Комплекс безопасности "Континент". Версия 4
Комментарии к сборке 4.1.0.2825

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

Список сокращений

АП	Абонентский пункт
БД	База данных
БРП	База решающих правил
ДА	Детектор атак
КУ	Криптоускоритель
ЛМ	Локальное меню
МК	Менеджер конфигурации
МЭ	Межсетевой экран
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
РЦУС	Резервный центр управления сетью
СД	Сервер доступа
СМА	Система мониторинга и аудита
СОВ	Система обнаружения вторжений
УБ	Узел безопасности
ЦУС	Центр управления сетью
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
HSM	Hardware Security Module
MTU	Maximum Transmission Unit
NAT	Network Address Translation
SNAT	Source Network Address Translation
UTC	Coordinated Universal Time (англ.)
UTM	Unified Threat Management

Оглавление

1. Основные возможности

Ниже приводятся сведения об основных возможностях комплекса "Континент" версии 4.1.0.2825.

1.1. Версия 4.1.0.2825

1. Реализованы следующие режимы работы УБ:

- UTM;
- Высокопроизводительный МЭ;
- Детектор атак.

2. В режиме UTM на одном УБ могут одновременно использоваться следующие компоненты:

- ЦУС;
- межсетевой экран;
- приоритизация трафика;
- L2VPN;
- L3VPN;
- детектор атак;
- сервер доступа;
- идентификация пользователей;
- модуль поведенческого анализа.

3. Реализован отказоустойчивый кластер УБ.

4. Реализован механизм приоритизации информационных потоков (QoS).

5. Реализован механизм подключения к нескольким каналам провайдеров (Multi-WAN).

6. Реализована подпись обновлений БРП и ее проверка.

7. Реализовано использование исключений при HTTPS-инспекции.

8. Расширен список протоколов для nDPI.

9. Реализован импорт правил из Check Point R77.30 и R80.20.

10. Реализован импорт пользовательских сигнатур для СОВ из файла.

11. Реализован экспорт данных о потоках по протоколу Netflow.

12. Реалзиван механизм аутентификации при синхронизации времени по протоколу NTP.

13. Обновлен список категорий БРП СОВ.

14. Реализовано управление сбором данных о событиях в nxlog.

15. Реализовано управление из МК доступом к УБ по протоколу SSH.

16. Реализован механизм генерации файлов конфигурации для большого количества УБ.

17. Реализована динамическая маршрутизация (OSFP, BGP) в режиме NF2.

18. Реализовано управление составом ядер, используемых для обработки трафика в NF2.

19. Реализована интеграция с Active Directory:

- возможен импорт учетных записей пользователей в БД ЦУС;
- возможно использование учетных записей в правилах фильтрации.

20. Реализован высокопроизводительный МЭ.

21. Реализованы агент аутентификации пользователей и Captive Portal для контролируемого доступа пользователей к веб-ресурсам.

22. Выполнена английская локализация интерфейса.

23. По умолчанию доступ по SSH-протоколу к УБ закрыт, реализована настройка контролируемого доступа.

24. Реализован DHCP-ретранслятор.

25. Реализована автоматическая настройка Proxy ARP при создании правил трансляции SNAT и DNAT.

26. Реализован импорт сетевых объектов из файла.

2. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	УБ	USB-флеш-накопитель
		МК	USB-флеш-накопитель
2	Операционная система	РМ администратора	Windows Server 2016; Windows Server 2012 R2 Standard; Windows Server 2008 R2 Standard; Windows 10 x64 Enterprise; Windows 8.1 x64 Enterprise
3	Аппаратные платформы	IPC-10	LN-010A
		IPC-25	MS-S115
		IPC-50	LN-010C
		IPC-50	LN-010M
		IPC-100	S102
		IPC-400	S021
		IPC-500	LN-015B
		IPC-500M	LN-015M
		IPC-500F	LN-015C
		IPC-600	DV-030A
		IPC-600M	DV-030M
		IPC-800F	DV-030B
		IPC-1000	S021
		IPC-1000F	S021
		IPC-1000F	DV-031B
		IPC-1000F2	S021
		IPC-1000FM	DV-031M
		IPC-1000NF2	DV-031F
		IPC-3000F	LN-021
		IPC-3000F	S021
		IPC-3000FM	LN-021M
		IPC-3000FC	LN-021A
		IPC-3000NF2	LN-021E
		IPC-R300	SC R300
		IPC-R550	SC R300
		IPC-R10	SC R15
		ICP-R50	SC R15

4	Внешнее ПО	Версия внешней БД Postgresql – 11.1. Версия поискового движка Elasticsearch – 6.1	

3. Особенности работы и ограничения

3.1. Общие

1. Идентификатор УБ, который запрашивается при установке ПО на аппаратную платформу, в МК обозначается в свойствах УБ как "Идентификатор".

2. В названии УБ нельзя использовать символы кириллицы. В названии хоста, домена из специальных символов можно использовать только дефис.

3. После удаления УБ из базы ЦУС необходимо сохранить изменения в конфигурации, иначе, если ID вновь созданного УБ будет совпадать с ID только что удаленного узла, то это приведет к системной ошибке.

4. Настройка комплекса с помощью МК во время автоматического обновления БРП с сервера обновления запрещается. Переподключение рекомендуется выполнять после перезагрузки ЦУС с новой версией По или после обновления МК на новую версию ПО.

5. После установки обновления ПО на ЦУС, МК отключается от ЦУС. Для дальнейшей работы требуется переподключение.

6. Если при выполнении длительной по времени задачи произойдет смена сертификата управления ЦУС, то по завершении операции соединение МК с ЦУС будет разорвано.

7. Для смены сертификата управления необходимо создать новый сертификат и назначить его нужному узлу в МК. При этом последовательность действий должна быть следующей:

- выпуск нового сертификата;
- его назначение узлу без отзыва старого сертификата;
- установка политики;
- удаление старого сертификата.

8. Программное обеспечение МК совместимо с ПО "Код Безопасности CSP" только версии 4.0.857.0.

9. При удалении МК программное обеспечение "Код Безопасности CSP" не удаляется.

10. Не рекомендуется создавать резервную копию с количеством записей в журналах более 100 млн.

11. При создании сертификатов канала связи УБ и ЦУС рекомендуется использовать внутренние ресурсы комплекса без привлечения внешних удостоверяющих центров сертификации.

12. В названии сертификатов нельзя использовать символы кириллицы. Название сертификата не должно содержать более 45 символов.

13. Если установить УБ в режиме UTM с включенной инспекцией протоколов или WEB/FTP-фильтрацией между прокси-сервером и компьютером пользователя, то клиентский трафик при выходе в интернет через прокси не будет фильтроваться и подвергаться инспекции.

14. Если между УБ и ЦУС не будет связи на момент истечения срока действия сертификата канала управления УБ – ЦУС, то невозможно будет его поменять вручную. Рекомендуется строго следить за сроком действия сертификатов (при этом необходимо ориентироваться на даты, а не на статус "Действительности/Недействительности" сертификатов).

15. В текущей версии не поддерживается иерархическая структура сети.

16. В текущей версии комплекса не поддерживается управление узлами безопасности других версий.

17. При включении механизма WEB/FTP фильтрации поддерживается корректная работа следующих FTP-серверов:

Серверы	Microsoft Internet Information Services (7.5.7600.16385)
	ProFTPD 1.3.5a
	Vstpd 3.0.3
Клиенты	wget 1.17.1, curl 7.47.0, fetch, ftp (Unix)
	Filezilla 3.22.1
	Windows FTP Client (Explorer 11.0.9600.17031)
	WinSCP 5.9.3 (сборка 7136)

18. Подключение АП4 к СД4 по протоколу UDP не поддерживается.

19. После создания и редактирования учетной записи администратора и пользовательской роли происходит автоматическое сохранение конфигурации с формированием задачи на установку политики.

20. Получение адресов от DHCP-сервера по каналу L3VPN возможно только при наличии на УБ статических маршрутов до сетей DHCP-клиентов и при включении подсети DHCP-клиентов в L3VPN.

21. В настройках сервиса DHCP как после включения режима сервера или ретранслятора, так и после отключения сервиса во избежание появления ошибок необходимо нажимать кнопку "Применить" перед переходом на другую вкладку настроек УБ. Если этого не делать, возможно появление ошибок при отключении DHCP и последующем удалении адреса на интерфейсе, который использовался для настройки DHCP.

22. При настройке LDAP-профиля в поле "База поиска" не допускается использование пробелов между компонентами базы поиска.

23. При подключении к УБ по SSH-протоколу при быстром неоднократном вводе неправильного пароля блокировка учетной записи происходит с задержкой. В результате могут быть пропущены дополнительные попытки ввода неправильного пароля.

24. Если профиль DHCP настраивается для работы через relay-агент, то в профиле нельзя указывать интерфейс, на котором настроено несколько IP-адресов.

25. Пользователи, уже подключенные к серверу доступа, во время установки политики автоматически переподключаются, даже если для них нет изменений в этой политике. Рекомендуется в правило удалённого доступа добавлять группу пользователей и внутри группы выполнять операции добавление/ изменение/ удаление пользователей. В таком случае при применении политики автоматическое переподключение пользователей к серверу доступа выполняться не будет.

26. При переключении виртуального коммутатора (L2VPN) с динамического обучения на обучение в режиме sticky, MAC-адреса сохраняют тип "Динамический" (в режиме обучения sticky MAC-адреса хостов записываются в таблицу коммутации как статические). Чтобы сменить тип MAC-адресов на "Статический" рекомендуется выключить виртуальный коммутатор (который ранее работал в режиме динамического обучения), установить политику на УБ, участвующие в L2VPN, включить виртуальный коммутатор и повторно поставить политику на УБ.

27. В текущей версии комплекса выполняется динамическое обучение MAC-адресов на туннельных интерфейсах виртуального коммутатора, даже если настройка "Динамическое обучение" выключена.

28. При подключении к платформе IPC-R300 и IPC-R550 через последовательный порт не отображается меню настроек ПАК «Соболь».

29. В текущей версии протокол IPv6 не поддерживается.

30. В текущей версии комплекса не поддерживается совместная работа режимов "Приоритизация трафика" и "L3VPN".

31. Изменения приоритета не применяются к related-сессиям.

32. В текущей версии комплекса отсутствует возможность задания логина и пароля при подключении к прокси-серверу для обновления ПО комплекса, БРП и фидов Kaspersky.

33. При импорте правил МЭ и правил трансляции сетевых адресов из CheckPoint необходимо выбрать имя политики и версию набора правил в раскрывающемся списке, включая случаи если имя политики по умолчанию соответсвует политике, из которой производится импорт правил.

34. В текущей версии комплекса отсутствует возможность добавить в МК сертификат, выпущенный сторонним УЦ, если запрос на сертификат не был сформирован в МК.

35. Для работы канала управления МК–ЦУС требуется пропускная способность канала не менее 1024 Кбит/с.

36. Для работы канала управления ЦУС–УБ требуется пропускная способность канала не менее 1024 Кбит/с.

3.2. Особенности восстановления резервной копии ПО

1. После восстановления настроек мониторинга из резервной копии на ЦУС для корректного восстановления настроек сбора статистики для УБ необходимо перезагрузить УБ.

2. В текущей версии комплекса после восстановления ЦУС из резервной копии индексация событий может занять продолжительное время.

3. При восстановлении данных мониторинга и аудита из резервной копии на ЦУС с настроенной удаленной БД выполняется полная переиндексация БД на ЦУС и самой удаленной БД. Полная переиндексация БД занимает длительное время.

4. При восстановлении резервной копии УБ с установленным пакетом расширенного контроля приложений на УБ без пакета расширенного контроля приложений,например, когда УБ находится в состоянии сразу после установки ПО до инициализации, после подключения восстановленного узла к ЦУС необходимо установить пакет расширенного контроля приложений и применить политику.

5. После восстановления конфигурации УБ из резервной копии, содержащей более раннюю версию конфигурации, чем на данный момент на нем установлена, на ЦУС не поступает информация о том, что у восстановленного из бекапа УБ изменилась версия конфигурации.

3.3. Управление узлами безопасности

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

2. В локальном меню УБ невозможно просмотреть/изменить адрес ЦУС, к которому он подключен, но его можно добавить.Дополнительные адреса, через которые УБ могут подключиться к ЦУС, можно задать через МК.

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

4. Перед началом процедуры инициализации УБ необходимо убедиться в отсутствии внешнего носителя в USB-разъеме.

5. Настройка часового пояса осуществляется:

- для ЦУС – после его настройки;
- для УБ – после их подключения к ЦУС.

6. 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 неприменные 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.

7. Если монитор не поддерживает стандарт VESA, то аппаратная платформа не загружается.

8. Подключение УБ к домену Active Directory осуществляется по протоколу LDAPS. Подключение по протоколу LDAP не поддерживается.

9. Агент аутентификации не может подключиться к УБ по IP-адресу, подключение выполняется только по доменному имени.

10. Для схемы L3VPN с топологией "Полносвязная сеть" между двумя УБ, находящимися за StaticNat, тоннель не построится.

11. Для схемы L3VPN с топологией "Централизованная сеть" между двумя УБ, находящимися за StaticNat тоннель построится, если один из них не является центральным узлом L3VPN сети.

12. При создании на УБ более 500 VLAN-интерфейсов возможно замедление работы МК.

13. Установка политики разблокирует порты, ранее блокированные механизмом port security.

14. Полученные в результате обучения в sticky-режиме MAC-адреса устройств удаляются из таблицы коммутации после перезагрузки УБ, а также после установки политики на УБ.

15. Особенность смены режимов работы УБ с UTM на "Высокопроизводительный МЭ" и обратно. После смены режима для корректной работы Proxy ARP необходимо отключить правила NAT типа «Отправителя» и «Получателя», поставить политику на УБ, затем восстановить (включить) правила NAT и снова установить политику.

16. Сервер доступа принимает запрос на подключение от АП на всех интерфейсах УБ.

17. В текущей версии комплекса при настройке СД в МК не поддерживается назначение нескольких пулов IP-адресов АП.

18. В случае, если L2VPN используется для защиты канала между портами коммутационного оборудования с включенным протоколом LACP, рекомендуется использовать настройку Pseudo Wire виртуального коммутатора.

19. Откат обновления ПО ЦУС выполнять не рекомендуется.

20. После переключения УБ из UTM в ДА необходимо перезагрузить УБ для его дальнейшей корректной работы в режиме ДА.

21. После восстановления копии резервного ЦУС на РЦУС и в дальнейшем переключении ЦУС на этом узле в активный режим, на остальных РЦУС произойдет автоматическая синхронизация БД с этим ЦУС.

22. В ЛМ поиск по кнопке F7 осуществляется только по строкам только ниже выделенной.

23. Запросы на порты 443 (СД) и 80, 443 (Captive Portal) при активированном на УБ соответствующем компоненте не обрабатываются правилом DNAT и принимаются узлом безопасности. При направлении запроса на УБ с настроенным proxy arp правило DNAT сработает и перенаправление произойдет.

24. При миграции резервных копий, созданных на версии 4.0.3, на версию 4.1.0 необходимо удалить из конфигурации NAT правила, в которых не совпадают протоколы в параметрах "Исходный пакет" и "Преобразованный пакет", и NAT правила, для которых установлена инспекция протоколов в сервисах.

25. Для корректной работы веб-мониторинга, при смене активного ЦУС на резервный необходимо выпустить на резервном ЦУС новый корневой сертификат с алгоритмом подписи RSA и выпустить персональный сертификат для веб-мониторинга с этим корневым сертификатом.

26. Если после смены активного ЦУС на резервный необходимо выпустить персональный сертификат УБ, необходимо на резервном ЦУС выпустить новый корневой сертификат с алгоритмом подписи ГОСТ 34.10-2012 (256) и выпустить персональный сертификат для УБ с этим корневым сертификатом.

27. Если на узле добавлено несколько сертификатов с ролью "Сервер доступа", то активным сертификатом, используемым для подключения удаленных клиентов с АП будет сертификат с последней датой окончания действия сертификата.

28. Задача установки обновления ipoque на узел без лицензии на соответствующий компонент завершается ошибкой. В МК отсутствует описание ошибки при попытке установить обновление.

3.4. Особенности управления кластером УБ

1. Создание и восстановление резервной копии кластера выполняется совместно с резервным копированием и восстановлением БД ЦУС. Перед созданием кластера необходимо убедиться в идентичности настроек интерфейсов типа "bond" и "vlan". Если после создания кластера не добавляются кластерные виртуальные интерфейсы, необходимо исключить из состава кластера УБ, настроить на УБ виртуальные интерфейсы и заново добавить узлы в кластер. После восстановления кластера из резервной копии необходимо установить на кластер политику.

2. СД в составе кластера запускается на основном и резервном узлах. Для его настройки необходимо выпускать сертификат СД для каждого УБ в кластере.

3. Сервер доступа не синхронизирует подключения пользователей к СД в режиме кластера. Если в кластере произошла смена основного УБ на резервный, то пользователям АП для продолжения работы после разрыва соединения необходимо снова подключиться.

4. Не рекомендуется использовать агрегированные сетевые интерфейсы для сети синхронизации и для резервирования сети синхронизации в кластере, т. к. в этом случае не гарантируется корректная работа сети синхронизации.

5. Не рекомендуется установка локальной политики на УБ, объединенных в кластер, так как это может привести к конфликту версий конфигурации.

6. В случае разрыва сети синхронизации с последующим нарушением связей между всеми внутренними и внешними интерфейсами узлов кластера возникает ситуация split brain – оба узла кластера становятся активными.

Для восстановления работоспособности кластера необходимо восстановить сеть синхронизации.

7. В одном широковещательном домене (L2-сегменте) допустимо использование только одного кластера.

8. При отправке транзитных пакетов в L3VPN-туннель в кластере в качестве IP-адреса отправителя используется адрес внешнего интерфейса активного в данный момент УБ, а не виртуальный IP-адрес самого кластера.

9. В текущей версии комплекса кластер формируется только на базе двух УБ.

10. На УБ, входящих в кластер, отсутствует синхронизация установленных сессий пользователей Captive Portal.

11. При создании/удалении интерфейса с типом "Резервирование сети синхронизации" сетевой трафик, идущий через кластер, будет прерываться на 5–15 с во время установки политики с данными настройками.

12. В режиме синхронизации "ALARM" при выбранном транспортном протоколе синхронизации "Multicast UDP" трафик основного УБ перенаправляется на основной канал, а трафик резервного УБ остается на резервном канале при соблюдении следующих условий:

- основной и резервный каналы сети синхронизации были поочередно отключены, и возникла ситуация split brain;
- затем основной и резервный каналы сети синхронизации были поочередно включены соответственно.

После выключения/включения линка резервного канала весь трафик синхронизации направляется по основному каналу.

13. В канале синхронизации допустимой является задержка не более 30 мс.

14. Автоматическое переключение активности в кластере с резервного узла на основной при включённой опции "Автоматическое переключение при восстановлении основного узла безопасности" может происходить с задержкой в несколько секунд. При этом прерываний трафика при переключении нет, либо они минимальны (менее 1сек).

15. Запрещено настраивать DHCP-профиль в режиме "Ретранслятор" в кластере.

16. Счетчики переданных данных между УБ в составе кластера не синхронизируются.

17. Компоненты QoS, Multi-WAN и Поведенческий анализ необходимо настраивать после создания кластера, их конфигурация не наследуется из УБ.

18. Для корректной работы Captive Portal на кластере, необходимо создать отдельный сертификат Портала аутентификации для каждого УБ, входящего в кластер и привязать их к узлам. Эти сертификаты не будут отображаться на вкладке "Идентификация пользователей" окна свойств УБ.

19. Не рекомендуется использовать агрегацию LACP на интерфейсах кластера в режиме NF2.

20. Правило DNAT не работает, если для параметра "Получатель" указан диапазон или сеть, в которую входит один из адресов УБ кластера.

3.5. Особенности работы УБ с криптоускорителем

1. Если между двумя узлами безопасности, образующими VPN-канал и имеющими в своем составе КУ, расположено устройство с трансляцией адресов (например, маршрутизатор), такое устройство должно удовлетворять следующим условиям:

- трансляция адресов должна осуществляться в обе стороны, например, NAT 1:1;
- если осуществляется трансляция udp-портов, номера udp-портов после трансляции не должны выходить за границы диапазона 10000-10255.

2. УБ с КУ на границе с сетью Интернет рекомендуется использовать в режиме HSM.

3. Шифрование трафика на УБ, имеющем в своем составе КУ, выполняется только средствами КУ.

4. Если объект имеет доступ к хотя бы одной VPN-сети за УБ с КУ, то он будет иметь доступ ко всем VPN-сетям за этим УБ с КУ.

5. В текущей версии комплекса маршрутизация трафика из одной локальной сети, находящейся за одним внутренним интерфейсом, в другую, находящейся за другим внутренним интерфейсом, на УБ с КУ не реализована.

6. Использование криптоускорителей в кластере поддерживается только в режиме HSM.

7. В текущей версии комплекса УБ с КУ не пропускает фрагментированный трафик.

8. IP-адреса внешних интерфейсов КУ, находящихся в разных сетях и использующих маршрутизатор, не должны совпадать в первом октете.

9. Не рекомендуется совместное использование программного и аппаратного VPN, так как возможно возникновение проблем, приводящих к нестабильной связи между клиентами, подключенных к УБ с КУ и L2VPN.

10. Особенность работы УБ с КУ в режимах L2VPN и L3VPN. На УБ с установленным компонентом L2VPN в режиме transparent действует ограничение в 512 MAC-адресов. В виртуальном коммутаторе считается общее количество MAC-адреса на всех УБ. В режиме pseudowire нет ограничений по количеству MAC-адресов.

На УБ с установленным компонентом L3VPN действует ограничение в 256 ARP-записей.

3.6. 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. После импорта БРП из файла посредством МК необходимо обновить список сигнатур, сохранить конфигурацию, затем установить политику.

3. 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.

4. Одновременное отключение большого количества сигнатур, загруженных на УБ, увеличивает время выполнения команды. При необходимости следует отключать сигнатуры частями. Отключать можно только пользовательские сигнатуры, вендорские – нельзя.

5. При фильтрации сетевого трафика средствами ДА не учитывается номер порта, указанный в поле "Сервис" в настройках правил фильтрации.

6. Не поддерживается настройка виртуальных интерфейсов bridge и loopback на интерфейсах Inline, Monitor.

7. В текущей версии комплекса инверсия пользовательских переменных СОВ устанавливается в контекстном меню переменной. Инверсия встроенных переменных СОВ устанавливается с помощью символа "!" перед переменной.

8. В текущей версии комплекса не поддерживается работа с диапазоном адресов в списках исключений, на которые не распространяется контроль приложений в профиле СОВ.

9. Если после обновления с версии 4.0.3 на версию 4.1 в логах регистрируются ошибки, относящиеся к сигнатурам, рекомендуется обновить БРП.

3.7. Система мониторинга и аудита

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 классу, 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. 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".

4. Если часовой пояс в настройках мониторинга и РМ администратора различается, то в системном журнале, журнале сетевой безопасности и журнале управления фильтры по времени работают по часовому поясу на РМ администратора.

5. 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.

6. Подключение к системе мониторинга с использованием сертификата администратора отсутствует. Подключение возможно только с использованием логина и пароля администратора.

7. Для открытия журнала большого объема (более 100 млн записей) рекомендуется выполнять фильтрацию сообщений (по важности, классу, дате и др.).

8. Экспорт журнала в СМА выполняется со скоростью не более 1 МБ/с.

9. Для открытия экспортированных журналов необходимо использовать кодировку UTF-8.

10. При установке политик, связанных с редактированием/добавлением маршрутов, сертификатов, IP-адресов, в системном журнале регистрируется критическое сообщение "Узел % был отключен (% время в секундах %)".

11. После выпуска двух сертификатов RSA в ЛМ и удаления второго из них в МК доступ к СМА с использованием первого сертификата невозможен. Для восстановления доступа к СМА необходимо выпустить и применить третий сертификат.

12. При использовании твердотельного накопителя SSD возможны кратковременные ложные срабатывания правил мониторинга, определяющих наличие сбойных блоков на диске, и генерация событий мониторинга с уровнем важности "критический".

13. При настройке отправки журналов по расписанию на внешний syslog-сервер или ЦУС не учитывается часовой пояс узла. Временные интервалы необходимо указывать относительно UTC.

14. Для ускорения обработки запросов в журналах комплекса рекомендуется выполнять регулярное удаление устаревших записей. Для этого необходимо корректно настроить автоматическую очистку журналов.

15. Возможны сбои в работе УБ на базе платформы IPC-100 при группировке более 10 млн записей по IP-адресу.

16. При использовании УБ на базе платформ IPC-100, IPC-500 рекомендуется одновременная работа в СМА только одному администратору ввиду ограниченной производительности платформ.

17. Не рекомендуется одновременное подключение к системе мониторинга более 3 пользователей.

18. Граничные значения температур в мониторинге, предназначенные для уведомления администратора, могут отличаться для разных платформ. Если граничные значения температур не соответствуют используемой платформе, то их возможно перенастроить в общем шаблоне структуры мониторинга.

19. В режиме NF2, пропускная способность всех интерфейсов в командной строке и в SNMP отображается как 10M.

3.8. Межсетевой экран

1. Если на УБ сначала настроить правило WEB/FTP-фильтрации, затем правило контроля приложений/инспекции протоколов с одинаковыми критериями срабатывания (отправитель, получатель, порты), то будет выполнено только правило WEB/FTP-фильтрации.

2. Не поддерживается использование антиспуфинга в автоматическом режиме при асимметричных маршрутах на внутренних интерфейсах.

3. В VPN-канале не функционируют механизмы WEB/FTP-фильтрации и инспекции протоколов.

4. При настройке в правилах фильтрации временных интервалов, устанавливаемых на узлы безопасности, находящиеся в разных часовых поясах, следует учитывать разницу во времени между УБ.

В ходе эксплуатации комплекса может возникнуть ошибка применения политики:

- если разница между концом суток и концом временного интервала меньше разницы между часовым поясом УБ и UTC-0;
- или разница между началом суток и началом временного интервала меньше разницы между часовым поясом УБ и UTC-0.

5. Одновременная настройка WEB/FTP-фильтрации и инспекции протоколов в одном правиле фильтрации не поддерживается.

6. Одновременная настройка WEB/FTP-фильтрации и контроля приложений в одном правиле фильтрации не поддерживается.

7. Использование SSL/TLS-инспекции в рамках WEB/FTP-фильтрации может привести к сбоям в работе приложений, использующих SSL-соединение. В комплексе "Континент" корректная работа таких приложений обеспечивается путем их включения в список исключений. В этом случае они не подвергаются SSL/TLS-инспекции. В текущей версии в

список входят следующие приложения: Skype, WhatsApp, Dropbox, ICQ (официальный клиент), сервер обновления Windows (Windows Update), Google Drive, Яндекс Диск.

Наличие списка исключений может привести к невозможности блокировки некоторых ресурсов, имеющих отношение к вышеперечисленным сервисам, средствами WEB/FTP-фильтрации (например, к поддоменам microsoft.com или skype.com).

8. Особенности режима высокой производительности МЭ в текущей версии комплекса:

- не работает утилита диагностики интерфейсов;
- в BIOS Setup УБ должен быть выключен режим Hyber-Threading;
- на ЦУС режим высокой производительности МЭ не поддерживается;
- в сетевых интерфейсах поддерживается только значение MTU=1500. Переключение из стандартного режима МЭ с установленным значением MTU, отличным от 1500, в высокопроизводительный режим не происходит;
- не поддерживается динамическая маршрутизация;
- не поддерживается настройка инерфейсов bridge и loopback;
- не поддерживается настройка метрик маршрутов;
- режим высокой производительности МЭ поддерживается только на старших платформах;
- в режимах трансляции адресов "Скрыть" и "Отправителя" src port в преобразованном пакете подменяется на произвольное значение в промежутке от 1024 до 65536 (в том числе в случае, когда src port свободен);
- использование NAT правил с типом "Отобразить" для объединения двух пересекающихся подсетей в L3VPN невозможно;
- не поддерживается работа WEB/FTP-фильтрации, защита от вредоносных WEB-сайтов, контроля приложений, аутентификации пользователей,СД, L2VPN, ДА, модуля поведенческого анализа в режиме высокоскоростного МЭ.

9. В случае работы SIP-сервиса на нестандартном порту (отличном от 5060) не поддерживается автоматическая регистрация связанных с основным SIP-соединением вспомогательных сессий, что делает невозможным нормальное использование этого сервиса. В правилах фильтрации следует открывать соответствующие порты для телефонов той или иной марки. Ограничение справедливо для режима UTM.

10. При попытке установить hotfix с пакетом расширенного контроля приложений на УБ без лицензии на расширенный контроль приложений узел будет перезагружен.

11. В правилах трансляции недопустимо использовать в качестве критериев срабатывания сервисы с инспекцией протоколов.

12. Инспекция протокола FTP на УБ в режиме UTM реализуется корректно только в случае, когда запрос на подключение к FTP-серверу выполняется по стандартным портам.

13. Не рекомендуется настраивать динамическую маршрутизацию на ЦУС.

14. В случае работы SIP-сервиса на стандартном порту (5060) автоматическая регистрация связанных с основным SIP-соединением вспомогательных сессий работает, когда весь трафик (SIP+RTP) проксируется через АТС (режим АТС-Proxy). Ограничение справедливо для режима UTM.

15. В текущей версии комплекса для корректной реализации динамической маршрутизации необходимо в конфигурационном файле BIRD продублировать статические маршруты.

16. После загрузки пакета обновлений для расширенного контроля приложений номер версии ПО УБ и значение его контрольной суммы не меняется.

17. В режиме "Высокопроизводительный МЭ" не работает динамическая маршрутизация по протоколу OSFP.

Компания "Код Безопасности"

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