УТВЕРЖДЕН

RU.НКБГ.30045-01 33-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ DIONIS-SMP 1.0

Руководство программиста

RU.НКБГ.30045-01 33

Листов 97

2022

Литера «$О_1$»

Инв. № подл.	Ф0234
Подпись и дата	
Взам. инв. №	
Инв. № дубл.	
Подпись и дата	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Настоящий документ представляет собой руководство программиста «Программного обеспечения Dionis-SMP 1.0» RU.НКБГ.30045-01 (далее – ПО Dionis-SMP 1.0).

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Назначение

ПО Dionis-SMP 1.0 предназначено для:

- управление функциями маршрутизации, межсетевого экранирования и обнаружения вторжений ПАК Dionis-NX и ПАК Dionis DPS;
- мониторинг параметров функционирования М-479Рх;
- мониторинг параметров функционирования М-479РхК;
- обновление программного обеспечения ПАК Dionis-NX и ПАК Dionis DPS;
- возможность работы с конфигурациями ПАК Dionis-NX и ПАК Dionis DPS:
  - загрузку конфигураций;
  - хранение истории конфигураций;
  - обнаружение изменений в конфигурациях;
  - редактирование конфигураций;
  - разбор конфигураций;
  - создание переменных для последующего их использования в скриптах;
- возможность изменения конфигурации ПАК Dionis-NX и ПАК Dionis DPS при помощи скриптов:
  - создание, редактирование, хранение скриптов;
  - создание, редактирование, хранение шаблонов переменных для скриптов;
  - выполнение скриптов на группе узлов ПАК Dionis-NX и ПАК Dionis DPS;
  - автоматизированное создание скриптов для изменения списков ACL;
  - автоматизированное создание скриптов для изменения списков NAT;
  - автоматизированное создание скриптов для изменения расписаний IPsec соединений;
  - автоматизированное создание скриптов для изменения пулов адресов IPsec соединений;
  - автоматизированное создание скриптов для изменения черных списков субъектов IPsec соединений;
- выполнение скриптов в заданный момент времени, периодически и по недельному расписанию;
- возможность обмена информацией по протоколам SMTP, syslog, Netflow;
- развертывание и функционирование в среде операционной системы специального назначения (ОС СН) Astra Linux Special Edition (версия 1.6) РУСБ.10015-01 (далее -ОС СН Astra Linux SE), сертифицированной по требованиям безопасности информации;

– представление текущих событий в контролируемых информационных системах в графическом виде;
– построение автоматизированных отчетов о событиях информационной безопасности в формате PDF;
– возможность поиска зарегистрированных уязвимостей информационной безопасности в базе данных общеизвестных уязвимостей CVE (Common Vulnerabilities and Exposures).

2.2 Условия применения

Для выполнения программного обеспечения Dionis-SMP 1.0 необходимо установить программно-аппаратное устройство «Сторож С» («Сторож»), предназначенное для защиты авторских прав разработчика и изготовителя ПО Dionis-SMP 1.0, а также обеспечения его бесперебойной работы.

Минимальной областью действия является локальная сеть, развернутая на Dionis-NX (см. Рисунок 1). Dionis-NX подключаются к компьютеру с установленным ПО Dionis-SMP 1.0, далее с помощью ПО Dionis-SMP 1.0 проводится мониторинг и управление параметрами работы Dionis-NX, обнаружение вторжений и сбор информации о работе сети.

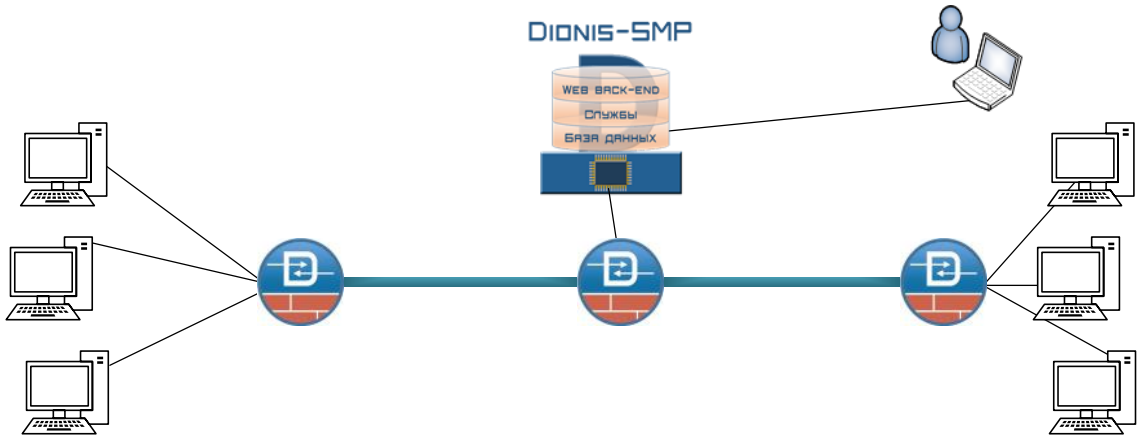


Рисунок 1 – Область действия ПО Dionis-SMP 1.0

В ПО Dionis-SMP 1.0 имеется возможность горизонтального масштабирования и объединения комплексов в иерархию с передачей информации об определенных событиях на верхние уровни иерархии, передачу конфигураций и правил обнаружения вторжений на нижние уровни иерархии, что позволяет строить системы управления произвольного масштаба (см. Рисунок 2).

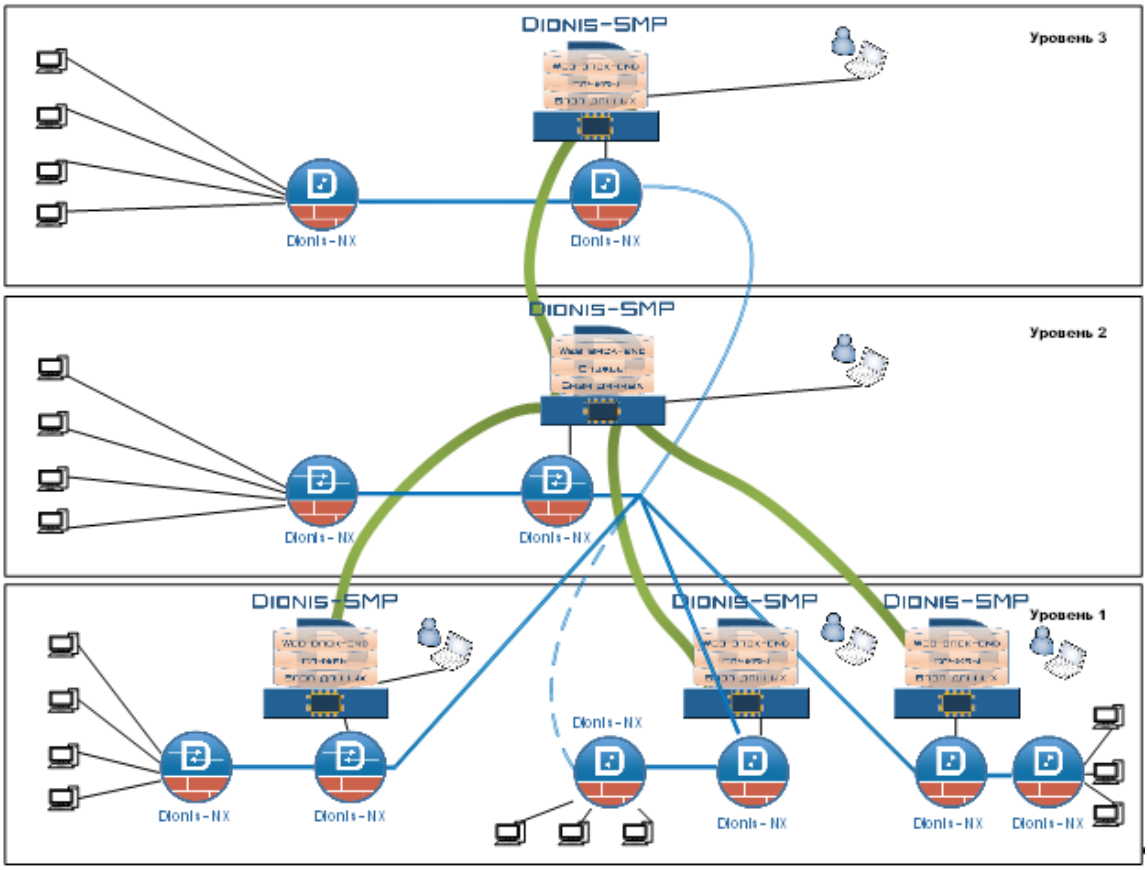


Рисунок 2 – Иерархия серверов с установленным ПО Dionis-SMP 1.0

2.3 Субъекты доступа (роли) ПО Dionis-SMP 1.0

Разделение доступа пользователей к ПО Dionis-SMP 1.0 реализовано на основе ролевой модели.

Разрешения на доступ к ПО Dionis-SMP 1.0 приведены далее:

- Администрирование устройств и топологии;
- Изменение правил IPS;
- Просмотр пользователей и ролей;
- Управление пользователями и ролями;
- Изменение скриптов и переменных;
- Очистка БД;
- Изменение системных настроек;
- Изменение правил корреляции;
- Управление подписками;
- Просмотр журналов аудита.

Субъектами доступа являются пользователи ПО Dionis-SMP 1.0 .

По умолчанию в системе доступно 3 роли:

– Системный администратор – роль позволяет осуществлять настройку и управление ПО Dionis-SMP 1.0 , а также управление пользователями и ролями. Содержит все вышеуказанные разрешения.

– Администратор – роль позволяет осуществлять настройку и управление ПО Dionis-SMP 1.0 , кроме управления пользователями и ролями. Содержит все разрешения, кроме управления пользователями и ролями.

– Оператор – роль позволяет осуществлять просмотр всей информации в системе, а также просмотр пользователей и ролей. Содержит все разрешения на просмотр информации, а также разрешение на просмотр пользователей и ролей.

Системный администратор имеет возможность создавать любое количество учетных записей с разными правами доступа кроме разрешений на управление пользователями и ролями.

В ПО Dionis-SMP 1.0 в обязательном порядке должна присутствовать предустановленная учетная запись пользователя admin с ролью Системный администратор.

В обязанности Системного администратора входят действия по соблюдению информационной безопасности в соответствии со своей должностной инструкцией, а также регламентами организации. В рамках своих полномочий по администрированию системы Системный администратор должен выполнять следующие функции:

- периодически осуществлять смену паролей пользователей ПО Dionis-SMP 1.0 ;
- анализировать содержимое журналов (логов) и реагировать на возникающие нештатные ситуации согласно должностной инструкции;
- обеспечивать своевременное архивирование журналов событий и обеспечивать надлежащее хранение данных архивов;
- проверять состояние используемых правил обнаружения атак, осуществлять проверку правильности их настройки;
- осуществлять выполнение скриптов на защищаемых устройствах;
- формировать отчеты по событиям, с периодичностью в соответствии с регламентом;
- предотвращает несанкционированные модификации программного обеспечения, добавление новых функций, несанкционированный доступ к информации, аппаратуре и другим общим ресурсам вычислительной сети.

2.4 Права на доступ к интерфейсам ПО Dionis-SMP 1.0

У разрешения на доступ есть контекст и права доступа.

Перечень контекстов приведен далее в таблице (Таблица 1).

Таблица 1

Название	Объекты доступа
attacks	Атаки
sensors	Устройства, Топология
rules	Правила СОВ
stats	Статистика
accounts	Пользователи, роли
scripts	Скрипты, переменные
profile	Настройки профиля
maintenance	Очистка БД
settings	Системные настройки
correlation_rules	Правила корреляции
correlation_groups	Группы правил корреляции

Перечень прав доступа приведен далее в таблице (Таблица 2):

Таблица 2

Название	Описание
edit	Доступ на редактирование
view	Доступ на просмотр

Связи разрешений ролей, контекстов доступа и прав доступа приведены далее в таблице (Таблица 3).

Таблица 3

Разрешение	Контекст	Доступ
attacks_viewer	attacks	view
sensors_viewer	sensors	view
sensors_admin	sensors	edit
rules_viewer	rules	view
rules_admin	rules	edit
statistics_viewer	stats	view
accounts_viewer	accounts	view

accounts_admin	accounts	view, edit
scripts_viewer	scripts	view
scripts_admin	scripts	view, edit
maintenance_viewer	maintenance	view
maintenance_admin	maintenance	view, edit
settings_viewer	settings	view
settings_admin	settings	view, edit
correlation_rules_viewer	correlation_rules	view
correlation_rules_admin	correlation_rules	view, edit
correlation_groups_viewer	correlation_groups	view
correlation_groups_admin	correlation_groups	view, edit

2.5 Описание принципов безопасной работы ПО Dionis-SMP 1.0

2.5.1 Общая информация

ПО Dionis-SMP 1.0 реализует следующие функции безопасности:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- регистрация событий безопасности (РСБ);
- обнаружение вторжений (СОВ);
- обеспечение целостности информационной системы и информации (ОЦЛ).

При использовании ПО Dionis-SMP 1.0 должны выполняться следующие меры по защите информации от несанкционированного доступа к информации:

- необходимо соблюдать парольную политику;
- пароль не должен включать в себя легко вычисляемые сочетания символов;
- личный пароль пользователь не имеет права сообщать никому;
- при вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

При эксплуатации ПО Dionis-SMP 1.0 запрещено:

- оставлять без контроля не заблокированное ПО Dionis-SMP 1.0 ;
- разглашать пароли, выводить пароли на дисплей, принтер или иные средства отображения информации.

2.5.2 Компрометация паролей

Под компрометацией паролей следует понимать следующее:

- физическую утерю носителя с парольной информацией;

- передачу идентификационной информации по открытым каналам связи;
- перехват пароля при распределении идентификаторов;
- сознательную передачу информации постороннему лицу.

При компрометации пароля пользователь ПО Dionis-SMP 1.0 обязан незамедлительно оповестить Системного администратора.

2.5.3 Описание параметров (настроек) безопасности ПО Dionis-SMP 1.0 , доступных каждой роли пользователей, и их безопасные значения

Настройки (параметры) безопасности ПО Dionis-SMP 1.0 доступны только пользователю с ролью Системный администратор и заключаются в возможности управления ролями пользователей ПО Dionis-SMP 1.0 . Пользователям должны назначаться минимальные права и привилегии, необходимые для выполнения ими своих должностных обязанностей (функций).

3 ПОДГОТОВКА К РАБОТЕ

3.1 Режимы работы с ПО Dionis-SMP 1.0

Все действия в ПО Dionis-SMP 1.0 всегда производятся от имени какой-либо учетной записи. Перед началом работы пользователь должен войти в систему -ввести своё имя (имя учетной записи) и затем ввести свой пароль. Учётная запись пользователя с ролью Системный администратор создается при установке ПО Dionis-SMP 1.0 с логином admin и паролем «123123».

3.2 Начало сеанса работы

Для аутентификации в консоли Системного администратора необходимо выполнить следующие действия:

1. Запустить интернет-обозреватель и в адресной строке набрать адрес http://<ip_или_имя_сервера>:<порт>.

ПО Dionis-SMP 1.0 поддерживает интернет-браузеры:

- Mozilla Firefox (версии не ниже 44.0.2);
- Google Chrome (версии не ниже 66.0.3359.139).

2. Авторизоваться под учетной записью пользователя с ролью Системный администратор, для чего в окне авторизации заполнить поля «Пользователь» и «Пароль».

3. Нажать кнопку «Вход».

Открывается WebUI пользователя.

После первого входа в систему рекомендуется сменить пароль. Для этого необходимо перейти в раздел «Управление пользователями». Перейти в карточку пользователя Системный администратор. В поле «Пароль» ввести новое значение пароля и нажать кнопку «Добавить». Пароль пользователя будет обновлён.

Новый пароль должен содержать:

- от 8 до 255 символов;
- заглавные буквы;
- строчные буквы;
- цифры;
- спецсимволы.

Срок действия установленного пароля составляет 45 дней. По истечении срока действия необходимо сменить пароль. Смена устаревшего пароля выполняется аналогично смене пароля после первого входа. Новый пароль должен отличаться от трех ранее вводимых паролей. После трех неуспешных попыток аутентификации учетная запись пользователя блокируется до разблокировки администратором.

По умолчанию для привилегированных учетных записей возможно не более одной

одновременной сессии доступа. Количество одновременных сессий указывается при создании учетной записи.

При превышении допустимого количества сессий отобразится окно с информационным сообщением (Рисунок 3).

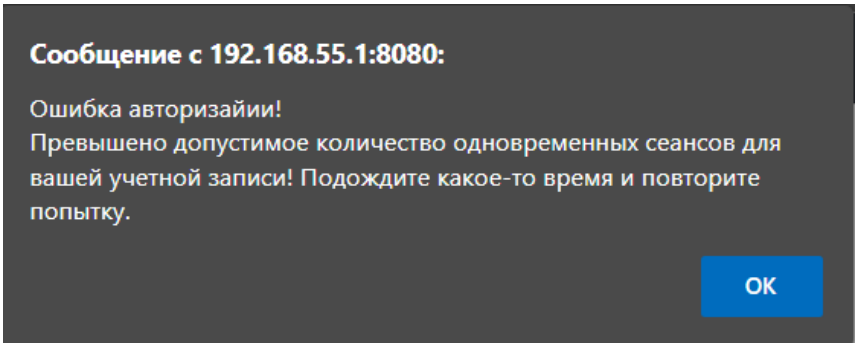


Рисунок 3

При нажатии кнопки «ОК» отобразится страница аутентификации для входа в систему.

Если после входа пользователь ПО Dionis-SMP 1.0 был неактивен более 5 минут, произойдет автоматический выход из нее и отобразится страница аутентификации. Настройка выполняется в конфигурационном файле ~/.config/factor/development.ini установлено значение auth_timeout_min=15. Для продолжения работы необходимо выполнить процедуру входа в ПО Dionis-SMP 1.0 , введя на странице аутентификации данные в поля «Пользователь» и «Пароль» и нажав кнопку «Войти» (см. Рисунок 4).

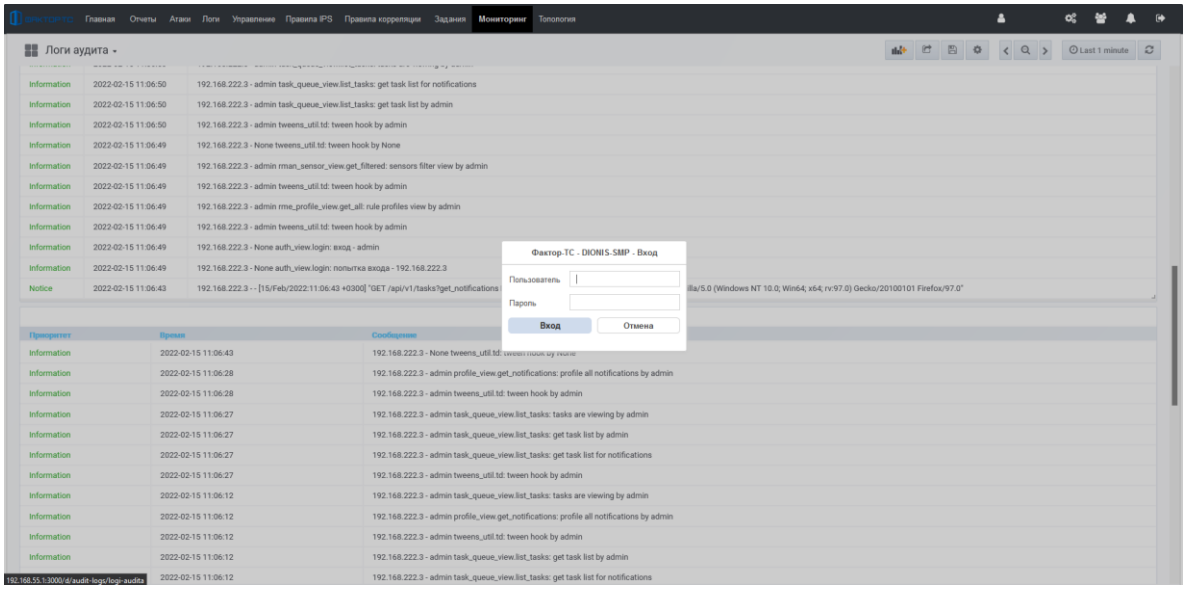


Рисунок 4

Если пользователь ПО Dionis-SMP 1.0 был неактивен в течение 45 дней, то его учетная запись блокируется. . Настройки выполняются в конфигурационном файле***~/.config/factor/development.ini*** установлено значение

user_security_inactive_minutes_to_block = 64800 (45 дней).

Главное окно интерфейса расположено на одноименной вкладке «Главная» и служит для предоставления пользователю информации о текущем состоянии системы (подробнее эта вкладка описана в разделе «**Мониторинг сообщений»** настоящего руководства.

3.3 Настройка общих параметров ПО Dionis-SMP 1.0

Интерфейс пользователя представлен в системе как web-страница.

Каждое страница интерфейса, вкладка, окно имеет разнообразный набор элементов управления. Основные использующиеся в интерфейсе элементы управления приведены в таблице (Таблица 4).

Таблица 4 – Элементы управления

Элемент интерфейса	Описание
Раскрывающийся список	Применяется для выбора одного из значений
Поле	Имя поля и текстовое поле для ввода значения
Кнопка	Применяет указанные значения в форме или вызывает следующее диалоговое окно для продолжения действий
Таблица	Сверху указано название таблицы. Далее указаны названия столбцов. При нажатии на название столбца выполняется сортировка записей таблицы в возрастающем (^) или убывающем (v) порядке
Кнопка	При нажатии удаляет выбранное значение на форме
Кнопка	При нажатии применяет изменения значений на форме
Кнопка	Вызывает диалоговое окно календаря для выбора значения типа datetime (Дата и время)
Вкладка	Используется для перехода между формами интерфейса. Текущая (активная) вкладка отображается подсвеченной
Переход	Применяется для перехода между страницами в таблицах в пределах одной формы. Кнопка «**Назад»** переходит на предыдущую страницу, а кнопка «**Вперед»** на следующую. Цифровое значение в этом элементе указывает на общее количество страниц
Анимированная иконка	Анимация указывает на выполнение операции, заданной пользователем
Кнопка	При нажатии осуществляется переход диалоговому окну добавления или создания записи / элемента

Основная информация в системе представлена в виде записей в таблице.

Пользователь имеет возможность выполнения сортировки записей таблиц в соответствии с требуемым столбцом (по возрастанию или убыванию значений столбца).

3.4 Пользовательские настройки

Управление пользователями и ролями доступно только Системному администратору.

Окно диалога **«Управление пользователями»** позволяет Системному администратору ПО Dionis-SMP 1.0 добавить нового пользователя и задать:

- имя (login) нового пользователя;
- email нового пользователя;
- пароль для нового пользователя;
- максимальное количество параллельных сессий;
- назначить роли пользователя.

Формирование списка пользователей и назначение ролей:

1. Нажать на кнопку «». Откроется окно «**Управление пользователями**».
2. Нажать кнопку .
3. Заполнить поля «**Имя пользователя**», «**Email**», «**Пароль**».
4. Назначить пользователю роль.
5. Указать максимальное количество параллельных сессий (по умолчания – 5).
6. Нажать на кнопку «**Добавить**».
7. Для изменения настроек в таблице окна **«Управление пользователями»** выбрать пользователя двойным кликом левой кнопки мыши.
8. Внести новые настройки.
9. Нажать кнопку «**Применить**».
10. Для удаления пользователя в таблице окна «**Управление пользователями**» выбрать пользователя двойным кликом левой кнопки мыши и нажать кнопку «Удалить».

Время, которое запрещено переиспользовать логин пользователя настраивается в конфигурационном файле***~/.config/factor/development.ini***, параметр user_security_forbid_id_reuse_minutes (по умолчанию этот параметр равен 1095 минут).

11. Нажать кнопку «**Удалить**».

Для блокировки пользователя нажать на значок «Блок» и подтвердить действие.

Для разблокировки пользователя нажать на значок «Блок» и подтвердить действие.

Также окно диалога **«Управление пользователями»** позволяет Системному администратору ПО Dionis-SMP 1.0 видеть количество активных сессий пользователей и их максимальное количество.

3.5 Настройки пользователя

Используйте окно диалога «**Настройки пользователя**» для создания заданий по оповещению о событиях.

В данном окне доступны виджеты:

- «**Имя пользователя**» - имя пользователя, авторизовавшегося в системе;
- «**Основной email**» - электронная почта пользователя;
- **«Дополнительный email»** - дополнительная электронная почта пользователя.

Всплывающие окна оповещений в Web-интерфейсе по умолчанию всегда включены.

Система настройки оповещений пользователя, которые будут приходить на его электронную почту, указанную в этой же форме или в специальный раздел «Оповещения»:

- создание/удаление/модификация устройств;
- о новых атаках с критерием;
- загрузка правил на устройство;
- загрузка правил в базу;
- об изменении конфигурации;
- об отключении устройств;
- о включении устройств;
- об инцидентах корреляции;
- о нарушении целостности ПО «DIONIS-SMP»;
- о превышении порогов(CPU, RAM, Disk space);
- событиях аудита;
- о новых snmp трапах;
- события ротации базы данных.
- об обновлении правил Factor-TS

Для изменения настроек пользователя:

1. Нажать на кнопку «  », с отображением имени текущего авторизованного пользователя (верхняя правая сторона интерфейса). Откроется окно «**Настройки пользователя**».

2. Выбрать в таблице «**Оповещения**» требуемый вариант события и нажать кнопку «**Подписка**».

3. Выбрать в открывшемся окне диалога «**Настройки нотификаций**» способ получения оповещения («в браузере» и/или «email»), задать название подписки и нажать кнопку «**Применить**».

Способы оповещения:

«В браузере» - всплывающие окна в web-интерфейсе;

«email» - оповещения приходят на указанную почту.

4. Если в окне диалога «**Настройки нотификаций**» был установлен переключатель «в браузере», то уведомления помимо электронной почты будут также приходить в специальный раздел «**Оповещения**».

5. Для получения оповещений только на дополнительный e-mail, выберете пункт «**Не использовать основной email для оповещения**».

6. Для перехода в раздел «**Оповещения**» нажать кнопку в правом верхнем углу окна, расположенную рядом со значком профиля (🔔).

7. Для закрытия модального окна необходимо нажать кнопку закрыть.

3.6 Оповещения

Используйте окно «**Оповещения**» для просмотра событий, выбранных в окне диалога «**Настройки пользователя**».

Просмотр оповещений:

1. Нажать на кнопку «🔔» (верхняя правая сторона интерфейса).

2. В появившемся окне «Оповещения» можно осуществлять просмотр полученных оповещений. Оно состоит из колонок – «Заголовок», «Статус», «Время создания», «Устройство», «Подписка». Статус оповещения принимает значение «В работе» после просмотра оповещения пользователем, до этого момента статус будет находиться в значении «Новое». Если выбрать в выпадающем меню «Показывать» пункт «Все», то будут показаны все оповещения, в том числе и уже прочитанные. При выборе в таблице конкретного оповещения в правой части экрана будет отображена дополнительная информация по данному оповещению.

3. Удалить просмотренные оповещения можно кнопкой «Очистить».

3.7 Системные настройки

Используйте окно диалога «**Системные настройки**» для получения информации о хранящейся информации, настройки значений параметров базы данных.

Окно «**Настройки**» позволяет получить информацию о хранящейся информации (MB) в следующих таблицах:

- pcap_table_2021_11_01;
- isp_attacks_2021_11_01;
- pcap_table_2021_11_02;
- isp_attacks_2021_11_02.

Любую из этих таблиц можно очистить (кнопка <**Очистка БД**>).

Так же окно «**Настройки**» позволяет настроить SMTP-сервер. Для перехода к настройке параметров необходимо нажать кнопку «» (SMTP-сервер) - должно выполняться только системным администратором с компетенциями в настройке ПО exim4.

Настройка параметров:

1. Для перехода к настройке параметров необходимо нажать кнопку «» (**Системные настройки**). Откроется окно «**Настройки**»

2. При нажатии на кнопку «**Системные настройки**» открывается окно «**Системные настройки**» со следующими параметрами «Информация», «База данных», «Мониторинг», «Контроль целостности», «Аутентификация», «Источники БРП».

3. Таблица окна «**Системные настройки**» позволяет:

– получить информацию о дате установки и сборки ПО Dionis-SMP 1.0, версии схемы базы данных;

– настроить значения параметров базы данных «Интервал запуска очистки базы данных», «Максимальный размер логов (Гбайт)», «Максимальный размер атак (Гбайт)», «Хранить записи логов не старше n дней», «Хранить записи атак не старше n дней»;

– установить значения параметров «Адрес системы», «Порт системы» для мониторинга;

– установить интервал запуска проверки целостности;

– установить настройки аутентификации:

- запрет использования последних n паролей (n=3);
- число неуспешных попыток аутентификации до блокировки (3);
- Интервал между попытками входа (1 минута);
- алфавит пароля заглавные буквы (ABCDEFGHIJKLMNOPQRSTUVWXYZ);
- алфавит пароля прописные буквы (abcdefghijklmnopqrstuvwxyz);
- алфавит пароля цифры (0123456789);
- алфавит пароля специальные символы !"#$%&'\()*+,-./:;<=>?@[]^_`{|}~;
- минимальная длина пароля (8 символов);

- срок действия пароля (84600 минут);

– установить источник БРП и настроить интервал проверки правил.

3.8 Сохранение/Восстановление полной конфигурации ПО Dionis-SMP 1.0

Для резервного копирования полной конфигурации ПО Dionis-SMP 1.0 выполните в командной строке ОС СН Astra Linux Special Edition (версия 1.6) следующие команды:

cd /opt/factor-ts/init/dr-snapper

./dr-snapper.sh take -p <<*имя_резервной копии*>>

Для восстановления конфигурации из резервной копии выполните в командной строке ОС СН Astra Linux Special Edition (версия 1.6) выполните следующие команды:

cd /opt/factor-ts/init/dr-snapper

./dr-snapper.sh restore -p <<*имя_резервной копии*>>

Для восстановления конфигурации «по умолчанию» выполните в командной строке ОС СН Astra Linux Special Edition (версия 1.6) выполните следующие команды:

cd /opt/factor-ts/init/dr-snapper

./dr-snapper.sh restore -p init

3.9 Выход из системы

Для выхода из системы пользователю необходимо нажать кнопку «» (выход), расположенную в правом верхнем углу окна интерфейса.

Система завершит текущую сессию пользователя и отобразит окно авторизации входа в систему.

4 УПРАВЛЕНИЕ ШЛЮЗАМИ БЕЗОПАСНОСТИ

Системный администратор имеет возможность создать любое количество учетных записей администраторов (возможно, с разными правами доступа), поэтому в дальнейшем будет говориться об учетной записи администратора.

4.1 Управление устройствами Dionis-NX и Dionis-DPS

Управление Dionis-NX и и Dionis-DPS осуществляется на странице «**Управление»** для работы со следующими компонентами системы:

- устройства (просмотр или редактирование сведений о шлюзе безопасности);
- группы устройств (просмотр, создание и редактирование групп устройств);
- скрипты (выполнение на устройствах или группах устройств);
- переменные;
- шаблоны переменных;
- ACL;
- соединения;
- IPsec;
- туннели;
- политики;
- сетевые объекты;
- туннели dikey;
- клучи dikey;
- кластеры;
- VRRP;
- обновление ПО.

4.1.1 Добавление устройства

Добавление нового устройства происходит на странице «**Управление> Устройства».**

Страницу визуально можно разделить на две части. Первая часть – таблица, содержащая записи добавленных ранее устройств, с отображением следующей информации в столбцах:

- «ИДЕНТИФИКАТОР УСТРОЙСТВА» - идентификатор, уникальный номер устройства в системе;

- «ИДЕНТИФИКАТОР ПЛАТФОРМЫ» - отображает заводской идентификатор;
- «ИМЯ» – краткое название устройства (при нажатии на значок лупы отображает поле для ввода названия для выполнения поиска записи в таблице);
- «ТИП» – тип устройства;
- «ПРОФИЛЬ» – наборов правил IPS для многократного использования;
- «IP» – IP-адрес устройства;
- «СТАТУС» – текущий статус соединения с устройством;
- «СИНХРОНИЗИРОВАНО» – статус синхронизации, обозначающий совпадение стартовой и текущей конфигурации на устройстве.
- «СТАТУС СОВ» – статус системы обнаружения вторжений (включен/выключен).
- «РЕЖИМ СОВ» – режим работы системы обнаружения вторжений.
- «ВЕРСИЯ» – версия программного обеспечения подключенного устройства.

Вторая часть страницы (при выборе ранее добавленного устройства) – это панель, для работы с устройствами из табличного списка, позволяющая редактировать информацию об устройствах, добавлять и удалять устройства, управлять устройствами.

Порядок добавления устройства:

1. Заполнить поле «ИД» – идентификатор, уникальный номер устройства в системе (не может повторяться).
2. Заполнить поле «Название».
3. Заполнить поле «Тип».
4. Заполнить поле «IP-адрес».
5. Заполнить поле «Пользователь».
6. Заполнить поле «Пароль».
7. При нажатии на кнопку «**Конфигурация SNMP**» заполнить поля:
   - SNMP Port;
   - SNMP Community;
   - SNMP Version.
8. Нажать кнопку «**Добавить**». Далее будет предложено подтвердить идентификацию устройства.

Запись об устройстве отобразится в таблице.

ПРИМЕЧАНИЕ. *Пока устройство не зарегистрировано в системе - функции конфигурирования, изменения расписаний и обновление ПО Dionis-SMP 1.0 недоступны.*

Сразу после добавления устройства статус его инициализации в системе имеет значение **ОК/Unknown**, что означает успешную регистрацию записи устройства в системе, но пока с устройством не организовано подключение, статус соединения имеет значение **Unknown**.

Если соединение установлено, статус принимает значение **ОК/New configuration**.

В случае, если значения были указаны неверно, связь с устройством не инициализируется, и в параметре «**Статус**» отобразится значение «**Недоступно/Failed to get config»**.

ПРИМЕЧАНИЕ. *При добавлении устройства системой автоматически ставится задания на получение его конфигурации (получение конфигурации вручную описано в п.4.1.4 настоящего руководства), на получение версии устройства и на получение информации из конфигурации.*

4.1.2 Удаление устройства

Для удаления устройства:

1. Выбрать его в таблице, щелкнув на строку записи.
2. Нажать кнопку «**Удалить**».
3. В диалоговом окне подтвердить удаление записи, нажав кнопку «**ОК**».

Выбранная запись будет удалена из системы.

4.1.3 Редактирование информации об устройствах

Порядок редактирования информации устройства:

1. Изменить поле «ИД» – идентификатор, уникальный номер устройства в системе (не может повторяться).
2. Изменить поле «Название».
3. Изменить поле «Тип».
4. Изменить поле «IP-адрес».
5. Изменить поле «Пользователь».
6. Изменить поле «Пароль».
7. При нажатии на кнопку «**Конфигурация SNMP**» изменить поля:
   - SNMP Port;
   - SNMP Community;
   - SNMP Version.
8. Нажать кнопку «**Изменить**».

Выбранная запись будет изменена в системе.

4.1.4 Получение конфигурации устройства

Чтобы получить конфигурацию устройства:

1. Перейти на страницу «**Управление> Устройства».**

2. Выбрать в таблице устройство, щелкнув на соответствующую ему запись в таблице.

3. В блоке «**Конфигурации**» (правая часть страницы, низ) нажать кнопку «**Просмотр**».

Система откроет окно «**Конфигурации устройства**» для выбранного устройства.

В верхней части окна приводится описывающая конфигурации таблица со столбцами:

- «НАЗВАНИЕ» - краткое название конфигурации;
- «ОПИСАНИЕ» – описание конфигурации;
- «КОММЕНТАРИЙ» – дополнительное поле;
- «УСТРОЙСТВО» – краткое название устройства;
- «БЕЗОПАСНЫЙ» – режим, позволяющий «откатить» все изменения;
- «ИЗМЕНЕНА» – дата и время последнего изменения конфигурации устройства.

Ниже таблицы расположены три текстовых поля для просмотра и сравнения конфигураций.

Для выполнения задания на получение текущей конфигурации устройства необходимо нажать кнопку «**Синхронизация**».

Для закрытия окна работы с конфигурациями устройства нажать кнопку «**Закрыть**».

4.1.5 Просмотр, редактирование конфигураций

4.1.5.1 Просмотр конфигурации

Для того чтобы просмотреть конфигурацию в окне «**Конфигурации устройства**» необходимо выбрать её в таблице, щелкнув на соответствующую строку. Конфигурация отобразится в первом текстовом поле.

Для поиска конфигураций воспользуйтесь поисковой строкой.

4.1.5.2 Редактирование конфигурации

Внесение изменений в конфигурацию:

- выбрать конфигурацию, щелкнув на соответствующей строке в таблице (код конфигурации отобразится в текстовом поле ниже);

- внести изменения в текстовую часть;
- нажать кнопку «**Сохранить**».

Изменения отредактированной конфигурации будут сохранены.

В табличной части окна появится запись, соответствующая измененной конфигурации.

4.1.5.3 Сравнение конфигураций

1. Выбрать конфигурации в таблице, нажать клавишу <CTRL> и выбрать конфигурации для сравнения, путём нажатия левой кнопки мыши на соответствующих строчках конфигурация.

2. Код конфигурации отобразится в текстовом поле.

3. Нажать кнопку «**Сравнить**».

4. В правой части окна в третьем текстовом поле отобразится сравнение выбранных конфигураций.

4.1.5.4 Проверить

Для проверки правильности конфигурации нажать кнопку «**Проверить**» При этом устройство будет перезагружено. С момента загрузки в течение следующих 5 минут устройство будет функционировать с новой конфигурацией. В течение этого времени администратор устройства должен убедиться, что устройство доступно и функционирует, как этого от него ожидается. Затем эту конфигурацию можно будет применить.

4.1.5.5 «Применить»

Для развертывания конфигурации на устройстве нажмите на кнопку «**Применить**».

4.1.5.6 «Применить изменения»

Для записи конфигурации в стартовую нажмите на кнопку «**Применить изменения**».

4.1.5.7 Синхронизация

Для выполнения задания на получение текущей конфигурации устройства необходимо нажать кнопку «**Синхронизация**».

4.1.5.8 Закрыть

Для закрытия окна работы с конфигурациями устройства нажать кнопку «**Закрыть**».

4.1.6 Настройка расписания

Для перехода в окно настройки расписания на устройстве используйте страницу «**Управление> Устройства».**

Существуют следующие типы расписания:

1) Обновление правил

Для выбранного устройства в соответствии с выбранным профилем правила будут обновляться по настроенному расписанию.

2) Синхронизация

Для выбранного устройства производить синхронизацию устройства по расписанию.

3) Выполнение сценария

Для выбранного устройства выполнять сценарий на устройстве по расписанию

4) Получить журналы

Для выбранного устройства получать журнал с устройства по расписанию.

4.1.6.1 Создание нового расписания обновления правил

Настройка расписания обновлений правил на устройстве:

- перейти на страницу «**Управление> Устройства»**;
- выбрать устройство, для которого необходимо выполнить настройку;
- нажать кнопку «**Расписание**» (система отобразит окно «**Расписание**» настройки расписания обновлений правил на выбранном устройстве);
- для поля **«Тип»** из выпадающего списка выбрать тип операции – «**Обновление правил**»;
- в поле «**Профиль**» выбрать из списка профиль, правила которого будут обновляться на устройстве по созданному расписанию;
- в поле «**Начало**», используя стандартную форму диалогового окна календаря, выбрать дату начала применения расписания;
- в поле «**Период**» выбрать одно из значений (ежедневно, еженедельно, ежемесячно, ежегодно и произвольно);
- в поле «**Время**» задать время выполнения операции;
- в поле «**Включить**» выбрать значение («да» или «нет»), означающее текущий статус создаваемого расписания;
- нажать кнопку «**Создать**» (запись нового расписания обновления правил на устройстве отобразится в таблице слева);
- для возврата на страницу «**Управление> Устройства»** нажмите кнопку «**Закрыть**» в правом верхнем углу окна «**Расписание**».

На выбранном устройстве правила будут обновляться в соответствии с настроенным расписанием обновления.

4.1.6.2 Создание нового расписания синхронизации

Настройка расписания синхронизации на устройстве:

- перейти на страницу «**Управление> Устройства»**;
- выбрать устройство, для которого необходимо выполнить настройку;
- нажать кнопку «**Расписание**» (система отобразит окно «**Расписание**» настройки расписания на выбранном устройстве);
- для поля **«Тип»** из выпадающего списка выбрать тип операции – «**Синхронизация**»;
- в поле «**Начало**», используя стандартную форму диалогового окна календаря, выбрать дату начала применения расписания;
- в поле «**Период**» выбрать одно из значений (ежедневно, еженедельно, ежемесячно, ежегодно и произвольно);
- в поле «**Время**» задать время выполнения операции;
- в поле «**Включить**» выбрать значение («да» или «нет»), означающее текущий статус создаваемого расписания;
- нажать кнопку «**Создать**» (запись нового расписания обновления правил на устройстве отобразится в таблице слева);
- для возврата на страницу «**Управление> Устройства»** нажмите кнопку «**Закрыть**» в правом верхнем углу окна «**Расписание**».

На выбранном устройстве будет производиться синхронизация в соответствии с настроенным расписанием.

4.1.6.3 Создание нового расписания выполнения сценария

Настройка расписания синхронизации на устройстве:

- перейти на страницу «**Управление> Устройства»**;
- выбрать устройство, для которого необходимо выполнить настройку;
- нажать кнопку «**Расписание**» (система отобразит окно «**Расписание**» настройки расписания на выбранном устройстве);
- для поля **«Тип»** из выпадающего списка выбрать тип операции – «**Выполнение сценария**»;
- в поле «**Сценарий**» выбрать из списка сценарий, который будет выполняться на устройстве по созданному расписанию;

- в поле «**Начало**», используя стандартную форму диалогового окна календаря, выбрать дату начала применения расписания;
- в поле «**Период**» выбрать одно из значений (ежедневно, еженедельно, ежемесячно, ежегодно и произвольно);
- в поле «**Время**» задать время выполнения операции;
- в поле «**Включить**» выбрать значение («да» или «нет»), означающее текущий статус создаваемого расписания;
- нажать кнопку «**Создать**» (запись нового расписания обновления правил на устройстве отобразится в таблице слева);
- для возврата на страницу «**Управление> Устройства»** нажмите кнопку «**Закрыть**» в правом верхнем углу окна «**Расписание**».

На выбранном устройстве будет выполняться сценарий в соответствии с настроенным расписанием.

4.1.6.4 Создание нового расписания получения журналов

Настройка расписания синхронизации на устройстве:

- перейти на страницу «**Управление> Устройства»**;
- выбрать устройство, для которого необходимо выполнить настройку;
- нажать кнопку «**Расписание**» (система отобразит окно «**Расписание**» настройки расписания на выбранном устройстве);
- для поля **«Тип»** из выпадающего списка выбрать тип операции – «**Получить журналы**»;
- в поле «**Начало**», используя стандартную форму диалогового окна календаря, выбрать дату начала применения расписания;
- в поле «**Период**» выбрать одно из значений (ежедневно, еженедельно, ежемесячно, ежегодно и произвольно);
- в поле «**Время**» задать время выполнения операции;
- в поле «**Включить**» выбрать значение («да» или «нет»), означающее текущий статус создаваемого расписания;
- нажать кнопку «**Создать**» (запись нового расписания обновления правил на устройстве отобразится в таблице слева);
- для возврата на страницу «**Управление> Устройства»** нажмите кнопку «**Закрыть**» в правом верхнем углу окна «**Расписание**».

На выбранном устройстве будет выполняться получение журналов от устройства в соответствии с настроенным расписанием.

4.1.6.5 Удаление расписания

Для удаления записи расписания работы с устройством:

1. Выбрать запись расписания в таблице;
2. Нажать кнопку «**Удалить**».

Расписание будет удалено.

4.1.7 Обновление ПО устройства

Используйте страницу «**Управление> Устройства»** для перехода в окно обновления ПО устройства.

Для выбранного устройства в соответствии с выбранной прошивкой ПО обновится.

4.1.7.1 Обновление ПО:

1. Перейти на страницу «**Управление> Устройства»**.
2. Выбрать устройство из списка на странице «**Управление> Устройства»** и нажать кнопку «**Обновление ПО**». Откроется окно «**Обновление ПО**», содержащее перечень файлов (прошивок) для обновления. Файлы предварительно выбираются администратором безопасности на странице «**Управление> Обновление» ПО**.
3. Выбрать из списка нужный файл обновления.
4. Задать «Имя системы» и «Имя дата слота».
5. Нажать кнопку «**Начать**».
6. Необходимо выбрать основной это маршрутизатор или резервный (для отказоустойчивого кластера).

Выполняться процедура обновления ПО устройства. На странице «**Задания**» создается соответствующая запись.

4.1.8 Использование правил

Модуль СОВ Dionis-NX анализирует трафик согласно заданным правилам обнаружения вторжений (сигнатурам). ПО Dionis-SMP 1.0 позволяет изменять заданные правила для устройств Dionis-NX.

Выбор профиля устройства и загрузка правил**:**

1. Настроить правила (страница **правила IPS**, подробное описание приведено в подразделе 4.2 настоящего руководства).
2. Выбрать устройство в таблице на странице «**Управление> Устройства»**, щелкнув на соответствующую строку.

3. Выбрать в раскрывающимся списке профиль для загрузки правил.

4. Нажать кнопку «**Загрузить**».

Устройство будет использовать отправленный ему набор правил для обнаружения атак и выполнять определенные пользователем действия.

4.1.9 Журналы

Для перехода в окно настройки журналов на устройстве используйте страницу «**Управление> Устройства»** и нажмите кнопку настройки  .

По умолчанию настроены следующие журналы:

- dish.log (show log dish number 10);
- service-ids.log (show service ids log number 10).

Для добавления нового журнала нажмите на  , укажите имя журнала и команду. Нажмите на кнопку «Применить на устройстве».

Для изменения журналов по умолчанию, которые получаются с устройства, нажмите кнопку «**Изменить дефолтные**».

Для закрытия настроек журналов нажмите  .

Для получения журналов с устройства нажмите на кнопку «**Получить журналы**».

4.1.9.1 «Просмотреть журналы»

Для просмотра полученных журналов нажмите «**Просмотреть журналы**».

Откроется окно «**Журналы**». В левой части окна отображается **Имя** и **ИД** устройств, подключенных к ПО Dionis-SMP 1.0. В правой части окна отображается таблица со столбцами:

- «**Устройство**» - имя устройства;
- «**Журнал**» - имя журнала;
- «**Время получения**».

При выборе устройства из списка слева, отобразятся полученные журналы. Данные журналы можно скачать, нажав кнопку  . Для удаления журнала нажмите кнопку  .

Возможен поиск по наименованиям журналов, устройств и их ИД. Также есть фильтрация отображения по группам устройств.

Для закрытия окна «**Журналы**» нажмите  .

4.1.10 Безопасный режим

Если устройство переведено в безопасный режим, то все сделанные изменения такого устройства можно в дальнейшем откатить или применить.

Используйте страницу «**Управление> Устройства»** и нажмите кнопку «**Добавить**» для добавления устройства в безопасный режим.

Для просмотра списка устройств в безопасном режиме нажмите «Просмотр».

4.1.11 Импорт\экспорт настроек устройств

Используйте страницу «**Управление> Устройства»** выберете устройство и нажмите кнопку «**Экспорт**» для экспорта текущей настройки устройства. Возможны два типа экспортируемого файла: json и csv.

Для импорта ранее сохраненной конфигурации нажмите на кнопку «**Импорт**» и выберите ранее сохраненный файл конфигурации.

4.1.12 Работа с группами устройств

При управлении устройствами ПО Dionis-SMP 1.0 может объединять устройства в логические группы.

Для работы с группами устройств необходимо перейти на страницу «**Управление> Группы устройств»**.

Страница разделена на три табличные части. Первая таблица содержит все группы устройств, созданных в системе. Вторая таблица содержит список всех устройств в системе. Третья таблица предназначена для просмотра устройств, включенных в конкретную группу.

В таблицах существует возможность осуществлять поиск устройства, используя соответствующее поле.

4.1.12.1 Создание группы устройств

Для создания группы:

1. Нажать кнопку «➕», расположенную в заголовке таблицы «**Группы устройств**».
2. Система отобразит диалоговое окно «**Добавление группы**».
3. Ввести название группы в поле «**Название**».
4. Нажать кнопку «**Добавить**».
5. Запись созданной группы отобразится в таблице «**Группы устройств**».

4.1.12.2 Добавление устройства в группу

Чтобы добавить устройство в группу:

1. Выбрать группу, щелкнув на строке группы в таблице.
2. В таблице со списком устройств поочередно выбрать устройства для включения в группу и после каждого выбора нажать кнопку «›».

3. Запись устройства будет перемещена в таблицу «**Устройства в группе**».

⚠ ***ВНИМАНИЕ!*** *– Любое устройство может принадлежать только одной группе!*

4.1.12.3 Удаление устройства из группы

Для того чтобы исключить устройство из группы:

1. Выбрать группу в таблице «**Группы устройств**», из которой требуется исключить устройство.

2. В таблице «**Устройства в группе**» поочередно выбрать записи, которые необходимо удалить и после каждого выбора нажать кнопку «‹».

4.1.13 Выполнение скриптов на устройстве

Скрипты, которые Администратор может выполнять на устройствах или группах устройств отображаются на странице «**Управление> Скрипты».**

Данная страница содержит четыре функциональных блока:

- таблица со списком доступных скриптов;
- таблица со списком отдельных устройств;
- таблица со списком групп устройств;
- информация о выбранном скрипте.

4.1.13.1 Выполнение скрипта на устройстве

Для выполнения скрипта на отдельном устройстве:

1. Выбрать запись в таблице скриптов, щелкнув на ней.
2. Информация о скрипте отобразится в поле «**Текст скрипта**».
3. Выбрать устройство, на котором требуется выполнить скрипт.
4. Проверить код скрипта.
5. Нажать кнопку «**Применить**».
6. Скрипт будет выполнен на выбранном устройстве.
7. На странице «**Управление> Задания»** будет создана соответствующая запись о совершенном действии/операции.

4.1.13.2 Выполнение скриптов на группе устройств

Для выполнения скрипта на группе устройств:

1. Выбрать скрипт в таблице, щелкнув на строку.
2. Информация о скрипте отобразится в поле «**Текст скрипта**».
3. Выбрать группу устройств, на устройствах которой будет выполнен скрипт.

4. Проверить код скрипта.

5. Нажать кнопку «**Применить**».

6. Скрипт будет выполнен на выбранной группе устройств.

7. На странице «**Управление> Задания»** будет создана соответствующая запись о совершенном действии/операции.

При выполнении скрипта на группе устройств, запись о выполнении операции создается на каждую операцию выполнения (**на каждое устройство**, а не одна запись на группу).

ПРИМЕЧАНИЕ. *– Если в группе, выбранной для выполнения скрипта, содержится большое количество устройств, выполнение скрипта может занять некоторое время.*

Запись о выполнении скрипта на устройстве может принимать следующие состояния:

- статус New - новый скрипт, не запущен на устройстве;
- статус *Run* - скрипт запущен на устройстве;
- статус *Processing* - скрипт выполняется на устройстве;
- статус *Done* - скрипт выполнен на устройстве.

4.1.13.3 Создание скрипта

Создание скриптов для выполнения на устройствах осуществляется на странице «**Управление> Скрипты».**

Для создания нового скрипта:

1. Заполнить поле «**Название**».
2. Заполнить поле «**Описание**».
3. Заполнить поле «**Текст скрипта**».
4. Нажать кнопку «**Создать**».

Примечание*. При создании скрипта можно использовать переменные. Если значение переменной не задано для устройства, то оно берется из шаблона переменной.*

На странице «**Управление> Скрипты»** в разделе «**Скрипты**» появится запись о новом скрипте.

ПРИМЕЧАНИЕ. *– Поля «**Название**» и «**Текст скрипта**» являются обязательными для заполнения. Если данные поля оставить пустыми, то при попытке создать скрипт система отобразит сообщение с описанием ошибки.*

4.1.13.4 Редактирование скрипта

Для того чтобы отредактировать скрипт:

1. Выбрать скрипт в таблице.
2. Внести изменения.
3. Нажать кнопку «**Изменить**».

4.1.13.5 Удаление скрипта

Для того чтобы удалить скрипт:

1. На странице «**Управление> Скрипты»** выбрать в таблице скрипт.
2. В разделе описания скрипта нажать кнопку «**Удалить**».
3. Подтвердите удаление, нажатием кнопки «ОК».

4.1.13.6 Экспорт/импорт скриптов

Для того чтобы сохранить скрипт на локальную машину пользователя:

1. На странице «**Управление> Скрипты»** выбрать в таблице скрипт.
2. В разделе описания скрипта нажать кнопку «**Экспорт**». Скрипт сохраниться в формате JSON.

Для того чтобы загрузить пользовательский скрипт:

1. На странице «**Управление> Скрипты»** в разделе описания скрипта нажать кнопку «**Импорт**».
2. Выбрать «**Добавить**» для добавления скрипта или «**Добавить и заменить**» для добавления скрипта с заменой.
3. В диалоговом окне выбрать скрипт в формате JSON и нажать «**Открыть**»

4.1.13.7 Проверка скриптов

Для проверки корректности скрипта:

1. Выбрать запись в таблице скриптов, щелкнув на ней.
2. Информация о скрипте отобразится в поле «**Текст скрипта**».
3. Выбрать устройство, на котором требуется проверить корректность скрипта.
4. Нажать кнопку «**Проверить**».
5. Скрипт будет проверен на корректность написания, при этом не будет выполнен.
6. На странице «**Управление> Задания»** будет создана соответствующая запись о совершенном действии/операции.

4.1.14 Работа с переменными

Переменные, доступные пользователю, расположены на странице «**Управление> Переменные».**

ПРИМЕЧАНИЕ. *– Переменные типов system/system_readonly необходимы для выполнения задания синхронизации устройств и появляются в системе автоматически при добавлении в неё устройств Dionis-NX и Dionis DPS, без явной необходимости их изменение не рекомендуется. Удалить эти переменные нельзя. Так же невозможно изменить переменные типа «System_readonly»*

В табличной части формы содержатся записи о переменных с атрибутами:

- «**Тип**» - тип используемой переменной;
- «**Описание**» - краткое описание переменной;
- «**Устройство**» - устройство, на котором выполняется переменная;
- «**Шаблон**» - определение имени и значения переменной.

4.1.14.1 Редактирование переменных

Для редактирования переменной:

1. Выбрать строку в таблице, щелкнув на ней.
2. В полях «**Шаблон**», «**Устройство**», «**Описание**», "**Данные**" внести необходимые изменения.
3. Нажать кнопку «**Изменить**».

ПРИМЕЧАНИЕ. *– Поля «**Шаблон**», «**Устройство**» и «**Данные**» являются обязательными для заполнения и не могут быть пустыми.*

4.1.14.2 Удаление переменной

Для удаления переменной:

1. Выбрать строку переменной в таблице.
2. Нажать на кнопку «**Удалить**».

4.1.15 Шаблоны переменных

Шаблоны переменных, доступные пользователю, приведены на странице «**Управление> Шаблоны переменных».**

Допустимый вид данных:

Строки - "dtn"

Цифры - 3

Булевы переменные - true|false

Массивы - ["sdds","dsad",false]

Объекты - {"a":[{"b":3, "c":{"a":4}}, 330], "b":true}

4.1.15.1 Создание шаблонов переменных

Для создания шаблона переменной:

1. Заполнить поле «**Название**». (Имя шаблона переменной. Не допускается символ пробела в имени).
2. Заполнить поле «**Описание**». (Краткое описание шаблона).
3. Заполнить поле «**Данные**». (Значение).
4. Нажать кнопку «**Создать**».

Шаблон переменной будет создан.

Запись шаблона отобразится в таблице, расположенной в левой части пользовательского интерфейса на странице «**Управление> Шаблоны переменных».**

4.1.15.2 Редактирование шаблонов переменных

Чтобы изменить шаблон:

1. Выбрать шаблон в таблице.
2. Внести изменения в полях «**Название**», «**Описание**», «**Данные**», «**Тип**».
3. Нажать кнопку «**Изменить**».

4.1.15.3 Удаление шаблонов переменных

Чтобы удалить шаблон:

1. Выбрать шаблон в таблице.
2. Нажать кнопку «**Удалить**».

Система запросит подтверждение данной операции, открыв соответствующее модальное окно, в котором администратору безопасности необходимо нажать на кнопку «**ОК**».

Запись шаблона переменной будет удалена.

4.1.15.4 Создание переменной из шаблона

Чтобы создать переменные из шаблона на странице «**Управление> Шаблоны переменных»**:

1. Выбрать шаблон в таблице.
2. Указать группу устройств, для которых будут использоваться переменные.
3. Нажать кнопку «**+ Создать**» в объединении кнопок «**Переменные**» на странице «**Управление> Шаблоны переменных».**
4. Переменные будут созданы для каждого устройства в выбранной группе.
5. На странице «**Управление> Переменные»** появится запись о новой переменной.

4.1.15.5 Обновление (изменение) переменной из шаблона

Для обновления переменной:

1. На странице «**Управление> Шаблоны переменных»** в таблице шаблонов переменных выбрать шаблон.
2. Отредактировать шаблон.
3. Заново выбрать в таблице шаблон.
4. Выбрать группу устройств, на которых будут исполнены переменные.
5. Нажать кнопку «**Обновить переменные**» в объединении кнопок «**Переменные**».
6. Проверить обновления переменных на странице «**Управление> Переменные»**.

4.1.15.6 Экспорт/импорт шаблонов переменных

Для того чтобы сохранить шаблон переменных на локальную машину пользователя:

1. На странице «**Управление> Шаблоны переменных»** выбрать в таблице шаблон.
2. Нажать кнопку «**Экспорт**». Шаблон сохраниться в формате JSON.

Для того чтобы загрузить шаблон переменных:

4. На странице «**Управление> Шаблоны переменных»** нажать кнопку «**Импорт**».
5. Выбрать «**Добавить**» для добавления шаблона или «**Добавить и заменить**» для добавления шаблона с заменой.
6. В диалоговом окне выбрать шаблон в формате JSON и нажать «**Открыть**»

4.1.16 Применение ACL

Списки ACL, которые пользователь может выполнять на устройствах, доступны на странице «**Управление> ACL»**. Появляются в системе после выполнения задания по получении информации из конфигурации.

Страница «**Управление> ACL»** визуально делится на три части:

- таблица со списком устройств (можно фильтровать по группе устройств, используя выпадающее меню);
- таблица с перечнем **ACL** скриптов (можно фильтровать по типу и использованию на устройстве, используя выпадающее меню);
- кнопки для выполнения операций.

В таблице со списками ACL содержатся следующие атрибуты:

- «**Название**» - указано название списка разрешённых операций, который в данный момент использован для «узла сети»;

- «**Устройство**» - устройство, для которого может быть применен скрипт;
- «**Тип**» указан вид списка (ACL или NAT);
- «**Применен**» - указывается дата и время последнего применения списка доступа к конкретному устройству;
- «**Используется**» - указывается текущий статус активности списка доступа («Да» или «Нет»).

4.1.16.1 Создание скриптов для изменения списков ACL

Создать новый скрипт для изменения списка ACL:

1. Выбрать устройство в первой таблице на странице «**Управление> ACL».**

2 Нажать кнопку «**Добавить**» (система отобразит окно диалога «**Создание ACL|NAT**» для задания параметров нового скрипта).

В верхней части окна расположена информация об устройстве, для которого будет создан новый список ACL.

Поля «**ID устройства**», «**Устройство**», «**IP устройства**», «**Тип устройства**» не доступны для редактирования.

Администратору безопасности необходимо указать «**Название списка**» и «**Тип**» (ACL или NAT).

3 Нажать кнопку «**Добавить**» для добавления строки параметров создаваемого списка.

4 Для поля «**Протокол**» выбрать вариант протокола, используя выпадающий список (TCP, UDP, ICMP и др.).

5 Для поля «**Адрес(а) источника**» указать IP-адрес, или несколько адресов, или диапазон адресов источника.

6 Для поля «**Порт(ы) источника**» указать порт, или несколько портов, или диапазон портов источника.

7 Для поля «**Адрес(а) приемника**» указать IP-адрес, или несколько адресов, или диапазон адресов приемника.

8 Для поля «**Порт(ы) приемника**» □ указать порт, или несколько портов, или диапазон портов приемника.

9 Для переключателя «**Запрет**» обозначающий запрет выделенных адресов установить (или нет) флаг.

10 В поле «**DIONIS специфичные опции**» задать специальные опции для устройств типа DIONIS.

11 Нажать кнопку «**Применить**». Появится окно с предупреждением: «Синхронизируйте устройство после выполнения задачи».

12 Выполните синхронизацию устройства.

Добавлять строки в таблицу можно используя соответствующую кнопку «**Добавить**».

Для удаления строки из списка необходимо нажать кнопку «**Удалить**», напротив строки, которую требуется удалить.

Для выхода без сохранения необходимо нажать на закрывающую кнопку .

4.1.16.2 Просмотр созданных фильтров ACL на устройстве

Просмотреть скрипт ACL, выполняемый на устройстве:

1. Перейти на страницу «**Управление> ACL».**
2. Выбрать устройство нажатием мыши. Отобразится список ACL на устройстве.
3. В таблице список ACL выбрать интересующую запись и открыть двойным щелчком по записи.

В результате откроется окно со списком ACL, доступный на выбранном устройстве.

4.1.16.3 Примеры скриптов ACL

Примеры скриптов для работы с ACL приведены в таблице (Таблица 5).

Таблица 5 – Примеры скриптов для работы с ACL

Действие	**Скрипт**	**Пример**
Создание ACL	acl-deny-ip	do configure terminal ip access-list acl-deny-ip no all deny src 1.2.3.4 deny dst 1.2.3.4
	acl-deny-proto	do configure terminal ip access-list acl-deny-proto no all deny icmp deny tcp dport 80 deny tcp sport 80
	ACL - apply	do configure terminal interface $interface$ ip access-group acl in ip access-group acl out
	ACL - remove	do configure terminal interface $interface$ no ip access-group acl in no ip access-group acl out
Удаление	ACL - delete	do configure terminal

списка ACL		no ip access-list acl

4.1.17 Соединения

Все установленные disec/ipsec-соединения отображаются на странице «**Управление> Соединения».**

Записи в окне представлены в табличном виде со столбцами:

- «Название» - название соединения;
- «Устройство» - устройство, с которого установлено соединение;
- «Тип» - тип протокола передачи данных;
- «Состояние» - текущее состояние соединения;
- «Подробности» - примечание, комментарий или описание соединения.

4.1.18 IPsec

Настройки IPsec отражены на странице «**Управление> IPsec**».

На странице «**Управление> IPsec**» три таблицы:

- **«Расписания»;**
- «**Черные списки**»;
- «**Пулы**».

4.1.18.1 Расписания

В таблице **«Расписания»** отображаются записи набора правил, определяющих временные промежутки, во время которых соединение запрещено или разрешено.

4.1.18.2 Черные списки

В таблице «**Черные списки**» отображаются записи списка X500-имён субъектов, соединения от которых будут отвергаться. Также, если в чёрный список были добавлены новые субъекты, то активные соединения с данными субъектами будут закрыты в течение минуты.

4.1.18.3 Пулы

Таблица «**Пулы**» правила сопоставления выдаваемых виртуальных адресов (групп адресов) с конкретными субъектами (группами субъектов). Данная возможность может использоваться для идентификации трафика от конкретного мобильного клиента внутри защищаемой сети, а также для разграничения доступа различных мобильных клиентов к различным ресурсам защищаемой сети.

4.1.19 Туннели

Используйте страницу «**Управление> Туннели**» для создания переменных и шаблонов disec, туннелей, маршрутизации. Созданные переменные и шаблоны применяются для построения защищенных каналов связи.

Страница «**Управление> Туннели**» содержит четыре функциональных блока:

– таблица со списком отдельных устройств (в блоке реализована возможность фильтрации устройств по выбранной группе);

– блок вкладок с визуализацией созданных туннелей, маршрутов для выбранных устройств;

– блок «**Работа с устройством**»;

– блок «**Шаблоны и переменные**».

4.1.19.1 Шаблоны и переменные

Создание DISEC переменных:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).

2. Нажать на кнопку **DISEC** в блоке «**Шаблоны и переменные**».

Появится окно «**Настройка DISEC**».

3. Заполнить поля окна «**Настройка DISEC**» (Таблица 6).

Таблица 6 – Поля окна «**Настройка DISEC**»

Serial	Номер серии ключей.
Local_CN	Локальный криптономер.
Local	Локальный конец туннеля в формате IP-адреса.
Lan	Название шаблона сети, который был создан ранее на вкладке «Сетевые объекты». Это информация нужна для корректного создания туннелей и маршрутов в дальнейшем.

4. Нажать кнопку «**ДАЛЕЕ**» для перехода к переменной следующего устройства.

5. Нажать кнопку «**ЗАВЕРШИТЬ**» для создания переменной или переменных.

4.1.19.2 Создание шаблонов ТУННЕЛЕЙ

1. Выделить в таблице несколько устройств с помощью клавиши CTRL и левой кнопки мыши.

2. Нажать на кнопку «**ТУННЕЛЕЙ**» в блоке «**Шаблоны и переменные**».

Появится окно «**Мастер создания криптосети».**

3. Соединить нужные устройства при помощи левой кнопки мыши на карте с устройствами.

Появится окно **«Создание tun связи».**

4. Заполнить все поля окна **«Создание tun связи».**

***Примечание**. Для корректного заполнения полей окна «**Создание tun связи**» рекомендуется ознакомиться с руководством по настройке программного обеспечения Dionis-NX.*

4.1.19.3 Редактирование шаблонов ТУННЕЛЕЙ

На странице «**Управление> Туннели**» в блоке вкладок с визуализацией созданных туннелей.

1. Выбрать шаблон туннеля дважды кликнув по его названию.
2. В появившемся окне можно изменить название и описание туннеля.
3. . Соединить нужные устройства при помощи левой кнопки мыши на карте с устройствами.

Появится окно **«Создание tun связи».**

4. Внести необходимые изменения и нажать кнопку «**СОЗДАТЬ**».
5. Нажать «**Изменить**» для сохранения настроек.

4.1.19.4 Удаление шаблонов ТУННЕЛЕЙ

Для удаления туннелей на странице «**Управление> Туннели**» в блоке вкладок с визуализацией созданных туннелей нажать на значок  .

4.1.20 Шаблоны МАРШРУТИЗАЦИИ

Используйте страницу «**Управление> Туннели**» для создания шаблонов маршрутизации.

4.1.20.1 Создание шаблона МАРШРУТИЗАЦИИ:

1. Выделить в таблице несколько устройств с помощью клавиши CTRL и левой кнопки мыши.
2. Нажать кнопку «**МАРШРУТИЗАЦИИ**» в блоке «**Шаблоны и переменные**».

Появится окно «**Мастер создания сети».**

6. Соединить устройства при помощи левой кнопки мыши на карте с устройствами.
3. Просмотреть все поля, в случае необходимости отредактировать их с помощью левой клавиши мыши, посредством перетаскивания нужных объектов
4. Нажать на кнопку «**СОЗДАТЬ**».

5. Задать имя шаблона и его описание.

6. Нажать на кнопку «**СОЗДАТЬ**» для создания шаблона МАРШРУТИЗАЦИИ.

7. Нажать на кнопку «**СОЗДАТЬ С ЗАДАЧАМИ**» для добавления шаблонов ТУННЕЛЕЙ и МАРШРУТИЗАЦИИ на устройства.

Всплывающее окно в правой верхней части экрана оповестит о изменениях.

4.1.21 Удаление и редактирование созданных ШАБЛОНОВ.

1. Открыть двойным щелчком левой кнопкой мыши в блоке вкладок необходимый шаблон.

2. Выбрать действие УДАЛИТЬ в окне «**Мастер создания».**

3. В окне «**Мастер создания»** нажать левой кнопкой мыши на линию, символизирующую канал связи.

4. Нажать кнопку ОК для подтверждения удаления.

5. Нажать ИЗМЕНИТЬ для подтверждения внесенных изменений.

6. Для удаления шаблона в блоке вкладок левой клавишей мыши нажать на значок корзины справа от выбранного шаблона.

Всплывающее сообщение в правой верхней части экрана оповестит о изменениях.

4.1.22 Работа с устройством (устройствами)

Этот блок предназначен для добавления или удаления шаблонов на устройства, которые находятся во вкладке управление, все выполненные действия вносят изменения в текущую конфигурацию устройства (running config), рекомендуется ее сохранять или использовать «**Безопасный режим**».

4.1.22.1 Создание маршрутов

Для создания маршрутов выполнить следующие действия:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).

2. Открыть вкладку «**Маршруты**» в блоке вкладок.

3. Выбрать шаблон(ы) маршрута.

4. Нажать на кнопку «**Создание маршрутов**» в блоке «**Работа с устройством**».

Всплывающее сообщение в правой верхней части экрана оповестит об изменениях.

4.1.22.2 Удаление маршрутов

Для удаления маршрутов выполнить следующие действия:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).

2. Открыть вкладку «**Маршруты» в** блоке вкладок.

3. Выбрать шаблон(ы) маршрута.

4. Нажать на кнопку «**Удаление маршрутов**» в блоке «**Работа с устройством**».

Всплывающее сообщение в правой верхней части экрана оповестит о изменениях.

4.1.22.3 Создание туннелей

Для создания туннелей выполнить следующие действия:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).

2. Открыть вкладку «**Туннели**» в блоке вкладок.

3. Выбрать шаблон(ы) туннеля.

4. Нажать на кнопку «**Создание туннелей**» в блоке «**Работа с устройством**».

Всплывающее сообщение в правой верхней части экрана оповестит о изменениях.

4.1.22.4 Удаление туннелей

Для удаления туннелей выполнить следующие действия:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).

2. Открыть вкладку «**Туннели**» в блоке вкладок.

3. Выбрать шаблон(ы) туннеля.

4. Нажать на кнопку «**Удаление туннелей**» в блоке «**Работа с устройством**».

4.1.22.5 Смена ключей

Новые ключи должны быть предварительно введены в устройства, на которых их планируется менять.

Для смены ключей выполнить следующие действия:

1. Выделить в таблице устройство с помощью левой кнопки мыши (или несколько устройств с помощью клавиши CTRL и левой кнопки мыши).
2. Открыть вкладку «**Туннели**» в блоке вкладок.
3. Выбрать шаблон(ы) туннеля.
4. Нажать на кнопку «**Сменить ключи**».
5. Ввести новый номер серии ключей.
6. Нажать кнопку «**Применить**».

4.1.23 Политики

Используйте страницу «**Управление> Политики**» для задания подробных политик (наборов правил) для устройств на основе источника/назначения сети/интерфейса, протокола, портов, позволяющих определить, какой трафик будет разрешен, запрещен или запротоколирован.

Страница «**Управление> Политики**» состоит из трех функциональных областей:

- Области инструментов;
- Области имен политик;
- Области визуализации данных о сформированных политиках.

4.1.23.1 Область инструментов

Наименование	Действие
НАЗВАНИЕ +	Открывает окно диалога для добавления названия политики.
Удалить строку	Удаляет текущую строку описания политики.
Расширенные настройки	Расширенные настройки параметров политики.
Добавить выше	Добавляет строку описания политики выше текущей строки.
Добавить ниже	Добавляет строку описания политики ниже текущей строки.
Добавить в конец	Добавляет строку описания политики в конец таблицы
Сохранить	Сохраняет сформированную политику
Копировать	Копирует выбранную политику
Применить	Формирует задание на применение сформированной политики для выбранных устройств.
Отменить	Формирует задание на отмену применения сформированной политики для выбранных устройств.
Удалить	Удаляет политику.
Экспорт	Экспорт политики на локальную машину в формате JSON
Импорт	Экспорт политики в формате JSON

4.1.23.2 Создание имени политики

Для создания имени политики выполнить следующие действия:

1. Нажать на кнопку «**НАЗВАНИЕ +**».
2. В появившемся окне диалога «**Создание политики**» вписать новое имя политики (поле «**Название**»).
3. Добавить комментарии (поле «**Описание**»).

4. Нажать на кнопку «**Создать**».

В области создания имени политики появится имя созданной политики.

⚠ ***ВНИМАНИЕ!*** – *Структура имени политики регламентирована. Имя должно состоять из латинских символов, чисел и _!*

4.1.23.3 Удаление строки

Для удаления строки:

1. Выбрать строку описания политики.
2. Нажать на кнопку «**Удалить строку».**

4.1.23.4 Расширенные настройки

Для выполнения расширенных настроек. Они позволяют задать «Видимость» правила. Это поле может принимать три значения:

1. LOCAL – политика применяется локально к устройству.

2. GROUP – политика применяется к группе устройств, если не создана группа во вкладке «группа устройств», то политика не сработает.

3. CONST – константная политика безотносительно устройств к которым она же применяется.

Добавление строки описания политики выше текущей строки.

Для добавления строки описания политики выше текущей строки:

1. Выбрать текущую строку описания политики.
2. Нажать на кнопку «**Добавить выше».**

В области визуализации данных о сформированных политиках появится новая пустая строка, расположенная выше текущей.

4.1.23.5 Добавление строки описания политики ниже текущей строки.

Для добавления строки описания политики ниже текущей строки:

1. Выбрать текущую строку описания политики.
2. Нажать на кнопку « Добавить ниже».

В области визуализации данных о сформированных политиках появится новая пустая строка, расположенная ниже текущей.

4.1.23.6 Добавление строки описания политики в конец списка сформированных политик.

Для добавления строки описания политики в конец списка:

1. Нажать на кнопку «**Добавить в конец**».

В области визуализации данных о сформированных политиках появится новая пустая строка, расположенная в конце списка.

4.1.23.7 Сохранение политики

Для сохранения политики выполнить следующие действия:

1. Выбрать из списка нужную политику.
2. Нажать кнопку «**Сохранить**».

4.1.23.8 Применение политики

Для применения политики выполнить следующие действия:

1. Выбрать из списка нужную политику.
2. Нажать кнопку «**Применить**».

Появится окно диалога «**Применение политики**».

3. Выбрать одно или несколько устройств (клавиши Shift или Ctrl).
4. Нажать кнопку «**Применить**».

В результате будет сформировано задание для устройства. Статус задания позволяет контролировать процедуру его выполнения.

Выделение задания на странице «**Задания**» приведет к появлению детализации состояния (область «**Подробное состояние**»).

4.1.23.9 Отмена применения политики

Для отмены применения политики выполнить следующие действия:

1. Выбрать из списка нужную политику.
2. Нажать кнопку «**Отменить**».

Появится окно диалога «**Отмена политики**».

3. Выбрать одно или несколько устройств (клавиши Shift или Ctrl).
4. Нажать кнопку «**Отменить**».

В результате будет сформировано задание для устройства. Статус задания позволяет контролировать процедуру его выполнения.

Выделение задания на странице «**Задания**» приведет к появлению детализации состояния (область «**Подробное состояние**»).

4.1.23.10 Удаление политики

Для удаления политики выполнить следующие действия:

1. В области имен политик выбрать политику для удаления.
2. Нажать на кнопку «**Удалить**» в области инструментов.

Политика с выбранным именем будет удалена.

4.1.23.11 Экспорт политики

Для экспорта политики на локальной машине выполнить следующие действия:

1. В области имен политик выбрать политику для удаления.
2. Нажать на кнопку «  **Экспорт**» в области инструментов.

Политика с выбранным именем будет сохранена на локальной машине в формате JSON.

4.1.23.12 Импорт политики

Для импорта политики выполнить следующие действия:

1. Нажать на кнопку «  **Импорт**» в области инструментов.
2. В появившемся окне «Импорт политики» указать название политики и выбрать файл в формате JSON с локальной машины.
3. Нажать кнопку «Импортировать»

Политика с выбранным именем появится в области визуализации данных о сформированных политиках.

4.1.23.13 Параметры политики (стандартные настройки)

Наименование	Описание
	Номер строки
ДЕЙСТВИЕ	• **deny**. Значение deny (запретить) предназначено для блокирования трафика • **permit**. Разрешить При разрешении пакет обрабатывается дальше, при запрете – сбрасывается. • **log.** Действие, которое служит для журналирования отдельных пакетов и событий. • **pass**. Правило прохода
СУБДЕЙСТВИЕ	**log alert**. Регистрация оповещения.
ПРОТОКОЛ	Выбор протокола из списков по первым буквам в т.ч. tcp, udp, udplite, ip, icmp, … и др
АДРЕС(А) ИСТОЧНИКА	IP АДРЕС(а)/сетевой объект/шаблон сетевого объекта источника
АДРЕС(А) ПРИЕМНИКА	IP АДРЕС(а)/сетевой объект/шаблон сетевого объекта приемника
СЕРВИС	Порт сервиса (услуги)
НАПРАВЛЕНИЕ	<->, ->
ПРИМЕЧАНИЕ	Комментарий

4.1.23.14 Параметры политики (расширенные настройки)

Наименование	Описание
	Номер строки
ДЕЙСТВИЕ	• **deny**. Значение deny (запретить) предназначено для блокирования трафика • **permit**. Разрешить При разрешении пакет обрабатывается дальше, при запрете – сбрасывается. • **log**. Действие, которое служит для журналирования отдельных пакетов и событий. • **pass**. Правило прохода
ВИДИМОСТЬ	LOCAL. GROUP. CONST.
АДРЕС(А) ИСТОЧНИКА	IP АДРЕС(а)/сетевой объект/шаблон сетевого объекта источника
ПОРТ(Ы) ИСТОЧНИКА	Список номеров портов, используемых выбранными протоколами для установки соединения между источником и приемником.
ВИДИМОСТЬ	LOCAL. GROUP. CONST.
АДРЕС(а) ПРИЕМНИКА	IP АДРЕС(а)/сетевой объект/шаблон сетевого объекта приемника
СЕРВИС	Порт сервиса (услуги)
НАПРАВЛЕНИЕ	<->, ->
ПРИМЕЧАНИЕ	Комментарий
СПЕЦИФИЧНЫЕ ОПЦИИ	Добавление специфичных опций политики.

4.1.24 Сетевые объекты

Используйте страницу «**Управление> Сетевые объекты**» для создания именованных объектов, за которыми могут скрываться отдельный IP адрес, список IP адресов, подсеть, список подсетей. Данные сетевые объекты в дальнейшем можно использовать при создании политик.

Страница «**Управление> Сетевые объекты**» состоит из функциональных областей.

Область переключения вкладок:

- «**Без привязки к интерфейсам**»;
- «**Привязка к устройствам**».

Вкладка «**Без привязки к интерфейсам**»:

- области названий сетевых объектов;
- области названий сервисов.

Вкладка «**Привязка к устройствам**»:

- область привязки к устройствам;

4.1.24.1 Добавление сетевого объекта

Для добавления сетевого объекта выполнить следующие действия:

1. Нажать кнопку «  » рядом с заголовком «**НАЗВАНИЕ СЕТЕВОГО ОБЪЕКТА».**

Появится окно диалога «**Создание сетевого объекта**».

2. Добавить название нового сетевого объекта.
3. Добавить значение адреса сетевого объекта и маски подсети.
4. Нажать на кнопку создать.

В области названий сетевых объектов появится строка с названием нового сетевого объекта.

4.1.24.2 Изменение адреса сетевого объекта и маски подсети

Для изменения адреса сетевого объекта и маски подсети выполнить следующие действия:

1. Выполнить двойной щелчок на строке с нужным названием сетевого объекта в области названий сетевых объектов.
2. В появившемся окне диалога «**Изменение сетевых объектов**» внести необходимые изменения.
3. Нажать на кнопку «**Изменить**».

Новое значение имени появится в области названий сетевых объектов, новые значения адреса сетевого объекта и маски подсети появится в области значений.

4.1.24.3 Удаление сетевого объекта

Для удаления сетевого объекта нажать на значок «  ».

4.1.24.4 Создание/изменение сетевой группы

Для создания сетевой группы выполнить следующие действия:

1. Нажать кнопку «  » рядом с заголовком «НАЗВАНИЕ СЕТЕВОГО ОБЪЕКТА».

Появится окно диалога «**Создание сетевой группы**».

2. Добавить название новой сетевой группы.
3. В левой части окна выбрать нужный сетевой объект.
4. Нажать на кнопку «  ».

5. Нажать на кнопку создать.

В области названий сетевых объектов в строке «Группа» появится строка с названием новой сетевой группы.

Для изменения сетевой группы выполнить следующие действия:

1. Выполнить двойной щелчок на строке с нужным названием сетевой группы в области названий сетевых объектов.

2. В появившемся окне диалога «**Изменение сетевой группы**» внести необходимые изменения.

3. Нажать на кнопку «**Изменить**».

4.1.24.5 Удаление сетевой группы

Для удаления сетевой группы нажать на значок « ».

4.1.24.6 Поиск по сетевым объектам

Для поиска по наименованию сетевого объекта нажмите на « » рядом с заголовком «НАЗВАНИЕ СЕТЕВОГО ОБЪЕКТА» и введите имя объекта. В таблице отобразятся подходящие варианты.

Для поиска по адресу сетевого объекта нажмите на « » рядом с заголовком «ЗНАЧЕНИЕ» и введите адрес объекта. В таблице отобразятся подходящие варианты.

4.1.24.7 Добавление сервиса

Для добавления сервиса выполнить следующие действия:

1. Нажать кнопку « » рядом с заголовком «**НАЗВАНИЕ СЕРВИСА**».

Появится окно диалога «**Создание сервиса**».

2. Добавить название нового сервиса.

3. Выбрать «**Тип**» («**Диапазон портов**» или «**Порт**»).

4. Задать в поле «**Порт**» значение.

5. Нажать на кнопку создать.

В области названий сервисов появится строка

В области названий сервисов появится строка с названием нового сервиса в зависимости от выбранного ТИПа сервиса.

4.1.24.8 Изменение сервиса

Для изменения сервиса выполнить следующие действия:

1. Выполнить двойной щелчок на строке с нужным названием сервиса в области названий сервисов.
2. В появившемся окне диалога «**Изменение сервиса**» внести необходимые изменения.
3. Нажать на кнопку «**Изменить**».

4.1.24.9 Удаление сервиса

Для удаления сервиса нажать на значок «  ».

4.1.24.10 Создание/изменение группы сервисов

Для создания группы выполнить следующие действия:

1. Нажать кнопку «  » рядом с заголовком «НАЗВАНИЕ СЕРВИСА».

Появится окно диалога «**Создание группы портов**».

2. Добавить название новой группы.
3. В левой части окна выбрать нужный сервис.
4. Нажать на кнопку «  ».
5. Нажать на кнопку создать.

В области названий сетевых сервисов в строке «Группа» появится строка с названием новой группы.

Для изменения сетевой группы выполнить следующие действия:

1. Выполнить двойной щелчок на строке с нужным названием группы в области названий сервисов.
2. В появившемся окне диалога «**Изменение портгруппы**» внести необходимые изменения.
3. Нажать на кнопку «**Изменить**».

4.1.24.11 Удаление группы сервисов

Для удаления группы сервисов нажать на значок «  ».

4.1.24.12 Поиск по сервисам

Для поиска по наименованию сервиса нажмите на « » рядом с заголовком «НАЗВАНИЕ СЕРВИСА» и введите имя объекта. В таблице отобразятся подходящие варианты.

Для поиска по порту сервиса нажмите на « » рядом с заголовком «ЗНАЧЕНИЕ» и введите значение порта. В таблице отобразятся подходящие варианты.

4.1.24.13 Привязка к устройствам

Используйте вкладку «**Привязка к устройствам**» на странице «**Управление> Сетевые объекты**» для привязки устройств к сетевым объектам.

1. Добавить название устройства.
2. Выбрать устройство, название сетевого объекта из выпадающего списка и шаблон.
3. Нажать кнопку «**Добавить**».

4.1.24.14 Привязывание сетевого объекта (добавление связи)

1. Нажать кнопку « » рядом с заголовком «**УСТРОЙСТВО».**
2. Выбрать имя устройства в появившемся окне диалога «**Привязывание сетевого объекта**».
3. Выбрать сетевой объект.
4. Выбрать название шаблона.
5. Нажать кнопку «Добавить».
6. Закрыть окно диалога «**Привязывание сетевого объекта**».

В области визуализации данных о привязке устройств к сетевым объектам появится новая запись.

4.1.24.15 Добавление нового шаблона

Для добавления нового шаблона выполнить следующие действия:

1. Нажать кнопку « » рядом с заголовком «**НАЗВАНИЕ ШАБЛОНА».**

Появится окно диалога «**Создание шаблона».**

2. Заполнить поле «**Название**».
3. Заполнить поле «**Описание**».
4. Нажать на кнопку «**Создать шаблон**».

Новое название шаблона будет доступно при выполнении процедуры привязывания сетевого объекта (см. пункт 4.1.20.4).

4.1.25 Туннели dikey

Для управления туннелями Dikey используйте страницу «**Управление>Туннели dikey**».

Страница «**Управление> Туннели dikey**» содержит три таблицы:

- список настроенных туннелей dikey;
- ключи dikey на устройстве 1;
- ключи dikey на устройстве 2.

Таблица со списком настроенных туннелей dikey имеет следующие атрибуты:

- ИД ТУННЕЛЯ
- АЛГОРИТМ
- УСТРОЙСТВО 1
- IP-АДРЕС 1
- КЛЮЧ 1
- УСТРОЙСТВО 2
- IP-АДРЕС 2
- КЛЮЧ 2.

При выборе туннеля отображаются ключи на устройствах данного туннеля.

Кнопка «Смена ключей» меняет ключи на устройствах на выбранные.

4.1.26 Ключи dikey

Для управления ключами Dikey используйте страницу «**Управление>ключи dikey**».

Страница «**Управление> Ключи dikey**» содержит две таблицы:

- список устройств из группы;
- ключи dikey.

В таблице подключённых устройств отображается ID и имя устройства. Реализован поиск по ID и имени устройства, а также выбор группы устройств.

В таблице «Ключи dikey» представлены следующие поля:

- УСТРОЙСТВО – устройство, на котором создана пара ключей;
- ЗАКРЫТЫЙ КЛЮЧ– метка о закрытом ключе (false, true);
- ИСПОЛЬЗУЕТСЯ – метка об использовании ключа (false, true);
- ИМЯ КЛЮЧА– наименование ключа.

Для создания пары ключей на выбранном устройстве нажмите кнопку «**Создать пару**». Для просмотра ключей на устройстве, выберите его в таблице список устройств. Для удаления неиспользуемых ключей нажмите кнопку «**Удалить неиспользуемые**».

4.1.27 Кластеры

Для управления кластерами используйте страницу «**Управление>Кластеры**».

Страница «**Управление> Кластеры**» содержит две таблицы:

– Список устройств из группы;

– кластеры.

В таблице подключённых устройств отображается ID и имя устройства. Реализован поиск по ID и имени устройства, а также выбор группы устройств.

В таблице «Кластеры» представлены следующие поля:

- УСТРОЙСТВО – ИД и имя устройства;
- СТАТУС – активен / не активен;
- СИНХРОНИЗИРОВАНО – статус синхронизации настроек и dikey (значения true/false);

Для синхронизации настроек кластера нажмите кнопку «Синхронизация настроек». Для синхронизации ключей dikey для выбранного кластера нажмите кнопку «Синхронизация dikey»

4.1.28 VRRP

Для управления сетевым протоколом VRRP используйте страницу «**Управление>VRRP**».

Страница «**Управление> VRRP**» содержит две таблицы:

– список устройств из группы;

– кластеры.

В таблице подключённых устройств отображается ID и имя устройства. Реализован поиск по ID и имени устройства, а также выбор группы устройств.

В таблице «Кластеры» представлены следующие поля:

- УСТРОЙСТВА – имя устройства;
- IP-АДРЕСА – отображение IPv4 и IPv6 адреса.

Для просмотра VRRP-кластеров на устройстве, выберите его в таблице список устройств.

4.1.29 Обновление ПО

Используйте страницу «**Управление> Обновление ПО**» для просмотра и загрузки файлов программного обеспечения устройств (образов системы).

4.1.29.1 Загрузка файла

Загрузить файл в систему:

1. Нажать кнопку « ✚ ».

Отобразится окно «**Добавление файла**».

2. Нажать кнопку «**Загрузить**».
3. Выбрать требуемый файл.

При успешной загрузке файла в диалоговом окне «**Добавление файлов**» отобразится сообщение имя загруженного файла, подсвеченное зелёным цветом, в поле «РАЗМЕР» будет указан размер файла в МБ, а в поле «ВРЕМЯ» - время его добавления в систему.

4. Нажать кнопку «**Закрыть**».

Файл отобразится в таблице на странице «**Управление> Обновление ПО**».

4.1.29.2 Удаление файла

Для того чтобы удалить файл в таблице на странице «**Управление> Обновление ПО**»:

1. Выбрать файл.
2. Выполнить двойной щелчок на соответствующей ему строке в таблице.

Система отобразит диалоговое окно «**Действия над файлами**».

3. Нажать кнопку «**Удалить».**

Система запросит подтверждение на совершение операции удаления.

4.2 Управление правилами на устройствах

Используйте страницу «**Правила IPS**» для управления правилами.

Функционально страница состоит из четырех блоков:

- блок применения фильтрации правил;
- блок управления профилями и группами;
- блок управления правилами (добавление новых правил, загрузка правил, импорт правил, экспорт правил);
- блок отображения записей правил в табличном виде.

ПРИМЕЧАНИЕ. *– Функции добавления, загрузки, экспорта и импорта правил будут недоступны, пока в системе не зарегистрирован хотя бы один профиль и/или группа правил.*

Каждая запись правила имеет следующий набор атрибутов:

- SID (Security IDentifier) это идентификатор безопасности. Каждое правило в системе имеет свой идентификатор;
- GID;
- «Действие»;
- «Приоритет»;
- «Протокол»;
- IP ИСТОЧНИКА;
- «ПОРТ ИСТОЧНИКА»;
- «Направление»;
- IP НАЗНАЧЕНИЯ;
- «ПОРТ НАЗНАЧЕНИЯ»;
- «Активно»;
- «Создано»;
- «Обновлено»;
- «Опции».

Используйте кнопку «**Все**», расположенную в нижней части окна, для отображения всех правил в таблице.

4.2.1 Создание и удаление профилей

Создание нового профиля:

1. Нажать кнопку «➕» (Таблица «**ПРОФИЛЬ**»).
2. Ввести в открывшемся диалоговом окне «**Добавление профиля**» его название.
3. Нажать кнопку «**Добавить**».

Новый профиль правил будет зарегистрирован в системе.

Удаление профиля:

1. Выполнить двойной щелчок на записи в таблице профилей.
2. В открывшемся диалоговом окне «**Изменение профиля**» нажать кнопку «**Удалить**».

⚠ ***ВНИМАНИЕ! –*** *При удалении профиля, все группы, входящие в состав профиля и правила, так же будут удалены!*

4.2.2 Создание и удаление групп

Для создания и удаления групп действия аналогичны созданию и удалению профилей.

Создание новой группы:

1. Нажать кнопку «➕» (Таблица «**ГРУППА»**).
2. Написать название группы в открывшемся диалоговом окне «**Добавление группы**».
3. Добавить описание группы.
4. Нажать кнопку «**Добавить**».

Новая группа будет зарегистрирована в системе.

ПРИМЕЧАНИЕ*. Группа не может быть создана, пока в системе не зарегистрировано ни одного профиля, поэтому, в момент создания группы необходимо выбрать профиль, щелкнув на его запись в таблице, к которому будет относиться создаваемая группа.*

Удаление группы:

1. Выполнить двойной щелчок на записи в таблице «**ГРУППА».**
2. В открывшемся диалоговом окне «**Редактирование группы**» нажать кнопку «**Удалить**».

4.2.3 Загрузка правил в профиль из архива

Загрузка правил в профиль из архива:

1. Выбрать профиль.
2. Нажать кнопку «☁ **Загрузить**».
3. Выбрать файл архива для загрузки (совместимый с форматом правил *Snort*).
4. Нажать кнопку «**Открыть**».

Загрузка правил начнет выполняться.

После того как процесс загрузки будет выполнен индикатор изменит свой вид на «Done». Архив начнет обрабатываться системой. Данный процесс может занять некоторое время, в зависимости от размера архива. По завершению процесса в профиле, в который был загружен архив, отобразятся группы и правила в них.

При выполнении данной операции системой создается соответствующая запись в журнале заданий (страница «**Задания**»). Администратор может контролировать процесс загрузки архива правил, наблюдая за статусом этого задания в журнале. По окончании загрузки статус задания примет значение «**Выполнено**».

4.2.4 Создание правил

Создание нового правила:

1. Выбрать профиль и группу.
2. Нажать кнопку «**Добавить**».
3. В открывшемся окне «**Добавление правила**» заполнить поля.
4. Нажать «**Добавить**» для сохранения правила (для отмены операции нажать «**Отмена**»).

Таблица 7 – Атрибуты формы «Добавление правила»

Поле	Описание
SID	Идентификатор безопасности, уникальный для каждого правила
GID	Generator Id Snort, идентификатор группы
Активно	**Y** или **N**
Приоритет	Приоритет выполнения правила
Тип	Выбор одного из значений результата выполнения правила: – **Alert** -создание оповещения; – **Drop** - блокирует пакет и записывает в журнал (лог) это событие; – **Log** - записать в журнал; – **Pass** - игнорировать пакет; – **Activate** - создает оповещение (предупреждение), а затем включение другого правила; – **Reject** - блокирует пакет, регистрирует его, а затем выполняет сброс протокола TCP (если протокол TCP) или сообщает о недоступности порта ICM (если протокол UDP); – **Dynamic** - находится в режиме ожидания до запуска правилом активации, а затем действует как правило журнала (логирования); – **Sdrop** - блокирует пакет, но не записывает в журнал.
Протокол	Добавить одного из значений: – **TCP**; – **UDP**; – **ICMP**;
IP источника	IP-адрес источника
Порт источника	Порт источника
Направление	Направление, возможен выбор одно из вариантов: «< >» - двунаправленный;

Поле	Описание
	«->» - к назначению; «<-» - к источнику. «НЕТ»
IP назначения	IP-адрес назначения
Порт назначения	Порт назначения
Описание	Краткое описание правила
Подстрока	Информация из предыдущих полей, а так же snort-специфический синтаксис.

Созданное правило отобразится в таблице новой строкой.

4.2.5 Правила Factor-TS

Для подключения и скачивания правил с ftp-сервера Factor-TS нажмите на кнопку «**Правила Factor-TS**». Адрес сервера указывается в «Системных настройках - > Источник БРП» (пункт 3.7 настоящего руководства).

Кнопка «**Скачать архив правил**» - скачать правила на локальную машину.

Кнопка «**Скачать внутрь системы**» - скачать на сервер с установленным ПО Dionis-SMP 1.0.

Кнопка «**Проверить версию**» - проверка версии правил внутри системы и на доверенном источнике.

Кнопка «**Проверить контрольную сумму**» - проверка контрольной суммы на доверенном источнике и внутри системы, суммы должны сходиться.

Кнопка «**Загрузить в профиль**» - доступно только после проверки контрольной суммы, необходимо ввести название профиля. После будет создан профиль с названием, какое указали и в нем будут правила (после выполнения задачи по их добавлению в профиль).

4.2.6 Редактирование правил

Редактирование правила:

1. Выбрать профиль и группу.
2. Найти правило в таблице записей правил.
3. Выбрать правило двойным щелчком.
4. Внести изменения в полях в открывшейся форме «**Редактирование правила**».
5. Нажать кнопку «**Изменить**».

4.2.7 Удаление правил

Удаление правила:

1. Выбрать профиль и группу.

2. Выбрать двойным щелчком правило в таблице.

3. В открывшейся форме «**Редактирование правила**» нажать кнопку «**Удалить**».

Система запросит подтверждение на выполнение операции.

4. Для удаления правила нажать **ОК**, для отмены нажать **Cancel**.

4.2.8 Импорт правил

Импорт правил осуществляется из файловой системы АРМ пользователя в БД. Все правила для устройства отправляются из БД.

Импорт правил:

1. Выбрать профиль, щелкнув на соответствующую строку в таблице «**Профиль**».

2. Нажать кнопку «**Импорт**».

3. Выбрать файл для импорта в появившемся диалоговом окне операционной системы.

4. Нажать кнопку «**Открыть**».

Когда для импорта выбран только профиль, то в момент выполнения операции импорта либо добавится новая группа правил, по названию файла, либо перепишется группа с таким названием.

Для выполнения импорта можно также выбрать профиль и группу одновременно. В этом случае правила в группе перепишутся.

4.2.9 Экспорт правил

Используйте возможность экспорта группы правил, хранящейся в БД, в файловую систему АРМ.

Экспорт правил:

1. Выбрать группу, щелкнув на соответствующую строку в таблице «Группа».

5. Нажать кнопку «**Экспорт**».

6. Нажать **ОК** в появившемся диалоговом окне операционной системы.

7. Указать путь для сохранения файла.

4.2.10 Сравнение и слияние изменений в профилях правил

Администратор имеет возможность сравнить набор правил, находящихся в разных профилях на наличие изменений в них.

4.2.10.1 Сравнение профилей правил

Для сравнения профилей:

1. Выделить (удерживая кнопку <**CTRL**> на клавиатуре) два профиля.

Появится диалоговое окно подтверждения выполнения операции.

2. Нажать **ОК**.

Система начинает процесс сравнения, который может занять определенное время (в зависимости от размера наборов правил). Во время операции система отображает анимированную иконку процесса.

После завершения операции сравнения в окне отобразится информация о разнице в группах правил и самих правилах в разных профилях.

3. Выбрать строку в таблице «Профили».

В таблице «**Группы**» отобразятся правила, в которых обнаружены изменения.

Изменения в таблице «**Группы**»:

1. Выбрать запись правила.

Откроется окно, в котором указаны параметры сравниваемых правил.

4.2.10.2 Слияние правил профилей

Выполнение слияния:

1. Нажмите на кнопку «» ».

В окне показа различий запускается процесс переноса изменений. Изменения из одного профиля перенесутся в другой.

После выполнения операции система отобразит результат выполнения данной операции.

4.2.10.3 Слияние групп правил

Выполнение слияния групп правил:

1. Выбрать в таблице «Группы» требуемые группы.
2. Нажать кнопку « » ».
3. Нажав кнопку **ОК** для подтверждения выполнения операции.

4.2.11 Настройка группы правил

Используйте страницу «**Правила IPS**» для быстрой настройки некоторых параметров всех правил в группе:

1. Выполнить двойной щелчок на записи группы.

Система отобразит окно настройки параметров группы правил.

2. Внести изменения в поля формы «**Редактирование группы**».
3. Нажать «**Изменить**».

Настройки правил внутри данной группы будут обновлены.

4. Для удаления группы правил нажмите «**Удалить**».

4.2.12 Отправка набора правил (профиля) на устройство

Отправка правил на устройство:

1. Перейти на страницу «**Управление> Устройства**».
2. Выбрать в таблице запись устройства, на которое необходимо отправить набор правил.
3. Выбрать профиль из выпадающего списка, правила которого требуется отправить на устройство.
4. Выбрать дополнительные опции обновления правил (light, default-config, default-tables, file-magic), подробнее в руководстве по настройке Dionis-NX.
5. Нажать кнопку «**Загрузить**».

Правила будут отправлены из БД на устройство. Для проверки результата данной операции Администратор имеет возможность просмотра соответствующей записи на странице «**Задания**».

При щелчке на строку задания в поле «Подробное состояние» должно быть указано:

done: update sensor rulese, что означает успешное применение набора правил на устройстве.

4.2.13 Правила корреляции

Используйте страницу «**Правила корреляции**» для создания правил и групп правил, сформированных с учетом корреляционных механизмов выявления угроз. Модуль корреляции не только автоматизирует процесс сопоставления разнородных данных, но и сам проводит анализ воздействия атак на ваши ресурсы.

Корреляция позволяет автоматизировать обнаружение событий, которые не должны возникать в вашей сети.

Страница «**Правила корреляции**» состоит из функциональных областей.

Область переключения вкладок:

- «**Правила**»;
- «**Группы правил**».

Вкладка «**Правила**»:

- область управления (кнопки «**Создать группу**» и «**Добавить в группу**»);
- область визуализации данных о правилах корреляции.

Таблица 8

Наименование	Описание
ИМЯ	Имя правила корреляции
ДЕЙСТВУЕТ С	Дата начала действия
ИСТОЧНИК	Атаки или логи
ДЕЙСТВУЕТ ДО	Дата окончания действия

Вкладка «**Группа правил**»:

- Область визуализации данных о группах правил корреляции.

Таблица 9

Наименование	Описание
ИМЯ	Имя правила корреляции
ИСТОЧНИК	Атаки или логи
ОПИСАНИЕ	Дополнительное описание правила корреляции
ЗНАЧЕНИЕ АГРЕГАЦИИ	Число событий
ТИП АГРЕГАЦИИ	Типичные агрегатные функции — COUNT.
ПРОДОЛЖИТЕЛЬНОСТЬ	Значение для выбранной единицы времени
ЕДИНИЦЫ	Единицы времени (SECONDS, MINUTES, HOURS)
АКТИВНО	Флаг отражающий активность действия
ДЕЙСТВУЕТ С	Дата начала действия
ДЕЙСТВУЕТ ДО	Дата окончания действия

4.2.13.1 Создание правила корреляции

Для создания правила корреляции выполнить следующие действия:

1. Нажать на кнопку «+».
2. Заполнить поле «**Имя**».
3. Выбрать необходимый источник данных из списка.
4. Выставить период действия правила (пункты действует с и действует до).
5. Заполнить поле «**Описание**».
6. Нажать на кнопку «**Настройки агрегации**».
7. Откроются дополнительные поля окна диалога «**Создание группы правил**» («**Продолжительность**», «**Единицы времени**», «**Тип агрегации»**, «**Значение агрегации**»).
8. Выбрать единицу времени (SECONDS, MINUTES, HOURS).
9. Задать продолжительность.
10. Выбрать тип агрегации.
11. Выбрать дискретное значение агрегации.

12. Установить флажок «**Создать группу**».
13. Нажать **Добавить условие.**
14. Нажать кнопку «Создать». Если был выставлен флажок создания группы, то откроется окно создания группы правил.

В области визуализации данных о правилах корреляции появится новая запись.

4.2.13.2 Создание группы правил корреляции

Для создания группы правил корреляции выполнить следующие действия:

1. Выделить необходимое число правил корреляции в области визуализации данных о правилах корреляции.
2. Нажать на кнопку «**Создать группу**».

Откроется окно диалога «**Настройка очередности правил**».

3. Удерживая нажатой левой клавишей мыши выделенную строку правил переместить ее на заданную позицию по вертикали.
4. Нажать на кнопку далее (откроется окно диалога «**Создание правила корреляции**»).
5. Заполнить поле «**Имя**».
6. Заполнить поле «**Описание**».
7. Нажать на кнопку «**Настройки агрегации**».

Откроются дополнительные поля окна диалога «**Создание группы правил**» («**Продолжительность**», «**Единицы времени**», «**Тип агрегации»**, «**Значение агрегации**»).

8. Выбрать единицу времени (SECONDS, MINUTES, HOURS).
9. Задать «**Продолжительность**».
10. Выбрать тип агрегации.
11. Выбрать дискретное значение агрегации.
12. Сформировать группу путем выставления операндов и префиксов.
13. Нажать кнопку «Создать».

В области визуализации данных о группах правил корреляции появится новая запись.

4.2.13.3 Редактирование правил корреляции

Для редактирования правил корреляции выполнить следующие действия:

1. Выполнить двойной щелчок на строке правил корреляции.

Откроется окно редактирования.

2. Отредактируйте поля «**Продолжительность**», «**Единицы времени**», «**Тип агрегации**», «**Значение агрегации**».
3. При необходимости нажмите на кнопку «**Добавить условие**» и сформируйте условие.
4. Нажмите на кнопку «**Обновить условия**».

Правило корреляции с текущим названием обновится в базе данных.

4.2.13.4 Добавление в группу правил корреляции

Для добавления в группу правил корреляции выполнить следующие действия:

1. Выделите группу правил с заданным именем.
2. Нажмите на кнопку «**Добавить в группу**».

Откроется окно диалога «**Добавление в группу правил**».

3. Выберите существующую группу из раскрывающегося списка, в которую нужно добавить правила с заданным именем.
4. Задайте операнд из выпадающего списка.
5. Выберите префикс из выпадающего списка.
6. Нажмите кнопку «**Добавить**».

4.2.13.5 Просмотр и удаление групп правил

Используйте вкладку «**Группа правил**» *для визуализации данных* о группах правил корреляции с учетом вложенности *и для удаления групп правил* по заданному имени.

Для просмотра группы правил, нажать «+» рядом с именем группы.

Для изменения «группы правил» дважды нажать правой кнопкой мыши на строке с именем группы.

Для удаления «группы правил», нажать на красный значок корзины в конце строки «группы правила».

5 МОНИТОРИНГ

5.1 Управление логами

5.1.1 Сбор и просмотр логов

Используйте страницу «**Логи**» для просмотра логов.

На странице приведена таблица с полями:

- ID УСТРОЙСТВА
- ГРУППА
- УСТРОЙСТВО
- ПРИОРИТЕТ
- УРОВЕНЬ
- ВРЕМЯ
- ТЕГ
- СООБЩЕНИЕ

Таблица 10 – Атрибуты окна «Логи»

Поле	Описание
ID УСТРОЙСТВА	Идентификационный номер устройства в системе
ГРУППА	Группа, к которой относится устройство
УСТРОЙСТВО	Название устройства, относительно которого зарегистрирована запись (лог) в журнале
ПРИОРИТЕТ	Все, Debug, Notice, Information, Warning, Error, Critical, Alert, Emergency.
УРОВЕНЬ	
ВРЕМЯ	Дата и время регистрации лога в журнале
ТЕГ	Тег
СООБЩЕНИЕ	Информационная часть лога

5.1.2 Фильтрация лог записей

Для поиска и чтения записей в журнале (таблице логов) на странице «**Логи**» используйте фильтр логов.

Применение фильтра к записям:

1. Выбрать критерии фильтра.
    - Тег;
    - Группа устройств;
    - ID устройства;
    - IP устройства;
    - Уровень;
    - Приоритет (Все, Debug, Notice, Information, Warning, Error, Critical, Alert, Emergency);
    - С момента (дата и время);
    - До момента (дата и время);
    - Сообщение.
2. Нажать кнопку « **Применить**».

В таблице логов останутся записи, соответствующие заданным критериям.

Так же существует предопределенный фильтр «Срабатывания firewall». Он выбирает все сообщения с тегом «kernel:» и сообщением «Packet filter alert:». Подробнее о таких пакетах написано в документации к Dionis-NX.

***Примечание**. – ПО Dionis-SMP 1.0 функционирует в реальном режиме времени. Не храните журналы логов более 60 дней. По истечении этого срока рекомендуется архивировать данные на внешних носителях (например, CDR или флэш-накопителях).*

5.2 Главная страница интерфейса

Страница «**Главная**» служит для предоставления администратору безопасности сводной информации об обнаруженных атаках, подключённых устройствах, топологии сети и оповещениях администратору. См. пункты 3.6, 5.4, 5.5, 5.7.

5.3 Страница «Отчеты»

На странице «**Отчёты**» выведены панели:

- «**Динамика атак**»;
- «**Атак за период**» (час, день, неделя, месяц);
- «**Статистика**» (действие над атакой, топ источников атак, топ приоритетов атак, топ протоколов атак, топ сервисов атак, топ типов атак, атаки за час, атаки за день);
- «**Устройства**» (подключенные к ПО Dionis-SMP 1.0);
- «**Атаки**» (таблица с перечнем зафиксированных атак, кнопка «Открыть» раскрывает окно с дополнительной информацией об атаке).

Для выбора информация применяются фильтры:

- выбор ИД устройства (или все устройства);
- выбор группы устройств (Теги);
- тип устройства (Dionis-NX, Cisco, …);
- действие (Logged, dropped, all);
- наличие pcap (Да, нет, все);
- SID (Все или задать значение);
- GID (Все или задать значение);
- приоритет (Все или задать значение);
- протокол (Все, IP, ICMP, IGMP, GGP, IP-ENCAP, ST, TCP, EGP, IGP, PUP, UDP, HMP, XNS-IDP, RDP, ISO-TP4, DCCP, XTP, DDP, IDPR-CMTP, IPv6, IPv6-Route, IPv6-Frag, IDRP, RSVP, GRE, IPSEC-ESP, IPSEC-AH, SKIP, IPv6-ICMP, IPv6-NoNxt, IPv6-Opts, RSPF, VMTP, EIGRP, OSPFIGP, AX.25, IPIP, ETHERIP, ENCAP, PIM, IPCOMP, VRRP, L2TP, ISIS, SCTP, FC, Mobility-Header, UDPLite, MPLS-in-IP, manet, HIP, Shim6, WESP, ROHC.);
- IP атакующего (Все или задать значение);
- порт атакующего (Все или задать значение);
- IP атакуемого (Все или задать значение);
- порт атакуемого (Все или задать значение);
- описание (Все или задать значение);
- включать в отчёт все атаки (Да, Нет).

Отчет формируется по заданному на Dashboard диапазону времени.

Для сохранения отчета в формате PDF нажмите на кнопку «**Сохранить как PDF**»

5.4 Страница «Атаки»

Используйте страницу «**Атаки**» для контроля информации о сетевых вторжениях.

Страница «**Атаки**» содержит три части:

- область визуального контроля (панель с динамической диаграммой атак),
- табличную часть с перечнем зафиксированных атак,
- область инструментов, предназначенную для выполнения фильтрации записей в таблице.

5.4.1 Информация о сетевых вторжениях.

Зафиксированные атаки содержат следующий набор атрибутов:

- **SID** - (Security Identifier) идентификатор атаки в системе;
- **GID** - (Group ID) идентификатор группы;
- «**Описание**» - описание;
- «**Имя устройства**» – имя устройства, зафиксировавшего атаку;
- **dev ID** - идентификатор устройства, подвергшегося атаке;
- «**Время**» – время момента атаки;
- «**Приоритет**» - приоритет атаки, в соответствии с правилом обнаружения;
- «**Действие**» - событие, активировавшееся при обнаружении атаки;
- **proto** - протокол, по которому совершена атака на устройство;
- **IP src** – IP адрес источника;
- «**Порт src**» – порт удаленного компьютера, с которого совершена атака;
- **IP dst** – IP-адрес получателя;
- «**Порт dst**» – порт компьютера получателя;
- «**Помечено**»;
- **Payload** – часть вредоносного ПО, которое выполняет вредоносные действия.

ПО Dionis-SMP 1.0 выполняет анализ наличия атак на основе заданных правил, (страница «**Правила IPS**» подраздел 4.2 настоящего руководства). Все правила объединены в группы в зависимости от типа атак (вторжений), к которым они относятся.

5.4.1.1 Просмотр и сохранение информации об атаке

Первоначально, при открытии страницы «**Атаки**» сортировка записей атак выполнена по приоритету атаки (от высокого к низкому). Пользователь имеет возможность настроить отображение записей по своему выбору, выполнив сортировку по любому из столбцов таблицы, например, по времени, если необходимо отобразить самые актуальные записи атак (вне зависимости от их приоритета).

Дополнительная информация об атаке:

1. Нажать кнопку «**Открыть**» (раскрывается окно с дополнительной информацией об атаке).
2. Нажать кнопку «**Сохранить pcap**» и указав путь для сохранения (Если в браузере включен режим «**Всегда указывать место для скачивания**»). Информация выгружается из системы в файл с форматом *.pcap, что позволяет

пользователю провести анализ данных используя специальное ПО, поддерживающее данный формат.

3. Для возврата на вкладку «**Атаки»** необходимо закрыть текущую вкладку.

Записи в таблице обновляются автоматически, по заданному администратором безопасности интервалу времени в секундах.

5.4.2 Фильтрация по полям событий о сетевых вторжениях

Для того чтобы отобразить в таблице атак записи, отвечающие заданным администратором безопасности критериям, предусмотрена возможность фильтрации.

В верхней части страницы расположены поля и выпадающие списки значений для выполнения фильтра.

«ИД устройства» - идентификатор устройства, подвергшегося атаке;

«Теги»- тег;

«Имя устройства» - имя устройства, зафиксировавшего атаку;

«Тип устройства» – варианты Dionis, Cisco, Generic;

«**Действие**» событие, активировавшееся при обнаружении атаки;

«Наличие pcap» - варианты да/нет;

SID - (Security Identifier) идентификатор атаки в системе;

GID - (Group ID) идентификатор группы;

«Приоритет» приоритет атаки, в соответствии с правилом обнаружения;

«Протокол» протокол, по которому совершена атака на устройство;

«IP атакующего» – IP адрес источника;

«Порт атакующего» – порт удаленного компьютера, с которого совершена атака;

«IP атакуемого» – IP-адрес получателя;

«Порт атакуемого» – порт компьютера получателя;

«**Описание**» - описание;

«**Страница атак**» - диапазон страниц.

Для выгрузки отчета об атаках в формате pdf нажмите на кнопку «**Сохранить как PDF**».

Для добавления новых панелей, изменения временного интервала см. п.5.7.1.1.

Для сохранения отчета в формате PDF нажмите на кнопку «**Сохранить как PDF**»

5.5 Страница «Топология»

Используйте страницу «**Топология**» для сканирования сети и отображения конфигурации графа, вершинам которого соответствуют подключенные к системе сетевые шлюзы безопасности.

«Физика включена» - для включение/выключение режима автоматического размещения устройств на топологии

«Мигание не доступных» - для включение/выключение режима индикации недоступных устройств

«Правка связей» - для включение/выключение режима редактирования топологии

«Закрепить узлы» - для перемещения всей топологии одновременно.

5.5.1 Манипуляции с процессом сканирования

5.5.1.1 Отображение

1. Выберете имя «Топологии» в выпадающем списке
2. Нажмете кнопку отобразить
3. Если выбрать узел нажатием левой клавиши мыши, то в правой части экрана будет показана информация о данном узле:

   Хост – общий идентификатор устройства;

   Название – имя узла, отображается на топологии;

   Группа – принадлежность хоста к различным отображениям сетевых устройств;

   Тип – логический тип устройства;

   IP – сетевой адрес устройства;

   Тип IP – версия сетевого протокола;

   Вендор IP – описание производителя устройства;

   OS – название операционной системы на устройстве;

   Точность – точность данных после сканирования.

5.5.1.2 Сканирование

1. Нажмите кнопку сканировать и откроется меню настройки сканирования.

2. Заполните поля названия, таймаута (времени максимальной продолжительности процесса сканирования) и набора сетей для сканирования

3. Нажмите сканировать. Создастся задача по сканированию сети.

4. Дождитесь завершения задачи, узнать о ее состоянии можно во вкладке «Задачи».

5.5.1.3 Загрузка результатов сканирования (xml файл в nmap-совместимом формате)

1. Нажмите кнопку «загрузить»
2. Заполните поле задания и нажмите кнопку «Файл». Откроется окно выбора файла для загрузки. После выбора файла создастся задача по загрузке, дождитесь завершения ее выполнения аналогично пункту сканирования.

5.5.1.4 Удаление

1. Выберите наименование «Топологии» из выпадающего списка и нажмите удалить.

5.5.2 Манипуляции с графом отображения

5.5.2.1 Контекстное меню

По правому щелчку мыши в области отображения графа открывается контекстное меню

Сохранить/Удалить позиции – сохраняет/удаляет текущее состояние отображения вершин графа.

Добавить позицию – добавляет новую позицию на топологию. При добавлении необходимо заполнить поля во всплывающем окне, такие же как в области «Узел»:

Хост – общий идентификатор устройства;

Название – имя узла, отображается на топологии;

Группа – принадлежность хоста к различным отображениям сетевых устройств;

Тип – логический тип устройства;

IP – сетевой адрес устройства;

Тип IP – версия сетевого протокола;

Вендор IP – описание производителя устройства;

OS – название операционной системы на устройстве;

Точность – точность данных после сканирования.

Фильтры:

– фильтрация вершин графа по типу соответствующего хоста (linux, window, cisco, dionis, dionis-lx, generic, router, printer);

– фильтрация вершин графа по типу связи (traced, туннель, маршрут, порт).

Сбросить фильтры – сбрасывает фильтры отображения графа.

Анализировать – запускает процесс парсинга конфигурации устройства и получения из него списка интерфейсов.

По правому щелчку мыши по устройству открывается контекстное меню (в зависимости от устрайства):

Закрепить;

Действия (Старт, стоп, Перезагрузка);

Получить консоль;

Сенсор;

Удалить.

В режиме «Правка связей» по правому щелчку мыши по связям открывается меню:

Редактировать – редактирование связи:

- выбор типа:Traced, Маршрут, Туннель, Порт;

- Указать вес;

Удалить – удаляет связь.

5.5.2.2 Область визуализации информации о вершине графа.

При щелчке мыши по вершине графа будет заполнена форма с информацией по результатам сканирования – хост (fqdn), название, группа отображения, ip адрес, тип и вендор ip, предполагаемая операционная система и оценка точности предположения, интерфейсы устройства и их состояние (в случае если устройство заведено в мониторинг и управление). Пункты название и группа являются изменяемыми и приводят к изменению отображения вершины графа.

5.5.2.3 Поиск узлов

Возможен поиск узлов по названию, в случае нахождения узла происходит его выделение и центрирование отображения на нем.

5.6 Страница «Задания»

Используйте страницу «**Задания**» для отображения всех действий с устройствами.

Зафиксированные задания имеют следующий набор атрибутов:

«**Название**» - название задания;

«**Действие**» - описание задания;

«**Статус**» - статус задания;

«**Тип**» - тип задания;

«**Объект**» - имя устройства;

«**Пользователь**» - имя пользователя, который назначил действие;

«**Время**» - время выполнения.

Предусмотрена фильтрация отображения списка заданий по заданным полям.

5.7 Страница «Мониторинг»

Мониторинг в системе предназначен для визуального контроля состояния системы и представляет собой графическую инструментальную панель (от англ. Dashboard).

Dashboard это набор строк, в каждой из которых есть одна или несколько панелей представления:

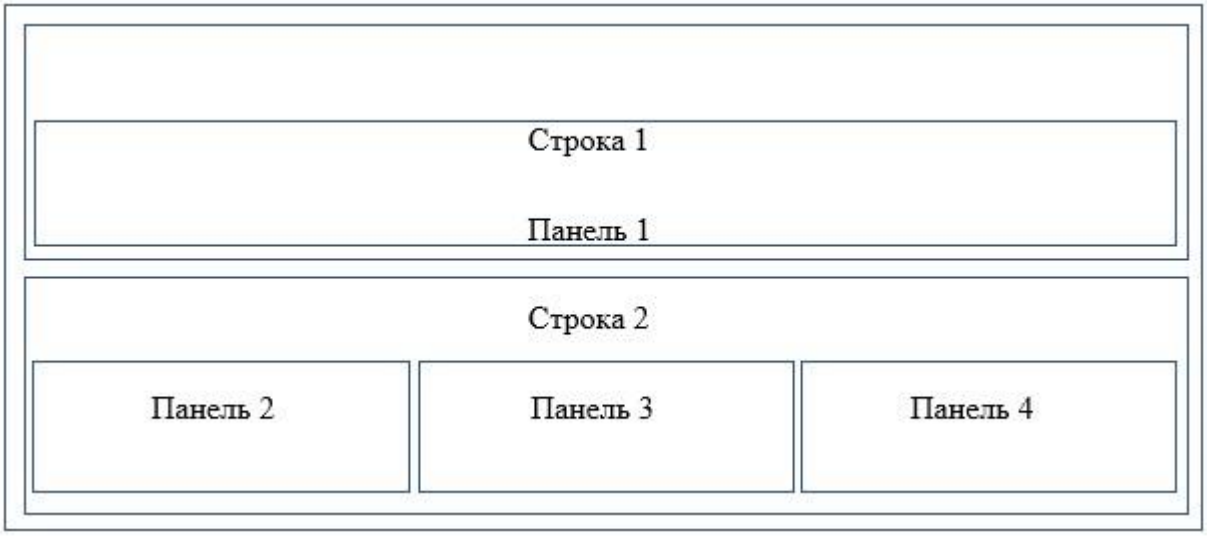


Рисунок 5 – Структура Dashboard

Dashboard служит для наглядного представления состояния соединений, загрузке CPU, а также позволяет пользователю получить графическую информацию о качестве соединения, интенсивности передачи данных, загрузки интерфейсов и другой информации.

На панели можно выводить графики, таблицы, цифровые панели, списки уведомлений, диаграммы.

По умолчанию страница «**Мониторинг**» состоит из следующих панелей:

– Устройства – список устройств, подключенных к ПО Dionis-SMP 1.0 ;

– Устройства в сети – граф устройств в сети.

– Время отклика на ping – время отклика (текущее (current), минимальное (min), максимальное (max), среднее (avg));

– SNMP traps - аварийные сообщения о событиях, происходящих в устройствах;

– График времени отклика на ping – график времени отклика по временной шкале;

– Доступность устройств – отображение доступности устройств по временной шкале.

Для того чтобы отобразить информацию только выбранных устройств на странице «Мониторинг», предусмотрена возможность фильтрации.

В верхней части страницы расположены поля и выпадающие списки значений для выполнения фильтра.

Для отображения подробной информации о конкретном устройстве нажмите на его наименование в панели «**Мониторинг>Устройства**» и откроется страница со следующими панелями:

- Загрузка CPU – график загрузки CPU;
- Состояние интерфейсов – список интерфейсов устройства (интерфейс, устройство, локальный IP-адрес, Статус);
- Температура;
- Использование оперативной памяти;
- Использование энергонезависимой памяти;
- Панели использования интерфейсов устройства.

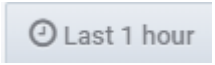
5.7.1 Описание Dashboard мониторинга

Dashboard состоит из двух функциональных областей:

- области визуального контроля;
- области инструментов.

5.7.1.1 Верхняя панель инструментов

Таблица 11 – Элементы панели инструментов

Элемент панели инструментов	**Действие**
Выпадающее окно **Dashboards** 	В раскрывающемся окне можно видеть, какой Dashboard показан в данный момент, и по нажатию на эту иконку переключиться на новый Dashboard. Здесь можно создать новую панель или папку, импортировать существующие панели мониторинга.
Добавить панель 	Добавляет новую панель представления в текущий Dashboard.
Совместное использование (Share) 	Возможность создать ссылку на Dashboard (Link), «сколку» Dashboard (Snapshot), экспортировать текущую Dashboard в файл JSON. Перед совместным использованием убедитесь, что Dashboard сохранена.
Сохранить 	Текущая Dashboard будет сохранена с текущим именем Dashboard.
Настройки 	Управление настройками и функциями Dashboard
Сдвиг назад 	Сдвиг временного диапазона назад.
Сдвиг левой границы 	Сдвиг левой границы временного диапазона.
Сдвиг вперед 	Сдвиг временного диапазона вперед.
Выбор времени 	Управление параметрами временного диапазона, параметрами автоматического обновления.
Кнопка обновления 	Ручное обновление. Выборка новых данных, обновление всех панелей.

5.7.2 Отображение информации и действия с графиком загрузки процессора устройства

Каждый график, расположенный на инструментальной панели, является интерактивным объектом. График может иметь различную форму представления

информации (например, гистограмма, диаграмма, тепловая карта[1]), с расположенным под ней перечнем отображаемых метрик и их значений, как пример:

- min – минимальное значение, за представленный на графике период;
- max - максимальное значение, за представленный на графике период;
- avg -среднее значение, за представленный на графике период;
- current -текущее значение метрик.

На рисунке 6 приведен график загрузки процессора на устройстве.

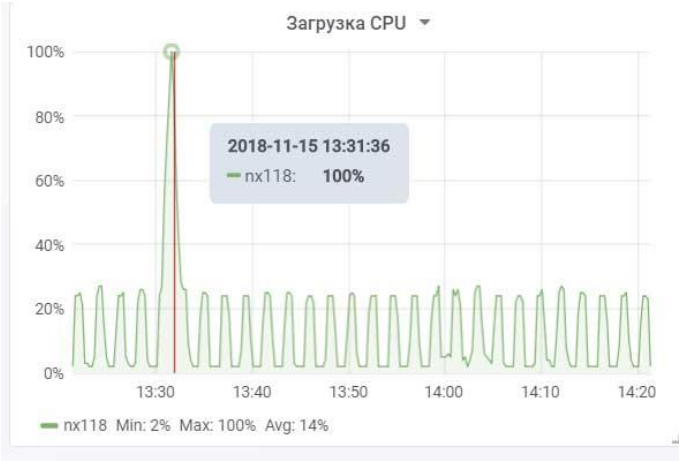


Рисунок 6 – График загрузки процессора устройства

Во времени отображаются значения, получаемые с устройства. При наведении указателя на конкретный момент времени графика начинает отображаться дополнительная секция, в которой указана загрузка процессора на каждом из устройств в выбранный момент времени. В легенде приводится перечень контролируемых устройств для данного графика и значения загрузки процессора в трёх вариантах: «min», «max» и «avg» (минимальное, максимальное и среднее) за промежуток времени, отображаемом на представленном графике.

При работе с графиками пользователю доступны действия по экспорту значений, а также изменению вида графика (см. Рисунок 7). Для выбора дополнительных действий с графиком необходимо нажать на название действия в выпадающем списке.

1 – графическое представление данных, где дополнительные переменные отображаются при помощи цвета

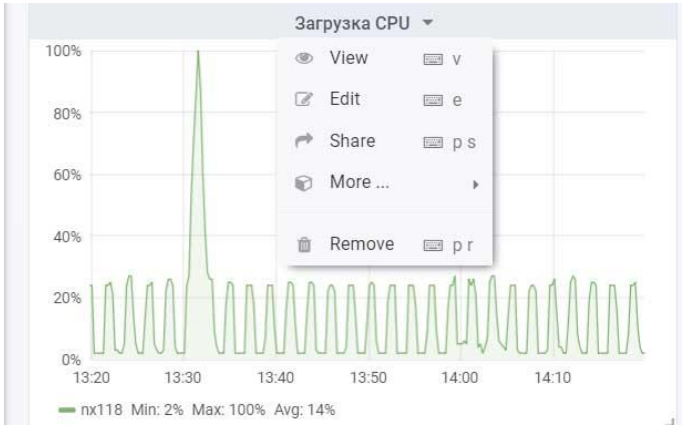


Рисунок 7 – Действия с графиком (View/Edit/Share/More/Remove)

5.7.3 Редактирование графиков и панелей

5.7.3.1 Действия при работе с графиком

Для добавления новой панели с графиком нажмите кнопку  «**Add panel**». Появится окно с выбором типа графика (см. Рисунок 8).

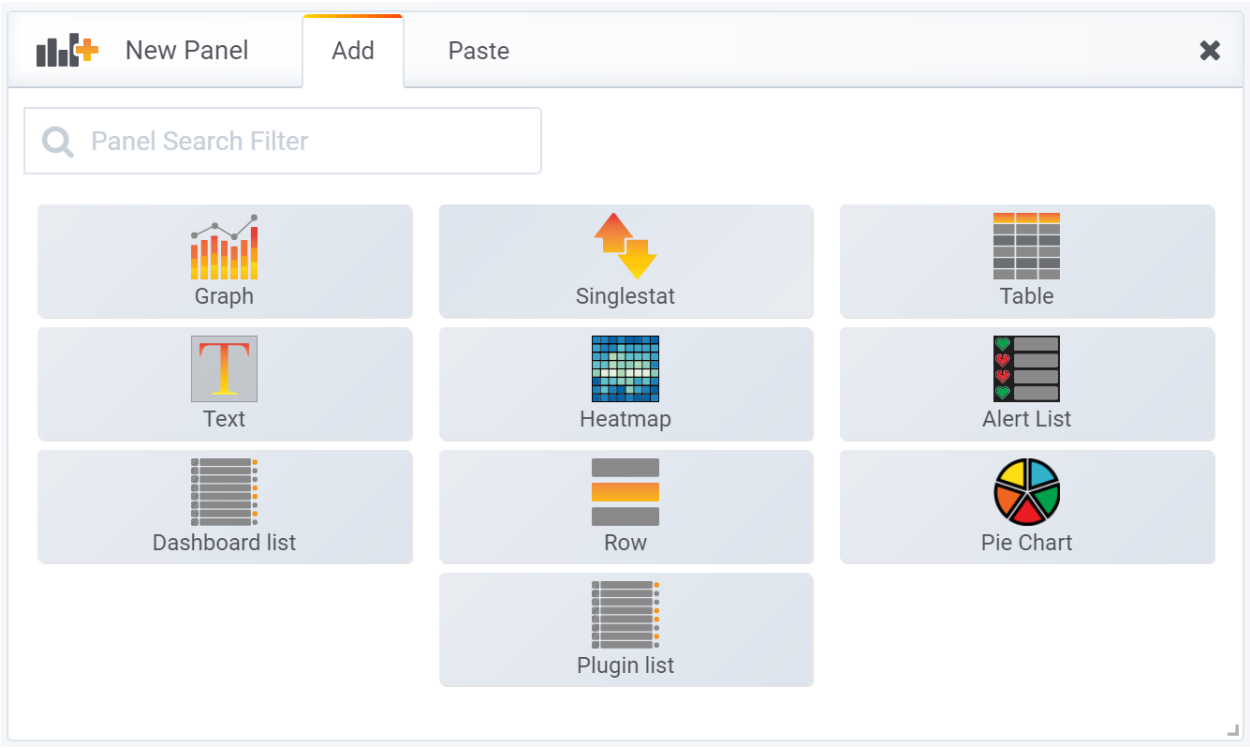


Рисунок 8 – Выбор типа графика

Доступны следующие типы:

- **Graph** – график;

- **Singlestat** - одиночный показатель;

- **Table** - таблица;

- **Text** - обычный текст;

- **Heatmap** - тепловая карта;

- **Alert List**- список предупреждений;

- **Dashboard list** - список доступных Dashboards;

- **Row** - разделитель, позволяющий создавать группы панелей;

- **Pie Chart** - график в виде диаграммы;

- **Plugin list** - список плагинов.

При нажатии на наименование панели появляется контекстное меню. Возможные варианты представлены в таблице (Таблица 12).

Таблица 12 – Описание действий при работе с графиком или панелью

Дополнительные действия	**Описание**
Просмотр (**View**)	Просмотр графика в полноэкранном режиме.
Редактирование (**Edit**)	Элемент выпадающего меню **Edit** открывает дополнительные параметры конфигурации для панели.
General	Вкладка **General** показывает и позволяет редактировать: • заголовок (**Title**) - название панели; • описание (**Description**) - описание панели; • прозрачный (**Transparent**) - если отмечено, удаляет сплошной фон панели (по умолчанию не отмечен); • повторение (**Repeat**) панели для каждого значения переменной; **Drilldown / detail link** - Раздел детализации позволяет добавлять динамические ссылки на панель, которая может ссылаться на другие информационные панели или URL-адреса.
Metrics	На вкладке **Metrics** находится редактор запросов для источника данных текущей панели. Используйте редактор для создания запросов. Результат визуализируется на панели в режиме реального времени.
Axes (для панели Graph, Heatmap)	Вкладка **настройки** осей координат.
Legend (для панели Graph)	Вкладка **Legend** управляет параметрами отображения «легенды».
Display (для панели Graph, Heatmap)	Вкладка **Display** управляет параметрами отображения информации.
Alert (для панели Graph)	Позволяет создавать сообщения по определенным параметрам.
Time range (для панели Graph, Singlestat, Table, Heatmap, Pie Chart)	Вкладка «Временной интервал» позволяет переопределить временной диапазон панели.
Value Mappings (для панели Singlestat)	Настройка сопоставления значений.

Дополнительные действия	**Описание**
Column Styles (для панели Table)	Настройка колонок таблицы.
Совместное использование (**Share**)	Предоставление информации панели другим пользователям.
Options	Общие параметры конкретной панели.
Дополнительно **(More)**	**Duplicate –** дублирование данной панели в текущий Dashboard; **Copy –** копирование данной панели; **Panel JSON** - Вызов JSON для конфигурации графика; **Export CSV (series as rows)** – экспорт значений в файл *.csv, с организацией форматирования значений по строкам (сначала идут строки значений одного типа метрик, потом следующего); **Export CSV (series as columns)** – экспорт значений в файл *.csv, с организацией форматирования значений по столбцам (в первом столбце указывается дата значения, в последующих столбцах – значения метрик, соответствующие этой дате); **Toggle legend** – скрывает/показывает легенду графика.
Удалить (**Remove**)	Удаление панели**.** Открывает окно диалога удаления панели. Перед окончательным удалением необходимо подтвердить необходимость удаления панели вместе с правилами оповещения.

Для настройки разделителя **Row** нажмите значок рядом с наименованием этого разделителя. В настройках можно изменить наименование элемента **Row** и задать значение параметра **Repeat for**, такие как **Disabled, Device, Interface, referrer, descr, offset, total**

5.7.3.2 Масштабирование графика

При работе с графиками пользователю предоставлена возможность масштабирования нужного ему диапазона (см. Рисунок 9). Для масштабирования графика необходимо навести курсор в начальную точку, и выбрав её, удерживая нажатую кнопку мыши переместить курсор в конечную точку.

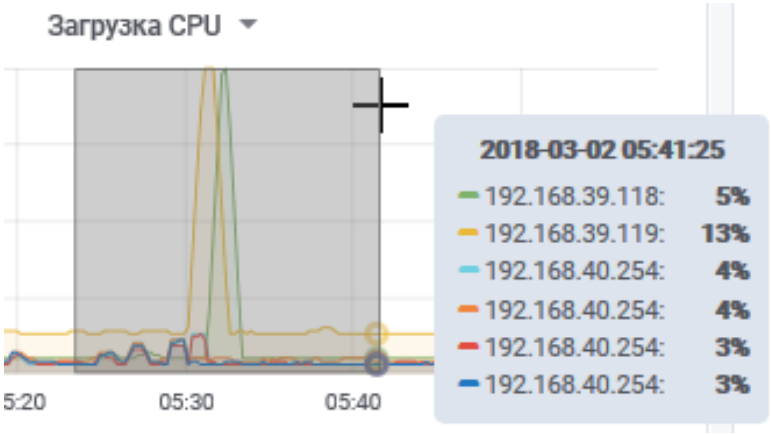


Рисунок 9 – Выбор отрезка для масштабирования

График автоматически масштабируется и отображает выбранный диапазон (см. Рисунок 10).

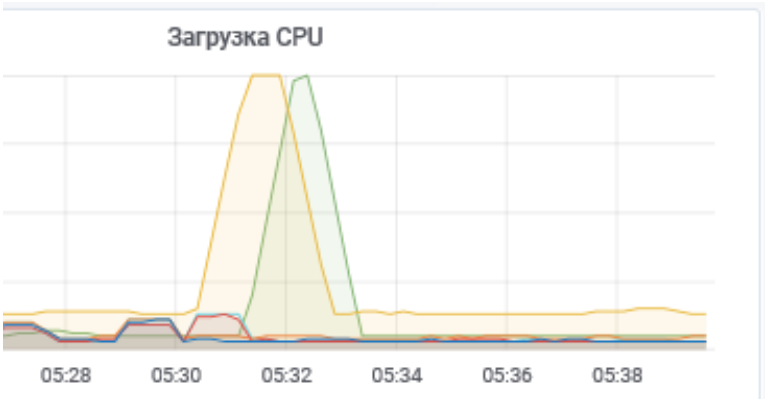


Рисунок 10 – Примененное масштабирование

Выбранный диапазон также отобразится на соответствующей кнопке панели инструментов (см. Рисунок 11).

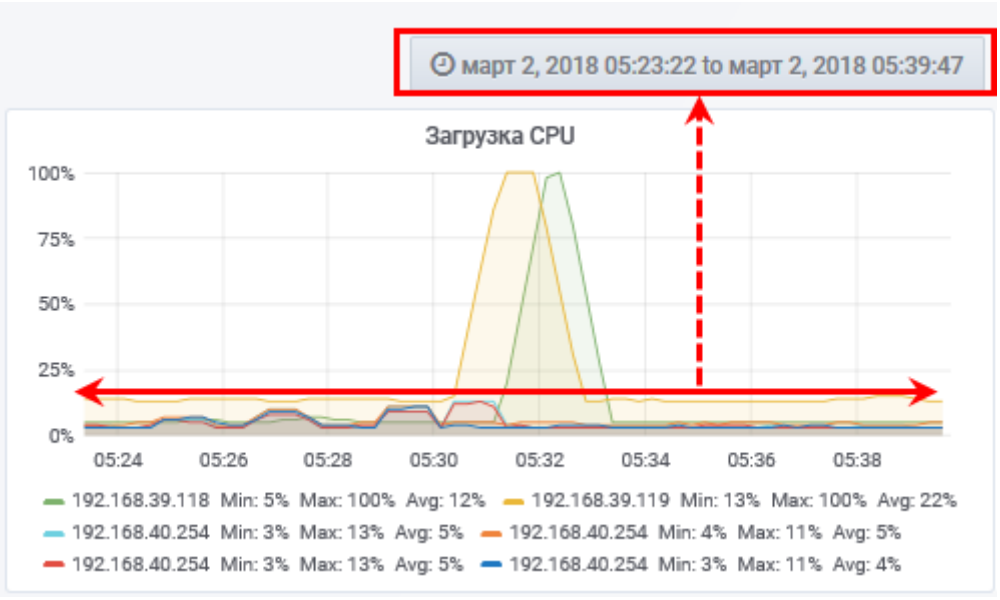


Рисунок 11 – Примененное масштабирование

5.7.3.3 Предоставление данных графика другим пользователям

Пользователь имеет возможность продемонстрировать панели отображения другим пользователям.

Предоставление данных графика:

1. Щелкнуть на его название.
2. Нажать пункт **Share** в выпадающем меню.
3. В результате откроется окно **Share Panel**.

Вкладка **Link.**

Используйте вкладку **Link** для формирования гиперссылки к графику. Опционально можно включить в ссылку текущий диапазон отображения по времени, переменные, выбрать тему представления:

1. Включить (или нет) в ссылку текущий диапазон отображения по времени **Current time range**;
2. Включить (или нет) переменные **Template variables**;
3. Выбрать тему предоставления графика (обычно светлая) **Theme**;
4. Нажать кнопку **Copy**.

Гиперссылка к графику скопируется в буфер обмена.

Вкладка **Embed**

Использовать вкладку **Embed** для создания, встроенного HTML кода, который может быть вставлен или включен в любую веб-страницу (пользователь, просматривающий страницу с встроенным кодом графика, должен быть авторизован).

Вкладка «**Snapshot**»

Вкладка «**Snapshot**» создаёт снимок состояния графика и позволяет совместно использовать интерактивную инструментальную панель. Снимок сохраняется внутри системы (кнопка **Local Snapshot**). В поле **Expire** можно указать дату истечения/удаления доступа к снимку.

5.7.3.4 Выбор диапазона значений графической информации

Пользователю доступна возможность уменьшать и/или увеличивать масштаб отображения информации на графике.

Для уменьшения и/или увеличения масштаба отображения информации на графике щелкнуть на кнопку текущего диапазона времени. В результате отобразится меню выбора диапазона представления информации.

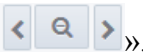
В данном меню пользователь имеет возможность быстрого выбора диапазона (область «Quick ranges»), в котором приведен перечень наиболее часто используемых диапазонов, а также задания диапазона вручную (область «Custom range»).

Для задания диапазона вручную:

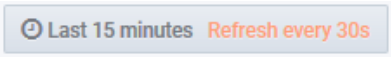
1. Указать начальную точку диапазона в поле **From**.
2. Указать конечную точку диапазона в поле **To**.
3. Выбрать период обновления данных в поле **Refreshing every**.
4. Нажать Apply (применить), чтобы использовать указанный диапазон в инструментальной панели.

После применения графики мониторинга обновят свои значения в соответствии с выбранными условиями.

5.7.3.5 Смещение диапазона значений графической информации

Для смещения диапазона используется кнопка «  ». Для смещения диапазона на более ранний отрезок времени нажать кнопку «<», и наоборот, для смещения диапазона на более поздний отрезок нажать кнопку «>». При этом смещение будет выполнено на расстояние, указанное на кнопке « 

».

Сама кнопка «  » служит для уменьшения графика на шаг, равный тому, что указан на кнопке « 

», при этом, каждый раз применяя уменьшение диапазона, указанный шаг также будет увеличиваться пропорционально, т.е. прогрессирующим способом.

5.7.4 Работа с Dashboard

Администратор имеет возможность конфигурирования инструментальной панели, создавая в ней новые графики.

Примечание. Предсозданные системные графики нельзя редактировать.

5.7.4.1 Создание новой инструментальной панели (New Dashboard)

Чтобы создать новое пространство для панелей/графиков (New Dashboard), необходимо воспользоваться одним из двух вариантов.

Вариант 1:

- на странице «**Мониторинг**» раскрыть левое боковое меню панели инструментов;
- в подменю **Create** перейти по ссылке **Dashboard**.

Вариант 2:

- на странице «**Мониторинг**» раскрыть левое боковое меню панели инструментов;
- в подменю **Dashboards** перейти по ссылке **Manage**;
- в открывшемся окне **Dashboards** нажать кнопку **+ Dashboard.**

В результате отобразится окно **New Dashboard**, где администратору безопасности предлагается выбрать тип визуализации новой панели:

- Graph - обычный график;
- Text - простой текст
- Dashboard list - перечень панелей;
- Singlestat - одиночные данные;
- Heatmap - тепловая карта;
- Row - строка;
- Plugin list - перечень дополнительных возможностей;
- Table - таблица;
- Alert list - перечень уведомлений;
- Pie Chart - диаграмма.

3. Выбрать вариант представления информации (например, график).

Отобразится новое рабочее пространство с созданным (и пока пустым) графиком.

4. Нажать на кнопку **Save dashboard** (**Ctrl+S**).
5. В открывшемся окне записать имя нового Dashboard и выбрать папку для сохранения.
6. Нажать кнопку **Save.**

Система отобразит всплывающее окно с сообщением об успешной операции создания.

5.7.4.2 Настройка графика

1. Навести курсор на заголовок графика <**Panel Title**>, и щелкнуть на раскрывающийся список.
2. Выбрать пункт **Edit**.

Появится окно с набором вкладок (открыта). Действия, которые можно осуществлять в окне описаны в Таблице 6.

2. Открыть вкладку **General.**
3. Задать название панели (графика) в поле **Title**.

4. Нажать кнопку закрыть**.**

ПРИМЕЧАНИЕ*. Настройка для допустимых типов визуализации разная.*

5.7.5 Настройка мониторинга

Для настройки мониторинга выбрать панель, перейти в меню **Edit** и выбрать вкладку **Metrics**. В результате откроется окно настройки источника данных. На вкладке Metrics находится редактор запросов для источника данных текущей панели. Используйте редактор для создания запросов. Результат визуализируется на панели в режиме реального времени.

5.7.6 Уведомления

Функция уведомления (оповещения) позволяет присоединять правила к графикам инструментальной панели мониторинга.

На вкладке **Уведомления (Alerts)** Администратор может настроить частоту уведомлений и условия, которые должны быть выполнены для изменения состояния уведомления и их запуска.

Для перехода в раздел настройки уведомлений необходимо в левой вертикальной панели инструментов раздела «**Мониторинг»** выбрать подменю **Alerting**.

Все созданные правила уведомлений мониторинга отображаются на вкладке управления уведомлениями **Alert Rules.**

На вкладке **Notification channels** выполняется настройка рассылки оповещений.

5.7.6.1 Создание и изменение уведомлений

Уведомления добавляются и настраиваются на вкладке **Alert** в окне редактирования (**Edit**) графика инструментальной панели мониторинга, позволяя создавать и визуализировать уведомления с помощью запросов.

ПРИМЕЧАНИЕ*. Уведомления доступны только для типа визуализации «Простой график».*

Создание уведомления:

1. Щелкнуть на заголовок графика и в выпадающем меню выбрать пункт **Edit.**
2. Перейти на вкладку **Alert.**

Если для данного графика еще не были созданы правила уведомлений, то на данной вкладке будет расположена кнопка **Create Alert**.

3. Нажать на кнопку **Create Alert**.

Раскроется форма создания правила уведомления.

В левой части формы расположены поля:

- **Alert Config** -настройка правила уведомления;
- **Notifications** - создание рассылки оповещений при срабатывании уведомления;
- **State History** - история срабатывания правил;
- **Delete** - удаление правил.

Рассмотрим в качестве примера создание уведомления при достижении загрузки процессора одного из устройств более чем 75 %.

На вкладке **Alert Config** выполнить действия:

1. Ввести название уведомления в поле **Name.**
2. Указать интервал проверки условий срабатывания уведомления в поле **Evaluate every**.
3. Сформировать условия (правило) уведомления, используя конструктор построения запроса в разделе «**Conditions**».
4. Нажать кнопку «» для добавления новой строки запроса.
5. Нажать кнопку «» для удаления строки конструкции.
6. Выбрать условие в строке конструкции, для продолжения формирования логического выражения.

После того как условие будет сформировано, оно отобразится на графике в верхней части окна, позволяя администратору визуально оценить созданное правило.

Появившийся элемент правила на графике интерактивен, что позволяет администратору использовать его для указания требуемого значения, исходя из представленной графической информации на графике. Передвижение поля элемента будет автоматически изменять значение в условии уведомления.

7. Указать действие в поле «**If no data or all values are null**», которое будет выполнено в случае отсутствия данных или если все значения равны нулю:
   - **Alerting** - уведомить;
   - **No Data** -никаких действий;
   - **Keep last state** - сохранить последнее состояние;
   - **Ok** - успешно;
8. Указать действие в поле **If execution error or timeout**, которое будет выполнено в случае возникновения таймаута или ошибки выполнения уведомления:
   - **Alerting** - уведомить;

- **Keep last state** - сохранить последнее состояние.

9. Нажать кнопку «**Test Rule**» для выполнения проверки сформированного условия.

На вкладке «**Notifications**» выполните следующие действия:

1. Перечислить e-mail адреса пользователей в поле **Send to**, которым необходимо отправить оповещение в случае срабатывания правила.
2. Указать текст отправляемого сообщения оповещения в поле **Message**.

Для сохранения созданного уведомления нажмите кнопку сохранения dashboard и введите описание произведенного изменения в инструментальной панели. Нажмите кнопку «**Save**».

⚠ ***ВНИМАНИЕ!*** *– Для применения изменений правил оповещения инструментальную панель мониторинга необходимо сохранить!*

После создания уведомления на вкладке **Alert** в окне **State History** будут фиксироваться события с заданными параметрами.

Все пользователи, указанные на вкладке «**Notifications**», получат оповещение на электронную почту при срабатывании правила уведомления.

5.7.6.2 Удаление уведомления

Для удаления уведомления необходимо:

1. Выбрать пункт **Delete на вкладке Alert.**

Откроется окно Delete Alert.

2. Нажать кнопку «**Delete**».

Уведомление будет удалено.

6 КОНФИГУРАЦИОННЫЕ ФАЙЛЫ ПО DIONIS-SMP 1.0

Для успешного запуска важно чтобы ПО Dionis-SMP 1.0 было корректно сконфигурировано, конфигурация ПО Dionis-SMP 1.0 происходит в файле development.ini, данный файл должен быть расположен в домашней директории пользователя по пути ***~/.config/factor/development.ini.***

Секция uwsgi

В данной секции указываются параметры uwsgi-сервера.

Секции app:main и server:main имеют отношение не посредственно к фреймворку pyramid.

Секция general

В данной секции описана конфигурация ПО Dionis-SMP 1.0 версия 2.0.

Таблица 13

Параметр	Назначение
pcap_tmp_dir	Директорий для временных файлов pcap
task_handler_svc_ipaddr	Хост
task_handler_svc_port	Порт
alert_enabled	Параметр, включающий уведомления
alert_manager_port	Порт сервиса уведомлений
alert_manager_host	Хост сервиса уведомлений
websocket_host	Хост для установления соединения через Websocket
websocket_port	Порт для установления соединения через Websocket
sched_svc_ipaddr	Хост сервиса расписаний
sched_svc_port	Порт сервиса расписаний
frontend_dir	Путь директории в которой расположены файлы web-интерфейса
default_lock_new_accounts	Создавать новых пользователей заблокированными
default_password_valid_days	Сколько действует пароль для нового пользователя
auth_max_login_attempts	Максимальное количество попыток аутентификации
admin_id	Идентификатор пользователя, который является администратором
storage_path	Путь хранения файлов

Секция alert_manager

Устанавливает настройки alert_manager.

Таблица 14

Параметр	Назначение
snmp_host	Хост snmp-exporter
snmp_port	Порт snmp-exporter
prometheus_host	Хост prometheus
prometheus_port	Порт prometheus
grafana_host	Хост Grafana
grafana_port	Порт Grafana
am_host	Хост AlertManager
am_port	Порт AlertManager
prometheus_path	Путь к конфигурационному файлу prometheus.yml
prometheus_targets_file	Путь к конфигурационному файлу static_targets.yml
prometheus_snmp_file	Путь к конфигурационному файлу snmp.yml
prometheus_login	Логин для подключения к prometheus
prometheus_pass	Пароль для подключения к prometheus

Секция database

Описывает подключение к базе данных postgresql.

Таблица 15

Параметр	Назначение
db_host	Хост
db_port	Порт
db_name	Имя базы данных
db_user	Пользователь для подключения к базе данных
db_password	Пароль для подключения к базе данных

Секция auth

Устанавливает параметры, связанные с аутентификацией.

Таблица 16

Параметр	Назначение
auth_timeout_min	Время жизни сессии аутентификации
auth_driver	Способ авторизации

Секция user_security

Устанавливает параметры, связанные с учетными записями пользователей.

Таблица 17

Параметр	Назначение
user_security_forbid_id_reuse_minutes	Время которое запрещено переиспользовать логин пользователя
user_security_inactive_minutes_to_block	Время которое пользователь может бездействовать прежде чем будет заблокирован

Секция sensor_security

Устанавливает параметры, связанные с учетными записями пользователей.

Таблица 18

Параметр	Назначение
sensor_security_forbid_id_reuse_minutes	Время, которое запрещено переиспользовать идентификатор устройства

7 АВАРИЙНЫЕ СИТУАЦИИ

В случае возникновения аварийной ситуации в работе интернет обозревателя («тонкого» клиента), данные, введенные пользователем, повреждены не будут.

В случае возникновения сбоя рекомендуется перезапустить систему. Если сбой повторяется, перегрузить компьютер и заново авторизоваться в системе.

При зависании очереди задач, рекомендуется выполнить вход в astra-linux под пользователем root, внимательно изучить логи сервиса celeryd (по пути /var/log/celery/), при необходимости - передать их разработчику, а также перезапустить сервис командой «/etc/init.d/celeryd restart».

8 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

8.1 Недостаточно прав для совершения операции

В случае, если у администратора недостаточно прав для совершения какого-либо действия, система выдает соответствующее сообщение (см. Рисунок 12).

Рисунок 12 – Недостаточно прав для совершения операции

8.2 Ошибка при авторизации пользователя

В случае неверного ввода имени пользователя или пароля при входе в систему отображается окно с соответствующей ошибкой (см. Рисунок 13).

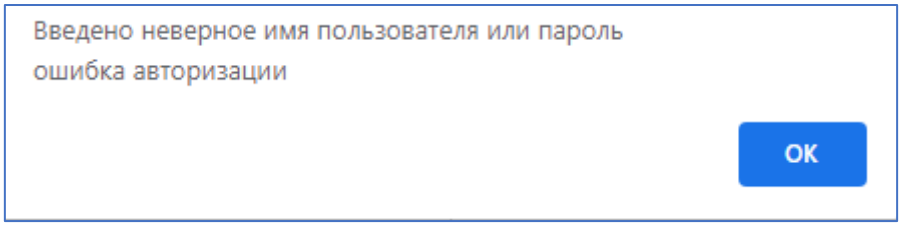


Рисунок 13 – Ошибка при авторизации пользователя

8.3 Ошибка при работе с устройствами

При создании или редактировании записи устройства его идентификатор должен быть уникальным. В противном случае система выдает сообщение о нарушении уникальности (Рисунок 14).

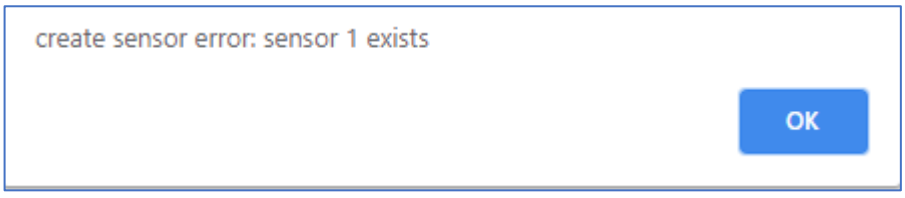


Рисунок 14 – Ошибка при создании записи нового устройства

9 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Система обладает стандартным веб-интерфейсом, поэтому администратору необходимо иметь опыт работы в операционных системах семейства Linux, а также опыт использования интернет-обозревателей (например, Internet Explorer, Chrome, Firefox).

Администратор должен иметь навыки написания скриптов в формате JSON и навыки написания правил для Snort.

Перед началом работы пользователю рекомендуется ознакомиться с документами, регламентирующими деятельность подразделений.

ПРИЛОЖЕНИЕ А

ПЕРЕЧЕНЬ ТЕРМИНОВ, ОПРЕДЕЛЕНИЙ И ОБОЗНАЧЕНИЙ

Используемые в настоящем документе сокращения, определения и основные понятия области автоматизированных систем определены в ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Также в тексте настоящего документа введены специальные термины на русском и английском языках (см. таблицу А.1).

Таблица А.1

Термин, сокращение, обозначение	**Определение**
ACL	Access Control List. Список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом
Dionis-NX	Программно-аппаратный комплекс, предназначенный для использования в роли маршрутизатора, крипто-маршрутизатора, межсетевого экрана и системы обнаружения и предотвращения вторжений. Все функциональные возможности, соответствующие определенным ролям, полностью реализованы в рамках единого программного обеспечения, установленного на каждом изделии
IKE	Протокол IKE (Internet Key Exchange обмен Internet-ключами) является гибридным протоколом, обеспечивающим специальный сервис для IPSec, а именно аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования, используемых в рамках IPSec
IPsec	IP Security – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов
NAT	Network Address Translation – механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов
SNMP	Simple Network Management Protocol – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
TCP	Transmission Control Protocol (TCP, протокол управления передачей) В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
UDP	User Datagram Protocol — протокол пользовательских датаграмм.
ICMP	Internet Control Message Protocol — протокол межсетевых управляющих сообщений

Лист регистрации изменений

Номер изменения	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводи-тельного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		14, 15			97	НКБГ.590-23			18.01.23
2		17, 60, 65, 77			97	НКБГ.604-23			30.06.23