КОД БЕЗОПАСНОСТИ

Континент
Версия 4

Руководство администратора

Модуль поведенческого анализа

RU.АМБС.58.29.12.001 90 10

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Документ предназначен для администраторов изделия " Континент.Версия 4" (далее — комплекс "Континент", комплекс). В документе содержатся сведения, необходимые администраторам для ознакомления с назначением и принципами функционирования модуля поведенческого анализа комплекса "Континент".

Дополнительные сведения, необходимые администратору комплекса, содержатся в документах [**1**] – [**7**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/products/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.
Страница службы технической поддержки на сайте компании "Код Безопасности" https://www.securitycode.ru/services/tech-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Список сокращений

МК	Менеджер конфигурации
МПА	Модуль поведенческого анализа
ОС	Операционная система
ЦУС	Центр управления сетью
УБ	Узел безопасности
DNS	Domain Name System
DoS	Denial of Service
FIN	Final
ICMP	Internet Control Message Protocol
IP	Internet Protocol
RST	Reset The Connection
SYN	Synchronize Sequence Numbers
UDP	User Datagram Protocol
UTM	Unified Threat Management
VPN	Virtual Private Network

Общие сведения

Назначение и основные функции

Модуль поведенческого анализа — это самообучаемый программный модуль, предназначенный для обнаружения атак сканирования, атак на основе корректности протоколов и угроз типа "отказ в обслуживании". В основе работы модуля лежат методики анализа характеристик сетевого трафика с учетом их изменений во времени с помощью набора шаблонов атак.

Наборы шаблонов, поддерживаемые МПА, представлены в таблице ниже.

Тип атаки	Название в МК	Краткое описание шаблона	Примечание
SYN-сканирование	SYN-scan	Шаблон обнаружения сканирования портов отправкой SYN-пакетов с одного IP-адреса	
FIN/RST-сканирование	FIN/RST-scan	Шаблон обнаружения сканирования портов отправкой FIN- или RST-пакетов с одного IP-адреса	
ICMP-сканирование	ICMP-scan	Шаблон обнаружения ICMP-сканирования установлением порогового значения количества ICMP ECHO REQUEST пакетов с одного IP-адреса	
UDP-сканирование	UDP-scan	Шаблон обнаружения ICMP PORT UNREACHABLE пакетов, отправляемых IP-адресу, с установлением порогового значения числа UDP-соединений с этого IP-адреса	
ICMP-пакеты, состоящие только из заголовка	Null Payload ICMP packet	Шаблон обнаружения ICMP-пакетов, состоящих только из заголовков	
Превышение размера DNS запроса/ответа	DNS max length	Шаблон обнаружения превышения максимального размера DNS-запроса/DNS-ответа	
Корректность пакетов	Packet Sanity	Шаблон проверки корректности параметров пакетов (TCP-флаги, ненулевые порты)	
Снижение размера пакета	Small Packet MTU	Шаблон обнаружения DoS-атаки, при которой атакующий отправляет большие объемы данных с использованием небольших пакетов. Пакеты имеют большие издержки, потребляя ресурсы сервера	
DNS-spoofing	DNS-spoofing	Шаблон обнаружения атаки MITM ("человек посередине"), в которой данные кеша доменных имен изменяются злоумышленником с целью возврата ложного IP-адреса	
Несовпадающие ответы DNS	DNS-mismatch	Шаблон обнаружения различных DNS-ответов на один DNS-запрос в течение заданного интервала времени	
Неверные ответы DNS	DNS-reply mismatch	Шаблон обнаружения DNS-ответов с несоответствующим идентификатором запроса или портом в течение заданного интервала времени	

Тип атаки	Название в МК	Краткое описание шаблона	Примечание
SYN-flood	SYN-flood	Шаблон обнаружения DoS-атаки, при которой осуществляется отправка, превышающая установленное количество SYN-пакетов в течение заданного интервала времени одному IP-адресу	
SMURF-атака	SMURF-attack	Шаблон обнаружения поддельного широковещательного пинг-запроса с использованием IP-адреса жертвы в качестве исходного IP-адреса. Все хосты сети отвечают на такой запрос	Источники атак не отслеживаются
FIN/RST-flood	FIN/RST-flood	Шаблон обнаружения DoS-атаки, при которой осуществляется отправка, превышающая установленное количество FIN- или RST-пакетов в течение заданного интервала времени одному IP-адресу	
FRAGGLE-атака	FRAGGLE-attack	Шаблон обнаружения атак, аналогичный SMURF, использующий поддельные широковещательные UDP-пакеты	
LAND-атака	LAND-attack	Шаблон обнаружения атаки, при которой осуществляется отправка SYN-пакетов с совпадающими адресами отправителя и получателя	Источники атак не отслеживаются

МПА анализирует внешний и внутренний трафик, в том числе трафик, поступающий из туннелей VPN после его расшифрования. Для блокировки трафика МПА создает правила фильтрации.

В случае обнаружения атаки МПА выполняет одно из трех действий:

- регистрирует событие в журнале сетевой безопасности и временно блокирует источник атаки;
- регистрирует событие в журнале сетевой безопасности;
- собирает статистику.

МПА функционирует в трех режимах. Названия и описания режимов представлены в таблице ниже.

Режим	Описание
Обучение по времени	Администратор задает временной промежуток работы модуля в режиме обучения. Изначально МПА работает с типовыми значениями. В процессе обучения модуль обрабатывает трафик, создает правила фильтрации и запоминает среднюю нагрузку узлов сети. Когда обучение заканчивается, модуль работает с теми значениями, которые получил в процессе обучения. Режим "Обучение по времени" включается для каждого нового IP-адреса в сети
Постоянное обучение	Модуль обрабатывает трафик, создает правила фильтрации и запоминает среднюю нагрузку узлов сети на протяжении всего периода активности
Приостановить	Модуль отключен

События, связанные с работой МПА как программного компонента УБ, регистрируются в системном журнале. В журнале управления регистрируются события, связанные с изменением конфигурации УБ или настроек МПА.

МПА функционирует только на УБ в режиме UTM.

Запуск Менеджера конфигурации

Для запуска Менеджера конфигурации:

- активируйте в главном меню ОС Windows команду "Код Безопасности | Менеджер конфигурации" или на рабочем столе ОС Windows ярлык приложения "Менеджер конфигурации".

  На экране появится окно "Менеджер конфигурации".

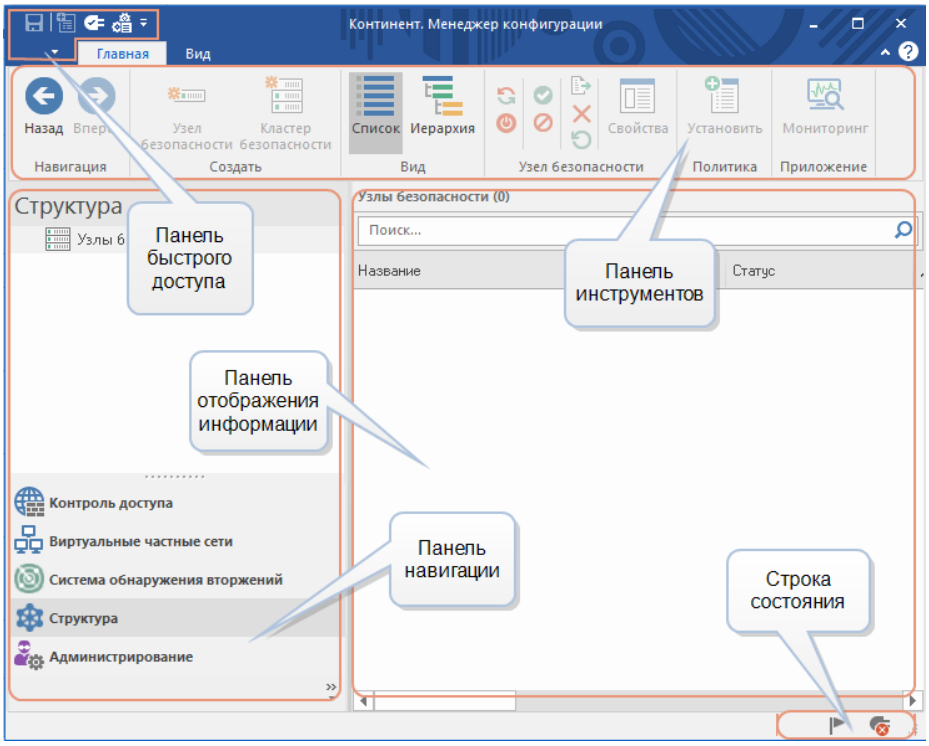
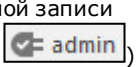


Рис.1 Окно "Менеджер конфигурации"

Окно "Менеджер конфигурации" содержит следующие основные элементы интерфейса:

Элемент интерфейса	Описание
Панель инструментов	Содержит набор инструментов и две вкладки: • "Главная" — отображает панель инструментов; • "Вид" — настраивает отображения элементов окна Менеджера конфигурации. Инструменты — это функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора подраздела на панели навигации, а их доступность определяется текущей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией
Панель быстрого доступа	Предназначена для быстрого доступа к часто используемым командам. Содержит настраиваемые кнопки: •  — сохранение текущей конфигурации; •  — установка политики безопасности; •  — настройка подключений к ЦУС и панели быстрого доступа; •  — установка соединения с ЦУС; •  — настройка панели быстрого доступа; •  — вызов меню команд быстрого доступа
Панель навигации	Содержит следующие разделы: • "Контроль доступа" — предназначен для управления правилами фильтрации и трансляции трафика; • "Виртуальные частные сети" — предназначен для создания и настройки VPN, организации удаленного доступа; • "Система обнаружения вторжений" — предназначен для настройки параметров системы обнаружения и предупреждения вторжений; • "Структура" — предназначен для управления параметрами УБ комплекса; • "Администрирование" — предназначен для управления сервисными функциями (работа с сертификатами, резервными копиями, управление лицензиями, обновлением и др.)
Панель отображения информации	Предназначена для отображения информации выбранного раздела панели навигации
Строка состояния	Содержит следующие данные: • число выполняемых задач и кнопку вызова центра уведомлений  , содержащего информацию о выполняемых задачах и ссылку на переход к общему списку задач; • пиктограмму состояния соединения с ЦУС (при установленном соединении — с именем учетной записи авторизованного администратора, к примеру )

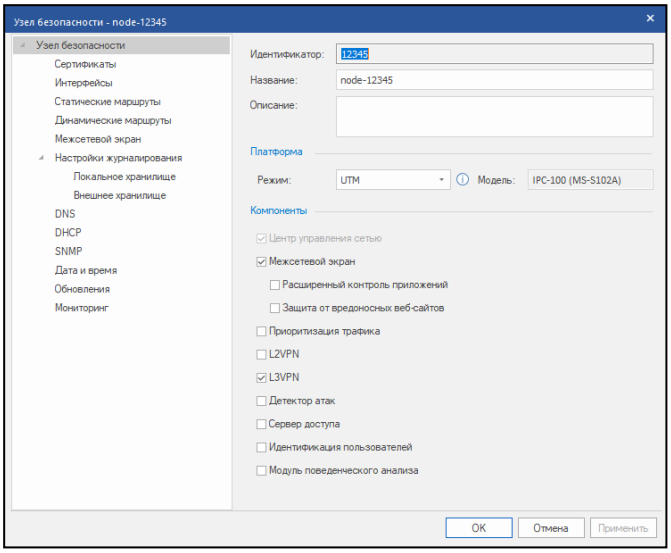
Эксплуатация

Активация МПА

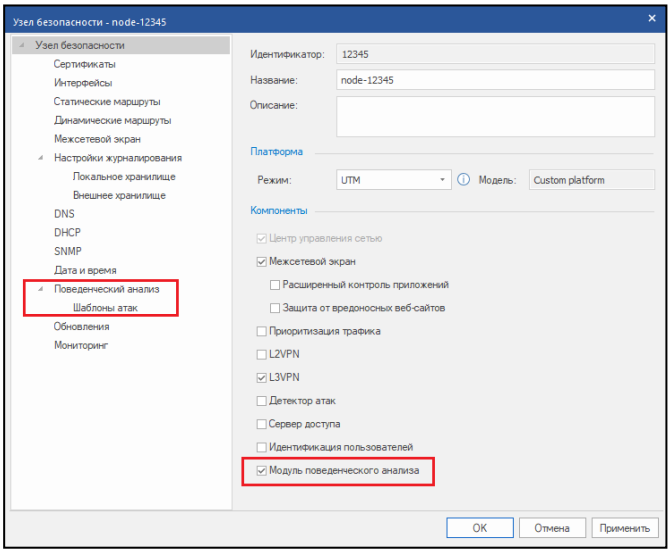
Перед активацией МПА убедитесь, что УБ находится в режиме UTM.

Для активации модуля:

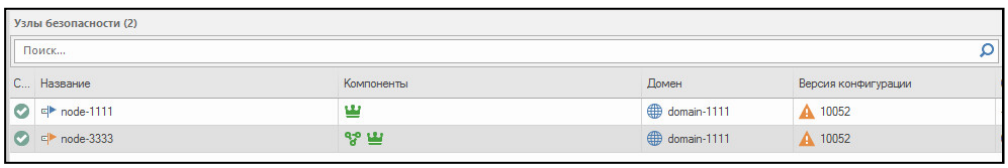
1. Перейдите в свойства узла безопасности в режиме UTM.



2. Отметьте в списке компонентов "Модуль поведенческого анализа".
   В меню "Узел безопасности" появятся новые пункты:



МПА будет активирован. В разделе "Структура" в столбце "Компоненты" появится значок  .

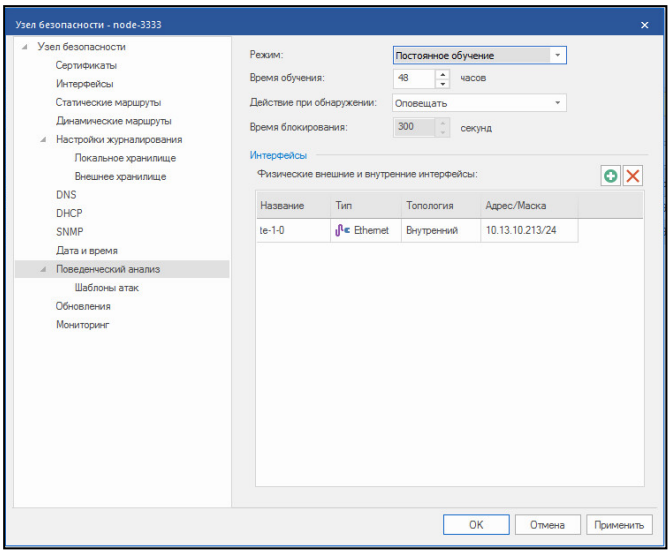


Настройка МПА

Для настройки МПА:

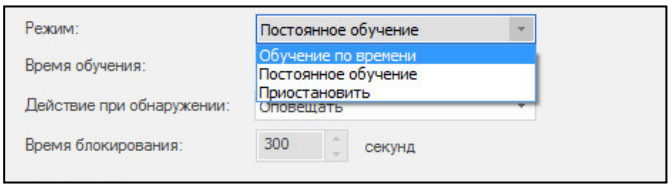
1. Выберите пункт "Поведенческий анализ".

   Окно примет вид:

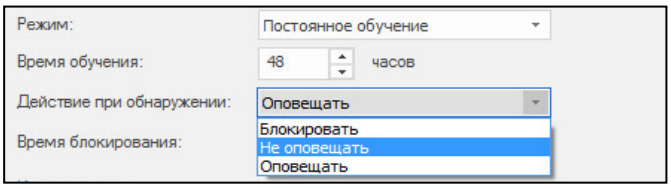


   Окно условно делится на две области: область настроек и область интерфейсов.

2. В области настроек установите режим работы МПА.

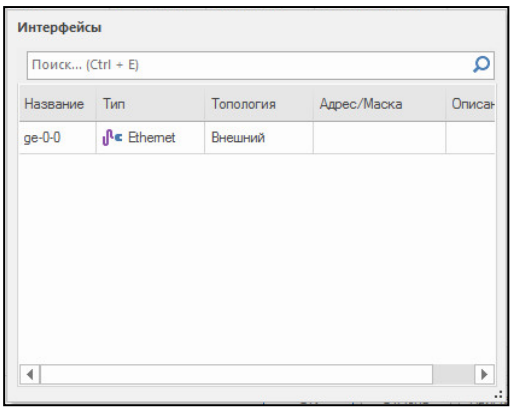


3. Задайте время обучения при необходимости.
4. Выберите действия МПА при обнаружении атаки из списка:

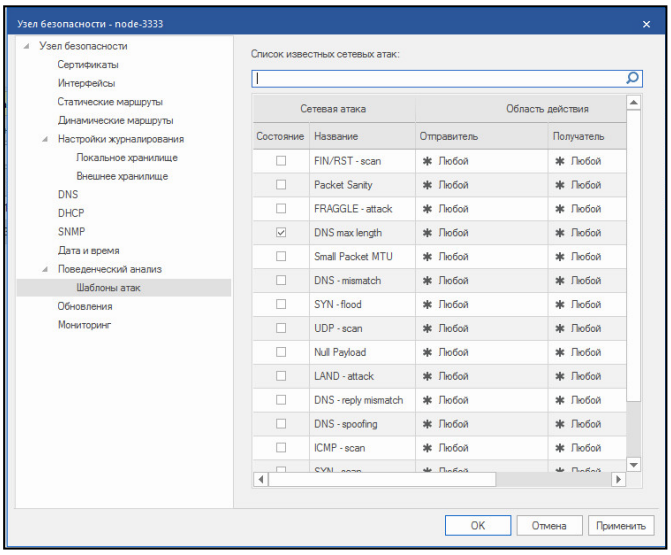


5. Задайте время блокировки при необходимости.
6. Укажите внутренние и внешние интерфейсы, на которые будет распространяться действие МПА. Нажмите кнопку  .

   Откроется окно:

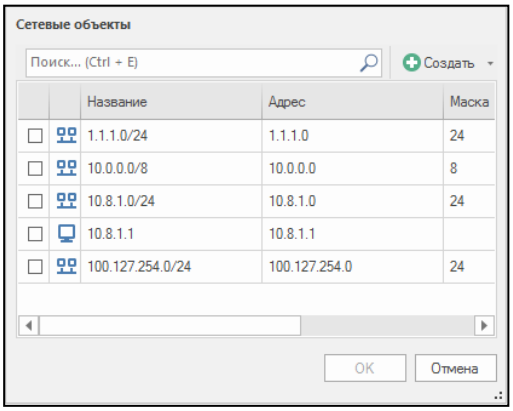


7. Выберите интерфейс. Он автоматически появится в таблице окна "Поведенческий анализ", окно "Интерфейсы" закроется. Чтобы удалить интерфейс, выберите его в таблице и нажмите кнопку .
8. Нажмите "Применить".
9. Выберите пункт "Шаблоны атак".



10. Отметьте поле в столбце "Состояние" для тех шаблонов атак, которые должен отслеживать МПА.
11. Для настройки полей "Отправитель" и "Получатель" наведите мышь на ячейку таблицы и нажмите кнопку .

    Появится окно:



12. Отметьте сетевые объекты и нажмите кнопку "ОК".

При необходимости в этом окне можно вызвать диалог создания нового сетевого объекта.

13. Нажмите "ОК" в окне "Узел безопасности".

14. Установите политику.

Команды локального меню

Операции в локальном меню УБ выполняются с помощью командной строки.

Чтобы открыть командную строку, запустите локальное меню УБ и перейдите "Инструменты | Диагностика | Командная строка".

Ipset-листы имеют название вида RG#_dos_protect, где # значение от 1 до 65534. При каждой установке политики значение увеличивается на единицу. После перезагрузки УБ значение RG# сбрасывается на "1"

Доступные к выполнению команды представлены в таблице ниже:

Команда	Описание
ipset list	Вывод всех ipset-листов, чтобы узнать значение RG#
ipset list RG#_dos_protect	Просмотр списка IP-адресов, заблокированных в данный момент модулем поведенческого анализа
ipset del RG#_dos_protect A.B.C.D	Удаление адреса A.B.C.D из списка заблокированных модулем поведенческого анализа, где A.B.C.D — условное обозначение
ipset flush RG#_ dos_protect	Полная очистка списка заблокированных МПА IP-адресов

Документация

1. Континент. Версия 4. Руководство администратора. Принципы функционирования.
2. Континент. Версия 4. Руководство администратора. Ввод в эксплуатацию.
3. Континент. Версия 4. Руководство администратора. Межсетевое экранирование.
4. Континент. Версия 4. Руководство администратора. Настройка VPN.
5. Континент. Версия 4. Руководство администратора. Обнаружение и предотвращение вторжений.
6. Континент. Версия 4. Руководство администратора. Сетевые функции.
7. Континент. Версия 4. Руководство администратора. Управление комплексом.