Sandbox

Настройка источников. Пользовательские параметры проверки

Дата редакции документа: 24.03.2025

Содержание

1. Об этом документе

Документ содержит справочную информацию о действиях, выполняемых для настройки статического и поведенческого анализа в параметрах источников Positive Technologies Sandbox (далее также — PT Sandbox).

Методика адресована специалистам, выполняющим первоначальную настройку и сопровождение PT Sandbox.

2. Параметры пользовательских правил (статический анализ файлов) для предварительной фильтрации

При проверке файлов PT Sandbox выявляет различные свойства файлов и по ряду признаков устанавливает для них метки. С помощью пользовательских правил вы можете указать свойства файлов, по которым PT Sandbox будет относить их к опасным или потенциально опасным объектам. При регистрации каждого источника существует общий базовый набор правил, включенных на определение потенциально опасных объектов для подсветки подозрительного содержимого в прошедших анализ файлах.

Для более тонкой настройки предусмотрена возможность редактирования существующих и добавления собственных правил. Далее приводится методика использования таких правил.

Принцип работы правил следующий: применяются все правила по очереди, вердикт выставляется по высшему уровню опасности: если сработали правила «опасный» и «потенциально опасный», то итоговый уровень опасности объекта — «опасный».

В этом разделе

2.1. Добавление нового правила

Для каждого регистрируемого источника (раздел **Источники**) нужно перейти на вкладку **Параметры проверки**. Здесь рассматриваются действия с блоком параметров **Пользовательские правила определения опасных и потенциально опасных файлов**.

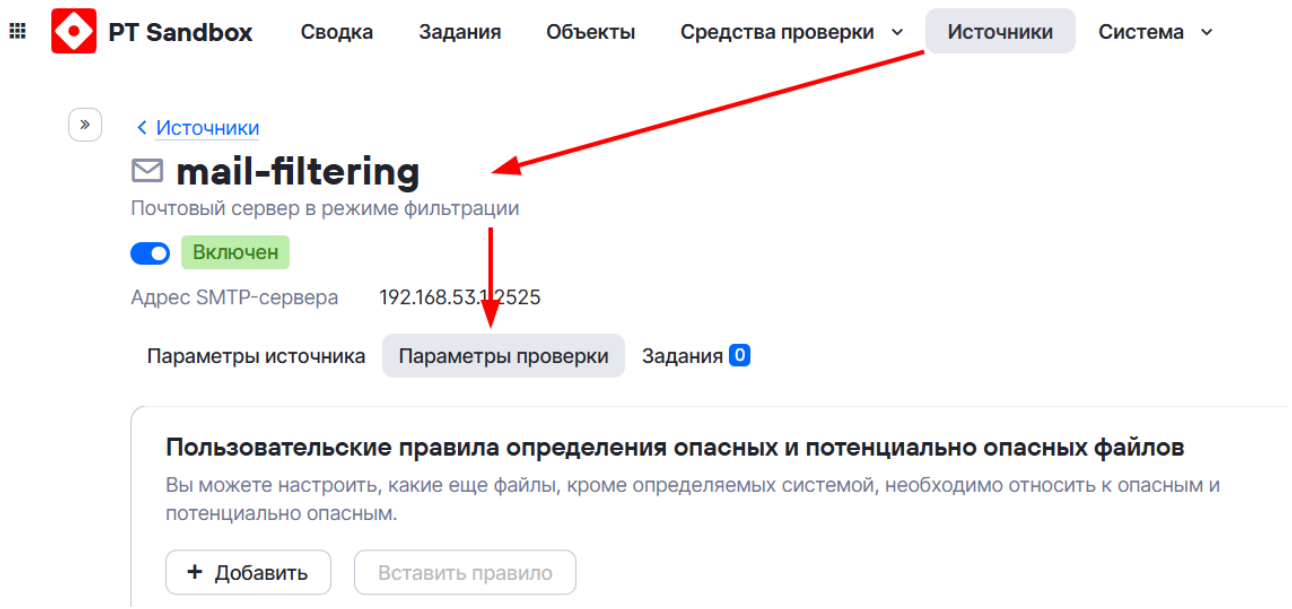

Рисунок 1. Переход на вкладку **Параметры проверки**

После нажатия кнопки **Добавить** задается название правила и его описание. Далее определяется **Назначаемый уровень опасности**. **Опасный** применяется для большинства сценариев блокировок по вердикту, **Потенциально опасный** — для первоначальной проверки работы правила, чтобы не блокировать файлы при ложноположительных срабатываниях.

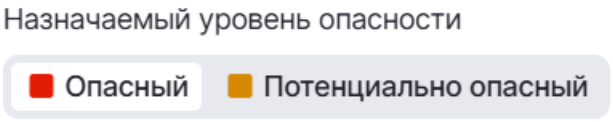

Рисунок 2. Назначаемый уровень опасности

После определения уровня опасности задается блок параметров, которыми определяется, какие файлы **Считать опасными**. Выделено два типа правил относительно наличия у проверяемых файлов обозначенных признаков: правила прямого действия (**Только файлы со всеми указанными признаками**) и правила обратного действия (**Все файлы, кроме файлов с указанными признаками**).

> **Внимание!** В случае правил прямого действия (**Только файлы со всеми указанными признаками**) под правило подпадают файлы, которые удовлетворяют одновременно всем критериям (логическое И). Но под правила обратного действия (**Все файлы, кроме файлов с указанными признаками**) будут подпадать файлы которые НЕ удовлетворяют хотя бы одному из критериев (логическое ИЛИ).

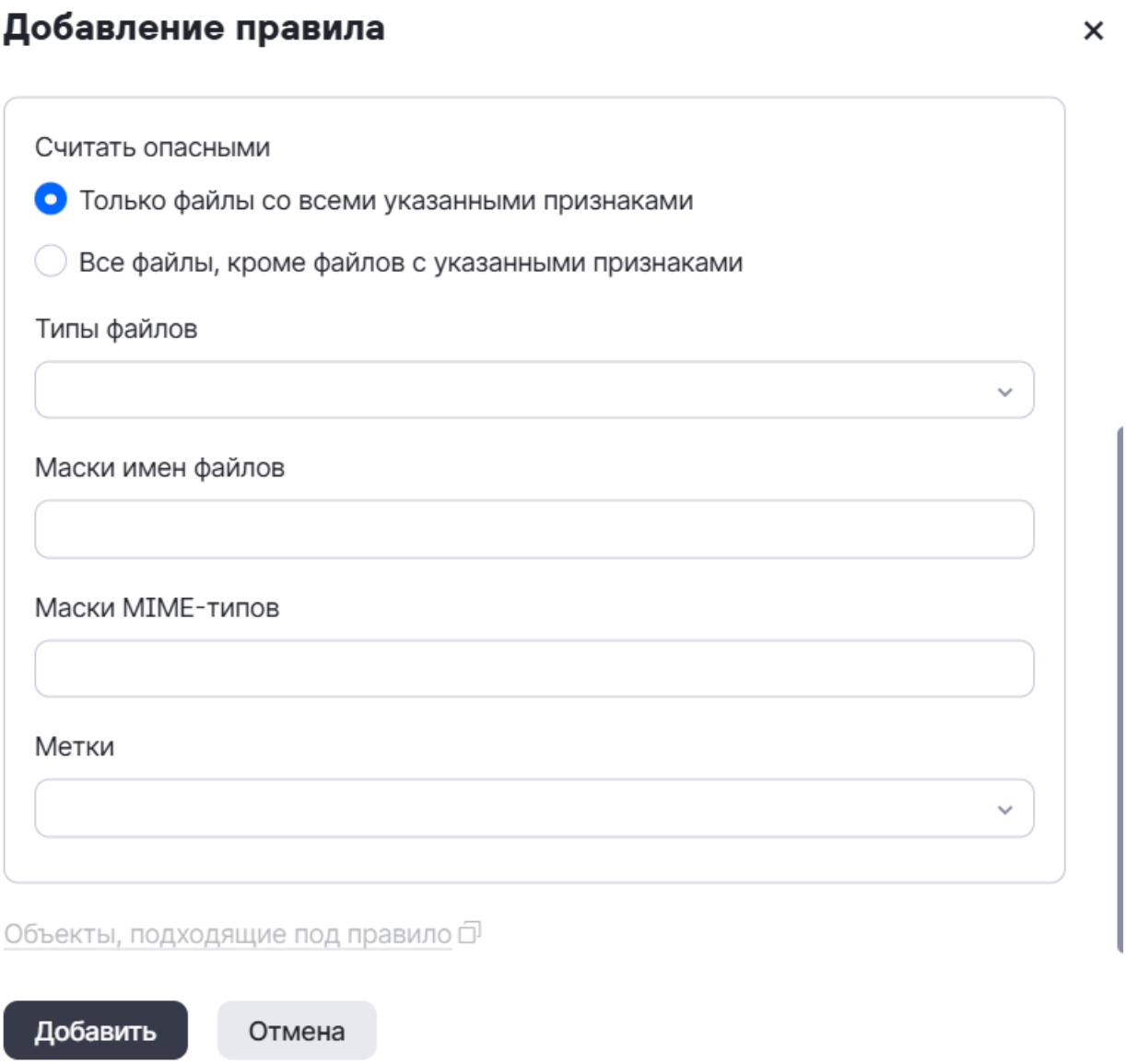

Рисунок 3. Добавление нового правила

Рассмотрим несколько примеров правил с указанием различных критериев.

2.2. Типы файлов

Пример 1: мы хотим отнести к опасным все EXE-файлы, поступающие из почтового источника. Для этого в раскрывающемся списке **Типы файлов** выбираем **EXE**.

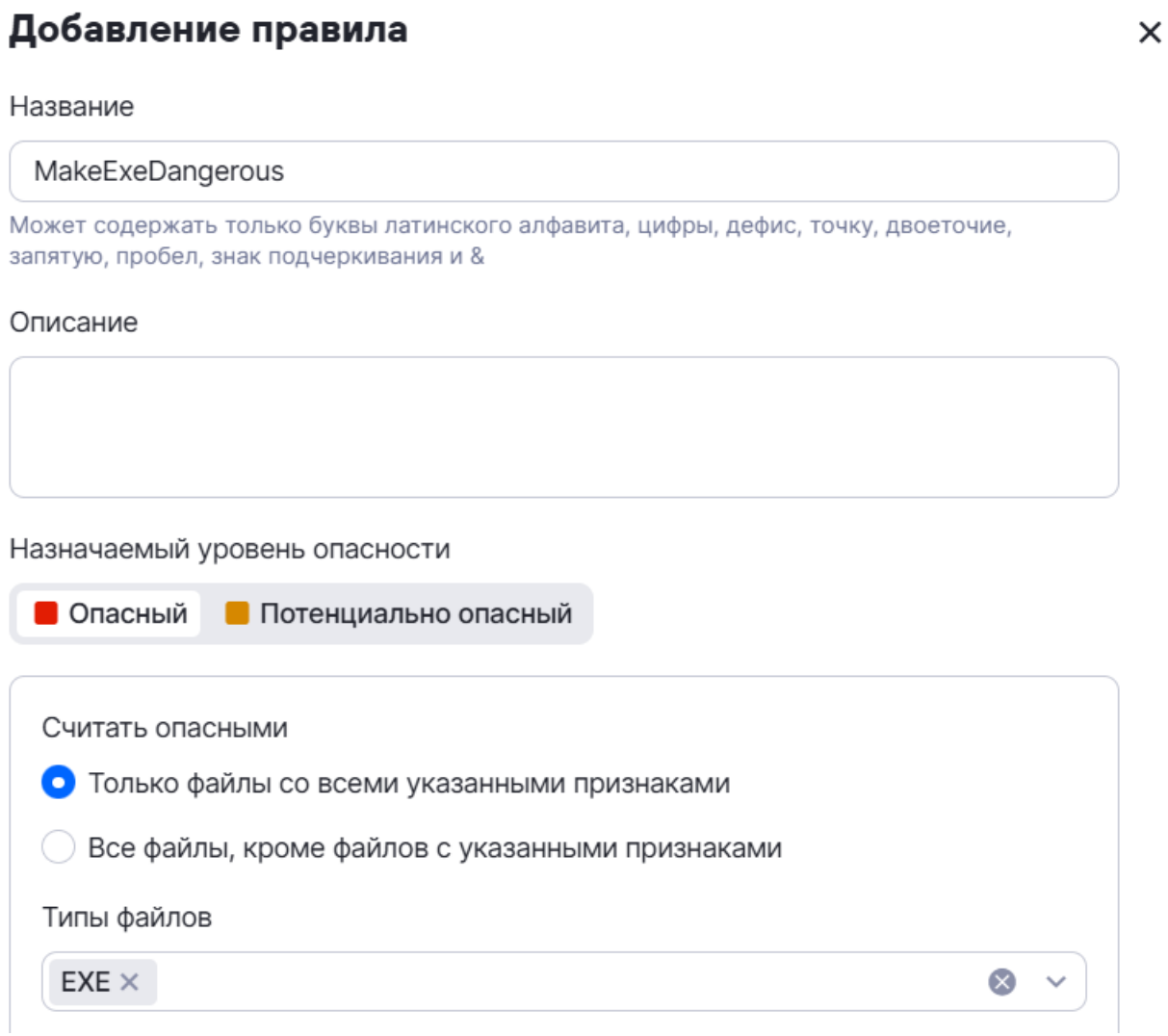

Рисунок 4. Создание правила для EXE-файлов

Пример 2: мы хотим отнести к опасным все файлы, кроме офисных, в нашем почтовом источнике. Для этого в раскрывающемся списке **Типы файлов** выбираем **Файлы офисных приложений**.

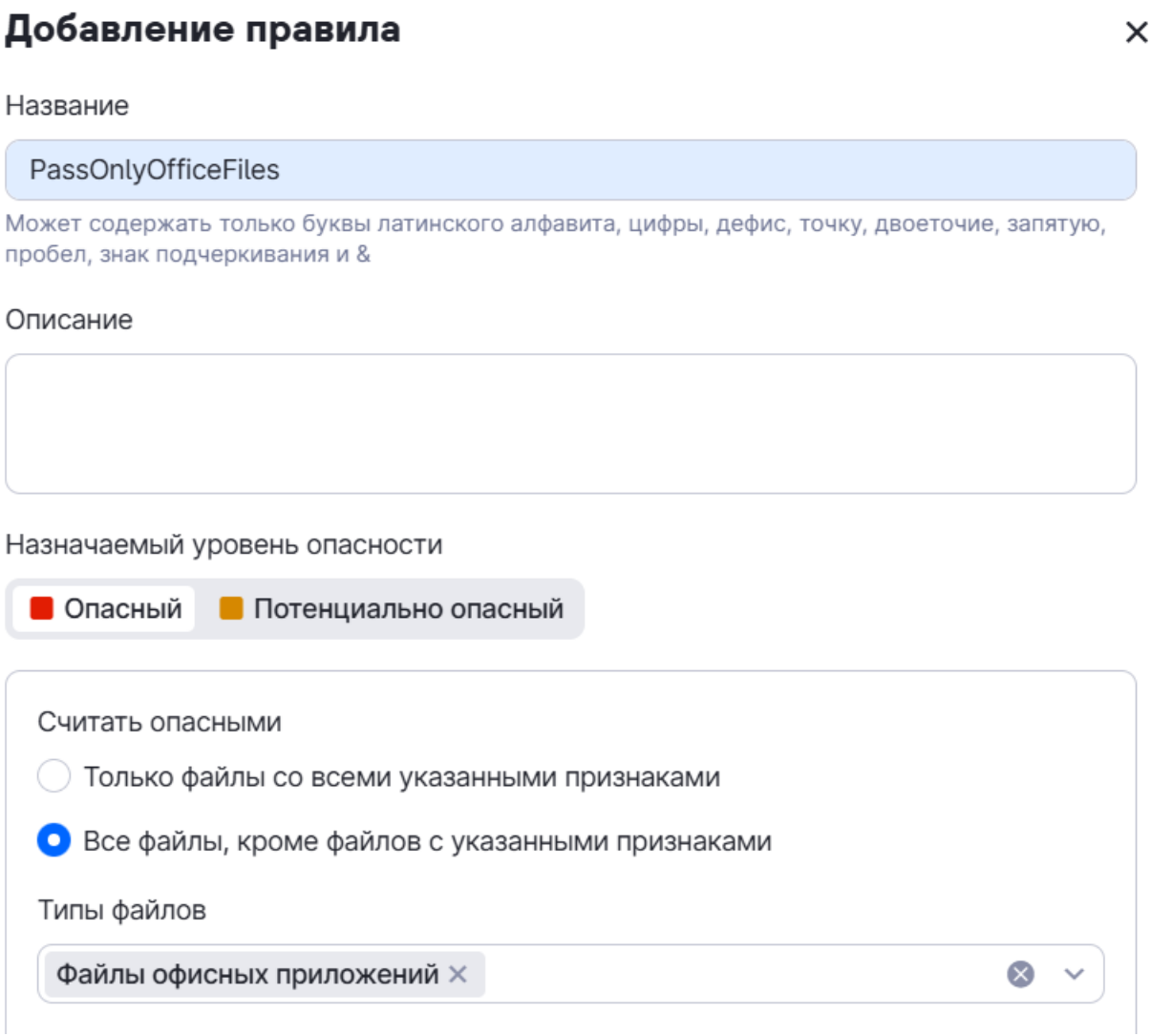

Рисунок 5. Создание правила для файлов офисных приложений

2.3. Маски имен файлов

Пример 3: рассмотрим сценарий, когда мы получаем имена вредоносных файлов из TI-отчета и хотим помечать их в качестве опасных.

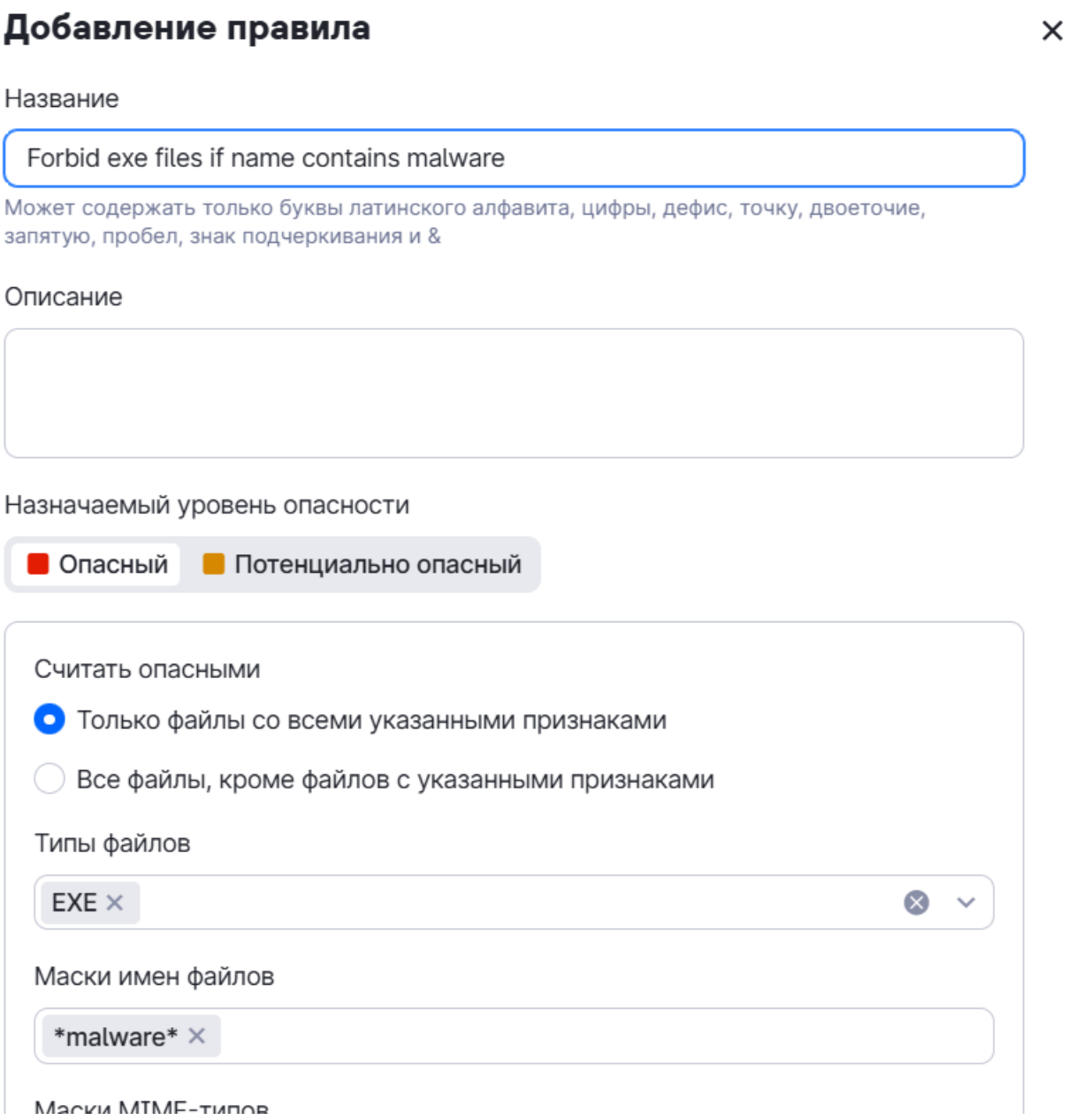

Рисунок 6. Создание правила для имен вредоносных файлов

Пример 4: отмечаем опасными все файлы, кроме тех исполняемых файлов, которые приходят нам с соответствующей пометкой от системы передачи файлов, — или кроме тех, которые содержат определенный постфикс в названии файла.

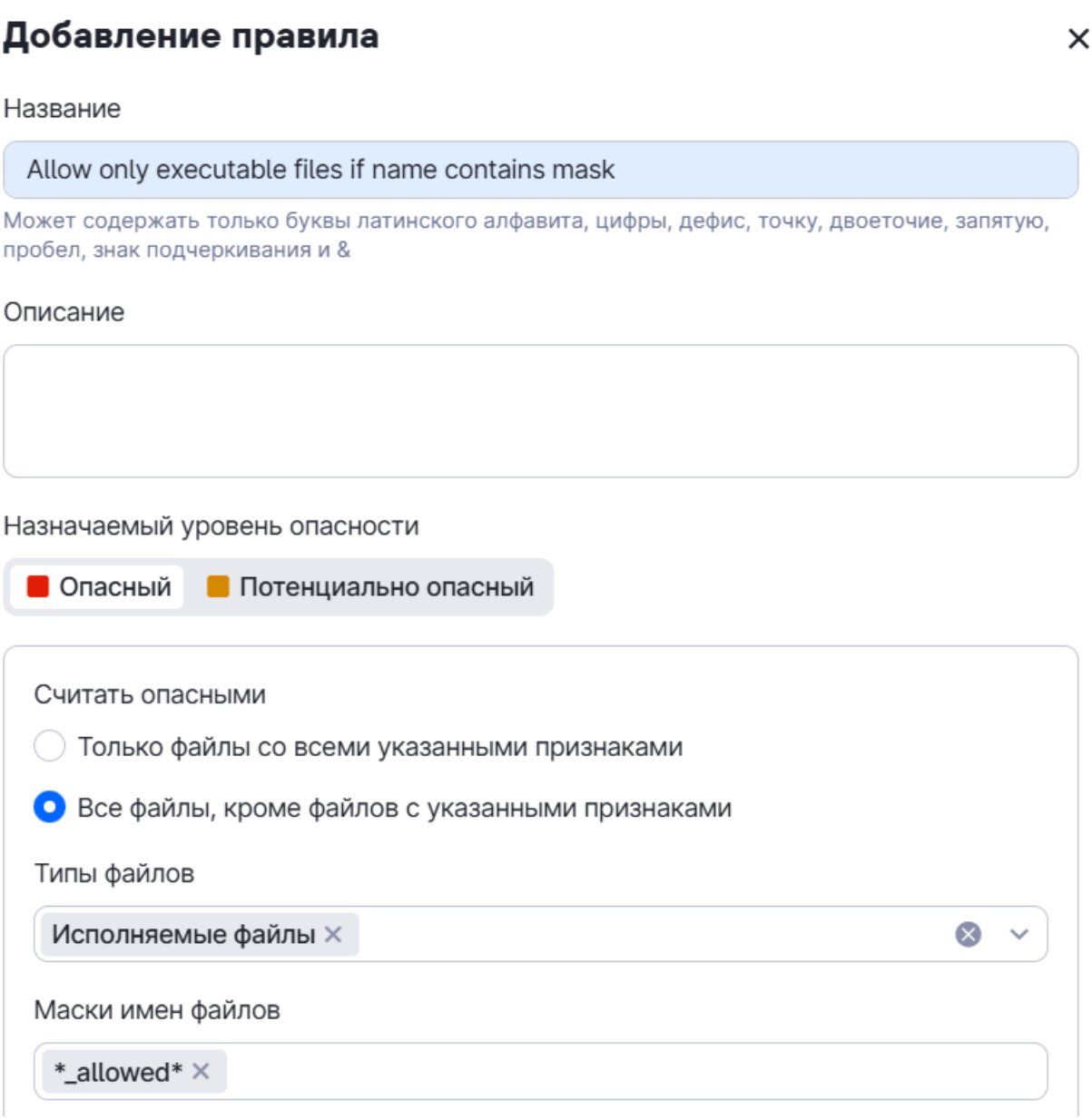

Рисунок 7. Создание правила для файлов с определенным постфиксом в названии

2.4. Маски MIME-типов

Пример 5: запрет по маске MIME-типа (обратите внимание на звездочку в конце: для работы маски она необходима).

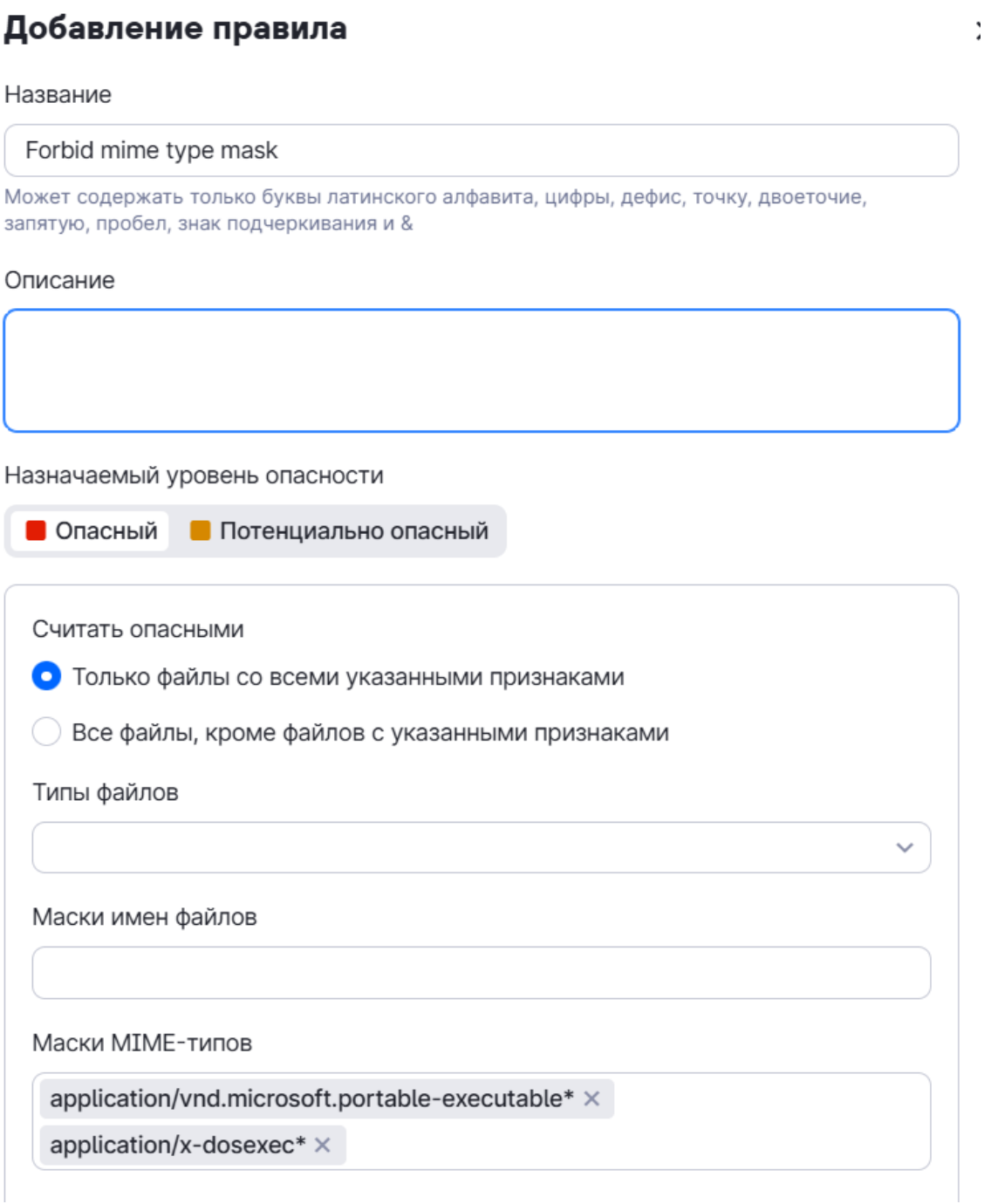

Рисунок 8. Создание правила с запретом по маске MIME-типа

Также маски MIME-типов могут быть полезны, когда нужно запретить (разрешить) подмножество форматов файлов, например определенные стандарты PDF-файлов, а не весь тип. И еще более важной может быть необходимость запретить (разрешить) файлы тех форматов, для которых нет определяемого типа файла.

2.5. Метки файлов

Перед тем как выполнять следующие шаги, обязательно ознакомьтесь с перечнем определяемых PT Sandbox меток объектов, который приведен в Справке специалиста по безопасности.

Последний критерий — **Метки**. В общем случае можно воспользоваться исходными правилами с метками, которые установлены по умолчанию.

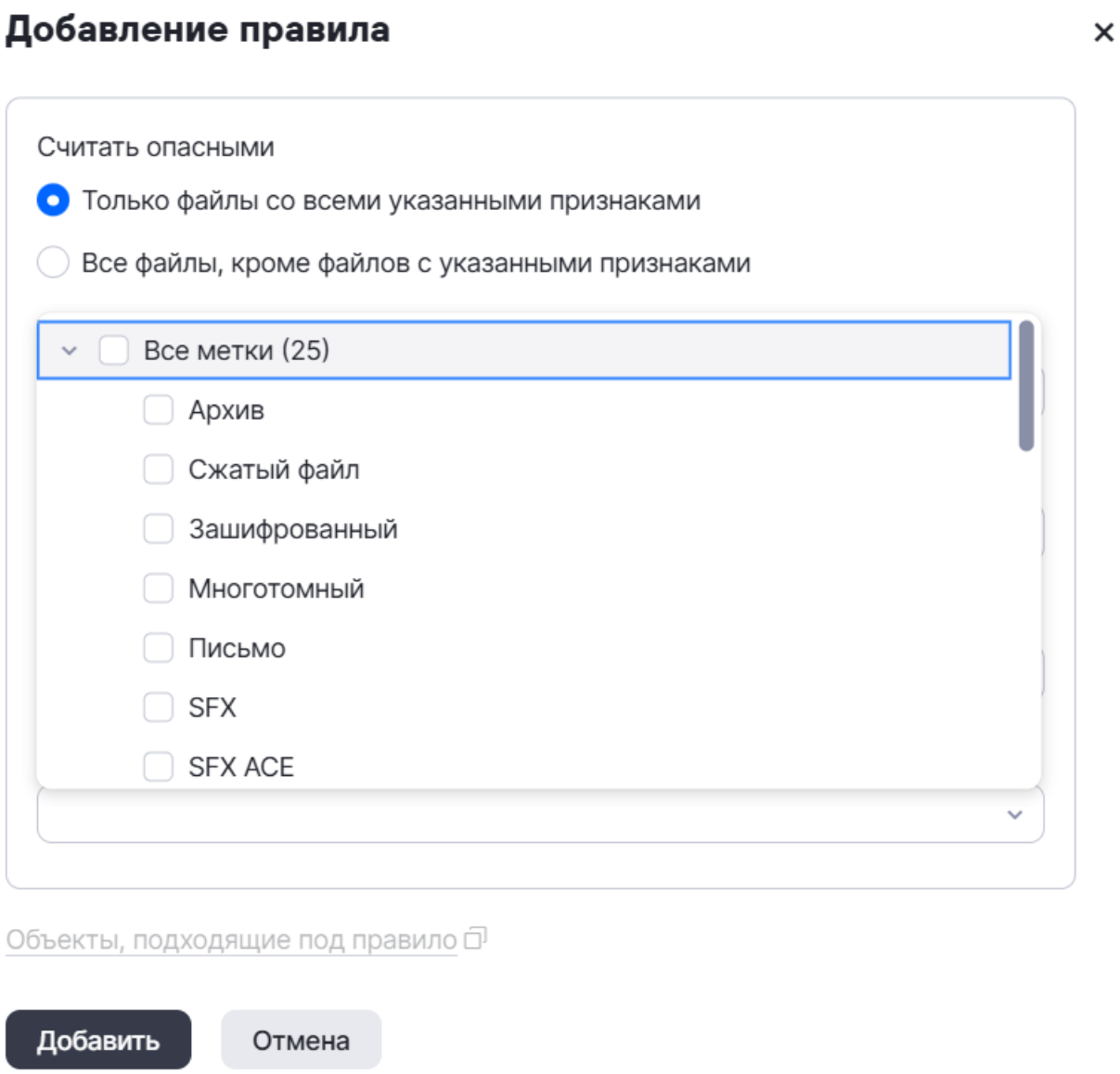

Рисунок 9. Список исходных правил с метками

Примерами здесь служат наборы базовых правил: PDF с Action (действиями), PDF со встроенными объектами (OLE), PDF с JavaScript-кодом, PDF с OpenAction (действия при открытии файла).

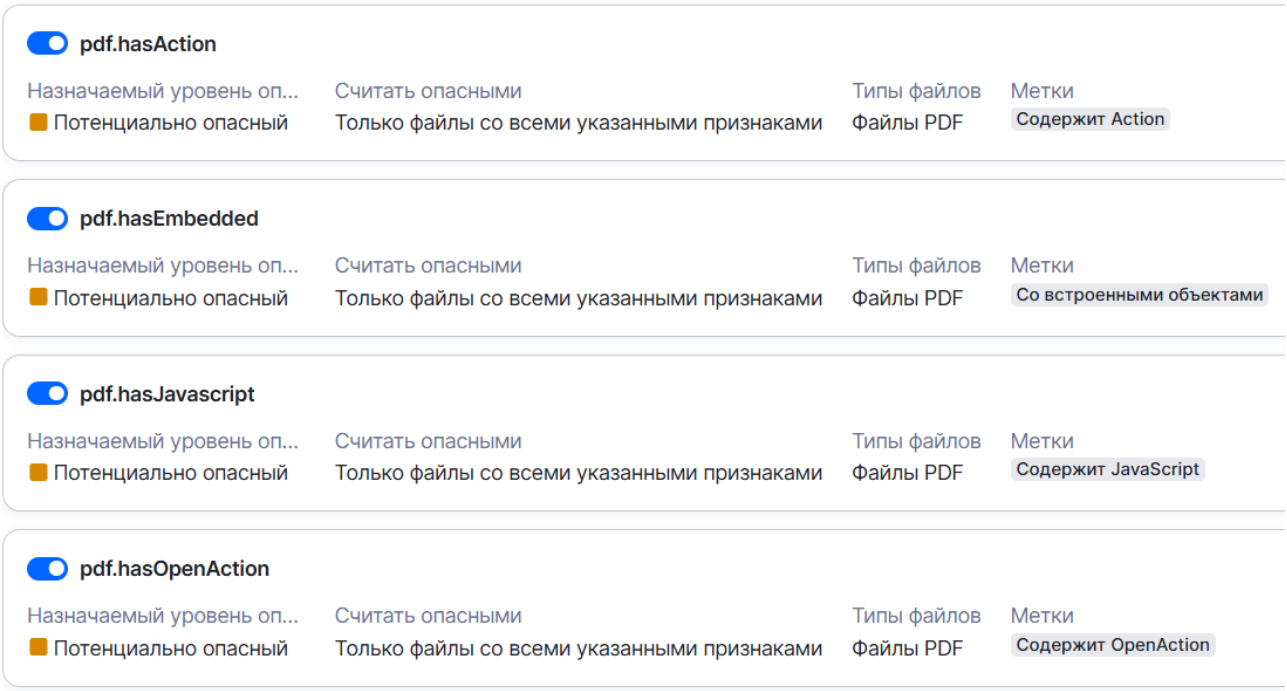

Рисунок 10. Наборы базовых правил

После применения созданных наборов правил следует какое-то время пронаблюдать за их работой и регулярно отслеживать их актуальность и применимость.

При наличии настроенного набора правил можем перейти к использованию опции **Прекращать проверку для всего задания** — в зависимости от красного («опасный») или желтого («потенциально опасный») вердикта. Включение этих опций позволяет экономить производительность системы путем остановки проверки на этапе статического анализа. По умолчанию обе опции выключены. Рассмотрим случаи, когда нужно их включение.

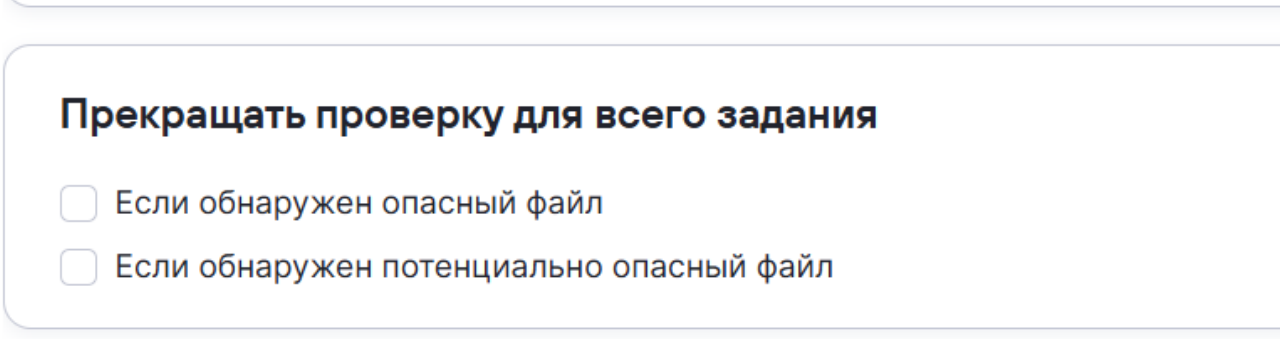

Рисунок 11. Опции прекращения проверки для всего задания

Первый вариант **Если обнаружен опасный файл** может быть отключен в случаях, когда требуется исследовать образцы с источника подробно, даже если уже обнаружен опасный файл (например, для тестирования работы PT Sandbox). В остальных случаях — включаем.

Второй вариант **Если обнаружен потенциально опасный файл** может быть включен, если есть потребность блокировать задания даже в случае нахождения потенциально опасных файлов.

Если правила статического анализа на этом этапе проверки срабатывают, то поведенческий анализ не запускается.

Далее переходим к пользовательским правилам поведенческого анализа.

3. Параметры пользовательских правил (поведенческий анализ файлов)

В этом блоке выполняется настройка основного инструмента из набора экспертизы PT Sandbox — включение обработки и определение параметров проверки файлов на выбранных образах операционных систем.

В этом разделе

3.1. Создание правила для исполняемых файлов Windows

Начальное разделение параметров запуска — по семействам операционных систем (Windows и GNU/Linux). Для этого опираемся на наиболее распространенные в инфраструктуре ОС и включаем в PT Sandbox поддерживаемые, список которых можно найти в Справке оператора безопасности.

В качестве первого примера набора правил рассмотрим настройку для семейства Windows, из которого выберем образ Windows 10-1803.

Первым настроим правило проверки на следующие **Типы проверяемых файлов**: исполняемые (приложения и системные) файлы.

Продолжительность наблюдения за файлом — 4 минуты (в принципе это значение можно увеличивать или уменьшать в зависимости от имеющихся аппаратных ресурсов, объема файлов и скорости их передачи). Если опираться на то, что мы настраиваем проверку почтового типа источника, то исполняемых файлов должно будет быть меньше, чем документов, и много ресурса проверки они не займут.

Расшифровывать и анализировать HTTPS-трафик в данном случае рекомендуется, чтобы сетевые правила могли отловить вредоносную активность в зашифрованном трафике.

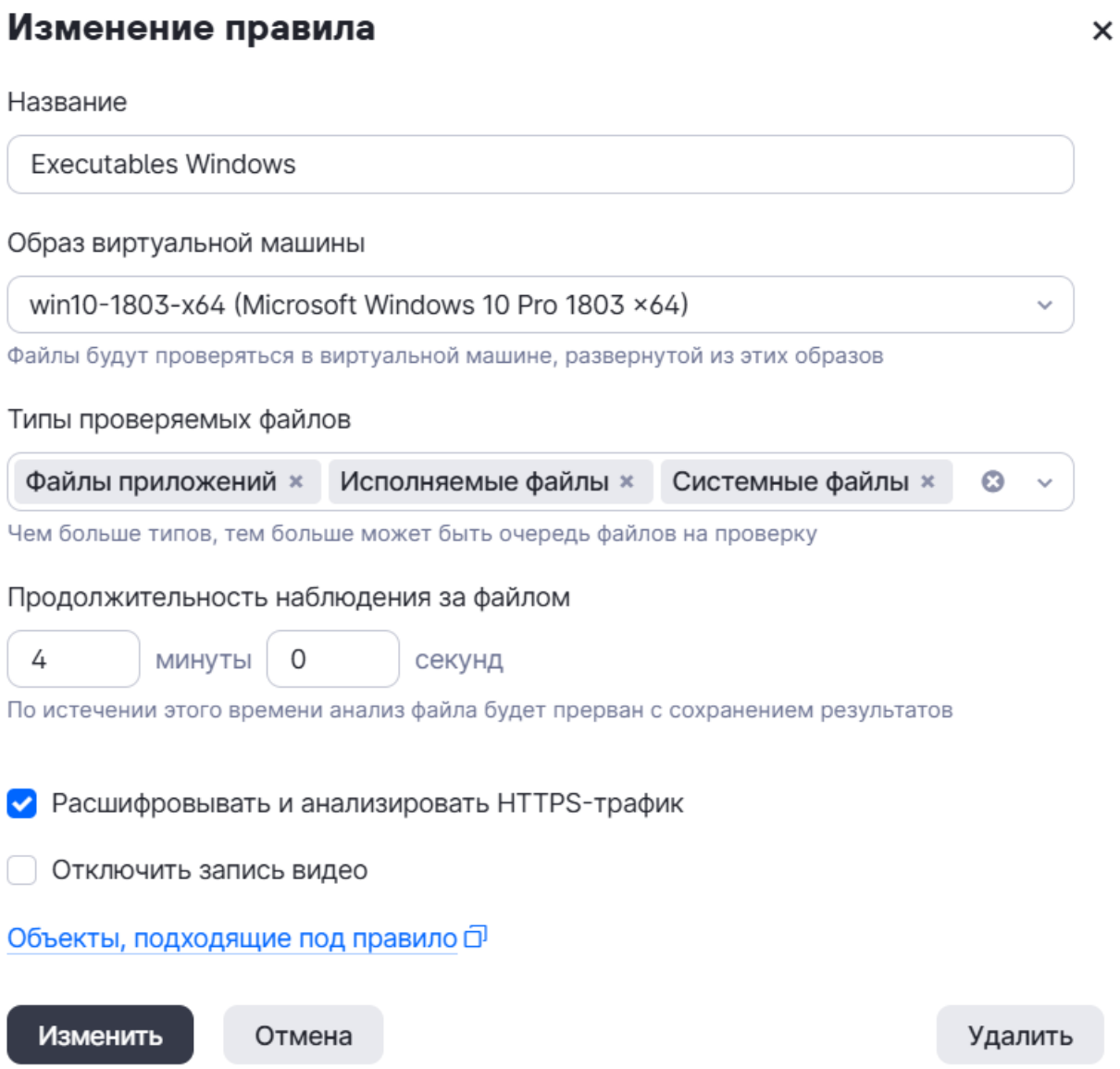

Рисунок 12. Создание правила для исполняемых файлов Windows

3.2. Создание правила для офисных файлов, Windows

Вторым настроим правило проверки на следующие **Типы проверяемых файлов**: файлы, которые обычно открываются офисным пакетом ПО.

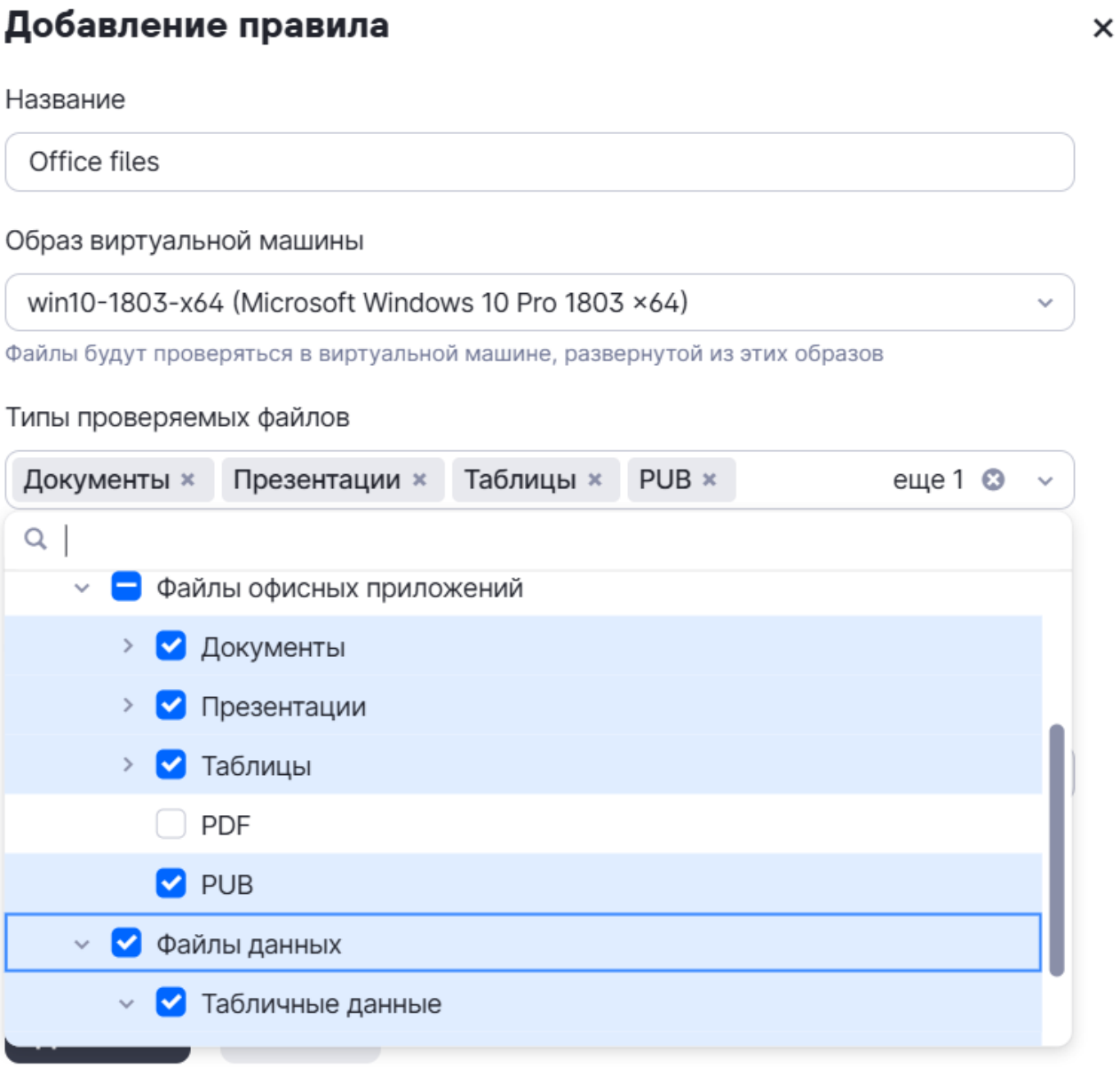

Рисунок 13. Создание правила для офисных файлов, Windows

Для этих файлов далее обратим внимание на определенные песочницей **Метки**.

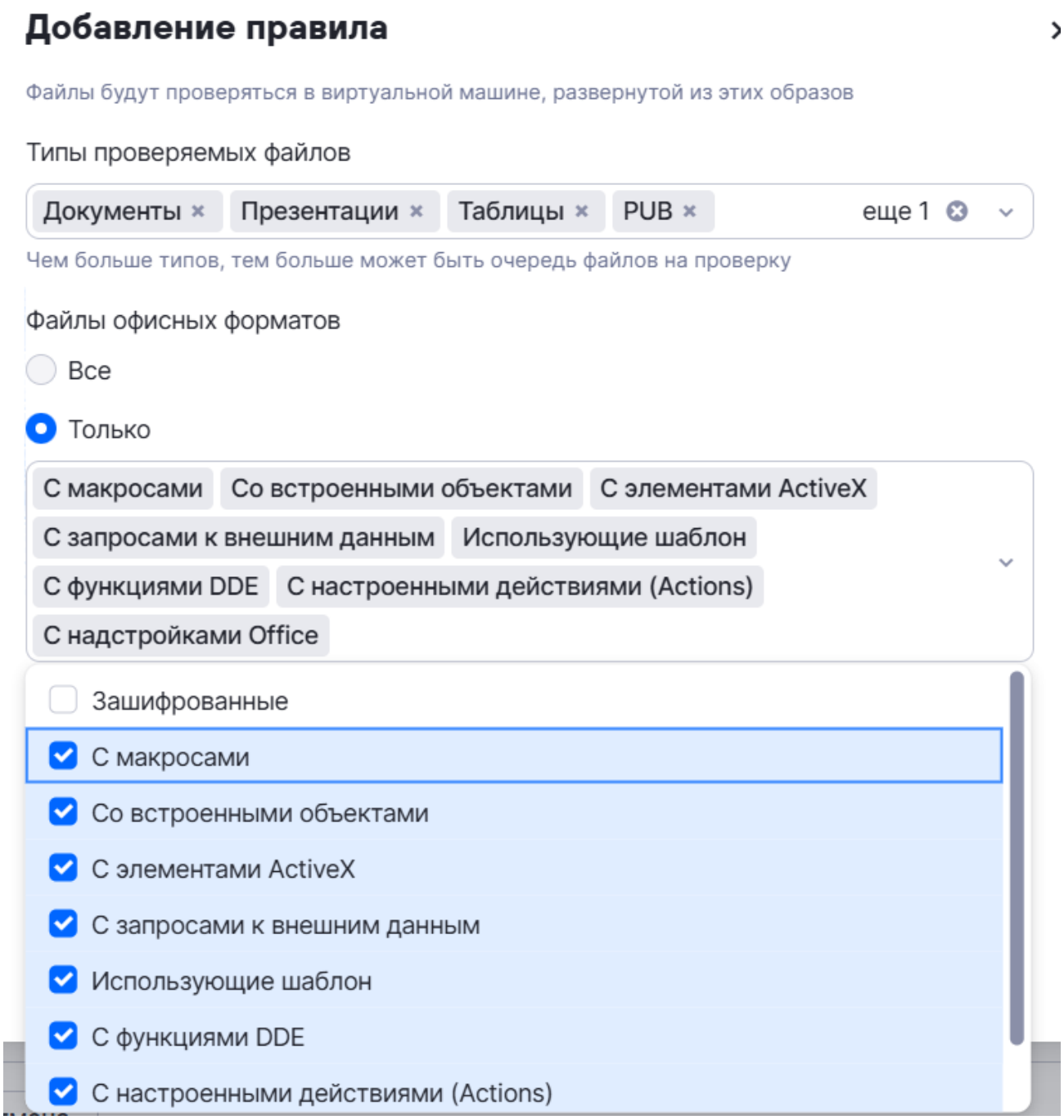

Рисунок 14. Добавление меток

Как правило, в поведенческом анализе есть смысл запускать файлы, метки в которых указывают на наличие активного содержимого. Это практически весь список, кроме метки **Зашифрованные**. Запуск файлов с такой меткой остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. **Продолжительность наблюдения за файлом**: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 3 минуты.

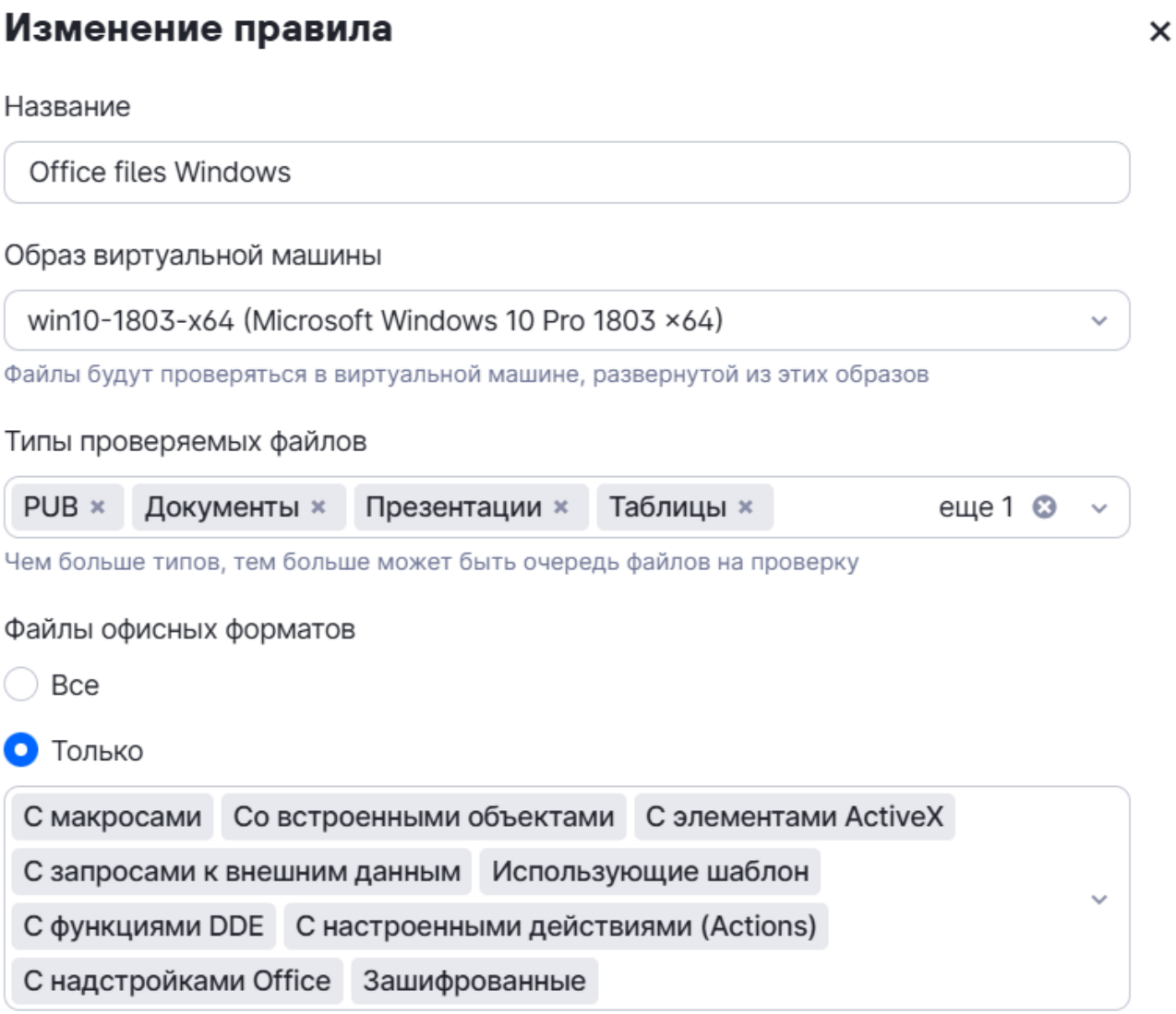

Рисунок 15. Выбор продолжительности наблюдения за файлом

3.3. Создание правила для PDF-файлов, Windows

Третье правило — по оставшемуся типу PDF.

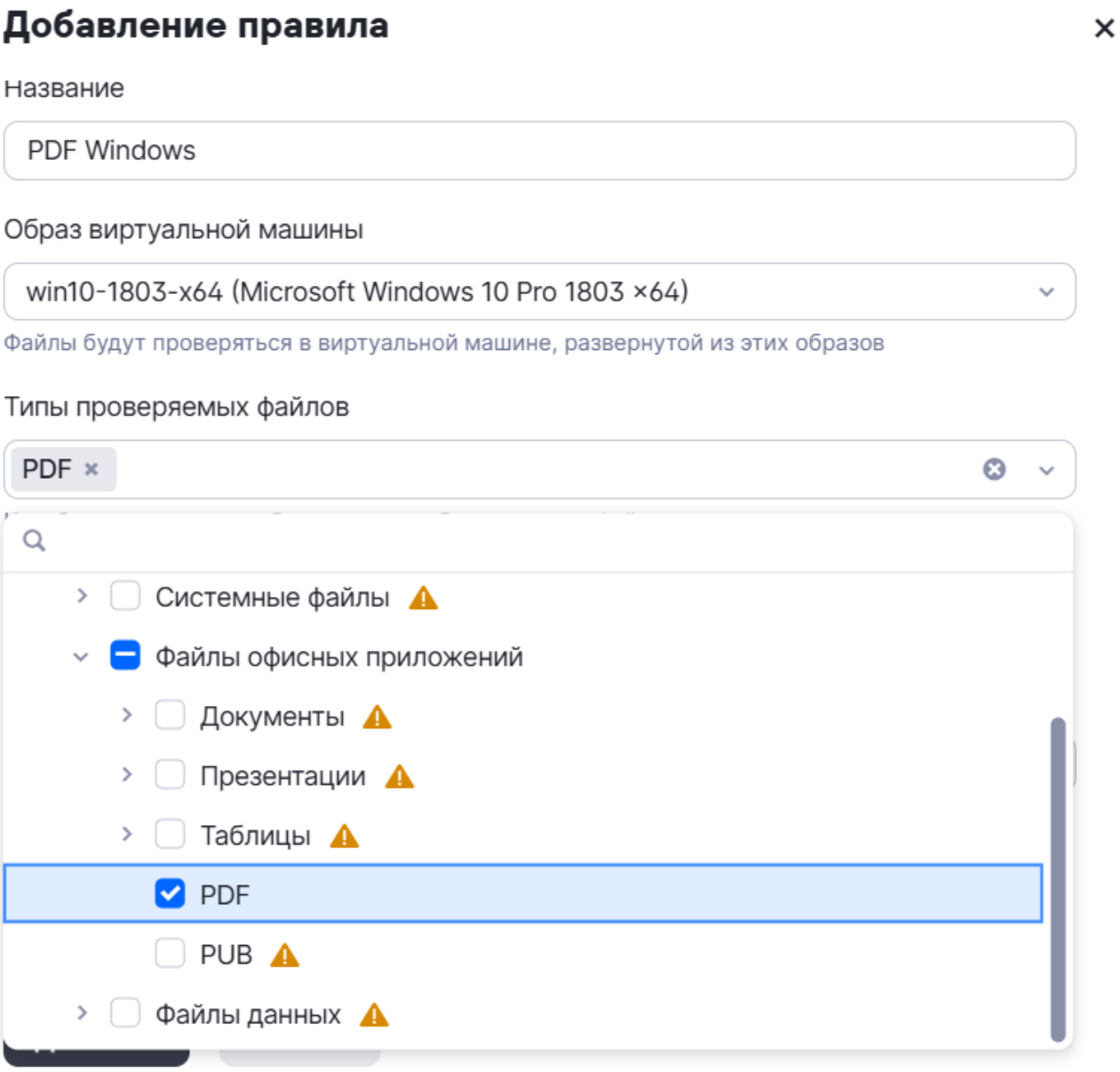

Рисунок 16. Создание правила для PDF-файлов, Windows

Для этих файлов далее также обратим внимание на определенные песочницей **Метки**.

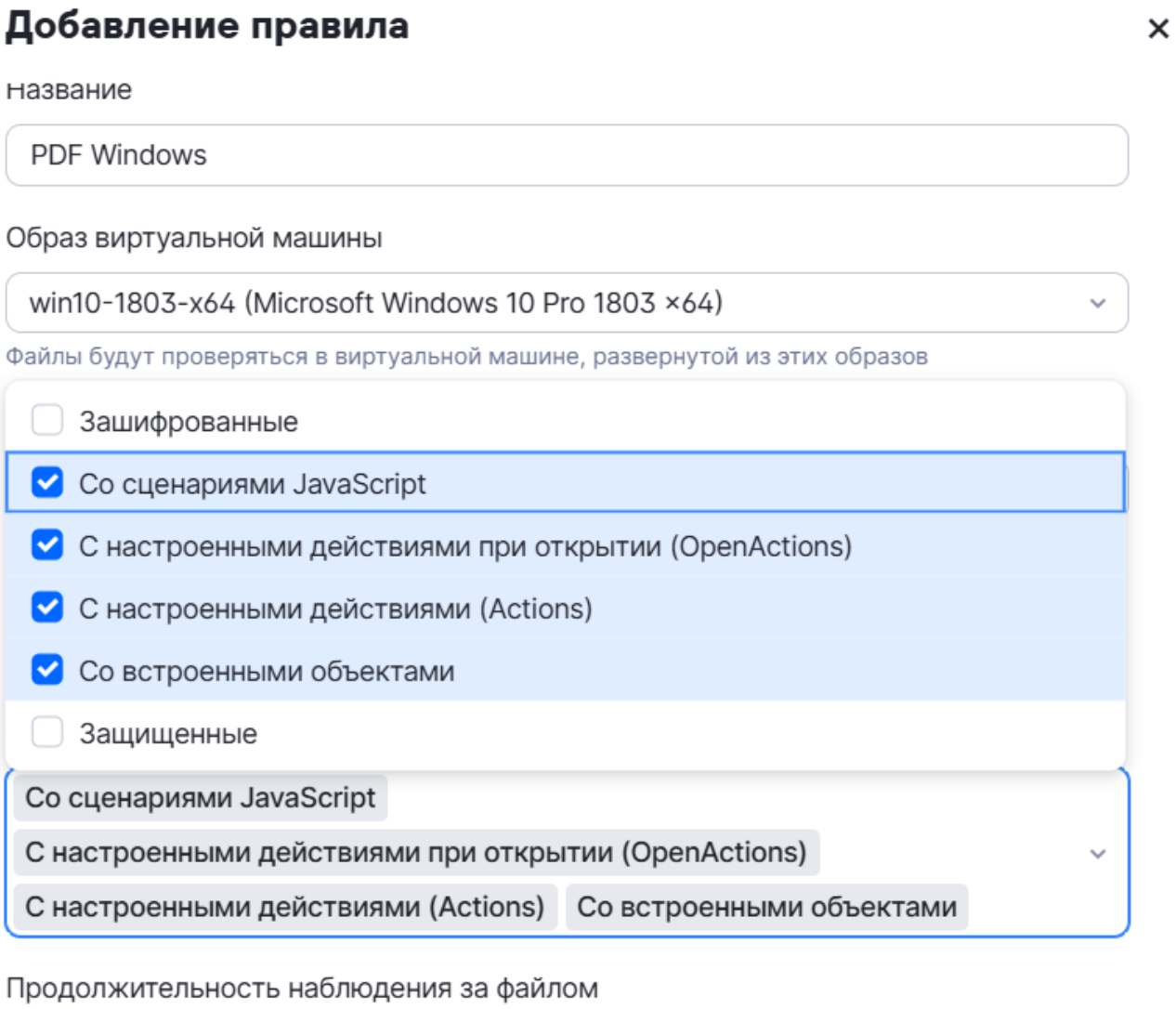

Рисунок 17. Добавление меток

Отмечаем в раскрывающемся списке все, кроме меток **Зашифрованные** и **Защищенные**. Запуск файлов с такими метками остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. Продолжительность: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 2 минуты.

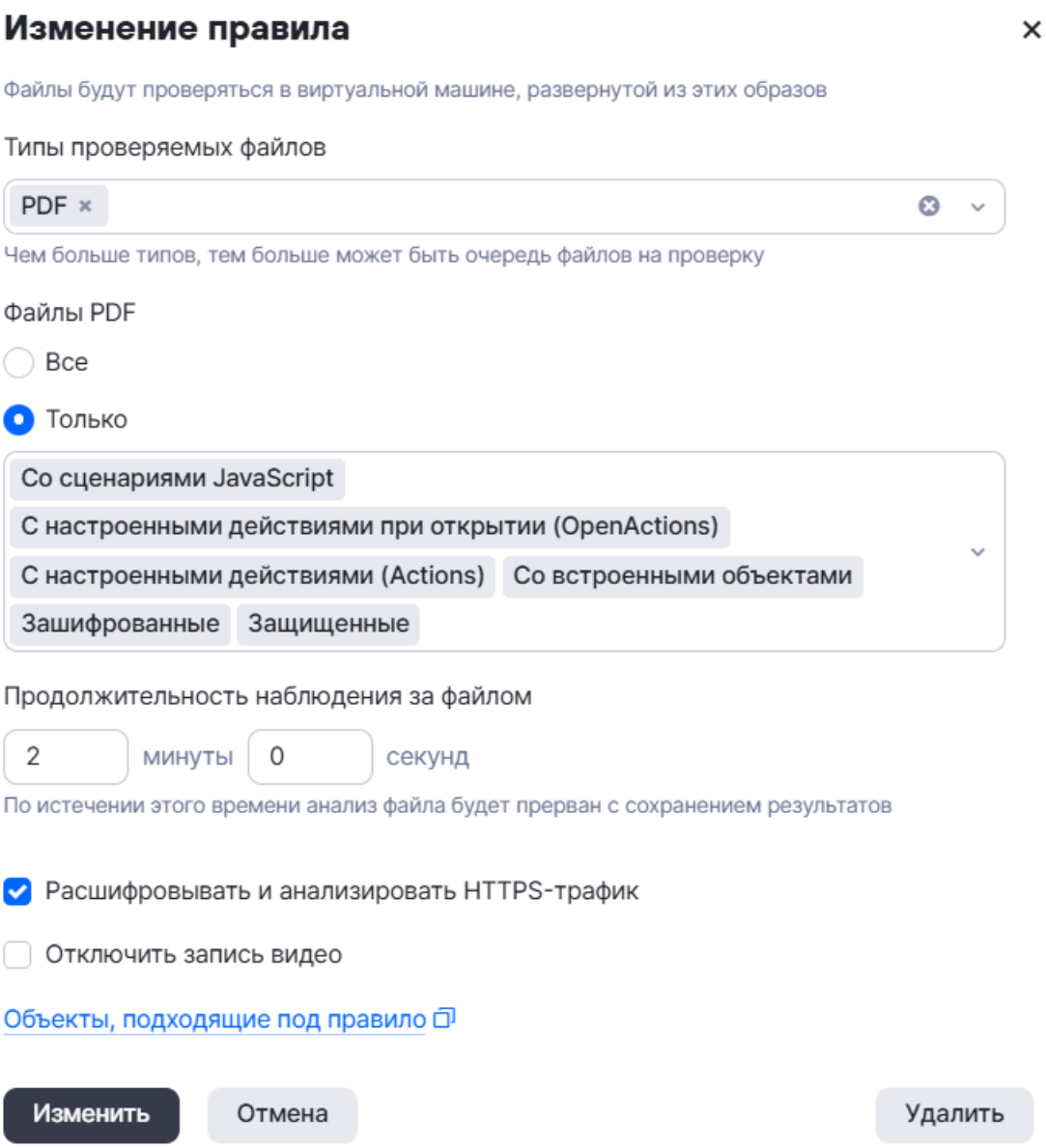

Рисунок 18. Выбор продолжительности наблюдения за файлом

Как результат, для проверок в поведенческом анализе на Windows получаем следующий набор правил.

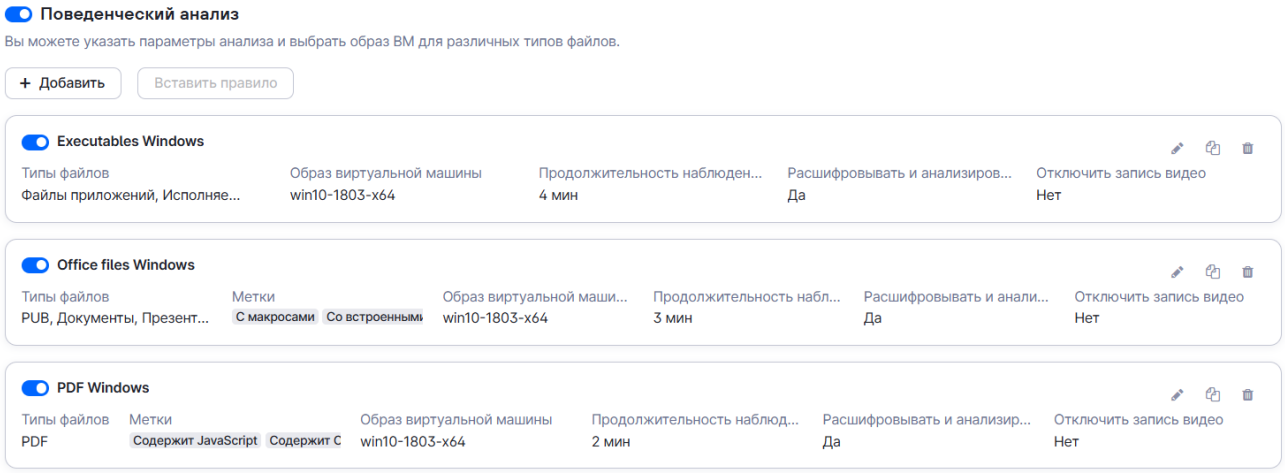

Рисунок 19. Набор правил для проверок в поведенческом анализе

3.4. Создание правила для исполняемых файлов, Linux

В качестве второго примера набора правил рассмотрим настройку для семейства GNU\Linux, из которого выберем образ Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64. Здесь обратим внимание, что в семействе GNU\Linux могут быть отличия типов анализируемых установочных пакетов в зависимости от базы дистрибутива (RPM или Debian).

Первым настроим правило проверки на следующие **Типы проверяемых файлов**: исполняемые (приложения и системные) файлы.

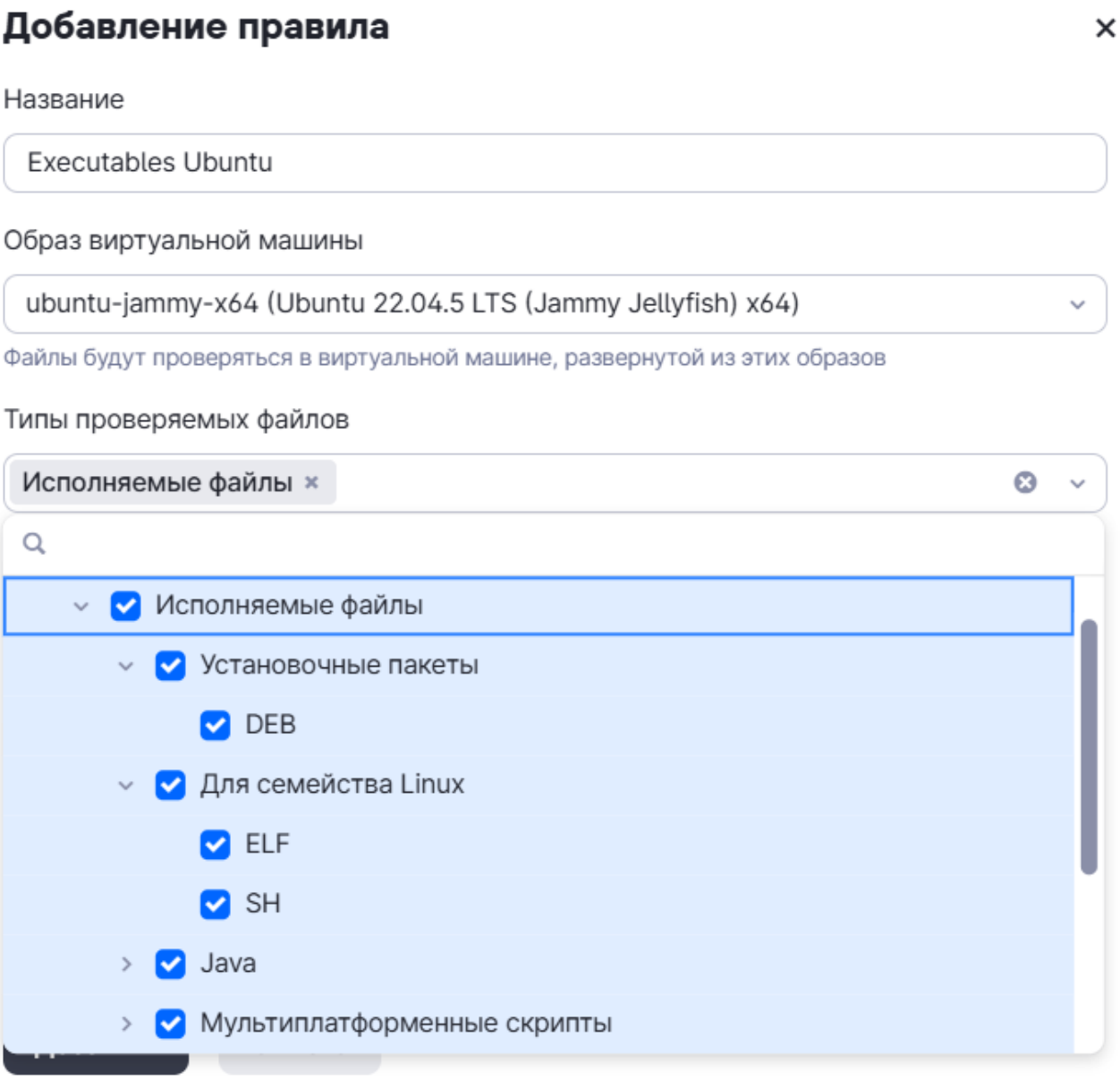

Рисунок 20. Создание правила для исполняемых файлов, Linux

Продолжительность наблюдения за файлом — 4 минуты.

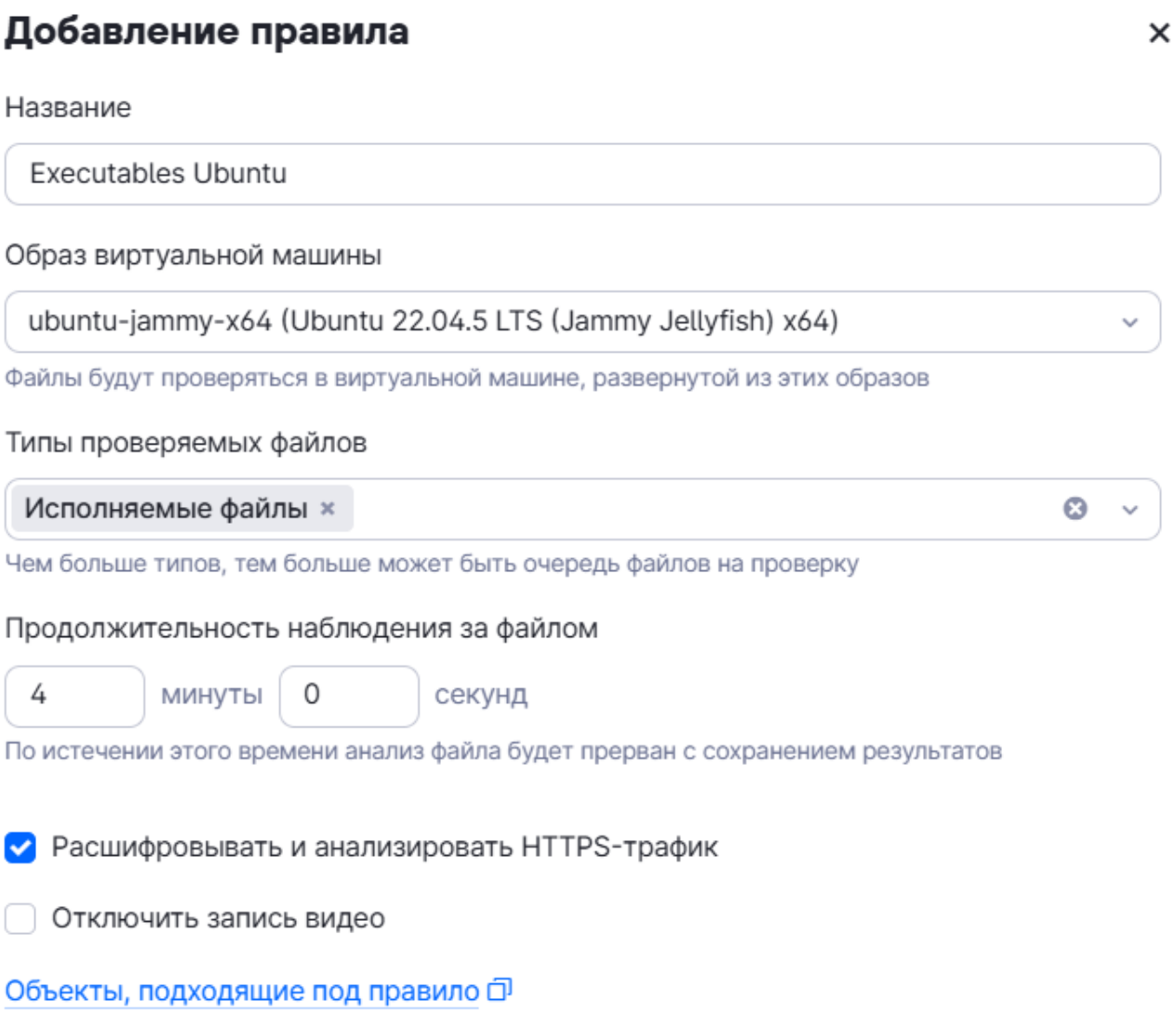

Рисунок 21. Выбор продолжительности наблюдения за файлом

3.5.Создание правила для офисных приложений, Linux

Вторым настроим правило для файлов офисных приложений.

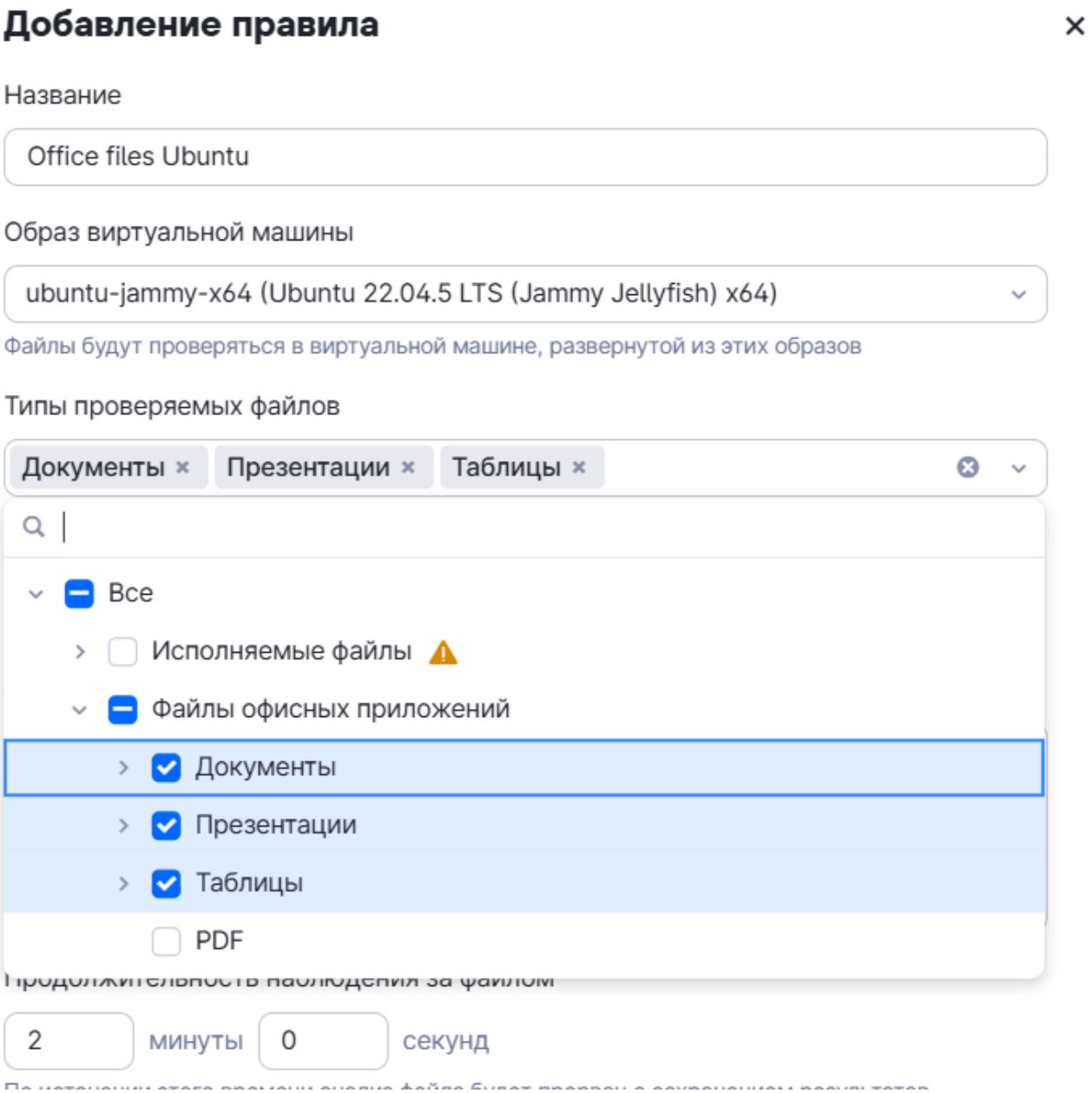

Рисунок 22. Создание правила для офисных приложений, Linux

Для этих файлов обратим внимание на определенные песочницей **Метки**.

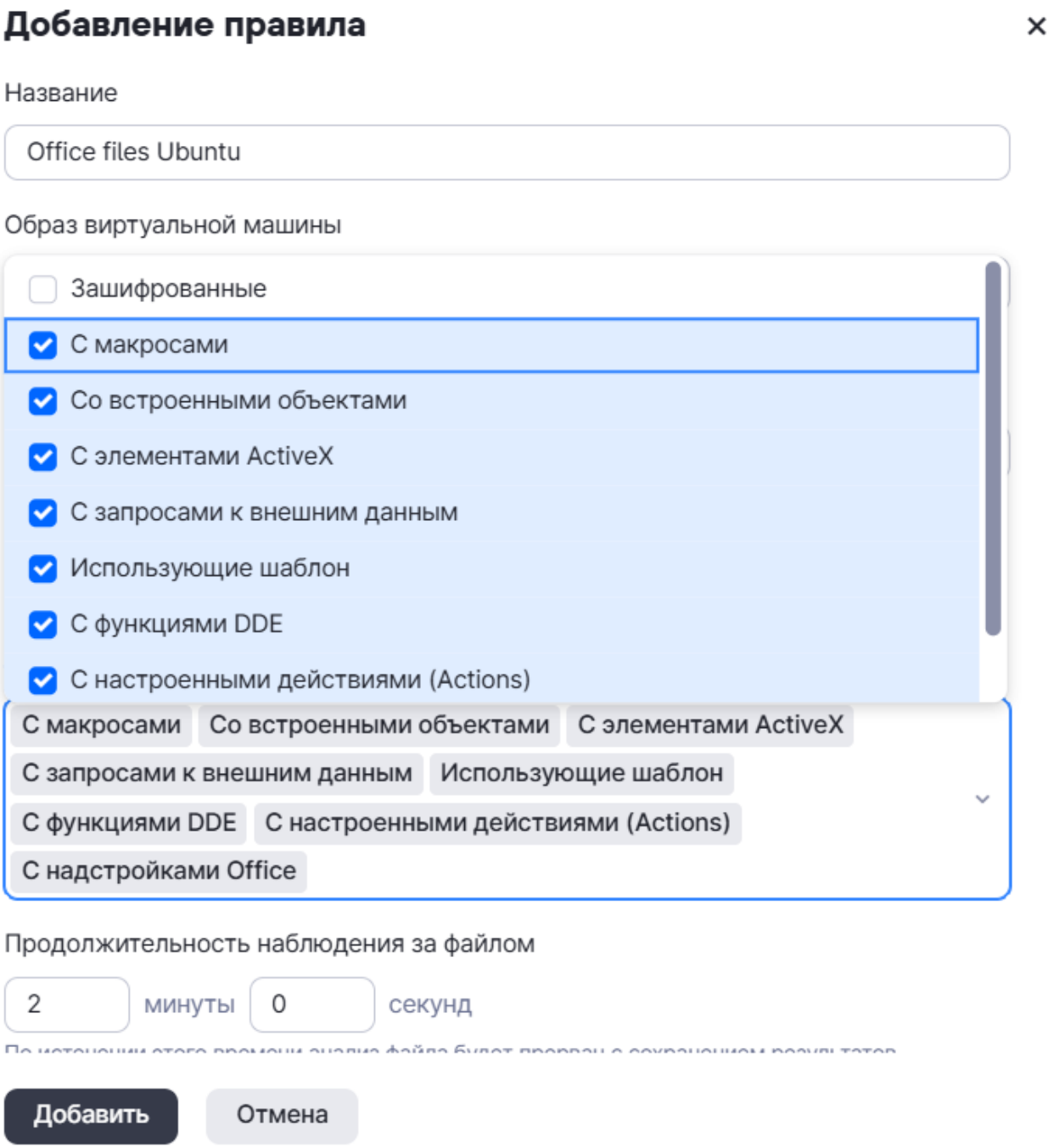

Рисунок 23. Добавление меток

Как правило, в поведенческом анализе есть смысл запускать файлы, метки в которых указывают на наличие активного содержимого. Это практически весь список, кроме метки **Зашифрованные**. Запуск файлов с такой меткой остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. **Продолжительность наблюдения за файлом**: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 3 минуты.

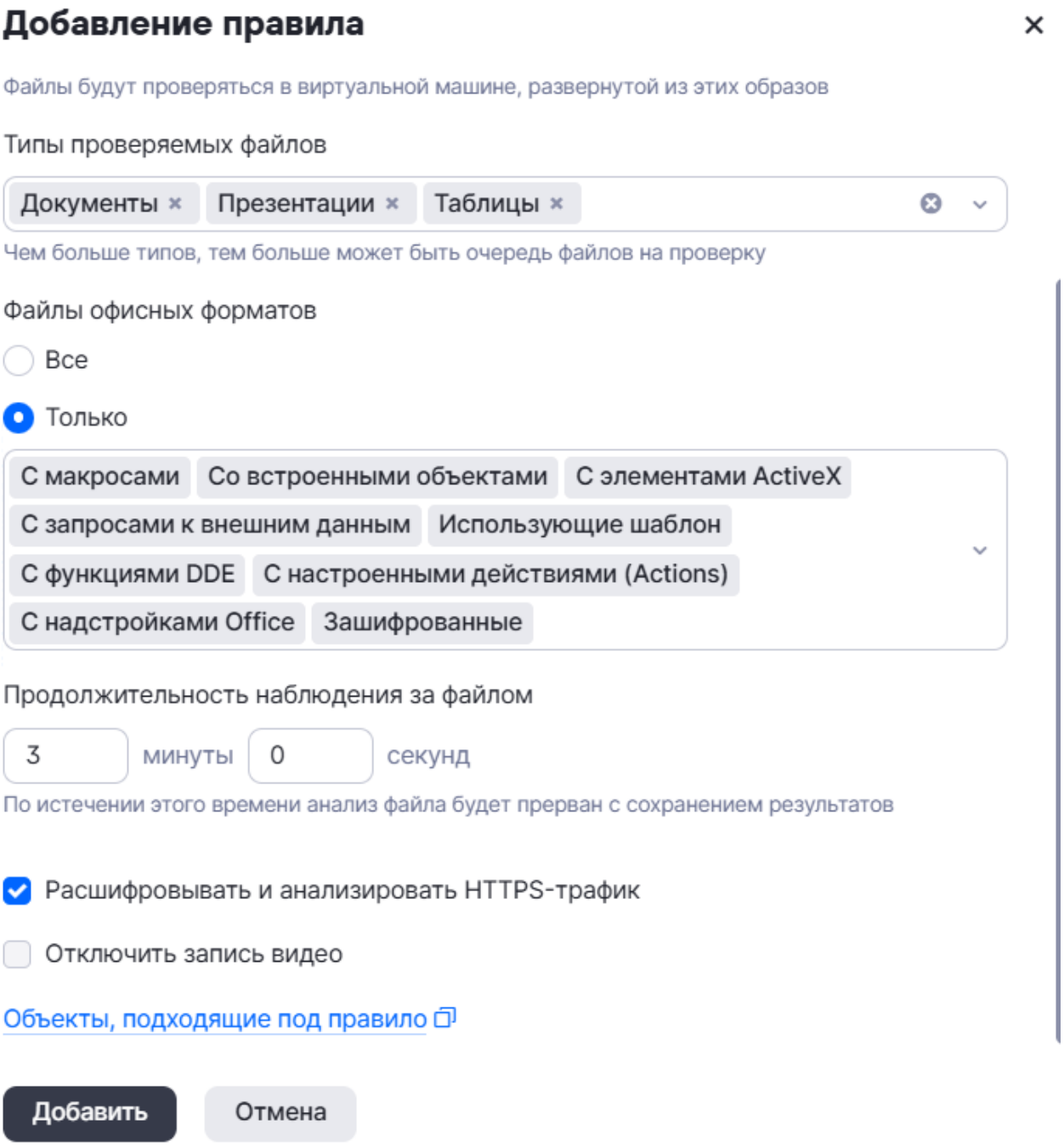

Рисунок 24. Выбор продолжительности наблюдения за файлом

3.6. Создание правила для PDF-файлов, Linux

Третье правило — по оставшемуся типу PDF.

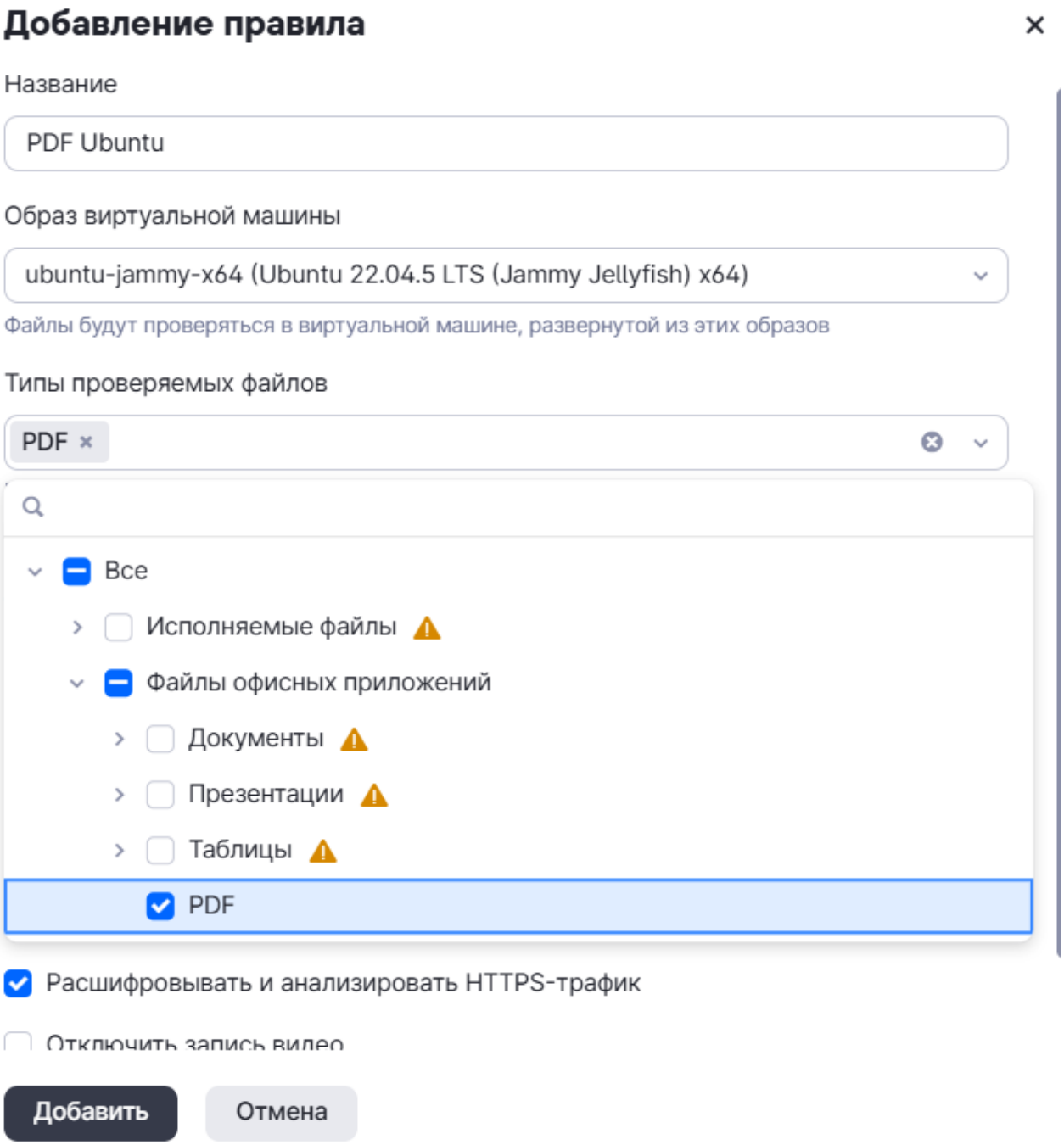

Рисунок 25. Создание правила для PDF-файлов, Linux

Для этих файлов обратим внимание на определенные песочницей **Метки**.

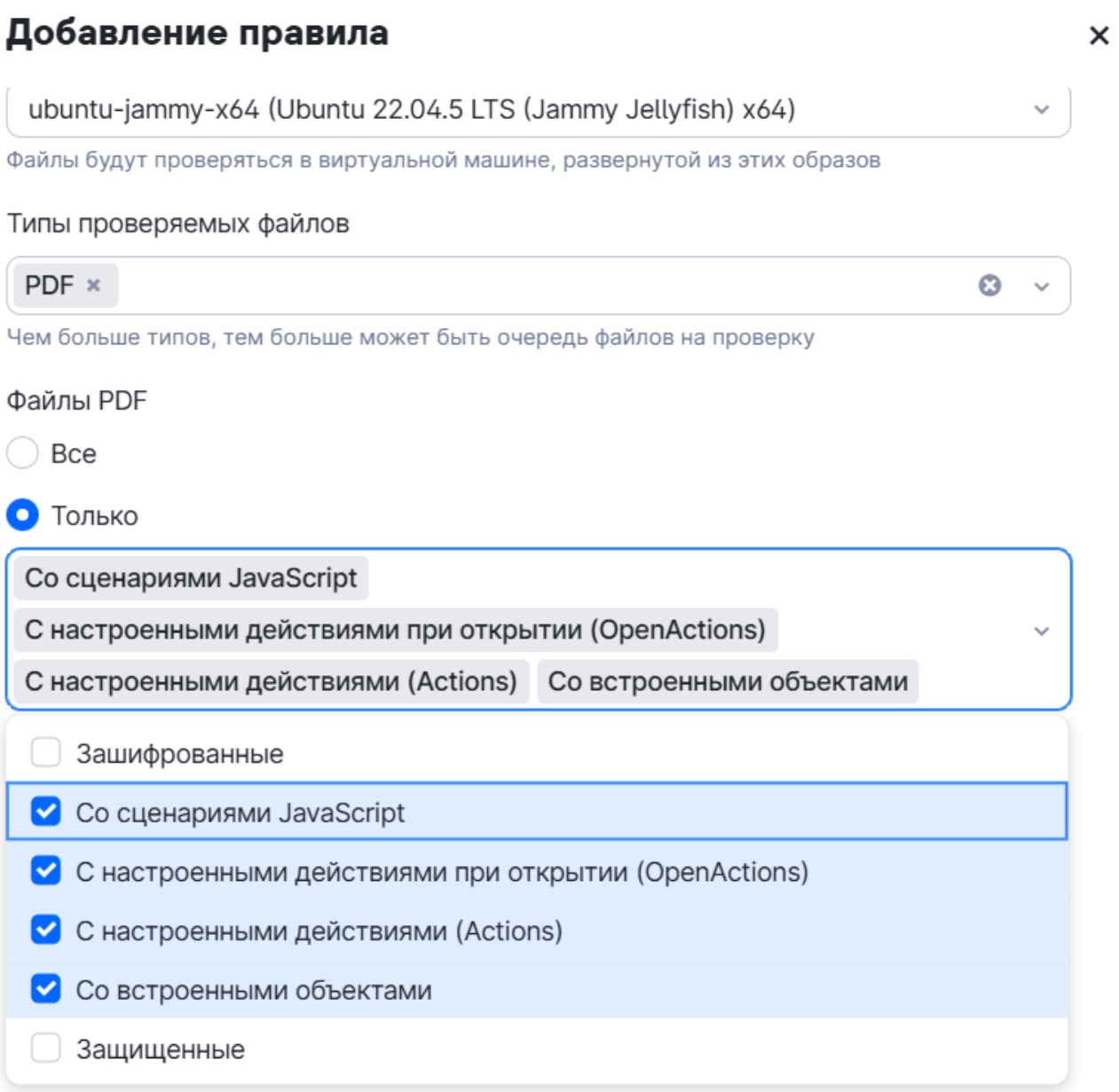

Рисунок 26. Добавление меток

Отмечаем в раскрывающемся списке всё, кроме меток **Зашифрованные** и **Защищенные**. Запуск файлов с такими метками остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. Продолжительность: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 2 минуты.

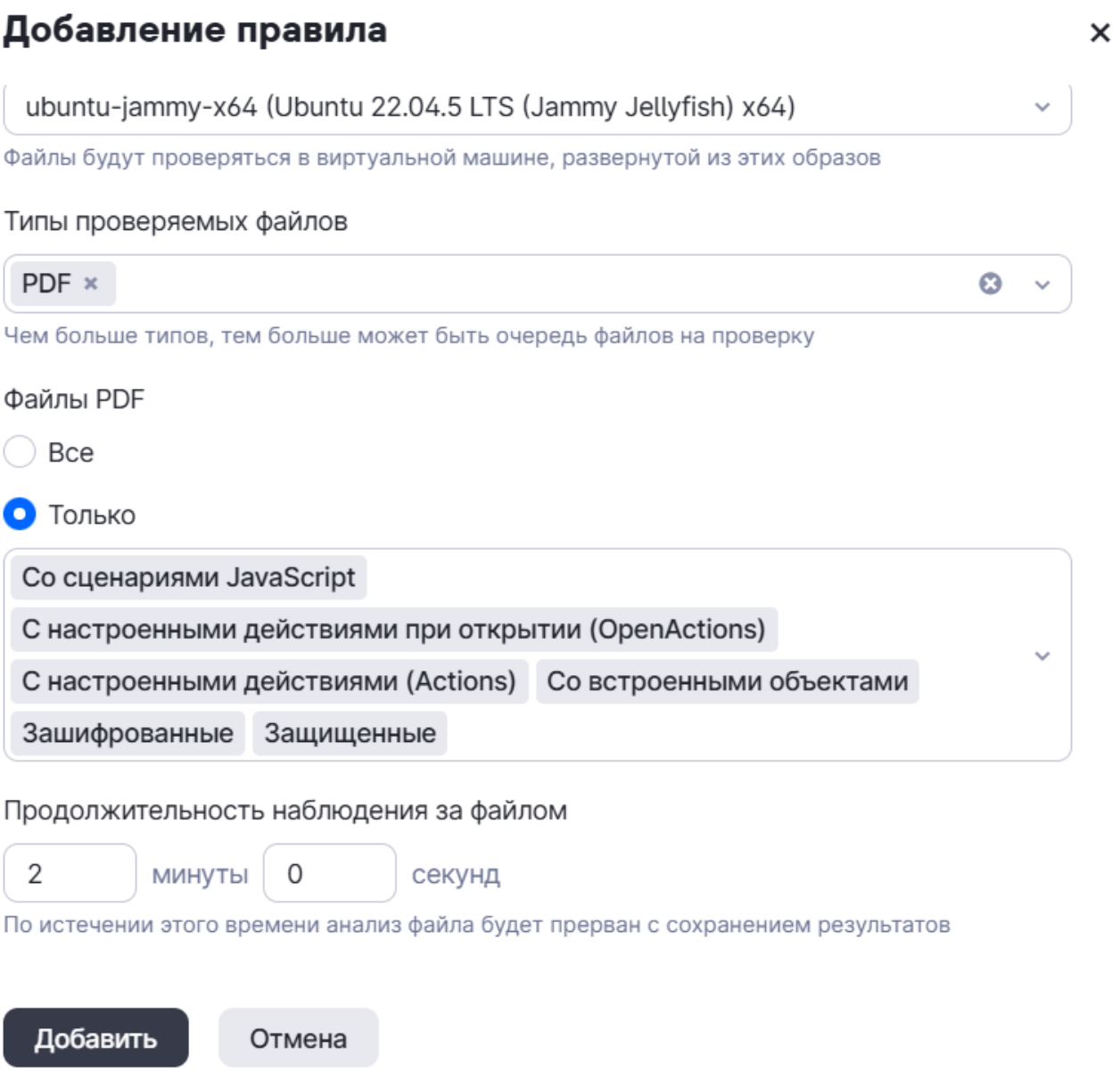

Рисунок 27. Выбор продолжительности наблюдения за файлом

Как результат, для проверок в поведенческом анализе на Ubuntu 22.04 LTS (Jammy Jellyfish) x64 получаем следующий набор правил.

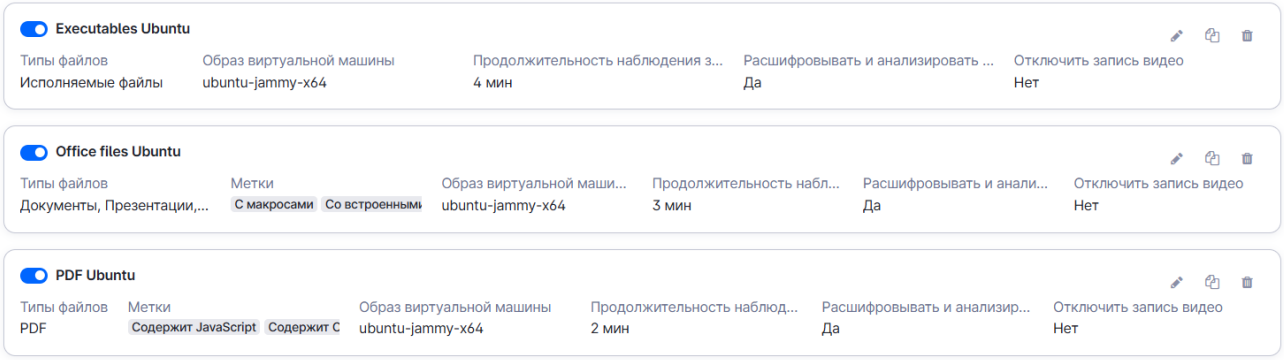

Рисунок 28. Набор правил для проверок в поведенческом анализе

После создания правил примените изменения в источнике, нажав кнопку **Сохранить**.

Для полноты проверок в инфраструктурах, где используются оба семейства ОС, основная практика — проверка файлов в обоих семействах. Если же стоит вопрос экономии ресурса, то допустимо снять дублирующие проверки одних и тех же типов файлов на разных видах образов.

4. Проверка правил

После сохранения параметров проверки для источника рекомендуется проследить за результатами проверки на потоке проверяемых файлов, в том числе возможно использование сервисов проверки защищенности. При обнаружении в результате проверок некорректных срабатываний (ложноположительных или ложноотрицательных) необходимо перенастроить наборы правил.