки синхронизации с БД КЦ-ЗПС или зависания при разблокировке компьютера или при выходе из спящего режима;
- при появлении запросов брандмауэра на разрешение сетевых вызовов для запускаемых подсистем клиента Secret Net Studio (при установке клиента или позже в процессе функционирования) — необходимо выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения).

37. Превентивная защита Dr.Web Enterprise Security Suite блокирует низкоуровневые операции с диском, в связи с чем блокируются операции включения и отключения механизма защиты дисков Secret Net Studio. На функционирование механизма защиты диска работа превентивной защиты не влияет.

> **Рекомендации:** Для включения и отключения механизма защиты дисков Secret Net Studio предварительно отключите Превентивную защиту Dr.Web Enterprise Security Suite.

38. Для корректной установки клиента на компьютер с установленным агентом DrWeb необходимо выполнить следующие действия:

- В DrWeb 11 отключите самозащиту на время установки;
- В DrWeb 12 разрешите работу групп "Ассоциации исполняемых файлов" и "Параметры оболочки Winlogon".

39. Совместная работа подсистем авторизации сетевых соединений и межсетевого экрана с DrWeb 12 поддерживается со следующими особенностями настройки правил доступа МЭ:

- параметр "Приложение" — для исходящих правил приложением, создающим соединение, всегда будет dwnetfilter.exe;
- параметр "Субъект доступа" — исходящие соединения всегда устанавливаются от имени учетной записи компьютера;
- параметр "Доступные субъекты безопасности процесса" — при исходящих соединениях подсистема МЭ всегда будет проверять субъект, от имени которого запущен процесс dwnetfilter.exe, а не процесс-инициатор сетевого соединения.

1.3. Другие средства защиты информации

1.3.1. ViPNet Client

40. Обеспечивается совместимость с ПО ViPNet Client версии 4.5.3.65102. При включенном контроле потоков совместимость обеспечивается не в полной мере.

41. Для корректного функционирования ПО ViPNet Client при работе в конфиденциальных сессиях необходимо выполнить следующие действия:

- Если приложение клиента почтовой системы из состава ПО ViPNet Client ранее не использовалось, выполните его запуск в неконфиденциальной сессии и отправьте любое почтовое сообщение.
- В программе настройки подсистемы полномочного управления доступом выполните следующие действия:
  - Отключите регистрацию событий обращения к log-файлам ПО ViPNet Client. Для этого в список раздела "Вручную | Общие | Аудит" добавьте следующие строки:

\infotecs\vipnet client\cryptapi.log
\infotecs\vipnet client\iplircontrol.log
\infotecs\vipnet client\Monitor.log
\infotecs\vipnet client\Monitori.log
\infotecs\vipnet client\rfacnmgr.log
\infotecs\vipnet client\rfmgr.log
\infotecs\vipnet client\rfmgrui.log

- В ключе системного реестра HKLM\System\CurrentControlSet\Services\SnFMac\Params создайте параметр ProcNotUpFile типа REG_MULTI_SZ (если такой параметр отсутствует) и добавьте в список значений этого параметра следующие строки:

  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\iplir.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\iplirmain.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\appwhere.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\mftp.ini
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\sesalrt.hst
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\rfmgrui.exe::\infotecs\vipnet client\shared.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\rfmgrui.exe::\infotecs\vipnet client\rf.ini
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\wmail.ini
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\appwhere.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\sesalrt.hst
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\ab.hst
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\shared.cfg
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\Monitor.exe::\infotecs\vipnet client\monitor.log
  \Device\HarddiskVolume2\Program Files\InfoTeCS\ViPNet Client\wmail.exe::\infotecs\vipnet client\mftp.ini

Примечание: Примеры путей приведены для случая, если ПО установлено в каталог по умолчанию. Начальная часть пути \Device\HarddiskVolume2\ указывает на системный диск C:\. Путь к исполняемым файлам в данном формате приводится в записях журнала Secret Net Studio — в дополнительных описаниях событий категории "Полномочное управление доступом".

1.3.2. "КриптоПро CSP"

42. Обеспечивается совместимость со следующими версиями СКЗИ "КриптоПро CSP":

- 5.0.12000;
- 5.0.11455;
- 4.0.9963;
- 4.0.9944.

43. При совместной работе с ПО "КриптоПро" необходимо устанавливать драйверы и программное обеспечение для работы персональных идентификаторов (например, eToken или Rutoken) после установки ПО "КриптоПро". Если средства поддержки персональных идентификаторов были установлены ранее, после установки ПО "КриптоПро" их нужно переустановить.

1.3.3. InfoWatch

44. Обеспечивается совместимость с InfoWatch Device Monitor следующих версий:

- 7.0;
- 6.11.

1.3.4. Solar Dozor

45. Обеспечивается совместимость с Solar Dozor.

1.4. Системы виртуализации

1.4.1. Общее

46. Механизм защиты "Доверенная среда" из состава клиента Secret Net Studio не функционирует в виртуальной среде.

1.4.2. Citrix

47. Обеспечивается совместимость со следующими версиями ПО Citrix (с учетом особенностей, изложенных ниже):

- Citrix XenApp 7 1912 LTSR;
- Citrix XenApp 7.15;
- Citrix XenDesktop 7 1912 LTSR;
- Citrix XenDesktop 7.15;
- Citrix PVD.

48. При наличии на компьютере ПО Citrix (установлен агент VDA из состава компонентов Citrix) драйвер-фильтр устройств системы Secret Net Studio автоматически переводится в режим совместимости для корректной ассоциации физических и логических USB-дисков. Первое включение этого режима сопровождается срабатыванием функционального контроля во время загрузки ОС с сообщением о нарушении конфигурации среды. Для продолжения работы необходимо перезагрузить компьютер. Срабатывание функционального контроля происходит однократно, и следующие загрузки выполняются штатно с действующим режимом совместимости. Также в случае удаления указанного компонента ПО Citrix отключается режим совместимости в Secret Net Studio, что аналогично приводит к однократному срабатыванию функционального контроля при следующей загрузке.

49. В ПО Citrix использование устройств на компьютерах-клиентах может быть реализовано в двух вариантах: 1) общее перенаправление USB-устройств (generic USB redirection), применяемое в продукте XenDesktop; и 2) перенаправление через виртуальные каналы (virtual channels), применяемое в продуктах XenDesktop и XenApp. При совместной работе с ПО Citrix в системе Secret Net Studio обеспечивается полноценный контроль только для устройств, подключенных к виртуальному рабочему столу в первом варианте — так как в этом случае устройство "переподключается" к системе, для него устанавливаются соответствующие драйверы и пр. Для устройств, перенаправляемых через виртуальные каналы, необходимо использовать средства контроля и блокировки в политиках безопасности Citrix.

> **Примечание:** Вариант общего перенаправления USB-устройств Citrix не поддерживается для устройств, подключенных к портам USB 3.0. Кроме того, для некоторых классов устройств такой тип перенаправления отключен по умолчанию. В варианте перенаправления через виртуальные каналы нужно учитывать, что если для устройства не предусмотрено использование виртуального канала, система выполняет перенаправление этого устройства первым способом.
>
> **Рекомендации:** При необходимости обеспечить контроль устройств средствами Secret Net Studio настройте параметры перенаправления в политиках Citrix. Сведения о политиках см. http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-article.html. Сведения о конфигурировании общего перенаправления USB-устройств см. http://support.citrix.com/article/CTX137939. Основные параметры, определяющие перенаправление устройств:
>
> - для USB-устройств:
> Client USB device redirection
> Client USB device redirection rules
> Client USB plug and play device redirection
> - для других устройств:
> Client COM port redirection
> Client LPT port redirection
> Client Drive redirection

50. На компьютере под управлением несерверной версии ОС (Windows 7/8.1/10), который используется для предоставления виртуальных рабочих столов (XenDesktop) или приложений (XenApp), ПО Citrix реализует особый порядок работы с сессиями пользователей при создании подключений. Из-за этого возможны ситуации зацикливания или блокировки сессий в следующих случаях:

- если включен режим контроля потоков конфиденциальной информации с параметром "строгий контроль терминальных подключений" и вход выполняется с компьютера, на котором не включен режим контроля потоков;
- если локально возобновляется прерванная сессия пользователя.

Рекомендации: Корректное взаимодействие с механизмом защиты входа Secret Net Studio обеспечивается, если для виртуализации рабочих столов и приложений используются компьютеры под управлением серверных версий ОС.

51. Защита сервера приложений Citrix XenApp обеспечивается со следующими особенностями:

- Для корректной работы подсистемы контроля печати отключите настройку "Isolate Application" для опубликованных приложений.
- Регистрация печати документов из опубликованных приложений осуществляется на сервере приложений (в том числе и при использовании локального принтера на компьютере–клиенте).
- Для корректной работы с конфиденциальными документами отключите возможность использования локальных дисков компьютера (клиента) для опубликованных приложений.
- При использовании механизма полномочного управления доступом в режиме контроля потоков с включенным дополнительным параметром "Строгий контроль терминальных подключений" для терминального входа в конфиденциальных сессиях не следует использовать учетную запись администратора Citrix.

1.4.3. VMware

52. Обеспечивается совместимость с системами VDI на базе VMware Horizon следующих версий (с учетом особенностей, изложенных ниже):

- 8 2103;
- 7.13.

53. При работе с виртуальными машинами на базе VMware возможна ситуация, когда виртуальное устройство не отправляет уведомление об изменении своего состояния. Из-за этого в дереве устройств может отображаться устаревшая информация об устройстве, и в журнале Secret Net Studio не регистрируется соответствующее событие.

Рекомендации: Для исключения подобного поведения в конфигурационный файл виртуальной машины добавьте параметр usb.EnablePnpMgr = "TRUE".

1.4.4. Microsoft

54. Обеспечивается совместимость с любыми штатными системами терминального доступа в рамках поддерживаемых ОС.

Примечание: Список поддерживаемых ОС приведен в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, управление, мониторинг и аудит" (см. раздел "Требования к аппаратному и программному обеспечению").

55. Обеспечивается совместимость с системами виртуализации на базе следующих ОС:

- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012/2012 R2.

56. Не поддерживается совместная работа подсистем защиты диска и полнодискового шифрования с системой виртуализации Hyper-V.

1.5. Офисные приложения

1.5.1. Microsoft Office

57. Обеспечивается совместимость со следующими версиями Microsoft Office Word, Excel (с учетом особенностей, изложенных ниже):

- 2019;
- 2016;
- 2013.

58. Если происходят ошибки при загрузке плагинов Secret Net Studio в приложения Microsoft Office, эти приложения могут отключить автоматическую загрузку плагинов. Это приведет к невозможности корректной передачи параметров печати документов в подсистему контроля печати. В частности, не будет учитываться заданное количество копий распечатываемых документов и могут неправильно обрабатываться параметры печати нескольких страниц на листе. Кроме того, в хранилище теневого копирования будет сохраняться не весь документ, а только та его часть, которая была отправлена на печать.

Рекомендации: Для решения проблемы выполните следующие действия с параметрами системного реестра:

- удалите параметр (параметры) HKCU\Software\Microsoft\Office\<Ver>\<App>\Resiliency\DisabledItems, где <Ver> — версия MSOffice (15 – 2013, 16 – 2016, 2019), а <App> — приложение Office (Word, Excel);
- восстановите значение 3 для параметра LoadBehavior (тип REG_DWORD) в ключе (ключах) HKLM\Software\Microsoft\Office\<App>\Addins\<Plug-in> (если установлена 32-разрядная версия Office в 64-разрядной ОС — ключ HKLM\Software\Wow6432Node\Microsoft\Office\<App>\Addins\<Plug-in>), где <App> — приложение Office (Word, Excel), а <Plug-in> — имя плагина, соответствующего приложению Office (SnMsoWordAgent.Addin или SnMsoExcelAgent.Addin).

59. Если пакет Microsoft Office установлен без поддержки VBA (Visual Basic for Application), приложения Office функционируют со следующими особенностями:

- при включенном режиме контроля печати для открываемых документов могут выводиться предупреждения об отсутствии поддержки макросов и элементов управления;
- создание и редактирование файла шаблона Normal.dot/Normal.dotm необходимо выполнять при отключенном режиме контроля печати.

60. В приложениях Microsoft Office версии 2013 и выше при включенном режиме маркировки с расширенной обработкой игнорируются параметры печати двух или более страниц на листе, заданные в приложении (из-за особенностей реализации печати в этих приложениях).

Рекомендации: При необходимости печати нескольких страниц на листе используйте параметры в диалоге настройки печати для принтера.

61. При переходе с Microsoft Office предыдущих версий на версию Microsoft Office 2013 возможна некорректная регистрация системного интерфейса, который используется для работы подсистемы контроля печати. В результате этого, при включенном режиме маркировки с расширенной обработкой, в некоторых приложениях Microsoft Office 2013 (например, Microsoft Excel) может блокироваться печать документов — после отправки на печать повторно выводится диалог настройки, но сам документ не распечатывается.

Рекомендации: Для восстановления возможности печати откройте окно командной строки, выполнив запуск от имени администратора, и введите команды:

- для 32-разрядной ОС:
  c:\windows\system32\regsrv32.exe c:\windows\system32\oleacc.dll
- для 64-разрядной ОС:
  c:\windows\syswow64\regsrv32.exe c:\windows\syswow64\oleacc.dll
  c:\windows\system32\regsrv32.exe c:\windows\system32\oleacc.dll

62. В некоторых приложениях (например, Microsoft PowerPoint 2013) 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.

63. Если в документе Microsoft Excel для листов указаны различные значения параметра "Качество печати" (например, для таблицы Лист1 указано значение "600 точек на дюйм", а для таблицы Лист2 — "1200 точек на дюйм"), при отправке этих листов на печать могут создаваться несколько заданий печати. Подробные сведения об этом см. http://support.microsoft.com/kb/168563. При включенном режиме маркировки (стандартная или расширенная обработка) подсистема контроля печати обрабатывает полученные задания печати документа по отдельности, в результате чего дополнительно могут проявляться следующие особенности:

- диалог для ввода значений в настраиваемые поля маркера выводится несколько раз — по количеству заданий печати;
- распечатывается несколько страниц с маркировкой на обратной стороне листа;
- в журнале Secret Net Studio регистрируется несколько групп событий печати.

Рекомендации: Укажите для документа одинаковые значения параметра "Качество печати" (сведения о способах изменения значений см. http://support.microsoft.com/kb/168563).

64. В приложении Microsoft Excel при печати документа может несколько раз выводиться диалог для ввода значений в настраиваемые поля маркера. Данная особенность проявляется при следующих условиях:

- включен режим маркировки со стандартной обработкой;
- печать выполняется на принтер с активной функцией двусторонней печати;
- в приложении выбран режим "Напечатать всю книгу" (Print Entire Workbook).

Рекомендации: Указывайте одинаковые значения в настраиваемых полях маркера в появляющихся диалогах или включите расширенную обработку для режима маркировки.

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

- если документ загружен из файла в приложение Microsoft 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).

66. В приложениях Microsoft Office изменения документа сохраняются не в исходном файле этого документа, а в новом файле с тем же именем. По этой причине в условиях дискреционного и/или полномочного разграничения доступа рекомендуется устанавливать нужные права доступа и категории конфиденциальности не непосредственно на сам файл, а использовать механизм наследования для каталогов, в которых содержатся данные файлы. Если же атрибуты безопасности заданы непосредственно для файла, возможны следующие проявления:

- сбрасываются явно заданные дискреционные права доступа при сохранении файла;
- сбрасывается или изменяется категория конфиденциальности документа при его сохранении;
- блокируется открытие файла с заданными категориями конфиденциальности из сетевого ресурса.

67. Чтобы обеспечить корректную работу приложения Microsoft Word в режиме контроля потоков, осуществляется перенаправление вывода для стандартных каталогов хранения шаблонов программы. Следствием этого является независимость сделанных изменений шаблонов MS Word в сессиях с различными уровнями конфиденциальности — так как используются разные каталоги для хранения файлов шаблонов. Тиражирование изменений в шаблоне можно выполнить следующим образом: отключите режим контроля потоков и в редакторе Word выполните нужные изменения шаблона. Затем войдите в систему с правами администратора, которому назначен наивысший уровень допуска к конфиденциальной информации и предоставлена привилегия на управление категориями конфиденциальности. Загрузите программу настройки подсистемы полномочного управления доступом и запустите процесс настройки параметров приложения Microsoft Office (для этого можно выбрать раздел "Вручную | Программы | Microsoft Office" и нажать кнопку "Настроить"). По окончании процесса настройки включите режим контроля потоков.

68. Если приложения Microsoft Office версии 2013 будут использоваться в режиме контроля потоков, перед включением режима рекомендуется выполнить очистку кэша ранее загруженных документов и отключить кэширование (для временных копий файлов установить режим удаления после закрытия) или ограничить время хранения файлов в кэше. Для управления параметрами кэша документов используется компонент "Центр отправки Office 2013". Запуск данного компонента необходимо выполнить как минимум один раз для автоматического создания каталога кэша. После этого может быть выполнена настройка перенаправления вывода файлов с помощью программы настройки подсистемы полномочного управления доступом.

1.5.2. OpenOffice

69. Обеспечивается совместимость с приложением OpenOffice версии 4.1.9.

70. Для работы с приложением OpenOffice в конфиденциальных сессиях рекомендуется в программе настройки для режима контроля потоков выполнить настройку параметров работы этого приложения. Процесс настройки можно запустить непосредственно для приложения (раздел "Вручную | Программы | Openoffice.org") или включить режим автоматической настройки приложения в разделе "Вручную | Программы" и затем либо выполнить настройку системы с текущими параметрами (раздел "Автоматически"), либо настроить профили пользователей (раздел "Вручную | Пользователи"). Если настройка приложения не выполнялась, во время работы в конфиденциальных сессиях при попытке сохранения изменений могут удаляться неконфиденциальные файлы, расположенные в неконфиденциальных каталогах.

71. Для корректной работы пакета OpenOffice в безопасной среде необходимо, чтобы все приложения OpenOffice были добавлены в белый список вручную либо в результате проверки.

1.5.3. LibreOffice

72. Обеспечивается совместимость со пакетом LibreOffice версии 7.1.1.

1.6. Продукты компании Adobe Systems

1.6.1. Adobe Reader

73. Обеспечивается совместимость с русскими и английскими версиями приложения Adobe Acrobat Reader DC (15.0) с учетом особенностей, изложенных ниже.

74. Если в приложении Adobe Reader действует защищенный режим при запуске (Protected Mode at startup), проявляются следующие особенности:

- невозможно выполнить копирование информации из изолированного процесса Adobe Reader в этот же процесс;
- при включенном режиме контроля потоков первый запуск приложения Adobe Reader нужно выполнить в неконфиденциальной сессии. Иначе при работе в конфиденциальных сессиях могут возникать сбои при печати документов.

Рекомендации: Защищенный режим можно отключить в диалоговом окне настройки свойств приложения. Для вызова диалогового окна используйте соответствующую команду меню в зависимости от версии и локализации приложения (например, "Редактирование | Установки" или "Edit | Preferences"). В диалоговом окне перейдите к разделу, в котором представлен параметр "Включить защищенный режим при запуске" ("Enable Protected Mode at startup") и удалите отметку из этого поля. Указанный параметр может быть представлен, в зависимости от версии и локализации приложения, в разделе "Защита (повышенный уровень)" ("Security (Enhanced)") или "Основные" ("General"). После отключения режима перезапустите приложение.

75. При работе с включенным режимом контроля потоков сохранение файлов из приложения Adobe Reader следует выполнять в каталог с уровнем конфиденциальности равным или превышающим уровень конфиденциальности сессии пользователя. Иначе исходный файл будет перемещен в служебный каталог с новым именем. Операция перемещения будет зафиксирована в журнале Secret Net Studio. Данное проявление связано с особенностью работы приложения Adobe Reader.

76. В безопасной среде не поддерживается работа Adobe Reader в защищенном режиме.

2. Особенности работы с другим ПО

2.1. "Континент-АП"

77. При совместном функционировании с СКЗИ "Континент-АП" версии 3.7.5 в журнале приложений Windows могут регистрироваться события "Запрошенная версия ядра не поддерживается". Эти события не оказывают никакого влияния на работоспособность обоих продуктов. Для подавления их регистрации в ключе системного реестра HKLM\System\CurrentControlSet\Services\SnCC0 создайте (если он отсутствует) параметр NoReportError (тип REG_DWORD) и присвойте ему значение, отличное от нуля.

2.2. ViPNet CSP

78. Если на компьютере установлено ПО "ViPNet CSP" и "КриптоПро CSP", режим совместимости с Microsoft CryptoAPI должен быть включен только в одном из этих продуктов. Иначе могут периодически возникать сбои работы системы. Сведения о настройке совместной работы продуктов см. в документации на ПО "ViPNet CSP". При установке клиента Secret Net Studio автоматически проверяется наличие ПО "ViPNet CSP" и "КриптоПро CSP", и в случае обнаружения нестабильной конфигурации установка прерывается с выдачей соответствующего сообщения. Если указанное ПО устанавливается после установки клиента, рекомендуется сначала установить продукт "ViPNet CSP", затем "КриптоПро CSP" и после этого настроить их совместную работу.

2.3. Symantec AntiVirus

79. При совместной работе с ПО Symantec AntiVirus версии 10.0 могут регистрироваться нарушения целостности из-за того, что данное приложение в каждом сеансе регистрирует и удаляет собственную службу в реестре.

> **Рекомендации:** При необходимости использования Symantec AntiVirus снимите с контроля ветви реестра HKLM\System\CurrentControlSet\Services\EraserUtilDrv10500 и HKLM\System\CurrentControlSet\Services.

2.4. Браузеры

80. Механизм контроля скриптов СЗИ Secret Net Studio 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.

81. 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 "Контроль программ и данных" настройки параметров ресурса.

2.5. Microsoft Access

82. При включенном механизме затирания данных может произойти уничтожение содержимого файлов баз данных Microsoft Access, если в параметрах Access включен режим "сжимать при закрытии". Это происходит из-за особенности процедуры сжатия файлов в программе Microsoft Access — при сжатии программа удаляет существующий файл и заменяет его сжатым.

2.6. Docker

83. Secret Net Studio блокирует работу ПО Docker во избежание снижения уровня защищенности системы.

2.7. Windows Sandbox

84. Secret Net Studio блокирует работу ПО Windows Sandbox во избежание снижения уровня защищенности системы.

2.8. HP Client Security

85. Из-за особенностей реализации ПО HP Client Security (предустанавливается на некоторых моделях компьютеров компании HP), после установки СЗИ Secret Net Studio невозможно использовать биометрическую авторизацию с использованием отпечатков пальцев в указанном ПО.

2.9. PDF24 Creator

86. При использовании ПО PDF24 Creator версии 7 и выше могут возникать ошибки во время преобразования документов в формат PDF, связанные с невозможностью обращения к виртуальному принтеру приложения.

> **Рекомендации:** При возникновении ошибок укажите принтер PDF24 PDF в качестве принтера по умолчанию (на время преобразования документа).

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