# Средство криптографической защиты информации "Континент-АП"
# Версия 3.7
# Комментарии к релизу 3.7.7.651

Документ содержит описание новых возможностей изделия "Средство криптографической защиты информации "Континент-АП". Версия 3.7" (далее – СКЗИ "Континент-АП", АП) релизной сборки 3.7.7.651 по сравнению со сборкой 3.7.5.514, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации АП.

## Список сокращений

| | |
|---|---|
| АП | Абонентский пункт |
| ДСЧ | Датчик случайных чисел |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| ПУ | Программа управления |
| ПУ СД | Программа управления сервером доступа |
| СД | Сервер доступа |
| СЗИ | Средство защиты информации |
| СКЗИ | Средство криптографической защиты информации |

# Оглавление

# 1. Изменения и новые возможности

## 1.1. Сборка 3.7.7.651

**1.** В исполнении 4 СКЗИ "Континент-АП" реализована возможность использования СЗИ Secret Net Studio.

**2.** Реализована поддержка ключевых носителей JaCarta PKI, JaCarta ГОСТ.

**3.** В исполнениях 2, 3, 4 добавлена поддержка сертифицированных ФСБ России ПАК "Соболь" версий 3.1, 3.2.

**4.** Исправлена проблема с обновлением ОС Windows 10, приводящее к ошибке отсутствия файла c3ppp_vi.sys.

**5.** Обновлен список файлов, требующих контроля их целостности.

**6.** Исправлена проблема установки ПО абонентского пункта предыдущих версий — если пользователю, выполнявшему установку ПО АП доменной политикой запрещалась запись в ветку реестра Windows "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet", это могло приводить к неработоспособности запрета незащищенных соединений.

# 2. Ограничения на поддержку аппаратных и программных средств

| | | | |
|---|---|---|---|
| **1** | Ключевые документы | Носители | • Дискета 3,5";<br>• USB-флеш-накопитель;<br>• RuToken ЭЦП<br>• USB-ключ eToken PRO (Java);<br>• смарт-карта eToken Pro (Java);<br>• RuToken S/ЭЦП;<br>• Secret Net Card/Secret Net Touch Memory Card;<br>• iButton DS1994/DS1995/DS1996;<br>• JaCarta PKI;<br>• JaCarta ГОСТ |
| **2** | Операционная система | АП | • Windows 10 версий 1703, 1709 (кроме всех выпусков Home Edition);<br>• Windows 8.1;<br>• Windows 7 SP1 (кроме всех выпусков Starter и Home Edition);<br>• Windows Server 2012 R2 Standard;<br>• Windows Server 2008 R2 SP1 |
| **3** | Предыдущие версии СКЗИ "Континент-АП" | Обновление предыдущих версий | 3.7.5.514, 3.7.5.474 |
| **4** | Устанавливаемые продукты | ПАК "Соболь" 3.0/3.1/3.2 | Исполнения АП – 2, 3, 4 |
| | | СКЗИ "КриптоПро CSP" 4.0 (версия 4.0.9842) | Исполнение АП – 3 |
| | | СЗИ Secret Net 7 (версия 7.4.544.0)/ Secret Net Studio (версии 8.2.1156, 8.3.1406) | Исполнение АП – 4 |

# 3. Особенности работы и ограничения

## 3.1. Общесистемные

**1.** Установку и удаление СКЗИ "Континент-АП" должен осуществлять пользователь, наделенный правами локального администратора компьютера.

**2.** Возможность подключения АП к СД до регистрации пользователя в ОС при совместном использовании с СЗИ Secret Net 7 не поддерживается.

**3.** Сообщение "Ошибка работы с криптопровайдером 0x0000001F. Присоединенное к системе устройство не работает" отображается при отсутствии на компьютере драйвера ПАК "Соболь". Проверить наличие драйвера можно в диспетчере устройств "Устройства идентификации> ПАК "Соболь".

**4.** USB-флеш-накопители объемом в 16 МБ и выше, определяемые системой как жесткий диск HDD, не используются в качестве ключевого устройства.

**5.** Для работы с криптопровайдером "Код Безопасности CSP" используются сертификаты, соответствующие ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012, для работы с криптопровайдером "КриптоПро CSP" – только ГОСТ Р 34.10-2001.

**6.** Начиная с 1 января 2019 года в СКЗИ "Континент-АП" запрещается использовать сертификаты, сформированные согласно ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94.

**7.** Корректное функционирование АП в среде ОС Windows 10 Insider Preview не гарантируется.

**8.** В АП, функционирующем под управлением англоязычной ОС Windows 10 версии 1709, не рекомендуется использовать символы кириллицы в названии контейнера закрытых ключей пользовательского сертификата.

**9.** Если на компьютере используется UEFI с возможностью включения/отключения опции безопасной загрузки (Secure Boot), перед установкой АП данную опцию необходимо отключить. В противном случае установка АП завершится с ошибкой.

## 3.2. Абонентский пункт

**1.** После установки АП в списке приложений, запускаемых при входе пользователя в систему, добавляется программа eapsigner161.exe. Если данную программу отключить (или пометить как запрещенную для автозапуска в ОС Windows 10), подключение АП к СД будет доступно только в режиме аутентификации с использованием расширенного сертификата. При попытке подключения АП, работающего в другом режиме аутентификации, будет появляться сообщение об ошибке: "Сервер отказал в доступе пользователю. Причина отказа: Client-Cert not found".

**2.** При подключении АП к СД в режиме запрета незащищенных соединений 3G/4G-модемы используются только в режиме CDC-Ethernet.

**3.** Для низкого уровня безопасности используется биологический ДСЧ. Для среднего и высокого уровней используется физический ДСЧ ПАК "Соболь".

**4.** В случае возникновения ошибок при установке АП повторите попытку установки при отключенных сетевых устройствах.

**5.** При установке АП на ноутбук набор энтропии с помощью сенсорной панели (тачпада) затруднителен. Поэтому набор энтропии следует выполнять с помощью манипулятора "мышь".

**6.** Набор энтропии при использовании средств удаленного доступа (RDP) невозможен.

**7.** Особенности совместной работы АП с продуктом "Антивирус Касперского" версий 6.0 и 7.0. Для корректного соединения АП с сервером доступа необходимо в антивирусной программе отключить режим проверки всех портов.

**8.** Особенность работы СКЗИ "КриптоПро CSP". Для смены пользователя компьютера необходимо завершить работу предыдущего пользователя (LogOff), а затем войти под новой учетной записью. При использовании команды Switch User возможна некорректная работа абонентского пункта.

**9.** Стандартным портом для соединения АП и СД является порт 4433. Если используется другой порт, то его номер должен быть указан явным образом в настройках подключения АП через двоеточие после IP-адреса сервера доступа.

**10.** Особенности использования FTP-сервера для хранения обновлений ПО АП. Для корректной проверки наличия обновления на FTP-сервере должен быть разрешен анонимный вход пользователей. В противном случае сообщения об обновлении поступать на АП не будут.

**11.** Не рекомендуется совместная установка ПУ СД и АП на один компьютер.

**12.** Для обеспечения совместной работы криптопровайдера "Код Безопасности CSP" и носителей eToken необходимо установить ПО "Единый Клиент JaCarta".

**13.** Особенность совместной работы абонентского пункта и СЗИ Secret Net 7/Secret Net Studio. Если криптопровайдер "Код Безопасности CSP" не может обнаружить на eToken закрытый ключ пользователя, необходимо ввести PIN-код этого носителя.

**14.** Если криптопровайдер "Код Безопасности CSP" не может обнаружить на eToken закрытый ключ пользователя, созданный средствами этого криптопровайдера, необходимо ввести PIN-код носителя с помощью программы "Код Безопасности CSP".

**15.** Особенность создания запроса на получение сертификата внешнего удостоверяющего центра. В поле ввода адреса нельзя использовать заглавные буквы. При заполнении текстовых полей запроса не допускается использование символов пробела до и после вводимого текста.

**16.** Производительность АП в режиме защищенного соединения можно повысить путем отключения функции TCP Delayed ACK в настройках сетевой карты:

- "Подключение через прокси" – на компьютере с установленным прокси-сервером;
- "Потоковое подключение (TCP)" " на компьютере с установленным АП.

**17.** Особенность настройки режима защищенного соединения "Подключение через прокси". Формат адреса прокси-сервера, указываемый в поле "Сервер", зависит от протокола аутентификации, используемого на прокси-сервере:

- Basic и NTLM – IP-адрес или сетевое имя;
- Kerberos и Negotiate – только сетевое имя.

**18.** В случае отмены набора энтропии после обновления ПО АП (с версий 3.7.5.514, 3.7.5.474 на 3.7.7.651) и перезагрузки ОС при попытке подключения АП к СД на экране появится сообщение "Ошибка 0x000000578, доп. код 0x00003AFC". Для устранения ошибки необходимо закрыть ПУ АП и запустить ее заново. На экране появится окно для набора энтропии.

**19.** В ходе процесса обновления предыдущей версии АП на экране появится сообщение об ошибке контроля целостности с просьбой обратиться к администратору. Сообщение носит информационный характер, его появление связано с обновлением списка файлов СКЗИ "Континент-АП" 3.7.7.651, требующих контроля их целостности, и не требует прерывания процесса обновления.

**20.** При установленном СЗИ SNS/SNS Studio аутентификация АП (исполнение 4) до входа в ОС невозможна.

**21.** Для аутентификации АП (исполнения 1, 2, 3) до входа в ОС под учетной записью локального пользователя необходимо правильно указать учетные данные – "имя компьютера\логин".

**22.** Функционирование СКЗИ "Континент-АП" в среде ОС Windows 10 сборки 1709, работающей в нагруженном режиме, может привести к падению ОС. Это связано с изменениями в сетевом стеке операционной системы.

## 3.3. Межсетевой экран

**1.** При использовании МЭ рекомендуется отключать Windows Firewall.

**2.** Для корректной работы фильтра список правил фильтрации не должен быть пустым. При установке МЭ по умолчанию задаются правила pass::; и pass:;, разрешающие прохождение любых пакетов через фильтр.

**3.** При установке АП задается признак вхождения компьютера в домен, и автоматически формируются правила фильтрации, действующие до входа пользователя в систему. Если компьютер не входит в домен, формируются два правила фильтрации, разрешающие DHCP (pass:udp port 67, pass:udp port 68). Если компьютер входит в домен, формируется более развернутый список правил фильтрации, действующих до входа пользователя в систему.

**4.** Регистрируемые события передаются в собственный журнал Terminal Station. Если установлено ПО Secret Net 7/Secret Net Studio, события также передаются в журнал Secret Net/Secret Net Studio.

**Компания "Код Безопасности"**

| | |
|---|---|
| Почтовый адрес: | 115127, Россия, Москва, а/я 66 |
| Телефон: | 8 495 982-30-20 |
| Факс: | 8 495 744-29-31 |
| E-mail: | info@securitycode.ru |
| Сайт: | http://www.securitycode.ru |