

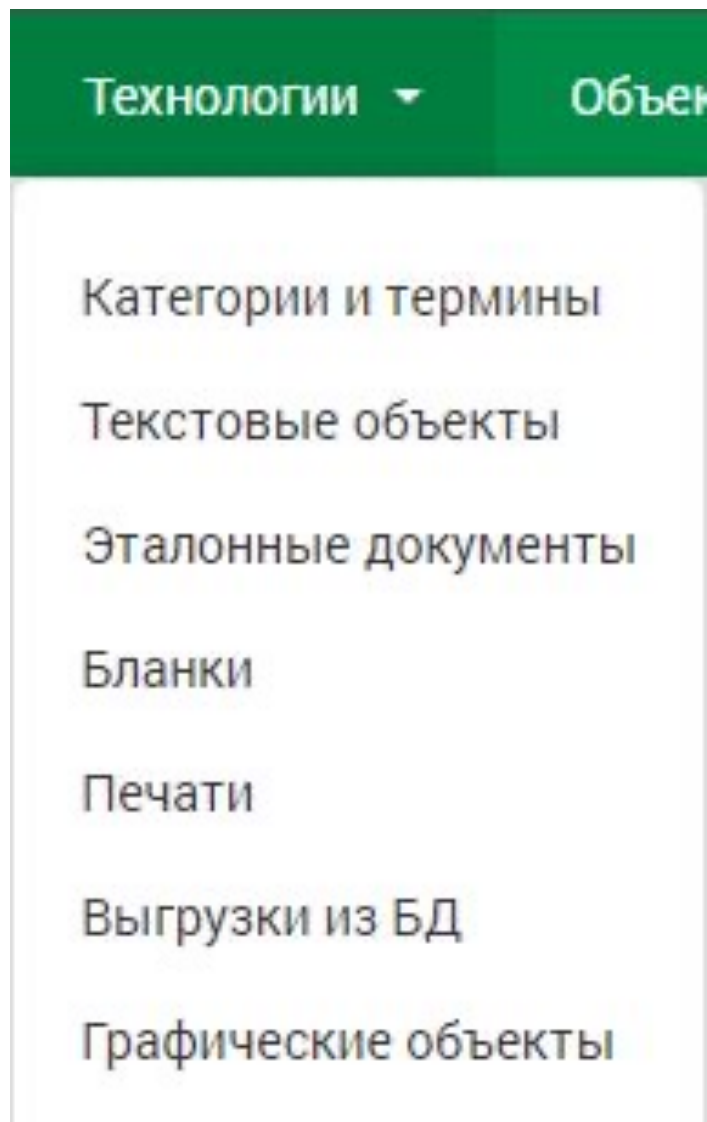
InfoWatch Traffic Monitor

Создание тестовой
политики



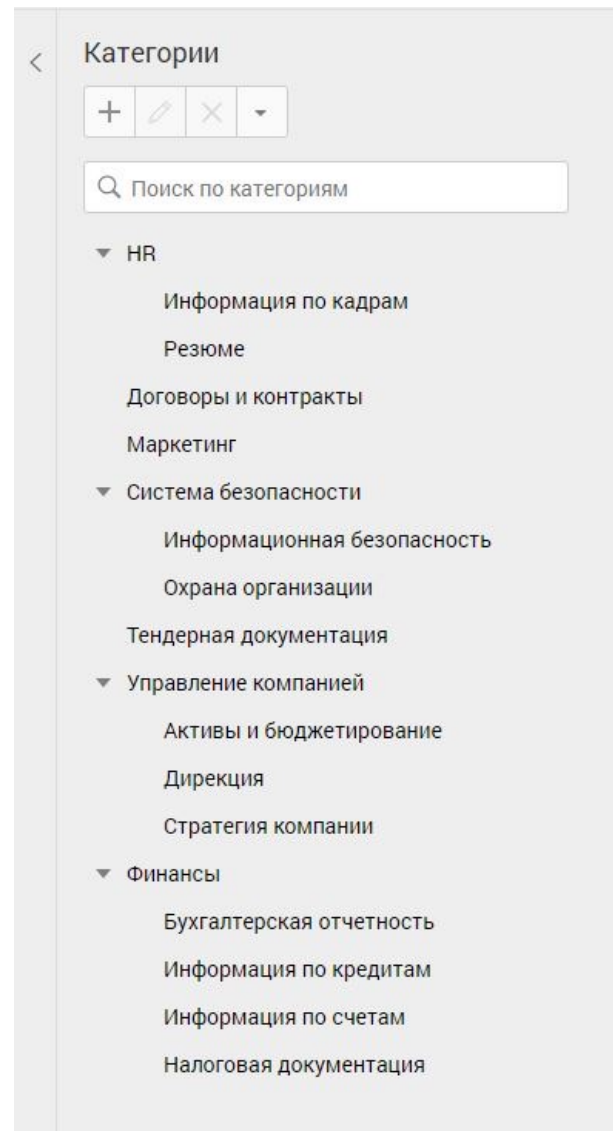
INFOWATCH

Выбор технологии



Для создания тестовой политики будет использован раздел технологии «Категории и термины». **В первую очередь необходимо добавить термин, который будет защищать политика.** В этом случае будет слово «тест». Для добавления термина нужно выбрать «Технологии», «Категории и термины».

Создание каталога





В разделе «Категории» необходимо создать новый каталог. Для этого нажать «+» в левом углу на панели инструментов данной технологии. И дать название «Тестовый каталог».

Добавление термина



Тестовый

+ ✎ ✕ 🔍 Поиск

▲ Текст термина	Характеристический	Вес	Учитывать регистр	Учитывать морфол...	Язык
Тест	Да		Да	Нет	 Русский
тест	Да		Нет	Да	 Русский

В данный каталог добавить термин «тест». При добавлении стоит учитывать:
характеристический, морфологию и регистр.
После создания термина, нужно создать объект защиты.

Создание объекта защиты



Редактировать



Название

Тестовый объект

Статус [?]



Элементы технологий

Условия обнаружения

Добавить условие

Условие



Тестовый
Категория.



Описание

Создан: 14.04.2020 21:13

Изменен: 14.04.2020 21:13

Сохранить

Отменить

Создание объекта защиты



Для создания объекта защиты необходимо перейти в раздел «Объекты защиты» и создать новый объект защиты, нажав «+» в левом углу на панели инструментов. Далее дать «Тестовый объект защиты». После этого добавить созданный ранее «Тестовый каталог» из раздела «Категории и термины». **После добавление обязательно указать условие обнаружения данного элемента.**

Создание ПОЛИТИКИ



Политика защиты данных

Добавить правило ▾

Название

Тестовая политика

Период действия

Все время ▾

Статус



Защищаемые данные

Выбрать

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

Каталоги объектов защиты

Тестовый каталог



Описание

Введите описание

Создан: 14.04.2020 13:09

Изменен: 14.04.2020 21:13

Сохранить

Отменить

Создание ПОЛИТИКИ



Следующим шагом нужно создать политику. Для этого перейти в раздел «Политику», нажать «Добавить политику», выбрать «Политику защиты данных». После необходимо настроить политику. Поменять название на «Тестовая политика» и обязательно выбрать объект защиты. **Если не выбрать объект защиты, политика будет работать на любые данные, таким образом политика будет перехватывать весь трафик.** После создания политики необходимо настроить правила передачи, копирования, хранения и буфера обмена.

Настройка правила передачи



Правило передачи

Направление маршрута

→ В одну сторону

↔ В оба направления

Тип события

Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, Viber, WhatsApp, XMPP, Yahoo!, ВКонтакте, Почта в Браузере, Почта на Клиенте, SMS

Компьютеры

Начните вводить текст

Отправители ?

=

company ×

Получатели ?

≠

company ×

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

Тест ×

Назначить отправителю статус

Выберите статус

Удалить событие



Сохранить

Отменить

Настройка правила передачи



Первым будет правило передачи. При настройке правила передачи необходимо обязательно выбрать тип события. Далее выбрать отправителя и получателя в данном случае отправители – сотрудники компании, получатели все, кроме сотрудников компании. Назначить событию вердикт «Разрешить», уровень угрозы «Низкий», тег «Тест». **Данная политика проверяется просто, достаточно отправить сообщение со словом «Тест».**

Настройка правила копирования



Правило копирования

Тип события Фотосъемка, FTP, Внешнее устройство, Облачное хранилище, Печать

Компьютеры Начните вводить текст +

Ресурс = Начните вводить текст +

Отправители ? = 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 ✓ Разрешить

Назначить событию уровень нарушения ● Низкий

Назначить событию теги Тест × +

Назначить отправителю статус Выберите статус

Удалить событие ⏻

Сохранить

Отменить

Настройка правила копирования



При настройке правила копирования нужно обязательно выбрать тип события. Далее назначить уровень угрозы «Низкий», тег «Тест». **Правило копирования можно проверить с помощью флеш-накопителя.** Для этого его необходимо подключить к компьютеру и скинуть на него документ с термином «Тест».

Настройка правила хранения



Правило хранения

Тип события Краулер ▾

Место хранения = ▾ Начните вводить текст +

Владельцы файла = ▾ Начните вводить текст +

Кому доступен файл = ▾ Начните вводить текст +

Действия при срабатывании правила

Отправить почтовое уведомление ? ▾ Начните вводить текст +

Назначить событию вердикт ☒ Разрешить

Назначить событию уровень нарушения ☐ Низкий ▾

Назначить событию теги × +

Назначить отправителю статус ▾

Удалить событие ☐

Сохранить

Отменить

Краулер

Редактировать сканер



Crawler

Разделяемые сетевые ресурсы

Дата запуска: 14.04.2020, 21:23:44

Статус: Закончено

Новых файлов: 1

Настройка правила хранения



При настройке правила хранения также обязательно выбрать тип события. После назначить событию вердикт «Разрешить», уровень угрозы «Низкий», тег «Тест». **Для проверки правила хранения необходимо документ с термином «Тест» поместить в папку сканирования Crawler, а после запустить задачу сканирования.**

Настройка правила буфера обмена



Правило на буфер обмена

Персоны = Начните вводить текст +

Компьютеры Начните вводить текст +

Только для терминальной сессии ? ☐

Приложение-источник = Начните вводить текст +

Приложение-приемник = 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 ☒ Разрешить

Назначить событию уровень нарушения ☒ Низкий ▾

Назначить событию теги Тест × +

Назначить отправителю статус Выберите статус ▾

Удалить событие ☐

Сохранить

Отменить

Создание правила


Наименование: Буфер обмена

Перехватчик: Clipboard Monitor ▾

Правило применяется на ОС: Windows

Перехватывать вставку из буфера обмена

☒ В приложения терминальной сессии

☐ В приложения кроме терминальных сессий 

☐ В пределах одного и того же приложения

☐ Создавать снимки экрана при копировании в буфер обмена и вставке из него

☒ Действует всегда

Действует с: ▾ ▾

По: ▾ ▾

Сохранить

Отмена

Настройка правила буфера обмена



Для настройки правила буфера обмена назначить событию вердикт «Разрешить», уровень угрозы «Низкий», тег «Тест». Для корректной работоспособности нужно настроить правило в Device Monitor используя перехватчик Clipboard Monitor.

Для проверки правила буфера обмена достаточно скопировать термин «Тест» в буфер обмена.

События по всем типам правил



	ID: 115, вторник, 14 апреля 2020 21:54:39
Отправители	UserDE
Получатели	Тестовая политика
Политики	Тест ×
Теги	notepad → microsoft word
Приложения	

	ID: 403, вторник, 14 апреля 2020 21:23:45 1
Отправители	UserDE
Получатели	еще 2
Политики	Тестовая политика
Теги	Тест ×
Описание	[Документ Microsoft Word]: \\192.168.1.50\Fold\Тест.docx

	ID: 402, вторник, 14 апреля 2020 21:22:57 1
Отправители	UserDE
Получатели	Generic USB Flash Disk USB Device
Политики	Тестовая политика
Теги	Тест ×
Описание	Загрузка файла: Тест.docx (Документ Microsoft Word).

	ID: 105, вторник, 14 апреля 2020 21:20:36
Отправители	UserDE
Получатели	dlptest.com
Политики	Тестовая политика
Теги	Тест ×
Описание	dlptest.com : отправка сообщения

После проверки всех правил, в раздел «События» придут события по каждому правилу.