

## Модуль С

Выполнил студент:

Брушневский Илья Ильич

Проверил преподаватель:

Попов Никита Вячеславович

### Задание 1

Вы редактируете конфигурацию с 28.10.2022 15:00. | Применить | Сохранить | Сбросить | Версия действующей конфигурации

Добавить политику | Фильтр

Рисунок 107 – Отключенные политики по умолчанию

### Задание 2

InfoWatch Traffic Monitor Enterprise

← → ⌛ Не защищено | https://172.16.8.4/organization/group/D23D0B4CFCFB4261A9CE723BC7E9A2380000000

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Еще Помощь

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 28.10.2022 15:28. Версия действующей конфигурации N

Группы + ✎ ✖ 🔍

Поиск по группам

Все элементы

demo.lab

demo

Пользовательские группы

VIP

Подозрительные сотрудники

Подозрительные сотрудники

Персоны 3 Компьютеры Поиск персон Снимают: Любые Статусы: Любые

Agafonov A Luka  
менеджер отдела договоров  
agafonov.l@demo.lab  
79992702909  
lagafonov@demo

Agafonov Y Sozon  
бухгалтер  
agafonov.y@demo.lab  
79992702932  
sagafonov@demo

Agamat Makeev  
magamat@demo.lab  
magamat@demo

Рисунок 108 – Пользовательская группа в ТМ

### Задание 3

The screenshot shows the 'Списки веб-ресурсов' (List of web resources) configuration page in InfoWatch Traffic Monitor Enterprise. On the left, there is a sidebar with a tree view under 'Списки веб-ресурсов'. The 'Партнёрские домены' (Partner domains) node is selected, showing a list of domains: 'act-demolab.ru', 'megademo.lab', and 'sysdem.lab'. A search bar and a 'Поиск' (Search) button are at the top right of the main content area.

Рисунок 109 – Список веб-ресурсов

### Задание 4

The screenshot shows the 'Периметры' (Perimeters) configuration page for a company in InfoWatch Traffic Monitor Enterprise. The 'Компания' (Company) section is selected. In the 'Редактирование' (Editing) panel, the 'Название' (Name) is set to 'Компания', the 'Группа персон' (Person group) is 'demo.lab', and the 'Список веб-ресурсов' (List of web resources) includes 'Партнёрские домены' (Partner domains). The 'Описание' (Description) field states: 'Персоны и компьютеры компании. Используется для контроля информации, передаваемой за периметр компании.' (Persons and computers of the company. Used for controlling information transmitted beyond the company perimeter.)

Рисунок 110 – Настройка периметра компании

The screenshot shows the 'Периметры' (Perimeters) configuration page for email filtering in InfoWatch Traffic Monitor Enterprise. The 'Исключить из перехвата' (Exclude from capture) section is selected. In the 'Редактирование' (Editing) panel, the 'Название' (Name) is 'Исключить из перехвата', the 'Адрес электронной почты' (Email address) is 'kornilov@demo.lab', and the 'Описание' (Description) field states: 'Если включена политика "Исключить из перехвата", то почтовые сообщения, отправленные входящими в данный периметр персонами,' (If the "Exclude from capture" policy is enabled, then emails sent by persons within this perimeter will be excluded.)

Рисунок 111 – Настройка исключений из перехвата

## Политика 1

Настройка исключений из перехвата в политики 1:

- Политика 1.1: Название - Политика 1.1, Период действия - Все время, Статус - Включен.
- Зашieldые данные: Выбрано для обнаружения хотя бы одного вхождения в каждый из типов данных.
- Объекты защиты: Номер СНИЛС, Удостоверение личности.
- Файловые типы: Графика, Текст.
- Файловые форматы: Изображение Sun Raster, Изображение PostScript.

Рисунок 112 – Дополнительная политика для Политики 1

Дополнительная политика для Политики 1:

- Правило передачи:
  - Направление маршрута: В одну сторону, В оба направления.
  - Тип события: Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Live, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте.
  - Компьютеры: Напишите вводить текст.
  - Отправители: Financial.
  - Получатели: Напишите вводить текст.
  - Дни действия правила: Любой день недели.
  - Часы действия правила: 0:00 - 0:00.
- Действия при срабатывании правила:
  - Отправить почтовое уведомление: Напишите вводить текст.
  - Назначить событию вердикт: Заблокировать.
  - Назначить событию уровень нарушения: Средний.
  - Назначить событию тему: Политика 1.

Рисунок 113 – Настройка правила дополнительной политики для Политики 1

## Политика 2

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' interface. In the top navigation bar, there are three tabs: 'localhost.ttit.local - VMware ESXi', 'demo.lab - Console - VMware ESXi', and 'IWDM - Console - VMware ESXi'. The current tab is 'IWDM - Console - VMware ESXi'. Below the tabs, the URL is https://10.30.12.52/ui/#/console/5. The main menu includes 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краулер'. A search bar at the top right contains the text 'Не защищено' and the URL 'https://172.16.8.4/analysis/fingerprint/071377B369CE463CA61D239BEC66782700000000'. On the left, there's a sidebar with 'Каталоги эталонных документов' and a list of items: 'Автоматические эталонные докум...', 'Эталон 2', and 'Эталонные документы'. The main panel shows a table titled 'Вы редактируете конфигурацию' with the title 'Применение конфигурации'. It lists configuration settings: 'Название' (Value: Эталон 2), 'Описание', 'Порог цитируемости для текстовых данных' (Value: 35), 'Порог цитируемости для бинарных данных' (Value: 35), and 'Родительский каталог' (Value: Корневой каталог). A modal window titled 'Загрузка технологий' is open, showing three sections: 'Эталонные документы' (item 'Договор.doc' status 'Сохранено'), 'Бланки' (item 'Договор.doc' status 'Сохранено'), and 'Печати' (item 'Печать.pdf' status 'Сохранено').

Рисунок 114 – Создание эталонного документа для Политики 2

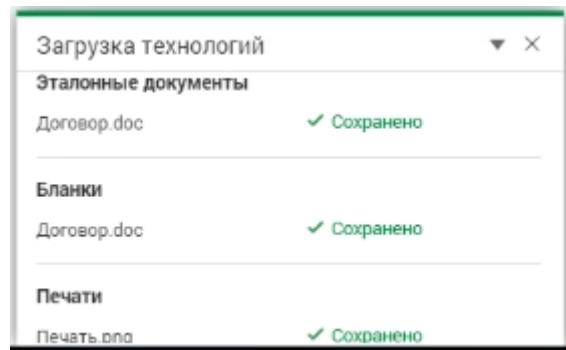


Рисунок 115 – Загрузка эталонных документов для политики 2

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' interface. The top navigation bar and URL are identical to the previous screenshot. The main menu and search bar are also present. The left sidebar shows 'Каталоги объектов защиты' with items like 'Грифованная информация', 'Демозаказ', 'Департамент 2', etc. The main panel shows a table titled 'Вы редактируете конфигурацию' with the title 'Редактировать'. It has fields for 'Название' (Value: 'Часть 1'), 'Статус' (Status: On), and tabs for 'Элементы технологий' (selected) and 'Условия обнаружения'. Under 'Элементы технологий', there is a button 'Выбрать элементы' and a list box containing 'Договор.doc' (Эталонный документ). There is also an 'Описание' field and a note indicating it was created on 28.10.2022 17:15 and last modified on 28.10.2022 17:15. At the bottom are 'Сохранить' and 'Отменить' buttons.

Рисунок 116 – Создание объекта защиты ч.1

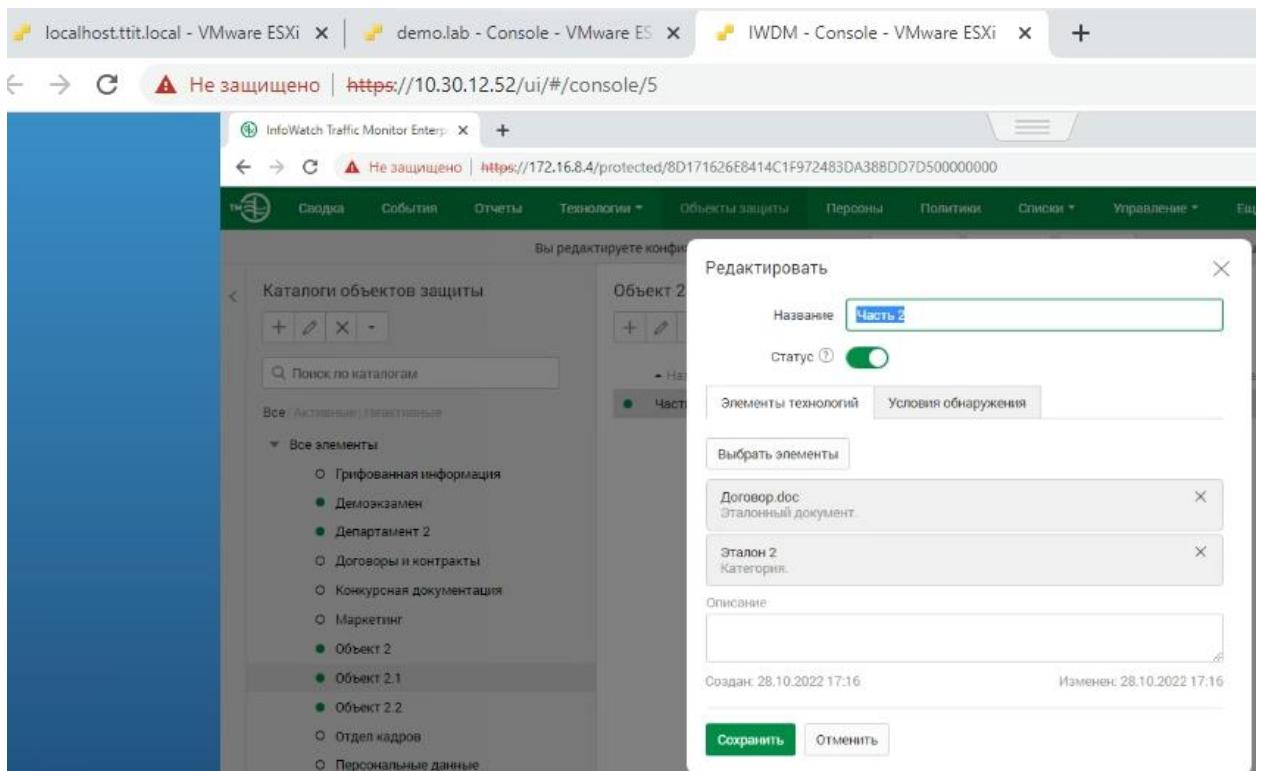


Рисунок 117 – Создание объекта защиты ч.2

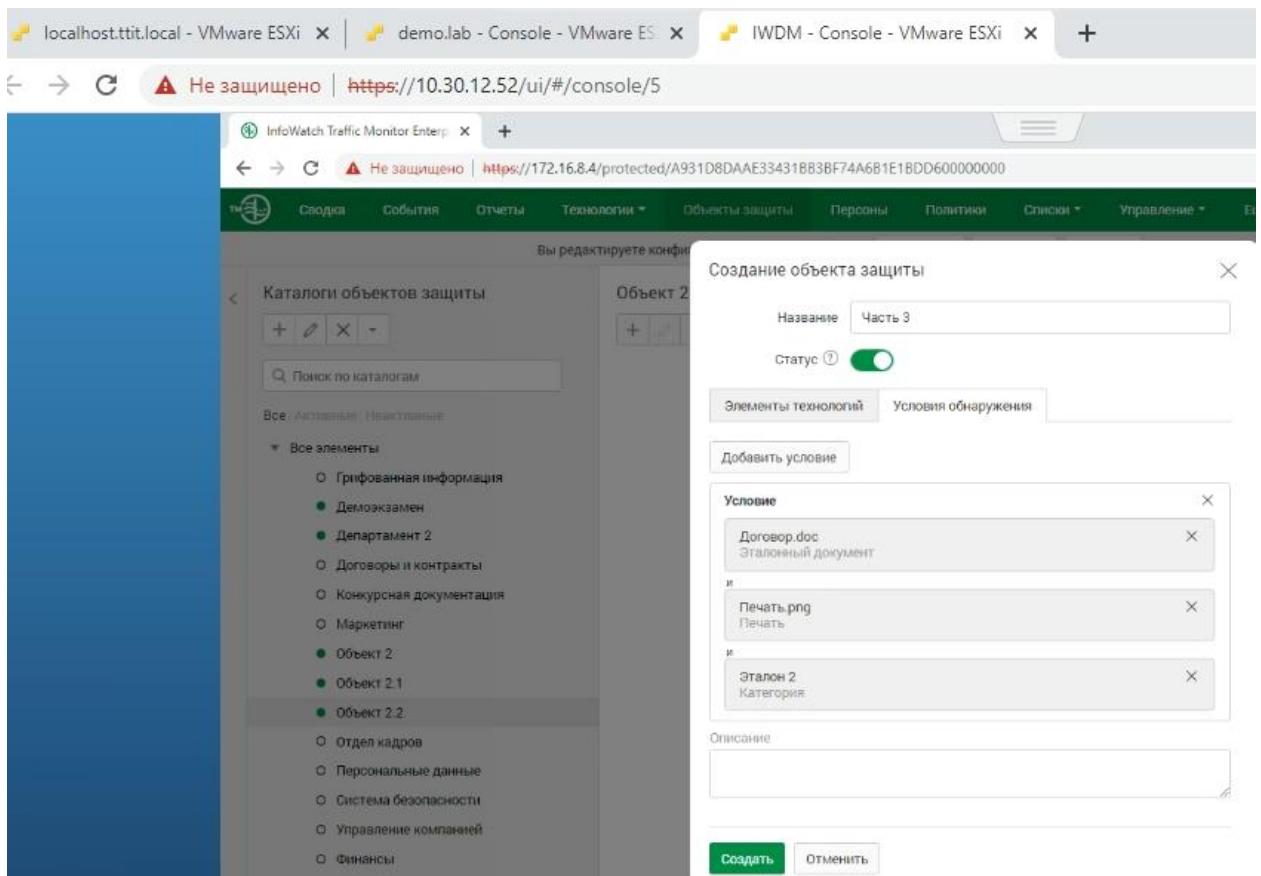


Рисунок 118 – Создание объекта защиты ч.3

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' application window. In the top navigation bar, there are tabs for 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', 'Еще', 'Поиск событий', and 'Офицер безопасности'. The main area displays a configuration page for policies. A modal window titled 'Добавить правило' (Add rule) is open, showing the configuration for 'Политика 2'. The configuration includes:

- Каталог объектов защиты:** Объект 2
- Передача 1:** Копирование, Хранение, Работа в приложениях
- Тип события:** Facebook, ICQ, MS Lync, Mail.Ru Агент, Skype, Telegram, XMPP, ВКонтакте, Веб-сообщение, Почта в Браузере, Почта на Клиенте
- Отправители:** Любой отправитель
- Направление маршрута:** Любой получатель
- Действия:** (empty)
- Действия по умолчанию:** не заданы

On the right side of the main window, there is a panel for 'Политика 2' with fields for 'Название' (Policy name), 'Период действия' (Period of validity), 'Статус' (Status), and 'Захищаемые данные' (Protected data). Below this is a section for 'Каталоги объектов защиты' (Object catalogs) with a search field for 'Объект 2'.

Рисунок 119 – Создание Политики 2 для объекта защиты 2

This screenshot shows the same application window as Figure 119, but with a different focus. A large modal window titled 'Правило передачи' (Transmission rule) is open on the right side of the screen. It contains several configuration sections:

- Направление маршрута:** → В одну сторону, ⇌ В оба направления
- Тип события:** Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте
- Компьютеры:** Начните вводить текст
- Отправители:** Любой отправитель
- Получатели:** Любой получатель
- Дни действия правила:** Любой день недели
- Часы действия правила:** 0:00 - 0:00
- Действия при срабатывании правила:**
  - Отправить уведомление
  - Назначить событию вердикт: Разрешить
  - Назначить событию уровень нарушения: Низкий
  - Назначить событию тип: Политика 2
  - Назначить отправителю статус: Выберите статус

The left side of the screen shows the same policy configuration interface as Figure 119, with multiple policy entries listed under 'Политики'.

Рисунок 120 – Создание правила передачи для политики 2

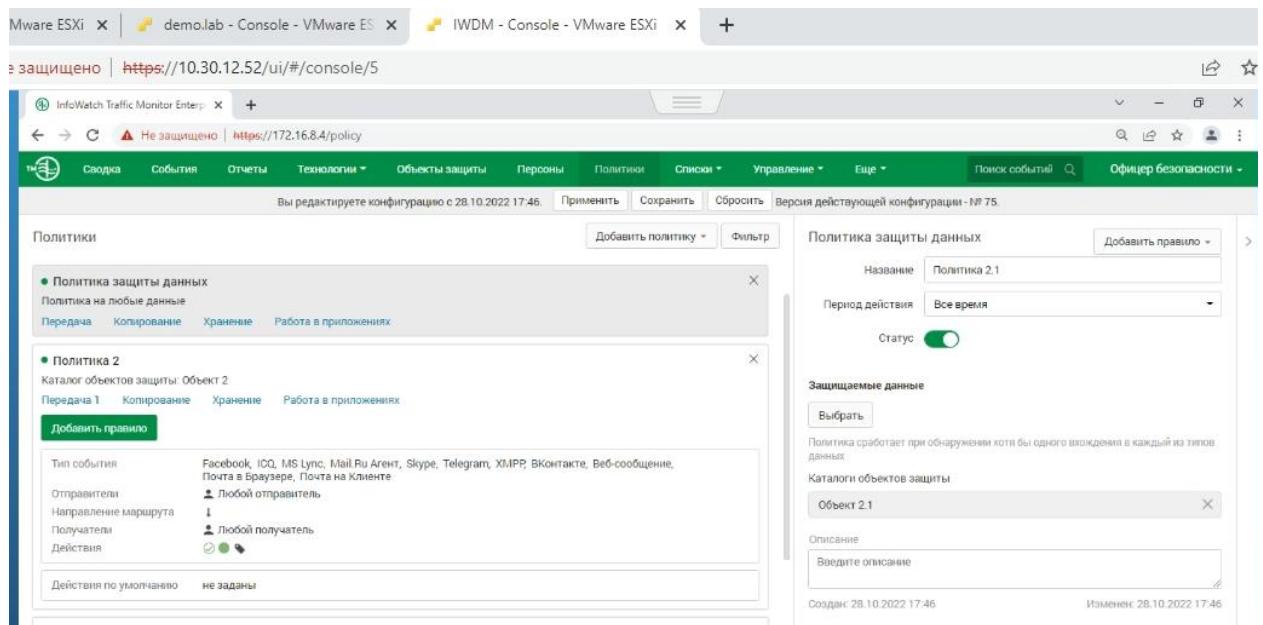


Рисунок 121 – Создание политики 2.1 для объекта защиты 2.1

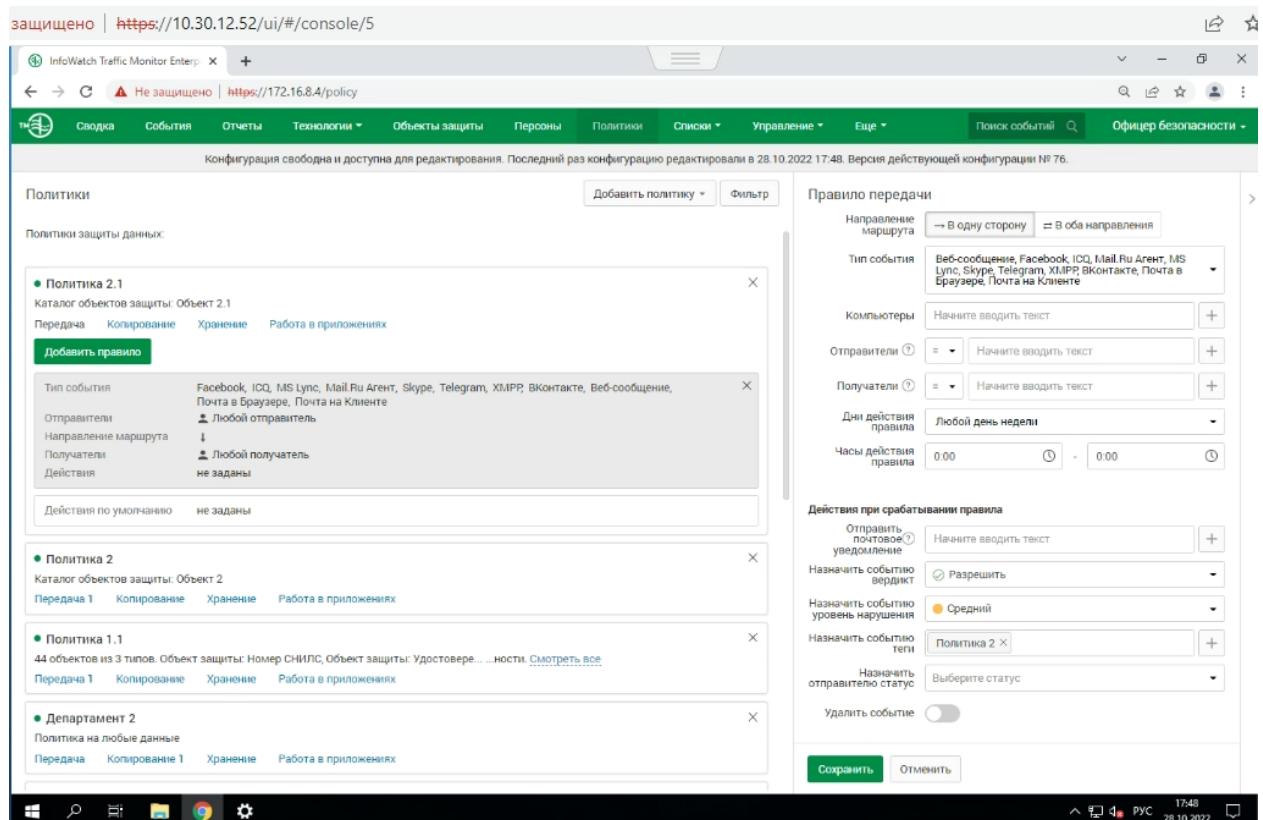


Рисунок 122 – Создание правила передачи 2.1 для политики 2.1

зашитено | <https://10.30.12.52/ui/#/console/5>

InfoWatch Traffic Monitor Enterprise | Не защищено | <https://172.16.8.4/policy>

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 28.10.2022 17:51. Версия действующей конфигурации № 79.

**Политики**

Добавить политику Фильтр

**Политика 2.2**

Название: Политика 2.2  
Период действия: Все время  
Статус: Включен

**Защищаемые данные**

Выбрать  
Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных  
Каталоги объектов защиты: Объект 2.2  
Описание: Введите описание  
Создан: 28.10.2022 17:50 Изменен: 28.10.2022 17:51

Политики защиты данных:

- Политика 2.2
 

Каталог объектов защиты: Объект 2.2  
Передача Копирование Хранение Работа в приложениях
- Политика 2.1
 

Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2
 

Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 1.1
 

44 объектов из 3 типов. Объект защиты: Номер СНИЛС, Объект защиты: Удостоверение...  
Передача 1 Копирование Хранение Работа в приложениях

Рисунок 123 – Создание политики 2.2 для объекта защиты 2.2

зашитено | <https://10.30.12.52/ui/#/console/5>

InfoWatch Traffic Monitor Enterprise | Не защищено | <https://172.16.8.4/policy>

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 28.10.2022 17:51. Версия действующей конфигурации № 79.

**Политики**

Добавить политику Фильтр

**Правило передачи**

Направление маршрута: В одну сторону В оба направления  
Тип события: Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, Вконтакте, Почта в Браузере, Почта на Клиенте  
Компьютеры: Начните вводить текст  
Отправители: Начните вводить текст  
Получатели: Начните вводить текст  
Дни действия правила: Любой день недели  
Часы действия правила: 0:00 - 0:00  
Действия при срабатывании правила

Отправить почтовое уведомление Начните вводить текст  
Назначить событию вердикт Заблокировать  
Назначить событию уровень нарушения Высокий  
Назначить событию теги Политика 2  
Назначить отправителю статус Выберите статус  
Удалить событие

**Добавить правило**

Тип события: Facebook, ICQ, MS Lync, Mail.Ru Агент, Skype, Telegram, XMPP, Вконтакте, Веб-сообщение, Почта в Браузере, Почта на Клиенте  
Отправители: Любой отправитель  
Направление маршрута: Любой получатель  
Получатели: Любой получатель  
Действия: не заданы

Действия по умолчанию: не заданы

**Политика 2.2**

Каталог объектов защиты: Объект 2.2  
Передача Копирование Хранение Работа в приложениях

**Политика 2.1**

Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях

**Политика 2**

Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях

**Политика 1.1**

44 объектов из 3 типов. Объект защиты: Номер СНИЛС, Объект защиты: Удостоверение...  
Передача 1 Копирование Хранение Работа в приложениях

Рисунок 124 – Создание правила передачи 2.2 для политики 2.2

## Политика 3

The screenshot shows the 'Policy' configuration page. At the top right, there are buttons for 'Применить' (Apply), 'Сохранить' (Save), and 'Сбросить' (Reset). Below these are buttons for 'Добавить политику' (Add policy) and 'Фильтр' (Filter). The main area displays a list of policies, with 'Политика 3' selected. The right side of the screen shows the configuration details for 'Политика 3', including its name ('Политика 3'), period of validity ('Все время' - All the time), and status ('Статус' - Enabled). A section for 'Контролируемые персоны' (Controlled persons) lists various groups and users. The bottom left shows the rule configuration for 'Политика 3', with a green 'Добавить правило' (Add rule) button.

Рисунок 125 – Создание политики 3

This screenshot continues from Figure 125, showing the detailed configuration of 'Политика 3'. On the right, the 'Правила' (Rules) section is expanded, showing the rule configuration. It includes fields for 'Уровень нарушения' (Violation level) set to 'Средний' (Medium), and 'Действия' (Actions) which include 'Начните вводить текст' (Start typing text) and 'Отправить почтовое уведомление' (Send email notification). The 'Действия' section also lists other actions like 'Заблокировать' (Block) and 'Назначить событию уровень нарушения' (Assign violation level to event).

Рисунок 126 – Создание правила для политики 3

защищено | <https://10.30.12.52/ui/#/console/5>

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Вы редактируете конфигурацию с 28.10.2022 18:00. Применить Сохранить Сбросить Версия действующей конфигурации - № 84.

**Политики**

**Политики защиты данных:**

- Политика 3.1  
43 объектов из 3 типов. Объект защиты: Номер кредитной карты, Файловый тип: Графика. Смотреть все  
Передача Копирование Хранение Работа в приложениях
- Политика 2.2  
Каталог объектов защиты: Объект 2.2  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2.1  
Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2  
Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 1.1  
44 объектов из 3 типов. Объект защиты: Номер СНИЛС, Объект защиты: Удостоверение личности. Смотреть все  
Передача 1 Копирование Хранение Работа в приложениях
- Департамент 2  
Политика на любые данные  
Передача Копирование 1 Хранение Работа в приложениях
- Демоэкзамен  
2 объектов из 2 типов. Каталог объектов защиты: Демоэкзамен, Объект защиты: Демоэкзамен. Смотреть все

**Добавить политику** Фильтр

**Политика 3.1**

Название Политика 3.1  
Период действия Все время  
Статус Включен

**Защищаемые данные**

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Объекты защиты

- Номер кредитной карты

Файловые типы

- Графика
- Текст

Файловые форматы

- Изображение Sun Raster
- Изображение PostScript
- Изображение PNG
- Изображение Corel Draw
- Документ SVG

**Сохранить** Отменить

Рисунок 127 – Создание дополнительной политики 3.1 для политики 3

защищено | <https://10.30.12.52/ui/#/console/5>

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 28.10.2022 18:05. Версия действующей конфигурации № 85.

**Политики**

**Правило передачи**

Направление маршрута → В одну сторону ⇌ В оба направления

Тип события Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте

Компьютеры Начните вводить текст +

Отправители ↳ ≠ ↳ Accounting +

Получатели ↳ = Начните вводить текст +

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

**Действия при срабатывании правила**

Отправить почтовое уведомление Начните вводить текст +

Назначить событию вердикт Заблокировать

Назначить событию уровень нарушения Средний

Назначить событию теги Политика 3 +

Назначить отправителю статус Выберите статус

Удалить событие

**Добавить правило**

Тип события Facebook, ICQ, MS Lync, Mail.Ru Агент, Skype, Telegram, XMPP, ВКонтакте, Веб-сообщение, Почта в Браузере, Почта на Клиенте  
Отправители Любой отправитель, кроме Accounting  
Направление маршрута ↓  
Получатели Любой получатель  
Действия не заданы  
Действия по умолчанию не заданы

**Политика 3.1**  
43 объектов из 3 типов. Объект защиты: Номер кредитной карты, Файловый тип: Графика. Смотреть все  
Передача Копирование Хранение Работа в приложениях

**Политика 2.2**  
Каталог объектов защиты: Объект 2.2  
Передача 1 Копирование Хранение Работа в приложениях

**Политика 2.1**  
Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях

**Политика 2**  
Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях

Рисунок 128 – Создание правила передачи для политики 3.1

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. At the top, there are two tabs: 'Не защищено' (Not Protected) and 'https://172.16.8.4/policy'. The main window displays 'Политики' (Policies) on the left, listing three policy items under 'Нецелевое использование ресурсов' (Unintended resource usage): 'Передача 1' (Copy), 'Хранение' (Storage), and 'Работа в приложениях' (Work in applications). To the right, a detailed view of 'Политика 3.1' (Policy 3.1) is shown, titled 'Политика контроля персон' (Person control policy). It includes sections for 'Уровень нарушения' (Violation level) set to 'Средний' (Medium), 'Связь с политикой' (Link to policy), 'Действия' (Actions) which include 'Заблокировать' (Block), and 'Назначить событие' (Assign event) with options like 'Средний' (Medium) and 'Выберите статус' (Select status). A large green button at the bottom right says 'Сохранить' (Save).

Рисунок 129 – Связь правила политики 3 и политики 3.1

## Политика 4

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. At the top, there is a message: 'Вы редактируете конфигурацию с 29.10.2022 06:14.' Below it are two sections: 'Каталоги печатей' (Print catalogs) on the left and 'Печать 4' (Print 4) on the right. The 'Печать 4' section includes a search bar 'Поиск' and a table with columns: Название (Name), Формат файла (File format), Название файла (File name), Размер файла (File size), Дата создания (Creation date), and Описание (Description). The table shows one entry: 'Печать.jpg' (Format: Изображение JPEG, File name: Печать.jpg, Size: 86.58 KB, Creation date: 29.10.2022 06...). A green 'Сохранить' (Save) button is located at the bottom right.

Рисунок 130 – Добавление печати в ТМ

The screenshot shows the 'Policy' section of the InfoWatch Traffic Monitor Enterprise web interface. On the left, there's a list of existing policies: 'Политика на любые данные' (with three sub-options: 'Передача 1', 'Копирование', 'Хранение', 'Работа в приложениях'), 'Скрытие действий сотрудников' (with three sub-options), and 'Исключение из перехвата' (with three sub-options). Below this is a section for 'Politiки контроля персон' (Person Control Policies) containing two entries: 'Политика 4' (selected) and 'Политика 3'. The 'Политика 4' entry shows it's associated with the 'Accounting' group and the 'Allowed RODC Password Replication Group'. On the right, the configuration for 'Политика 4' is detailed: it has a name 'Политика 4', a period of 'Все время' (All the time), and a status toggle switch. A note below says 'Контролируемые персоны' (Controlled persons) and lists several groups: Accounting, Allowed RODC Password Replication Group, BOD, Cert Publishers, CSAAdministrator, CSArchivingAdministrator, CSHelpDesk, CSLocationAdministrator, and CsPersistentChatAdministrator.

Рисунок 131 – Создание политики 4

This screenshot shows the configuration of the 'Политика 4' rule. It includes sections for 'Уровень нарушения' (Violation level: Низкий - Low), 'Связь с политикой' (Association with policy: Политика 4.1), and 'Действия' (Actions). The 'Действия' section contains several options: 'Отправить почтовое уведомление' (Send email notification), 'Назначить событию вердикт' (Assign verdict to event), 'Назначить событию уровень нарушения' (Assign violation level to event), 'Назначить событию теги' (Assign tags to event), and 'Назначитьрушителю статус' (Assign status to violator). There's also a 'Начните вводить текст' (Start typing text) input field and a 'Выберите статус' (Select status) dropdown. A 'Удалить событие' (Delete event) button is also present.

Рисунок 132 – Настройка правила для политики 4

InfoWatch Traffic Monitor Enterprise

Не защищено | https://172.16.8.4/policy

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.10.2022 06:40. Версия действующей конфигурации № 99.

**Политики**

Добавить политику Фильтр

Политики защиты данных:

- Политика 4.1  
3 объектов из 2 типов. Каталог объектов защиты: Печать 4, Объект защиты: Грифы ...ности. Смотреть все  
Передача Копирование Хранение Работа в приложениях
- Политика 3.1  
43 объектов из 3 типов. Объект защиты: Номер кред ... карты, Файловый тип: Графика. Смотреть все  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2.2  
Каталог объектов защиты: Объект 2.2  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2.1  
Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2  
Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях

**Политика 4.1**

Добавить правило

Название Политика 4.1

Период действия Всё время

Статус Включен

**Защищаемые данные**

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Каталоги объектов защиты

Печать 4

Объекты защиты

Грифы конфиденциальности

Грифы секретности

Описание

Введите описание

Создан: 29.10.2022 06:27 Изменен: 29.10.2022 06:40

Рисунок 133 – Настройка дополнительной политики 4.1 для политики 4

InfoWatch Traffic Monitor Enterprise

Не защищено | https://172.16.8.4/policy

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Еще Поиск событий Офицер безопасности

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.10.2022 06:40. Версия действующей конфигурации № 100.

**Политики**

Добавить политику Фильтр

Политики защиты данных:

- Политика 4.1  
3 объектов из 2 типов. Каталог объектов защиты: Печать 4, Объект защиты: Грифы ...ности. Смотреть все  
Передача Копирование Хранение Работа в приложениях
- Добавить правило
- Политика 3.1  
43 объектов из 3 типов. Объект защиты: Номер кред ... карты, Файловый тип: Графика. Смотреть все  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2.2  
Каталог объектов защиты: Объект 2.2  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2.1  
Каталог объектов защиты: Объект 2.1  
Передача 1 Копирование Хранение Работа в приложениях
- Политика 2  
Каталог объектов защиты: Объект 2  
Передача 1 Копирование Хранение Работа в приложениях

**Правило передачи**

Направление маршрута → В одну сторону ⇔ В оба направления

Тип события Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, Вконтакте, Почта в Браузере, Почта на Клиенте

Компьютеры Начните вводить текст

Отправители = Начните вводить текст

Получатели ≠ Sales, Kornilov V. Fedosej

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

**Действия при срабатывании правила**

Отправить почтовое уведомление Начните вводить текст

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Низкий

Назначить событию теги Политика 4

Назначить отправителю статус Выберите статус

Удалить событие

Сохранить Отменить

Рисунок 134 – Настройка правила дополнительной политики 4.1

## Политика 5

The screenshot shows the 'Categories' section of the term catalog configuration. On the left, a tree view lists categories like 'All elements', 'Demoezamen', 'Contracts and agreements', 'Category 5' (which is selected), 'Competitive documentation', and 'Marketing'. On the right, a table titled 'Category 5' lists terms with their characteristics:

| Text term   | Characteristic | Weight | Check for reg... | Check for mo... | Language |
|-------------|----------------|--------|------------------|-----------------|----------|
| covid       | Yes            | No     | No               | No              | Russian  |
| COVID       | Yes            | Yes    | No               | No              | Russian  |
| sars        | Yes            | No     | Yes              | Yes             | Russian  |
| SARS        | Yes            | Yes    | No               | No              | Russian  |
| coronavirus | Yes            | No     | Yes              | Yes             | Russian  |
| Coronavirus | Yes            | Yes    | No               | No              | Russian  |

Рисунок 135 – Создание и заполнение каталога терминов

The screenshot shows the 'Policy' configuration screen. On the left, a list of existing policies is shown:

- Policy 5 (selected): 2 objects from 2 types. Catalog of objects protected: Object protection 5. Protected object: Object 5. [View all](#). Actions: Transfer, Copying, Storage, Work in applications.
- Policy 4.1: 3 objects from 2 types. Catalog of objects protected: Print 4. Protected object: Graphics... [View all](#). Actions: Transfer 1, Copying, Storage, Work in applications.
- Policy 3.1: 43 objects from 3 types. Protected object: Credit... cards, File type: Graph. [View all](#). Actions: Transfer 1, Copying, Storage, Work in applications.
- Policy 2.2: Catalog of objects protected: Object 2.2. Actions: Transfer 1, Copying, Storage, Work in applications.
- Policy 2.1: Catalog of objects protected: Object 2.1. Actions: Transfer 1, Copying, Storage, Work in applications.

On the right, the details for 'Policy 5' are being configured:

- Policy 5** (Name: Policy 5, Period of validity: All time, Status: Enabled).
- Protected data**: Select [Select]. Note: The policy triggers when any occurrence of one of the types of data is found.
- Catalogs of protected objects**: Object protection 5.
- Protected objects**: Object 5.
- Description**: Please enter a description.
- Created: 29.10.2022 07:00 | Last modified: 29.10.2022 07:05

Рисунок 136 – Настройка политики 5.1

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' web interface. The main title bar displays the URL <https://172.16.8.4/policy>. The top navigation bar includes tabs for 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', 'Еще', 'Поиск событий', and 'Офицер безопасности'. A message at the top states: 'Вы редактируете конфигурацию с 29.10.2022 07:10.' Below this, there are sections for 'Политики' (with a 'Добавить политику' button) and 'Контролируемые персоны' (with a 'Выбрать' button). On the left, a sidebar lists existing policies: 'Политика 5' (Group: Users, Rules), 'Политика 4' (55 groups: Accounting, Allowed RODC Password Replication Group, etc.), and 'Политика 3' (55 groups: Allowed RODC Password Replication Group, BOD, etc.). The right side shows the configuration for 'Политика 5', including its name ('Политика 5'), period ('Все время'), status (switched on), and a note about monitoring events from users. The bottom right shows creation and modification times: 'Создан: 29.10.2022 07:10' and 'Изменен: 29.10.2022 07:10'.

Рисунок 137 – Создание Политики 5

This screenshot continues the process shown in Figure 137. It shows the 'Добавить правило' (Add Rule) button being clicked for 'Политика 5'. The 'Уровень нарушения' (Violation Level) is set to 'Низкий' (Low). In the 'Действия' (Actions) section, the 'Разрешить' (Allow) option is selected. Other action options like 'Отправить почтовое уведомление' (Send email notification) and 'Назначить событию вердикт' (Assign verdict to event) are also visible. The 'Связано с политикой' (Connected to policy) field contains the ID '06E3D886CF1F40FBBC449974C0542B8100000000'. The bottom right shows the 'Удалить событие' (Delete event) switch is turned off.

Рисунок 138 – Создание правила для политики 5

## Политика 6

The screenshot shows a software interface for managing protection objects. On the left, there is a sidebar titled 'Catalogs of protection objects' with a search bar and a list of objects. The list includes: Финансы, Управление компаний, Грифованная информация, Конкурсная документация, Система безопасности, Персональные данные, Отдел кадров, Договоры и контракты, Маркетинг, Объект 2, Объект 2.1, Объект 2.2, Печать 4, Объект защиты 5, and Объект защиты 6. The last item, 'Объект защиты 6', is selected. The main panel is titled 'Object of protection 6' and shows a search bar and a list of elements. The list includes: Название, Элементы технологий, and the selected item 'Объект 6'. Below this is a list of elements: ОКПО, ОКОПФ, ОКОГУ, ОКФС, ИНН, Номер телефона, Выгрузка из БД сеч.

Рисунок 139 – Создание объекта защиты и выбор текстовых объектов

The screenshot shows a dialog box titled 'Редактировать' (Edit) for creating a condition. It has fields for 'Name of condition' (Условие 6), 'Minimum number of rows' (4), and 'Condition of detection' (2+3+4+12+13). Below this is a section titled 'Available columns in selection' (Доступные столбцы в выборке) with a list of columns from 1 to 12. Column 8, 'Type of organization', is highlighted. At the bottom are 'Save' (Сохранить) and 'Cancel' (Отменить) buttons.

Рисунок 140 – Настройка условия выгрузки из БД

Правило передачи

Направление маршрута:  В одну сторону  В оба направления

Тип события: Веб-сообщение, Facebook, ICO, Mail.Ru Agent, MS Lync, Skype, Telegram, XMPP в Контакте, Почта в Браузере, Почта на Клиенте

Компьютеры: Начните вводить текст

Отправители:  IT  X

Получатели:  Начните вводить текст  X

Дни действия правила: Любой день недели

Часы действия правила: 0:00  - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление: Начните вводить текст

Назначить событию вердикт:  Разрешить  Запретить

Назначить событию уровень нарушения: Средний

Назначить событию теги: Политика 6  X

Рисунок 141 – Настройка правила передачи дополнительной политики 6.1

Политика контроля персон

Уровень нарушения: Средний

Связь с политикой: Политика 6.1

Действия

Отправить почтовое уведомление: Начните вводить текст

Назначить событию вердикт:  Разрешить  Запретить

Назначить событию уровень нарушения: Средний

Назначить событию теги: Политика 6  X

Назначить нарушителю статус: Выберите статус

Удалить событие:

Рисунок 142 – Привязка политики 6.1 к правилу политики 6

## Политика 7

| Категории   | Список терминов 7   |       |                    |                       |                   |                       |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
|---|---|-------|--------------------|-----------------------|-------------------|-----------------------|------|---------------|-------|-----|---|----|-----|---------|------------------|--------|----|--|----|-----|---------|------------------|--------|-----|---|-----|----|---------|------------------|--------------------|-----|---|----|-----|---------|------------------|--------------------|----|--|----|-----|---------|------------------|
| <input type="button"/> + <input type="button"/> <input type="button"/> X <input type="button"/>   | <input type="button"/> + <input type="button"/> <input type="button"/> X <input type="button"/> Поиск |       |                    |                       |                   |                       |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| <input type="text"/> Поиск по категориям  |   |       |                    |                       |                   |                       |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| <ul style="list-style-type: none"> <li>- Текст термина</li> </ul>   |   |       |                    |                       |                   |                       |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| <table border="1"> <thead> <tr> <th>Ликет</th> <th>Характеристический</th> <th>Вес</th> <th>Учитывать регистр</th> <th>Учитывать морфолог...</th> <th>Язык</th> <th>Дата создания</th> </tr> </thead> <tbody> <tr> <td>пикет</td> <td>Нет</td> <td>1</td> <td>Да</td> <td>Нет</td> <td>Русский</td> <td>29.10.2022 11:08</td> </tr> <tr> <td>Митинг</td> <td>Да</td> <td></td> <td>Да</td> <td>Нет</td> <td>Русский</td> <td>29.10.2022 11:07</td> </tr> <tr> <td>митинг</td> <td>Нет</td> <td>1</td> <td>Нет</td> <td>Да</td> <td>Русский</td> <td>29.10.2022 11:07</td> </tr> <tr> <td>Маленькая зарплата</td> <td>Нет</td> <td>1</td> <td>Да</td> <td>Нет</td> <td>Русский</td> <td>29.10.2022 11:09</td> </tr> <tr> <td>маленькая зарплата</td> <td>Да</td> <td></td> <td>Да</td> <td>Нет</td> <td>Русский</td> <td>29.10.2022 11:08</td> </tr> </tbody> </table> |   | Ликет | Характеристический | Вес                   | Учитывать регистр | Учитывать морфолог... | Язык | Дата создания | пикет | Нет | 1 | Да | Нет | Русский | 29.10.2022 11:08 | Митинг | Да |  | Да | Нет | Русский | 29.10.2022 11:07 | митинг | Нет | 1 | Нет | Да | Русский | 29.10.2022 11:07 | Маленькая зарплата | Нет | 1 | Да | Нет | Русский | 29.10.2022 11:09 | маленькая зарплата | Да |  | Да | Нет | Русский | 29.10.2022 11:08 |
| Ликет   | Характеристический  | Вес   | Учитывать регистр  | Учитывать морфолог... | Язык              | Дата создания         |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| пикет   | Нет   | 1     | Да                 | Нет                   | Русский           | 29.10.2022 11:08      |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| Митинг  | Да  |       | Да                 | Нет                   | Русский           | 29.10.2022 11:07      |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| митинг  | Нет   | 1     | Нет                | Да                    | Русский           | 29.10.2022 11:07      |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| Маленькая зарплата  | Нет   | 1     | Да                 | Нет                   | Русский           | 29.10.2022 11:09      |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |
| маленькая зарплата  | Да  |       | Да                 | Нет                   | Русский           | 29.10.2022 11:08      |      |               |       |     |   |    |     |         |                  |        |    |  |    |     |         |                  |        |     |   |     |    |         |                  |                    |     |   |    |     |         |                  |                    |    |  |    |     |         |                  |

Рисунок 143 – Создание списка терминов для политики 7

<https://10.30.12.52/ui/#/console/5>

The screenshot shows a software interface for managing text objects. At the top, there's a navigation bar with links like 'Руководство пользователя', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краулер'. Below the navigation bar, a message says 'Вы редактируете конфиг' (You are editing the config). A title 'Текстовый объект 7' is displayed above a toolbar with icons for adding (+), editing (pencil), deleting (X), and saving (-). A search bar labeled 'Поиск' is also present. On the left, a sidebar lists 'Название' (Name) and 'Текст 7' is selected. In the main panel, a modal window titled 'Редактировать' (Edit) is open. It contains fields for 'Название' (Name) set to 'Текст 7' and 'Страна' (Country) set to 'Мировое сообщество'. Below these are 'Шаблоны текстовых объектов' (Text object templates) with a list of items: 'пикет', 'Пикет', 'митинг', 'Митинг', 'Маленькая зарплата', and 'маленькая зарплата'. There's also a 'Описание' (Description) section with a text input field containing 'Добавить описание' (Add description). At the bottom, status information shows 'Создан: 29.10.2022 11:17' (Created: 29.10.2022 11:17) and 'Изменен: 29.10.2022 11:17' (Modified: 29.10.2022 11:17). Finally, there are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Рисунок 144 – Текстовый объект 7

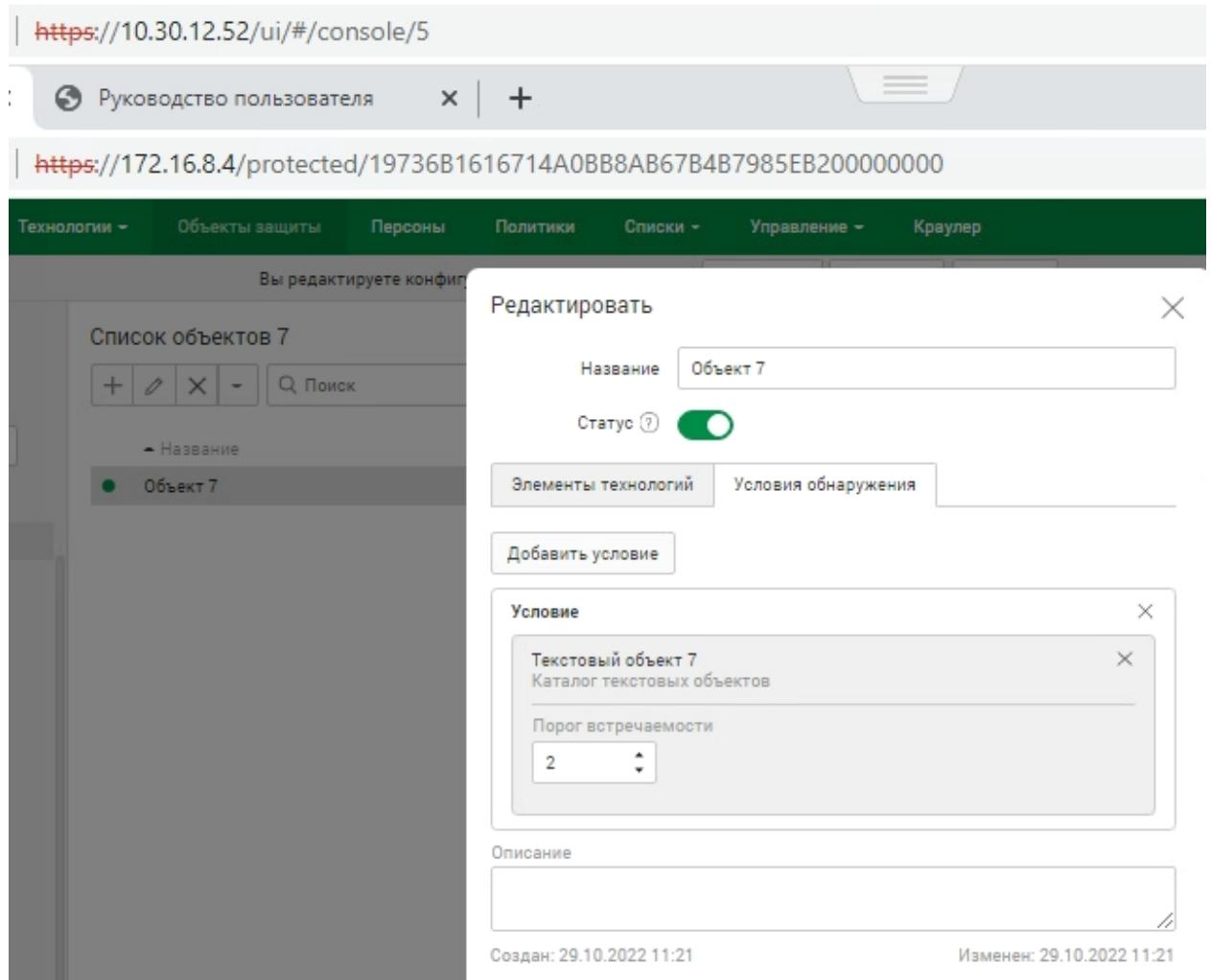


Рисунок 145 – Настройка объекта защиты 7

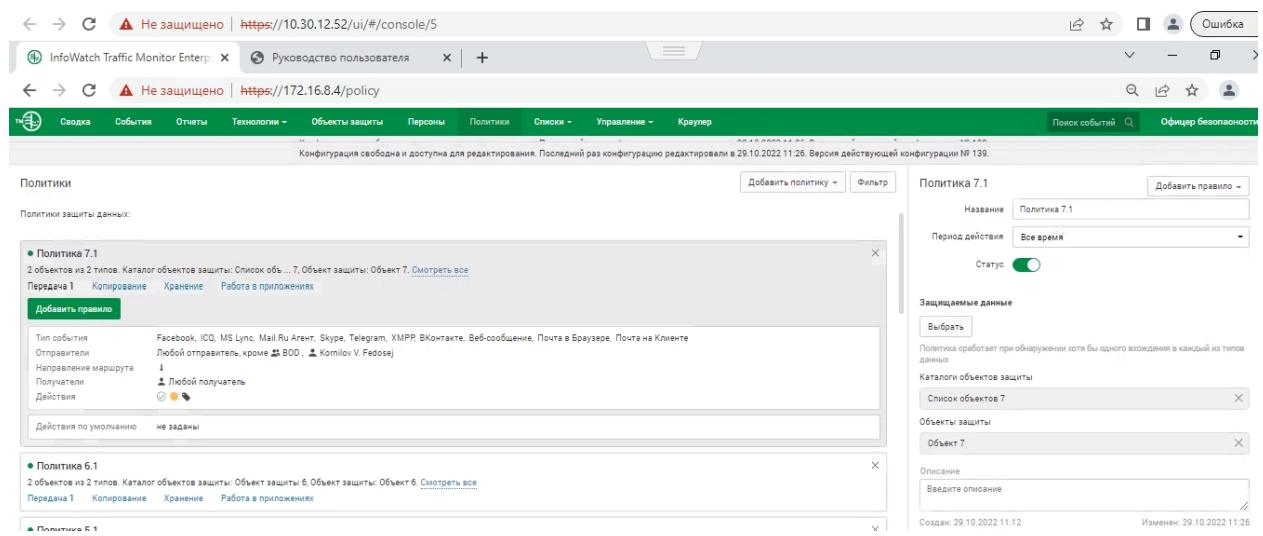


Рисунок 146 – Настройка правила и политики 7.1

Рисунок 147 – Настройка правила и политики 7

## Политика 8

Рисунок 148 – Создание списка терминов 8

Рисунок 149 – Настройка правила и политики 8.1

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. The main window displays 'Политики' (Policies) with 'Политика 8' selected. The policy details show it's for 'Users' group, level 'Низкий' (Low), and linked to 'Политика 8.1'. A 'Правила 1' section is present. Below, a 'Добавить правило' (Add rule) button is highlighted. To the right, another window titled 'Политика 8' shows its configuration: 'Название' (Name) is 'Политика 8', 'Период действия' (Period) is 'Все время' (All the time), and 'Статус' (Status) is turned on. It also lists 'Контролируемые персоны' (Controlled persons) with 'Выбрать' (Select) and 'Описание' (Description) fields.

Рисунок 150 – Настройка и связь политик 8 и 8.1

## Политика 9

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. The main window displays 'Текстовый объект 9' (Text object 9). On the right, a 'Шаблон' (Template) dialog is open. It shows a 'Статус?' (Status?) toggle switch turned on. Under 'Тип шаблона' (Template type), 'Строка' (String) is selected. The 'Регулярное выражение' (Regular expression) field contains 'magnet:/.+'. The 'Проверочный текст' (Check text) field contains 'magnet:/aboba'. A green box highlights the text 'magnet:/aboba'. Below are 'Проверить' (Check) and 'Описание' (Description) fields. At the bottom are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Рисунок 151 – Применение регулярного выражения в текстовом объекте

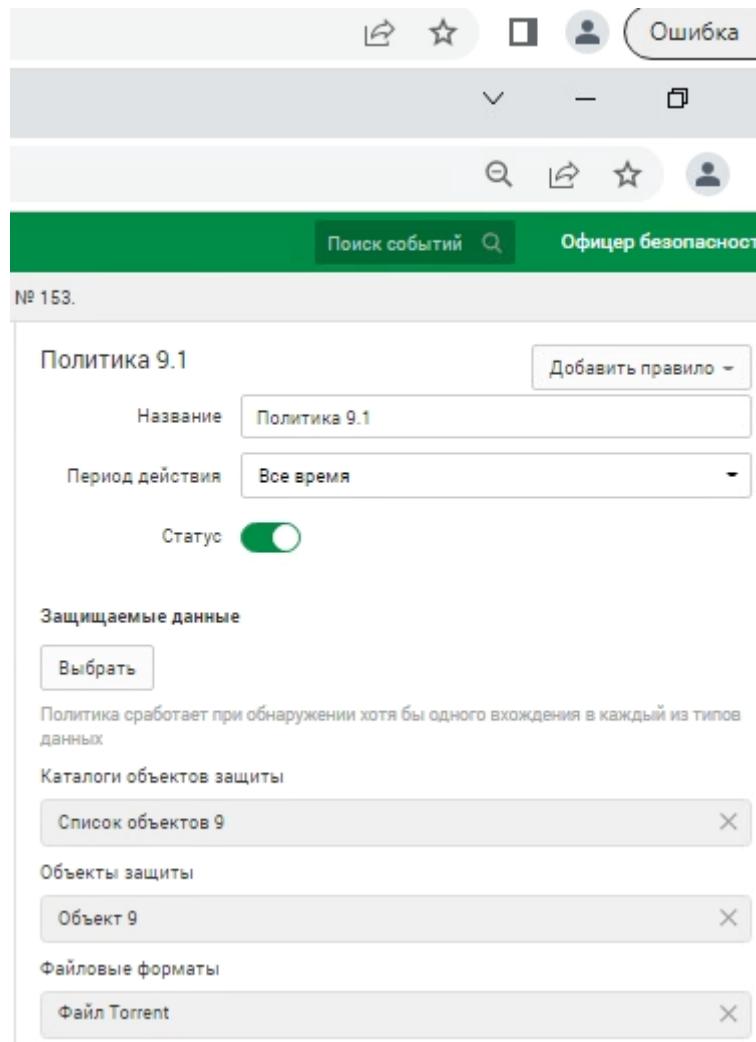


Рисунок 152 – Выбор защищаемых данных в политике 9.1

This screenshot shows the 'Officer of Security' application interface with multiple windows open. On the left, a sidebar lists 'Политики' (Policies) and 'Политики защиты данных' (Data protection policies). In the center, a window for 'Политика 9.1' is open, showing its configuration with the same parameters as in Figure 152. To the left of this window, another window titled 'Добавить правило' (Add rule) is visible, displaying the configuration of a transmission rule. This rule specifies 'Тип события' (Event type) as 'Facebook, ICQ, MS Lync, Mail.Ru Agent, Skype, Telegram, XMPP, ВКонтакте, Веб-сообщение, Почта в Браузере, Почта на Клиенте' (Facebook, ICQ, MS Lync, Mail.Ru Agent, Skype, Telegram, XMPP, VKontakte, Web-message, Mail in Browser, Mail on Client), 'Отправители' (Senders) as 'Любой отправитель' (Any sender), 'Направление маршрута' (Route direction) as 'Л' (L), 'Получатели' (Recipients) as 'Любой получатель' (Any recipient), and 'Действия' (Actions) as 'Copирование' (Copy). Below this, a note says 'Действия по умолчанию не заданы' (Default actions are not defined). To the right, other windows show 'Политика 8.1' and 'Политика 7.1' with their respective configurations.

Рисунок 153 – Настройка правила передачи в политике 9.1

Политики

- Нечеловеческое использование ресурсов
- Скрытие действий сотрудников
- Исключение из перехвата

Политика на любые данные  
Передача 1 Копирование Хранение Работа в приложениях

Политика на любые данные  
Передача 1 Копирование Хранение Работа в приложениях

Политика на любые данные  
Передача 1 Копирование Хранение Работа в приложениях

Политики контроля персон:

● Политика 9  
Группы: Users  
Правила 1  
Добавить правило

Уровень нарушения Средний  
Связано с политикой Политика 9.1  
Действия

Политика 9

Название Политика 9  
Период действия Все время  
Статус

Контролируемые персоны  
Выбрать

Политика срабатывает для событий, отправители которых входят в указанные группы, имеют указанные статусы и являются любой из указанных персон (должны быть выполнены все условия)

Группы  
Users

Описание  
Введите описание

Создан: 29.10.2022 12:44 Изменен: 29.10.2022 12:44

Активация Windows  
Чтобы активировать Windows, перейдите в

Рисунок 154 – Настройка правила и политики 9

## Политика 10

https://10.30.12.52/ui/#/console/5

Руководство пользователя +

https://172.16.8.4/analysis/text\_object/B85B835EFDCF47D7AE435AB6D591597400000000

Технологии Объекты защиты Персоны Политики Слияния Управление Краулер

Конфигурация свободна и доступна для изменения

Шаблон

Текстовый объект 10

+ X - Помощь

Название Текст 10

Статус?

Тип шаблона Стока Регулярное выражение

Регулярное выражение .+@(.demo|demolab|демо|демолаб).(ru|org|lab)

Проверочный текст aboba@demo.ru aboba@demolab.org aboba@демо.lab

Проверить

Описание

Сохранить Отменить

Рисунок 155 – Проверка регулярного выражения для почтовых адресов

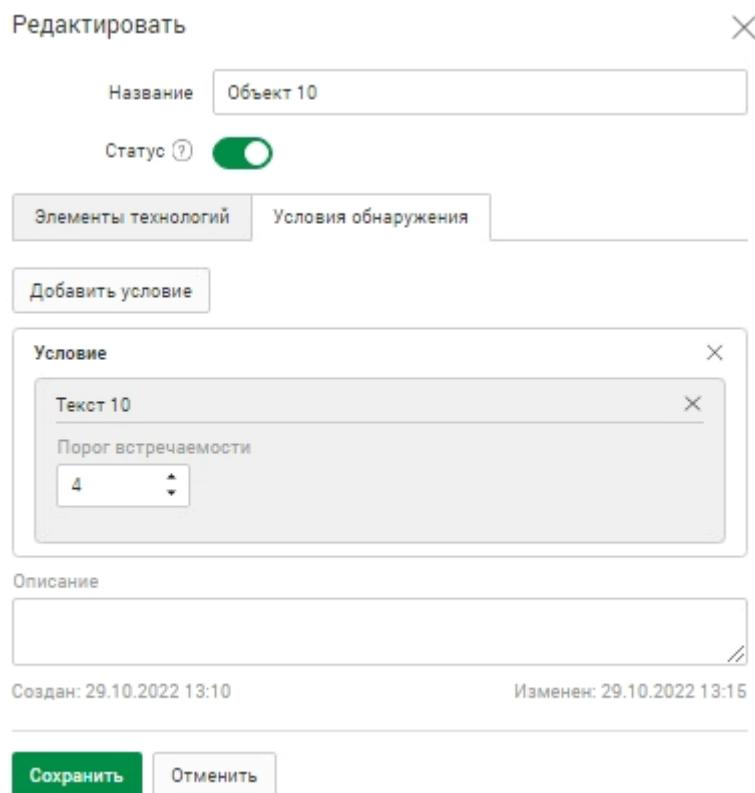


Рисунок 156 – Создание объекта защиты

Рисунок 157 – Создание правила и политики 10.1

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The top navigation bar includes tabs for 'Сводка' (Summary), 'События' (Events), 'Отчеты' (Reports), 'Технологии' (Technologies), 'Объекты защиты' (Protected Objects), 'Персоны' (Persons), 'Политики' (Policies), 'Списки' (Lists), 'Управление' (Management), 'Краулер' (Crawler), 'Поиск событий' (Event Search), and 'Офицер безопасности' (Security Officer). A banner at the top indicates 'Не защищено' (Not protected) and the URL 'https://172.16.8.4/policy'. The main content area displays policy configuration sections for 'Политики' (Policies) and 'Политика контроля персон' (Person Control Policy). The 'Политики' section contains three items: 'Нецелевое использование ресурсов' (Non-targeted resource usage), 'Скрытие действий сотрудников' (Hiding employee actions), and 'Политики на любые данные' (Any data policies). The 'Политика контроля персон' section shows a 'Высокий' (High) level of violation and a 'Политика 10.1' (Policy 10.1) entry. On the right, a sidebar titled 'Действия' (Actions) lists various configuration options for the selected policy.

Рисунок 158 – Создание правила и политики 10

Политика 11

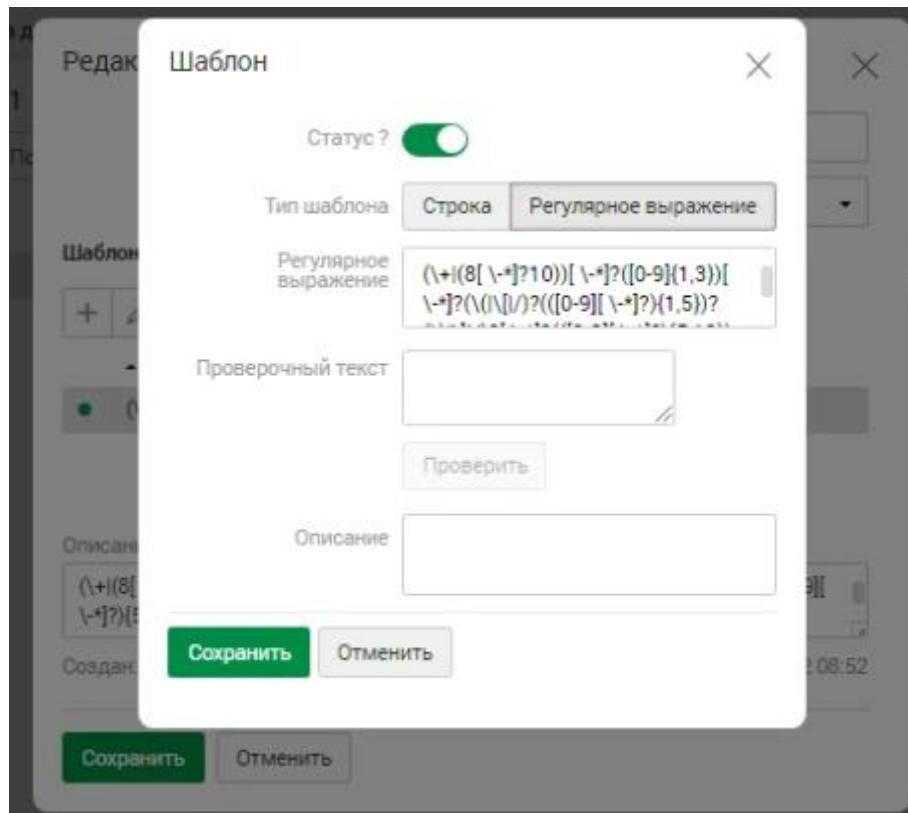


Рисунок 159 – проверка регулярного выражения для политики 11

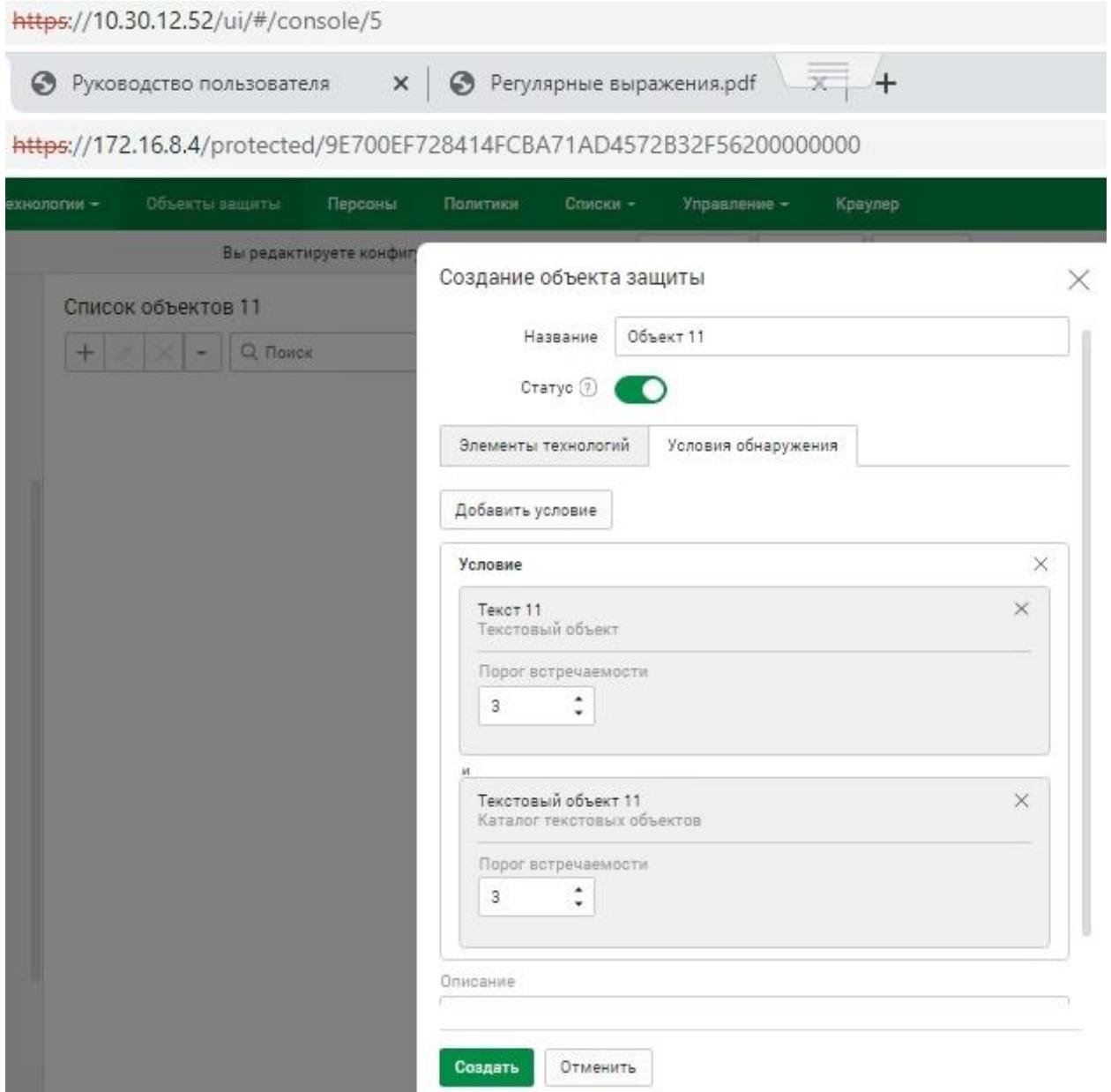


Рисунок 160 – Создание объекта защиты

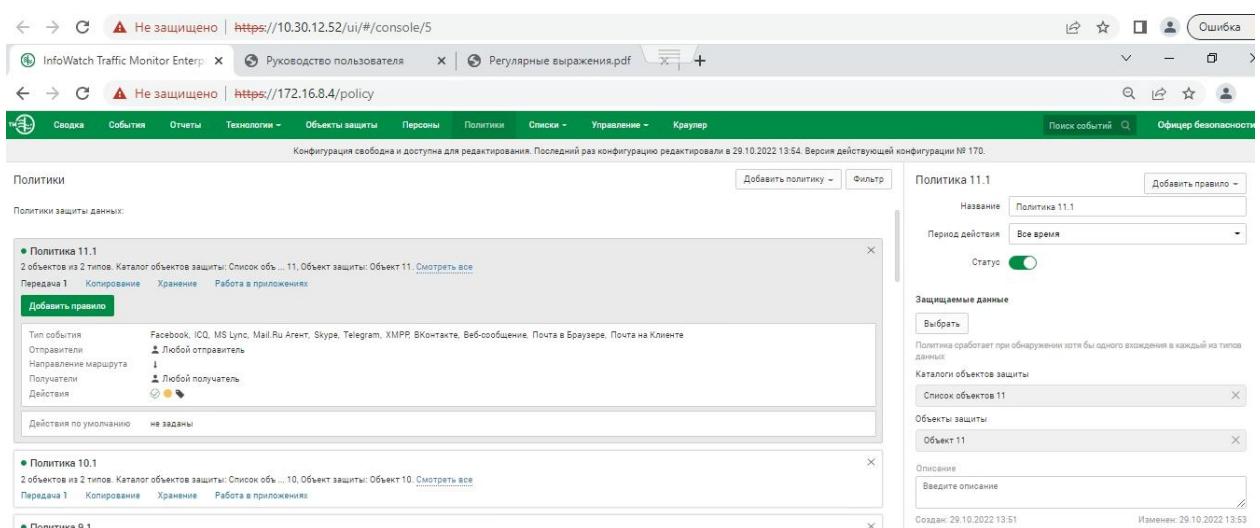


Рисунок 161 – Создание политики 11.1

Не защищено | <https://10.30.12.52/ui/#/console/5>

InfoWatch Traffic Monitor Enterpr × Руководство пользователя × Регулярные выражения.pdf +

Сводка События Отчеты Технологии - Объекты защиты Персоны Политики Списки - Управление - Краупер Помощь Ошибки

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.10.2022 13:56. Версия действующей конфигурации № 171.

Политики

13 файловых типов: Архив, Конструкторская документация, Смотреть все Передача 1 Копирование Хранение Работа в приложениях

Политики контроля персон:

• Политика 11 Группа Users Правила 1 Добавить правило Уровень нарушения Средний Связано с политикой Политика 11.1 Действия Выбрать Действия по умолчанию не заданы

• Политика 10 Группа Users

Политика 11 Название Политика 11 Добавить правило Период действия Все время Статус Вкл.

Контролируемые персоны Выбрать Политика работает для событий, отправители которых входят в указанные группы, имеют указанные статусы и являются любой из указанных персон (должны быть выполнены все условия)

Группы Users Описание Введите описание Создан: 29.10.2022 13:54 Изменен: 29.10.2022 13:54

Рисунок 162 – Создание политики 11

## Политика 12

Не защищено | <https://10.30.12.52/ui/#/console/5>

ffic Monitor Enterpr × Руководство пользователя × Регулярные выражения.pdf +

События Отчеты Технологии - Объекты защиты Персоны Политики Списки - Управление - Краупер

Выбор защищаемых данных

Каталоги объектов защиты Объекты защиты Файловые форматы

Размер файла Любой байт Любой байт

Признаки  Зашифрованные  Склейенные  Несоответствие сигнатуры и расширения

Файловые форматы

Архив  База данных  Таблица 1С  База данных ACE или JET

Сохранить Отменить

Рисунок 163 – Выбор зашифрованных архивов как защищаемых данных

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. On the left, there are three tabs: 'Не защищено' (Unprotected), 'Руководство пользователя' (User Guide), and 'Регулярные выражения.pdf'. The main area displays three existing policies: 'Политика 12', 'Политика 11', and 'Политика 10'. A 'Добавить правило' (Add Rule) button is visible. On the right, a large panel for creating a new rule is open. It includes fields for 'Направление маршрута' (Route direction), 'Тип события' (Event type), 'Отправители' (Senders), 'Направление' (Direction), 'Получатели' (Recipients), 'Дни действия правила' (Rule validity days), and 'Часы действия правила' (Rule validity hours). Below these, there are sections for 'Действия при срабатывании правила' (Actions when rule triggers) and 'Зашieldedные данные' (Shielded data). A note at the bottom right says 'Активация Windows' (Windows Activation).

Рисунок 164 – Создание политики 12

This screenshot is identical to Figure 164, showing the creation of Policy 12. The interface, rules listed, and configuration panel for the new rule are all the same.

Рисунок 165 – Создание политики 12