

# Объекты защиты. Создание и особенности

Объект защиты — это инструмент для анализа перехваченных данных на наличие в них элементов технологий таких как: текстовый объект, выгрузки из баз данных, эталонный документ и прочие из раздела «Технологии». Применение данного инструмента позволяет гибко настраивать систему на обнаружение определенных документов, используемых в компании.

Раздел «Объекты защиты» состоит из каталогов и действий для работы с ними. Список включает в себя предустановленные и пользовательские каталоги. Каждый из них имеет статус активности (включён/выключен), аналогичный статус и у объектов защиты. При создании нового объекта требуется выбирать элементы технологий и условия обнаружения.



Элементы технологий — элементы, на основе которых будут сформированы объекты защиты.

Условия обнаружения — условия детектирования добавленных элементов технологий. Поддерживаются две операции логическое «И» (конъюнкция) или логическое «ИЛИ» (дизъюнкция).

Для создания объекта защиты выполняются следующие этапы:

- создание каталога объекта защиты;
- создание объекта защиты;
- добавление элементов технологий;
- добавление условий обнаружения.

Рассмотрим каждый этап подробно. Работа с объектами защиты начинается с создания каталога. Для этого необходимо перейти в раздел «Объекты защиты» (*Рисунок 1*) и выбрать знак «+» для создания каталога (*Рисунок 2*).

В появившемся диалоговом окне ввести название, например, «Задание 1» и указать (или оставить по умолчанию) такие атрибуты каталога, как статус и описание. После этого нажать «Создать» (*Рисунок 3*), при необходимости данные параметры можно редактировать (нажать иконку ) или удалить созданный каталог (иконка ).

*Примечание: внутри существующих каталогов можно создать новые каталоги. Любой каталог имеет возможность перемещается по структуре каталогов.*



Рисунок 1 – Раздел «Объекты защиты»

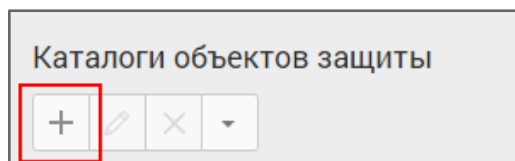


Рисунок 2 – Создание каталога объекта защиты

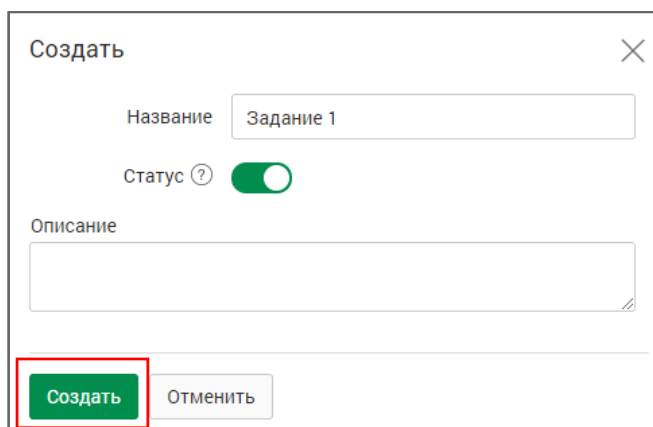


Рисунок 3 – Диалоговое окно создания каталога

Далее из списка каталогов в левой части рабочей области выбираем «Задание 1» (Рисунок 4). Для создания объекта защиты нажимаем «+» в правой части рабочей области (Рисунок 5). Появится окно с выбором технологий, которые будут входить в создаваемый объект (одна технология или несколько). Для примера будут выбраны технологии «Текстовые объекты» и «Графические объекты» (Рисунок 6 - 7). Для перехода к следующему этапу, аналогично предыдущему диалоговому окну, нажимаем кнопку «Создать».

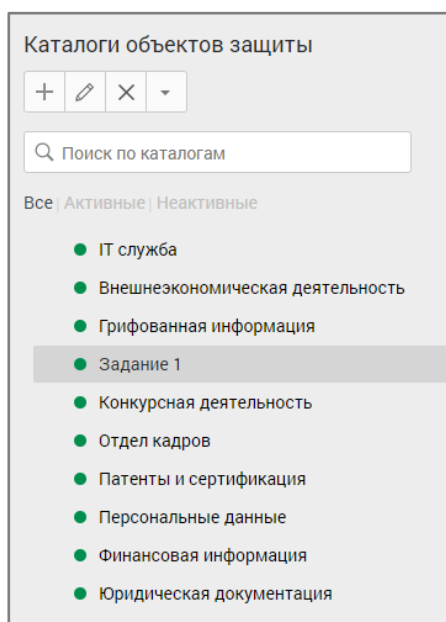


Рисунок 4 – Выбор каталога

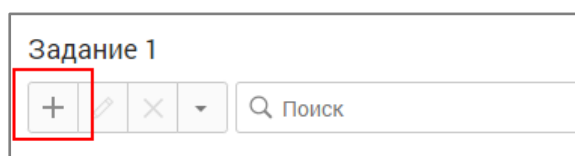


Рисунок 5 – Создание объекта защиты

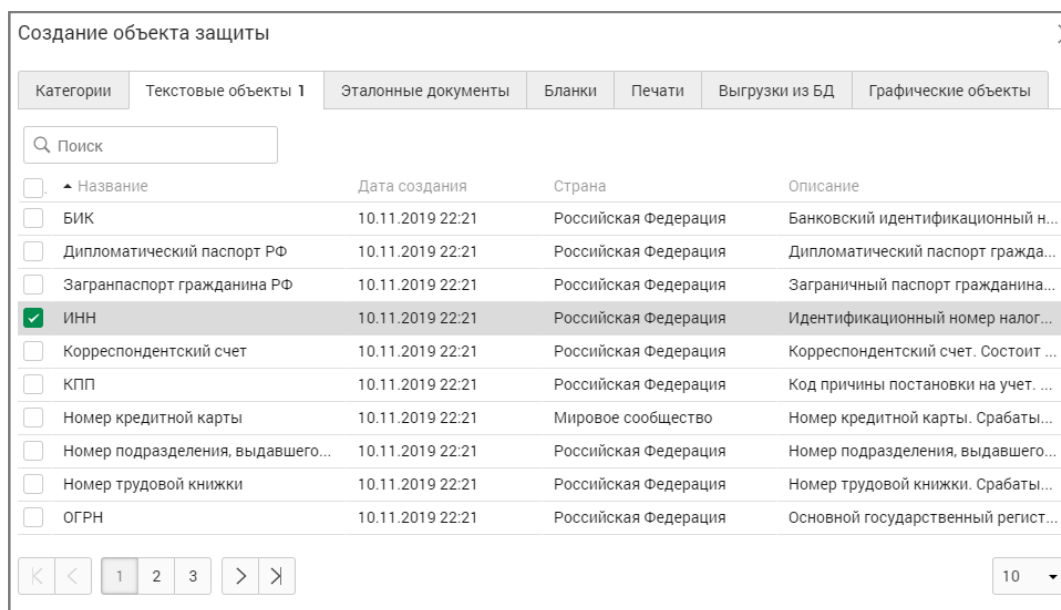


Рисунок 6 – Выбор технологии «Текстовые объекты»

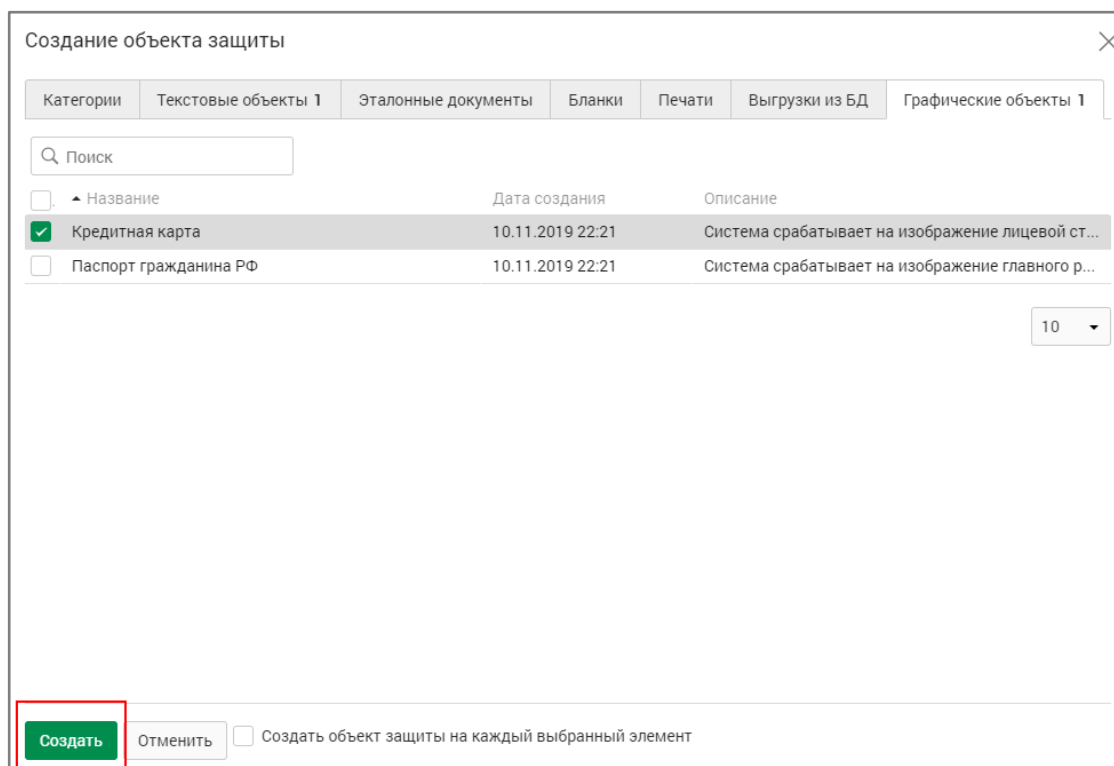


Рисунок 7 – Выбор технологии «Графические объекты»

Следующие диалоговое окно «Создание объекта защиты» позволяет ввести название объекта, на вкладке «Элементы технологий» (Рисунок 8) посмотреть, редактировать или добавить дополнительные элементы технологий и на вкладке «Условия обнаружения» (Рисунок 9) указать условия для детектирования объектов защиты в перехваченных данных. При необходимости заполнить поле с описанием.

На примере с прошлого этапа (Рисунок 6 - 7) видно, что элементы технологий автоматически установились (Рисунок 8). Если список требуется изменить, то каждый элемент имеет возможность удаления и вместо него выбрать новый, нажав кнопку

«**Выбрать элементы**». Для добавления условий обнаружения требуется выбрать элементы технологий из списка (Рисунок 10). Первый элемент выбирается всегда из списка, второй и последующие в зависимости от требуемой операции (И / ИЛИ).

Если необходимо, чтобы условия были объединены с помощью **И**, то второй элемент выбирается из списка, как и первый. Тогда добавленные условия будут помещены в один блок и объединены между собой операцией конъюнкции (Рисунок 11), для удаления одного из элементов нажимается иконка **×**.

Если необходимо, чтобы условия (или их группа) были объединены **ИЛИ**, то нужно нажать кнопку «**Добавить условие**» (Рисунок 12). Тогда будет создан новый блок, внутри которого можно добавлять новые условия.

После этих действий завершается создание объекта защиты, созданный объект появляется в каталоге (Рисунок 13) и готов к дальнейшему применению.

The screenshot shows a dialog box titled "Создание объекта защиты" with a close button (X) in the top right corner. It contains the following elements:

- A text input field labeled "Название" with the value "Задание 1".
- A status indicator labeled "Статус" with a question mark icon and a green toggle switch.
- Two tabs: "Элементы технологий" (active) and "Условия обнаружения".
- A button labeled "Выбрать элементы".
- A list of selected elements, each with a close button (X):
  - "ИНН" with the subtext "Текстовый объект."
  - "Кредитная карта" with the subtext "Графический объект."
- A text area labeled "Описание".
- Two buttons at the bottom: "Создать" (green) and "Отменить".

Рисунок 8 – Вкладка «Элементы технологий»

The screenshot shows the same dialog box, but with the "Условия обнаружения" tab selected. It contains the following elements:

- The "Название" field remains "Задание 1".
- The "Статус" indicator remains the same.
- The "Элементы технологий" tab is now inactive.
- A button labeled "Добавить условие".
- A list of conditions, each with a close button (X):
  - "Условие" with a dropdown menu showing "Добавить элемент технологий".
- The "Описание" text area remains empty.
- The "Создать" and "Отменить" buttons remain at the bottom.

Рисунок 9 – Вкладка «Условия обнаружения»

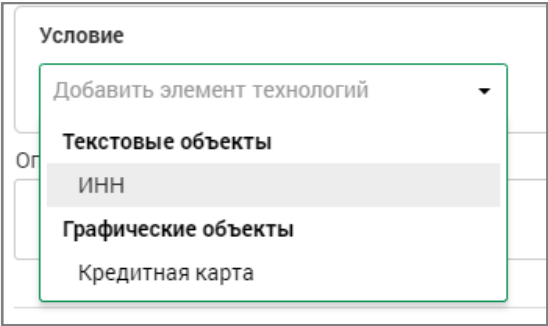


Рисунок 10 – Добавление элемента технологий на вкладке «Условия обнаружения»

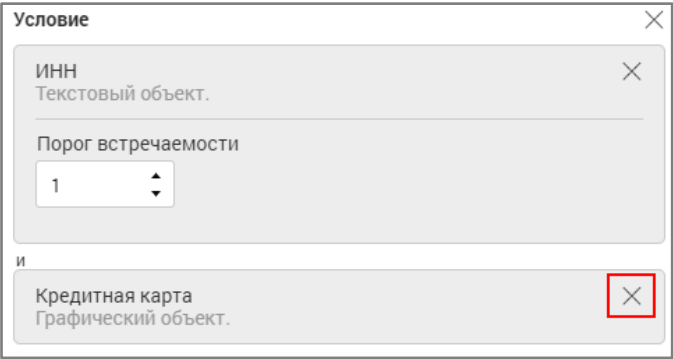


Рисунок 11 – Добавление условия (операция И)

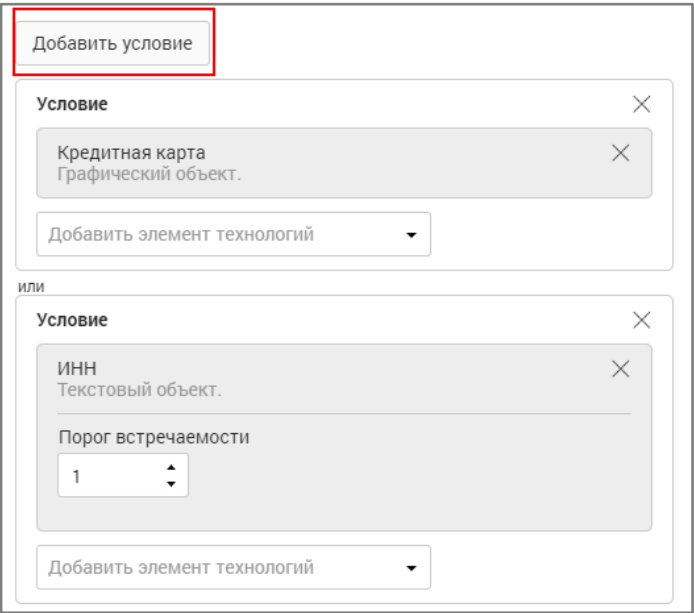


Рисунок 12 – Добавление условия (операция ИЛИ)

Задание 1				
<div><div><div></div><div></div><div></div><div></div></div><div>Поиск</div><div>Все</div></div>				
Название	Элементы технологий	Дата создания	Дата изменения	Описание
Задание 1	ИНН, Кредитная карта	11.11.2019 05:51	11.11.2019 05:51	

Рисунок 13 – Созданный объект защиты «Задание 1»