

Программный комплекс "Континент-СОА". Версия 4

Комментарии к сборке 4.0.3.6997

Документ содержит описание основных возможностей, особенностей работы и ограничений применения изделия "Программный комплекс "Континент-СОА". Версия 4" (далее – комплекс, ПК "Континент-СОА"), которые необходимо учитывать при эксплуатации комплекса.

Список сокращений

БД	База данных
БРП	База решающих правил
ДА	Детектор атак
МК	Менеджер конфигурации
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
СОА	Система обнаружения атак
СОВ	Система обнаружения вторжений
УБ	Узел безопасности
ЦУС	Центр управления сетью

Оглавление

1.	Размещение файлов на компакт-диске	3
1.1.	Диск 1	3
1.2.	Диск 2	3
1.3.	Диск 3	3
2.	Изменения и новые возможности	4
2.1.	Сборка 4.0.3.6997	4
3.	Ограничения на поддержку аппаратных и программных средств	4
4.	Особенности работы и ограничения	5
4.1.	Общие	5
4.2.	Система обнаружения вторжений	6
4.3.	Особенности обновления ПО	6
4.4.	Локальное управление узлами безопасности	7
4.5.	Система мониторинга	8

1. Размещение файлов на компакт-диске

1.1. Диск 1

Каталог	Содержимое
\.	Файлы обновления ПО ПК "Континент-СОА"
\images	Загрузочный образ ПК "Континент-СОА"
\isolinux	Загрузчик CentOS
\Packages	Пакеты с устанавливаемыми модулями
\repodata	Файлы хранилища
\Setup	Дистрибутив менеджера конфигураций ПК "Континент-СОА"
\Tools	Программа подсчета контрольных сумм и программа для записи образа диска на USB-флеш-накопитель
\USBFlash	Установочные образы модулей ПК "Континент-СОА", предназначенные для установки с USB-флеш-накопителя

1.2. Диск 2

Эксплуатационная документация	
Файл	Содержимое
Continent - Аудит - Admin Guide.pdf	Программный комплекс "Континент-СОА" Версия 4. Руководство администратора. Мониторинг и аудит
Continent - Deployment - Admin Guide.pdf	Программный комплекс "Континент-СОА" Версия 4. Руководство администратора. Ввод в эксплуатацию
Continent – IDS-IPS - Admin Guide.pdf	Программный комплекс "Континент-СОА" Версия 4. Руководство администратора. Обнаружение вторжений
Continent - IDS – Release Notes.pdf	Основные возможности, особенности работы и ограничения применения
Техническая документация	
Файл	Содержимое
RU.АМБС.58.29.12.008 30 – Формуляр.	Программный комплекс "Континент-СОА" Версия 4. Формуляр
RU.АМБС.58.29.12.008 30-1 - Приложение.pdf	Программный комплекс "Континент-СОА" Версия 4. Формуляр. Приложение 1
RU.АМБС.58.29.12.008 ТУ – Технические условия.pdf	Программный комплекс "Континент-СОА" Версия 4. Технические условия

1.3. Диск 3

Каталог	Содержимое
БРП\ids_update.json.gz	База решающих правил

2. Изменения и новые возможности

Ниже приводятся сведения об основных возможностях ПК "Континент-СОА" сборки 4.0.3.6997.

2.1. Сборка 4.0.3.6997

1. В блокировке конфигурации добавлена проверка на отсутствие администратора.
2. Добавлено обнаружение туннелей в dpi.
3. Повышена производительность.
4. Закрыты уязвимости CVE-2017-15377, CVE-2018-6794.
5. Исправлена восприимчивость встроенного NTP-сервера к атаке NTP Amplification Denial-Of-Service Attack CVE-2013-5211.
6. Актуализирован список команд в диагностической консоли.
7. Дополнено меню локального управления УБ и ЦУС.
8. В МК реализована возможность установления соединения с ЦУС в режиме "Только чтение".
9. Поддержка функции циклической записи сетевого трафика на внешний носитель.
10. Реализован механизм подключения к ГосСОПКА.
11. Улучшен механизм взаимодействия с Active Directory.

3. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	УБ	USB-флеш-накопитель
		МК	USB-флеш-накопитель
2	Операционная система	PM администратора	Windows Server 2016; Windows Server 2012 R2 Standard; Windows Server 2008 R2 Standard; Windows 10 x64 Enterprise; Windows 8.1 x64 Enterprise; Windows 7 SP1 x64 (кроме всех выпусков Starter и Home Edition)
3	Аппаратная платформа	Детектор атак	
		IPC-50	LN-010C
		IPC-500F	LN-015C
		IPC-800F	DV-030B
		IPC-1000NF2	DV-031F
		IPC-3000NF2	LN-021E
		Центр управления сетью	
		IPC-50M	LN-010M
		IPC-500M	LN-015M
		IPC-1000FM	DV-031M
		IPC-3000FM	LN-021M

4. Особенности работы и ограничения

4.1. Общие

1. Идентификатор шлюза, который запрашивается при установке ОС "Континент" на аппаратную платформу, в МК обозначается в свойствах УБ как "Серийный номер".
2. Не рекомендуется совместная установка TLS-клиента с "Код Безопасности CSP" и "КриптоПро CSP". В противном случае не гарантируется доступ к системе мониторинга и работа в МК.
3. При создании сертификата необходимо заполнить все поля диалога. При заполнении полей нельзя использовать символ кавычек и "!".
4. В названии домена или УБ нельзя использовать символы кириллицы.
5. При долговременном отсутствии связи между ЦУС и УБ может быть потеряна часть событий, отправляемых на ЦУС с УБ. Информацию о недостающих событиях можно найти в журналах УБ.
6. При превышении показателей производительности платформ, указанных в паспортах, возможно резкое снижение эффективности обнаружения атак.
7. В МК выполняемая задача при большом объеме передаваемых данных и медленной пропускной способности канала связи может завершиться по тайм-ауту со статусом "Ошибка", хотя при этом цели этой задачи могут быть успешно достигнуты за более длительный период времени.
8. После удаления УБ необходимо сохранить изменения в конфигурации, иначе ID вновь созданного УБ будет совпадать с ID только что удаленного узла, что приведет к ошибке.
9. Объем импортируемой с помощью МК резервной копии ограничен 4 Гбайт.
10. Настройка комплекса с помощью МК во время автоматического обновления БРП с сервера обновлений запрещается.
11. Если при выполнении длительной по времени задачи произойдет смена сертификата управления ЦУС, то по завершении операции соединение МК с ЦУС будет разорвано.
12. При повторной инициализации УБ в МК добавляется копия узла, созданного в результате первичной инициализации. В этом случае в МК узел, созданный в результате первичной инициализации, следует удалить вручную.
13. Создание сертификатов УБ возможно только по запросам.
14. При установке политики на отключенные или недоступные узлы она будет находиться в состоянии "Выполнение" до истечения тайм-аута 15 мин. и затем завершится со статусом "Ошибка".
15. Для смены сертификата управления требуется создать новый сертификат и назначить его нужному узлу в МК.
16. Для эффективной работы в МК его окно должно быть развернуто на весь размер экрана. Минимальное рекомендуемое разрешение экрана – 1024×768 пикселей.
17. Программное обеспечение МК совместимо с ПО "Код Безопасности CSP" только версии 4.0.2.55.
18. При удалении МК программное обеспечение "Код Безопасности CSP" не удаляется.
19. При использовании сертификатов внешнего УЦ аутентификация администраторов возможна только по логину и паролю.
20. Максимальное количество событий мониторинга и аудита для создания резервной копии не должно превышать 35 млн событий, иначе задача по созданию резервной копии завершится с ошибкой.
21. В текущей версии ПК "Континент-СОА" отсутствует возможность настройки уровня детализации событий, регистрируемых в журналах комплекса.
22. Если в лицензии не указан ID узла, то привязать лицензию можно только путем ее перемещения (drag-and-drop) из репозитория на необходимый узел.

4.2. Система обнаружения вторжений

1. При настройке списка переменных компонента "Детектор атак" (первоначально в нем указаны параметры по умолчанию) желательно использовать указанный формат записей. Если указать неверно параметр переменной ДА, политика успешно устанавливается, но СОВ перестает функционировать. В системных журналах появляется сообщение об ошибке в переменной (например, в HOME_NET). Для просмотра записей об ошибке необходимо перейти в системные журналы и сбросить фильтр, далее отфильтровать записи: по важности – Ошибка (ERR), по категории – Система.
2. Если при создании профиля СОВ отключить все вендорские правила, то после создания этого профиля они всё равно будут иметь способ противодействия такой же, какой установлен для них в полном наборе.
3. Дистанционное обновление по расписанию репутационных баз не поддерживается.
4. После принудительного обновления БРП через МК после загрузки новых решающих правил необходимо сохранить конфигурацию ЦУС, а затем установить на него политику.
5. Если после обновления БРП с сервера обновлений пользователь изменил, повредил или удалил сигнатуры, то повторно установить тот же набор сигнатур с сервера обновлений нельзя. Для решения этой проблемы необходимо обратиться в службу технической поддержки производителя.
6. Одновременное отключение большого количества сигнатур, загруженных на УБ, увеличивает время выполнения команды. При необходимости следует отключать сигнатуры частями.
7. При повторном открытии свойств профиля СОВ ранее выставленные отметки в чекбоксах не всегда отображаются. В таких случаях для отображения отметок в чекбоксах необходимо после установки отметок перейти на вкладку "Контроль приложений", проставить отметку в чекбоксе "Включить контроль приложений", убрать отметку в чекбоксе "Включить контроль приложений", нажать "Применить" и затем нажать "ОК", после чего установить политику на ДА.
8. В описании сетевого объекта или сервиса переменной СОВ нельзя использовать знак инверсии. Также нельзя использовать переменные с инверсией в составе других переменных.
9. При создании пользовательского профиля действие для пользовательских сигнатур автоматически выставляется "Оповещать" независимо от настройки. Для смены действия необходимо в списке с пользовательскими БРП для каждой конкретной сигнатуры выставить для конкретного профиля требуемое действие и сохранить изменения в конфигурации.
10. При большой нагрузке трафика возможно падение процесса контроля приложений на ДА в режиме Inline с последующим автоматическим перезапуском процесса, что не влияет на прохождение трафика.

4.3. Особенности обновления ПО

1. После обновления при создании пользовательской роли с полными полномочиями отсутствуют права для работы с вкладками "Структура" и "Администрирование".
2. После обновления не работает автоматическое издание сертификата управления для УБ. Обойти такое поведение можно перевыпуском сертификата вручную.
3. Перед обновлением ПО необходимо заменить существующие символы кириллицы в названиях узлов сети на латинские.
4. Обновление при наличии в составе аппаратной платформы дисков в RAID-массиве следует производить путем создания резервной копии БД, последующей локальной установки ОС новой версии и восстановления данных из сделанной копии. Дистанционное обновление не поддерживается.
5. Перед обновлением ПО необходимо удалить старый набор БРП и загрузить новый, в противном случае произойдет удвоение сигнатур.
6. Загрузка файлов обновления ПО в репозиторий по расписанию не производится.
7. После обновления комплекса или его восстановления из резервной копии ПК "Континент-СОА" необходимо изменить общие правила Disk_space_boot_critical и Disk_space_boot_warning для корневого домена.

Поле "Если":

```
filesystem.storage_devices.vg00.filesystems.Boot.usage.pused
```

заменить на:

```
filesystem.storage_devices.sda.filesystems.Boot.usage.pused
```

Поле "Причина":

Узел %host%. На разделе Boot использовано %value (filesystem.storage_devices.vg00.filesystems.Boot.usage.pused)%%

заменить на:

Узел %host%. На разделе Boot использовано %value (filesystem.storage_devices.sda.filesystems.Boot.usage.pused)%%

8. Перед обновлением ПО необходимо сделать резервную копию настроек мониторинга, иначе после обновления они восстановятся по умолчанию. Для восстановления настроек необходимо восстановить их из резервной копии. После этого необходимо произвести настройку общих шаблонов мониторинга в соответствии со следующим списком:

Имя правила	Содержание правила	Тип настройки
RAM_critical	Если ram.pused_buffers_cached >= 90 ...	Изменение
RAM_warning	Если ram.pused_buffers_cached >= 80 и ram.pused_buffers_cached < 90 ...	Изменение
Raid_status_check	Если: raid.devices.md126.status.check = 1; То: Предупреждение; Для: raid; Причина: Узел %host%. Выполняется проверка RAID	Добавление
Raid_status_degraded	Если: raid.devices.md126.status.degraded = 1 и raid.devices.md126.status.recovery != 1; То: Критичный; Для: raid; Причина: Узел %host%. RAID разрушен	Добавление
Raid_status_recovery	Если: raid.devices.md126.status.recovery = 1; То: Предупреждение; Для: raid; Причина: Узел %host%. Выполняется восстановление RAID	Добавление
Raid_status_resync	Если: raid.devices.md126.status.resync = 1; То: Предупреждение; Для: raid; Причина: Узел %host%. Выполняется ресинхронизация RAID	Добавление
Temperature_HDD1_critical	Если temperature.hdd.hdd1.now >= 55 ...	Изменение
Temperature_HDD1_warning	Если temperature.hdd.hdd1.now >= 45 и temperature.hdd.hdd1.now < 55 ...	Изменение
Temperature_HDD2_critical	Если temperature.hdd.hdd2.now >= 55 ...	Изменение
Temperature_HDD2_warning	Если temperature.hdd.hdd2.now >= 45 и temperature.hdd.hdd2.now < 55 ...	Изменение

9. После обновления ПО нужно заново настроить используемые фильтры по категории в виджетах панели мониторинга и статистики, а также используемые фильтры по категории и классификатору в сохраненных запросах для просмотра журнала сообщений COB.

10. Одновременное обновление ЦУС и УБ запрещается.

11. После отката обновления ПО УБ может потребоваться его повторная инициализация. Откат обновления не рекомендуется выполнять без крайней необходимости.

4.4. Локальное управление узлами безопасности

1. Отправка локальных изменений в настройках УБ на ЦУС может занимать до нескольких минут. Если конфигурация не отправилась в течение 1–2 минут, следует проверить наличие связи между ЦУС и УБ.

2. Средствами локального управления при диагностике сети использовать команду ping можно только на IP-адрес. При попытке использования на доменное имя появляется сообщение об ошибке, даже если в настройках узла указан адрес DNS-сервера. Через orepconsole возможно использование этой команды как на IP-адреса, так и на доменные имена.

3. В локальном меню УБ невозможно просмотреть/изменить адрес ЦУС, к которому он подключен, но его можно добавить.

4. При добавлении УБ через локальное меню проверка на уникальность ID отсутствует.

5. Перед началом процедуры инициализации УБ необходимо убедиться в отсутствии внешнего носителя в USB-разъеме.
6. Настройка часового пояса осуществляется:
 - для ЦУС – после его настройки;
 - для ДА – после их подключения к ЦУС.
7. Если во время применения локальных изменений нарушается связь между УБ и ЦУС, то локальные изменения применяются только на узле и не отправляются на ЦУС. В этом случае до перезагрузки в локальном меню узла появляется сообщение "Имеются непримененные локальные изменения". Для отправки изменений на ЦУС после восстановления связи УБ – ЦУС выберите пункт "Отправить локальные изменения на ЦУС" в разделе "Инструменты" локального меню узла.

4.5. Система мониторинга

1. Особенности мониторинга событий СОВ, зарегистрированных в предыдущих версиях ПО комплекса:
 - события СОВ могут быть зарегистрированы в журналах на английском языке;
 - для просмотра в журнале событий СОВ вместо фильтрации по классификатору следует использовать гибкий запрос и фильтр по категории, в котором необходимо удалить спецификатор точного соответствия, например:

категория.точно:"Возможная попытка утечки информации" -> категория:"Возможная попытка утечки информации";

category.raw:"Attempted information leak" -> category:"Attempted information leak";
 - не гарантируется корректная работа фильтра по категориям событий СОВ на виджетах панели мониторинга и статистики.
2. При использовании TLS-клиента вход в систему мониторинга возможен только по протоколу HTTPS (в противном случае произойдет ошибка CSRF-уязвимости).
3. При подключении к внешней БД с уже существующими таблицами и данными (СОВ, Аудит или Мониторинг) будет производиться переиндексация этих данных, что может занять длительное время (при 300 млн записей переиндексация может длиться больше суток).
4. При настройке системы мониторинга на работу с внешним сервером БД необходимо учитывать, что:
 - версии поискового движка elasticsearch (5.0.0 для сборки 4.0.3.6997) и СУБД postgresql (9.5.4 для сборки 4.0.3.6997) на ЦУС и внешнем сервере БД должны совпадать;
 - при потере соединения с внешней БД сайт мониторинга будет недоступен;
 - в технологическом отчете узла не будет данных аудита за последние сутки.
5. Для работы в Internet Explorer при использовании конфигурации усиленной безопасности для скачивания дампа атаки в журнале СОВ в список надежных сайтов необходимо добавить "about:blank".
6. Если часовой пояс в настройках мониторинга и РМ администратора различается, то в журналах аудита и СОВ фильтры по времени работают по часовому поясу на РМ администратора.
7. Особенности просмотра системы мониторинга через веб-браузер:
 - В случае длительного простоя системы с открытой панелью мониторинга возможно длительное восстановление функционирования браузера. После восстановления браузер продолжает функционировать корректно.
 - В случае сбоев в соединении с сервером после восстановления связи необходимо обновить страницу браузера. В противном случае функционирование системы будет ограниченным.
 - При работе с системой на нескольких вкладках веб-браузера Internet Explorer использование команды "Выйти" в меню пользователя на одной из этих вкладок приведет к открытию окна авторизации на всех используемых вкладках.
8. Если в настройках пользователя системы мониторинга задать группировку для счетчиков событий СОВ по сетевому интерфейсу, протоколу или сервису, то счетчики событий СОВ на верхней панели главного окна будут некорректно работать, отображая нулевые значения.
9. В настройках виджета "Структура" отсутствует автозаполнение при фильтрации по узлам. Фильтр работает по введенной подстроке.

10. В виджете "Таблица – Данные – Мониторинг" отображаются текущие или средние значения за 1, 5, 15 минут, в зависимости от настроек виджета. Уточнить текущий интервал можно, перейдя в режим конфигурирования виджета.
11. Подключение к системе мониторинга с использованием сертификата администратора отсутствует. Подключение возможно только с использованием логина и пароля администратора.
12. Для открытия журнала большого объема (более 100 млн записей) рекомендуется выполнять фильтрацию сообщений (по важности, категории, дате и др.).
13. Экспорт журнала в системе мониторинга выполняется со скоростью не более 1 Мбайт/с.

Компания "Код Безопасности"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	8 495 982-30-20
Факс:	8 495 744-29-31
Email:	info@securitycode.ru
Web:	https://www.securitycode.ru