Гарда Лабиринт

Руководство администратора. Модуль Приманки

gardatech.ru

2023

Тип документа:	Руководство администратора. Модуль Приманки
Дата выпуска:	03.11.2023
Статус документа:	Released
Версия:	1.8.0

ООО «Гарда Технологии»
Все права сохраняются за правообладателем.

ООО «Гарда Технологии» оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО «Гарда Технологии». Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким- либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО «Гарда Технологии». Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора для модуля Приманки Программного Комплекса "Гарда Лабиринт".

1.2 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.3 О компании

Гарда Технологии (входит в ГК Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.4 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по московскому времени).
- Email: glb.support@gardatech.ru.

2 Модуль Приманки

2.1 Назначение модуля

Модуль Приманки предназначен для постоянной доставки самораспаковывающегося архива, распространяющего приманки на АРМ предприятия. Приманки используются для увеличения вероятности взаимодействия злоумышленника с ловушкой. Приманка предлагает обратиться по адресу ловушки и провзаимодействовать с ней, таким образом злоумышленник выявлен на ранней стадии атаки и администратор ИБ или ИТ службы предприятия имеет возможность заранее реагировать на возникающие угрозы.

2.2 Принцип работы модуля

Комплекс предлагает скачать сконфигурированный самораспаковывающийся архив и разместить его на общедоступном в сети ресурсе для того чтобы групповой политикой домена или каким-то другим образом произошло обращение реального устройства к данному файлу. Далее в соответствии с заранее определенными правилами для определенных доменных групп или конкретных узлов происходит доставка Приманки на узел сети с которого произошло обращение с помощью самораспаковывающегося архива. Приманки представляют из себя различные артефакты, содержащие путь до ловушки и уникальную для каждого узла учетную запись.

2.3 Функциональные свойства приманок

- Имеется возможность распространять приманки типа SSH, RDP, FTP, HTML, SMB, MSSQL, MySQL
- Приманки распространяются в виде:
  - куки данных,
  - учетных данных в хранилище операционной системы,
  - в хранилище учетных данных браузера,
  - текстовый файл,
  - настроенное соединение putty.

- При распространении приманок не устанавливаются никакие программы, выполняющие роль агента на конечные узлы сети.
- В приманках уникальные учетные данные для каждого отдельного узла сети.
- Процесс доставки приманок на конечный узел не эксплуатирует протоколы и службы: PsExec, PaExec, WMI/RPC, WinRM, SSH, sh – скрипты.
- Доставка приманок должна происходить по защищенному шифрованием каналу связи.

3 Приманки

3.1 О разделе Приманки

Раздел **Приманки** используется для распространения приманок. Приманки – это некие записи (ярлыки, текстовые файлы, истории сессии и др.), которые распространяются на реальной инфраструктуре для дополнительного запутывания потенциального злоумышленника.

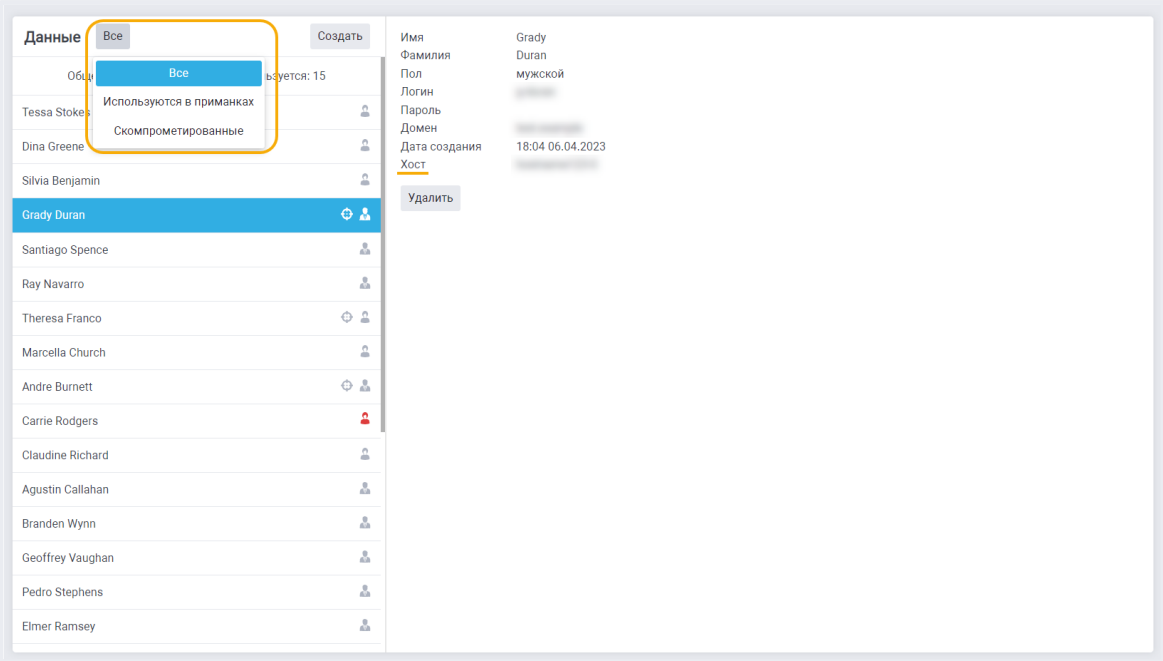
Раздел состоит из следующих подразделов: Данные, Распространение и Конфигурации.

3.2 Данные

Подраздел содержит авторизационные данные, которые используются в приманках для подключения к различным ловушкам. По нажатию на учетную запись в поле справа отображаются авторизационные данные. Для учетных записей, которые были использованы в приманках, также отображается имя **Хоста**, на котором была размещена данная учетная запись в виде приманки.

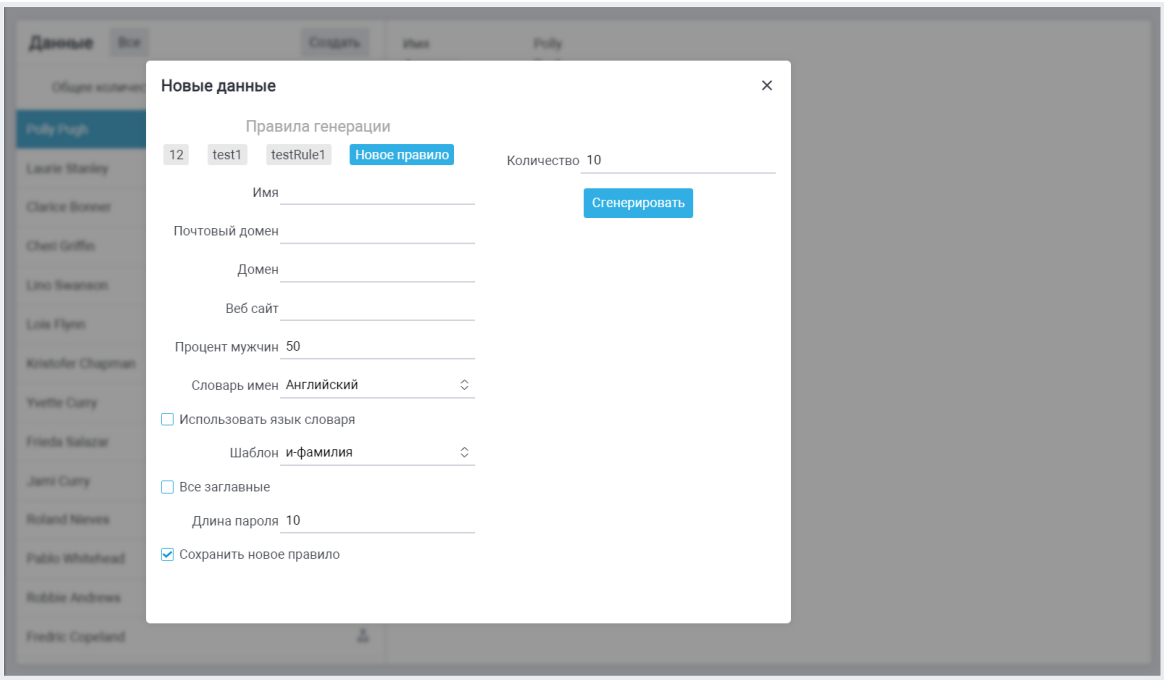
По нажатию на кнопку **Все** доступны следующие параметры фильтрации:

- **Все** - отобразить все созданные учетные записи.
- **Используются в приманках** - отобразить учетные записи, которые используются в приманках. В списке такая учетная запись отмечена пиктограммой  .
- **Скомпрометированные** - отобразить учетные записи, которые были обнаружены злоумышленником. В списке скомпрометированные учетные записи выделены красным цветом  .



Создание новых записей

Создание записей происходит по кнопке **Создать**. При нажатии на кнопку отобразится окно, в котором происходит настройка правил для генерации новых записей.



Основные параметры:

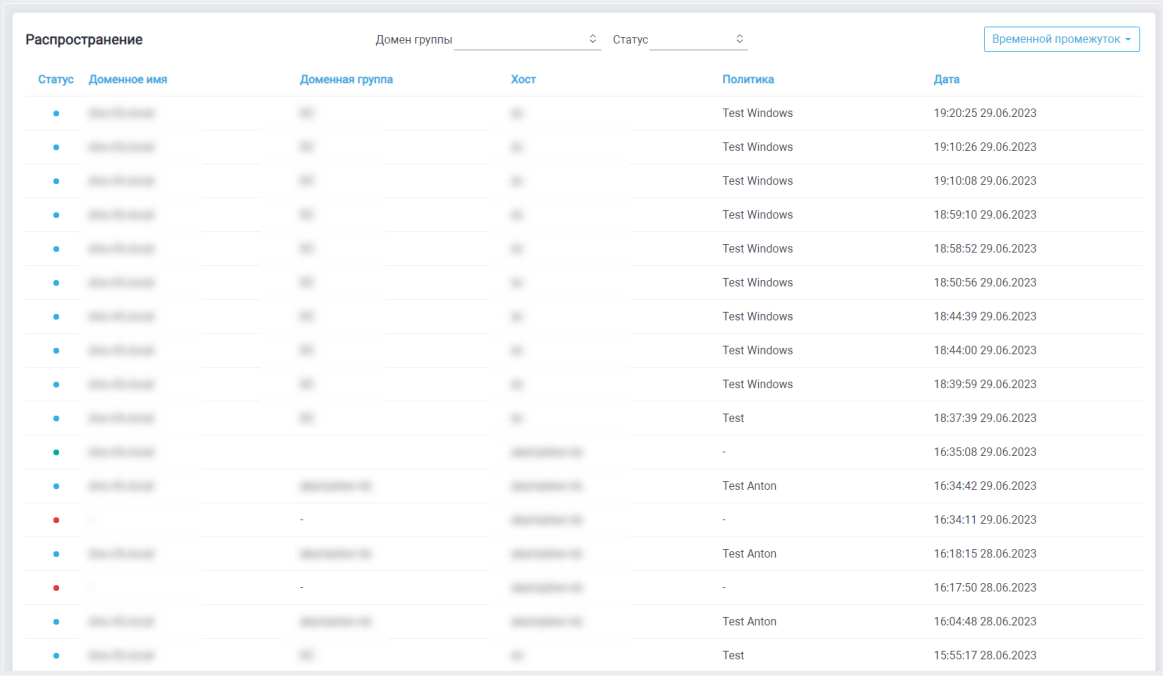
- **Имя** – имя правила для генерации.

- **Почтовый домен** – домен почты, который будет присвоен новым записям.
- **Домен**.
- **Веб сайт**.
- **Процент мужчин** – позволяет указать соотношение женщин и мужчин.
- **Словарь имен** – позволяет выбрать язык, на котором будут генерироваться записи.
- **Шаблон** – настройка формата отображения имени.
- **Все заглавные** – установить все заглавные буквы для пароля.
- **Длина пароля** – установить фиксированную длину пароля.
- **Сохранить новое правило** – позволяет сохранить правило для дальнейшего использования.
- **Количество** – количество генерируемых записей.

Для создания записей нужно заполнить все поля и нажать кнопку **Сгенерировать**.

3.3 Распространение

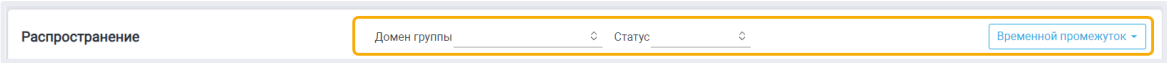
В подразделе **Распространение** отображаются результаты по распространению приманок с помощью групповой политики домена на реальные узлы.



Основные параметры:

- **Статус** – обозначает статус размещения приманки по узлам. Существуют следующие статусы:
  - Зеленый (Новый) – на машину были впервые размещены приманки.
  - Голубой (Обновлен) – на машине ранее уже были размещены приманки и их состав был актуализирован в соответствии с политикой.
  - Красный (Неуспешный) – при размещении приманок произошёл сбой.
- **Доменное имя**.
- **Доменная группа**.
- **Хост**.
- **Политика** – используемая политика распространения.
- **Дата** – время и дата события.

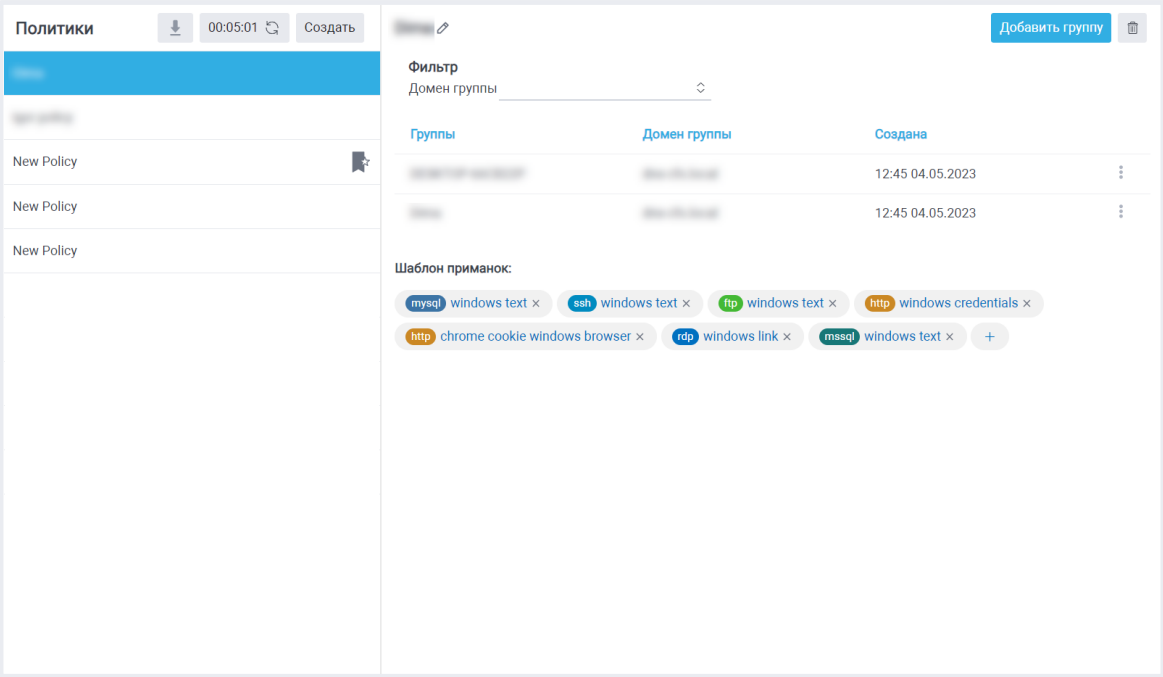
Политики можно отфильтровать по **Домену группы**, **Статусу** и **Временному промежутку**:



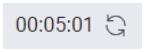
3.4 Конфигурации

3.4.1 О подразделе Конфигурации

Раздел позволяет создавать политики распространения приманок, настраивать конфигурацию приманок для выбранной политики распространения и выбирать политику по умолчанию. Политика создается для групп доменов и содержит заданный набор приманок.



При нажатии на кнопку  пользователь может скачать самораспаковывающийся архив вместе с актуальной конфигурацией сети, которая доступна супервизорам. Доступно скачивание версии архива для Windows и Linux.

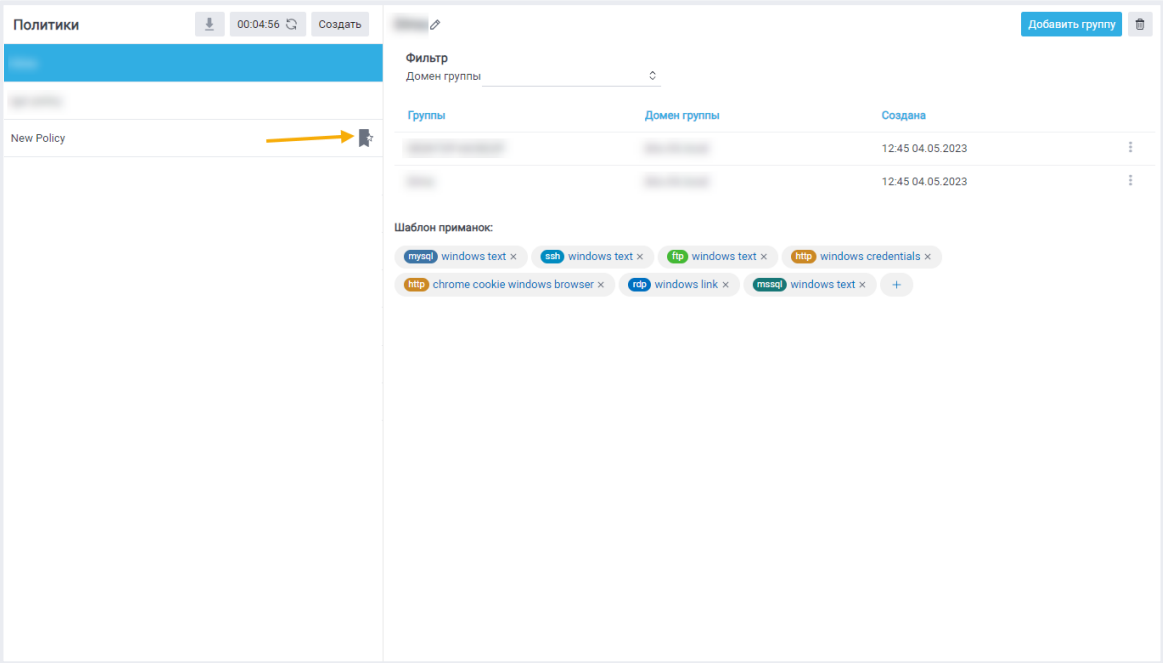
При нажатии на кнопку  будет подготовлен для скачивания исполняемый самораспаковывающийся архив с учетом актуальной конфигурации сети супервизоров. Кнопка также отображает время последней сборки архива. Если с момента последней сборки прошло более 24 часов, то на кнопке будет отображена дата сборки.

> ***Примечание:*** *Пользователю необходимо убедиться, что используется актуальная версия архива, так как Супервизор откажет в подключении с неактуальной версией. При изменении конфигурации сети супервизоров или обновлении Комплекса необходимо пересобрать архив, скачать и распространить его на необходимые узлы инфраструктуры.*

Выбор политики по умолчанию

Пользователь может выбрать одну из политик, которая будет использоваться по умолчанию. Политика по умолчанию будет применена для входящих в нее групп доменов, а также для всех хостов, которые не включены ни в один из доменов и

работают в одноранговой сети. Для того чтобы назначить политику по умолчанию, необходимо напротив выбранной политики нажать кнопку **Сделать политику по-умолчанию**.



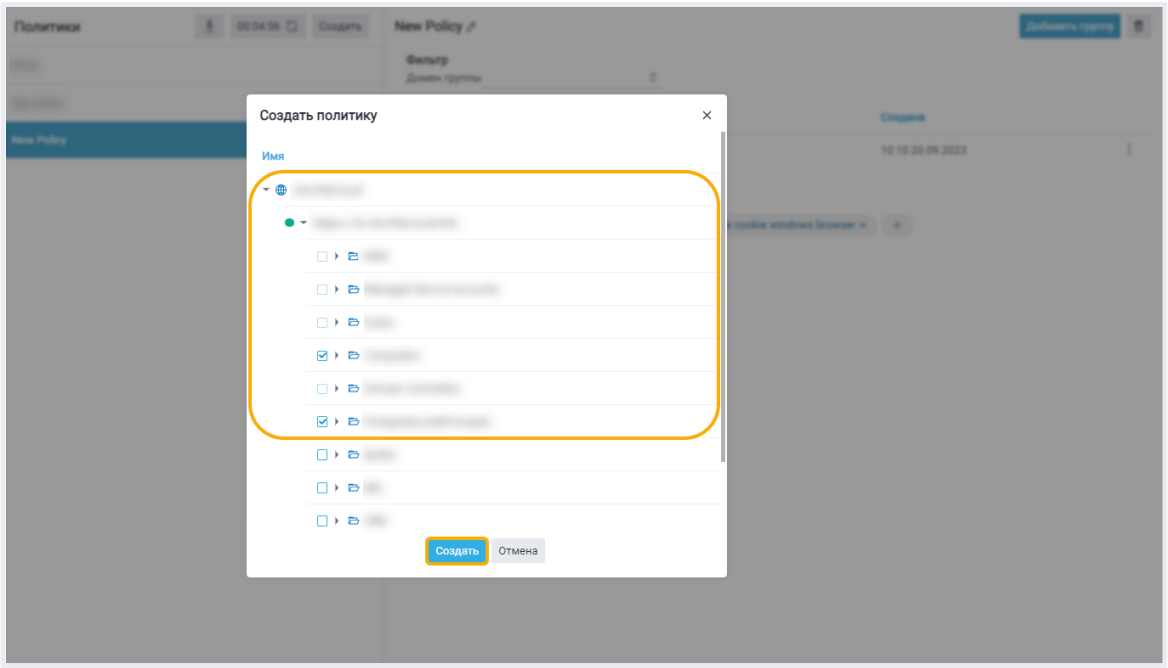
3.4.2 Настройка политик

Для создания политики выполните следующие действия:

1. На панели **Политики** нажмите кнопку **Создать**.
2. В окне **Создать политику** выберите из списка необходимый домен и доменную группу.

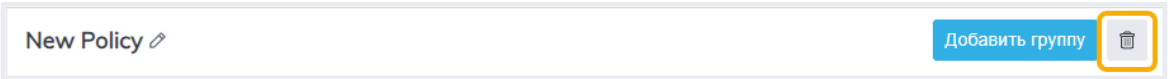
> ***Примечание:*** *Для групп дочерних уровней используется политика ближайшей по иерархии родительской группы.*

3. Нажмите **Создать**.



Новая политика появится в списке политик на панели слева.

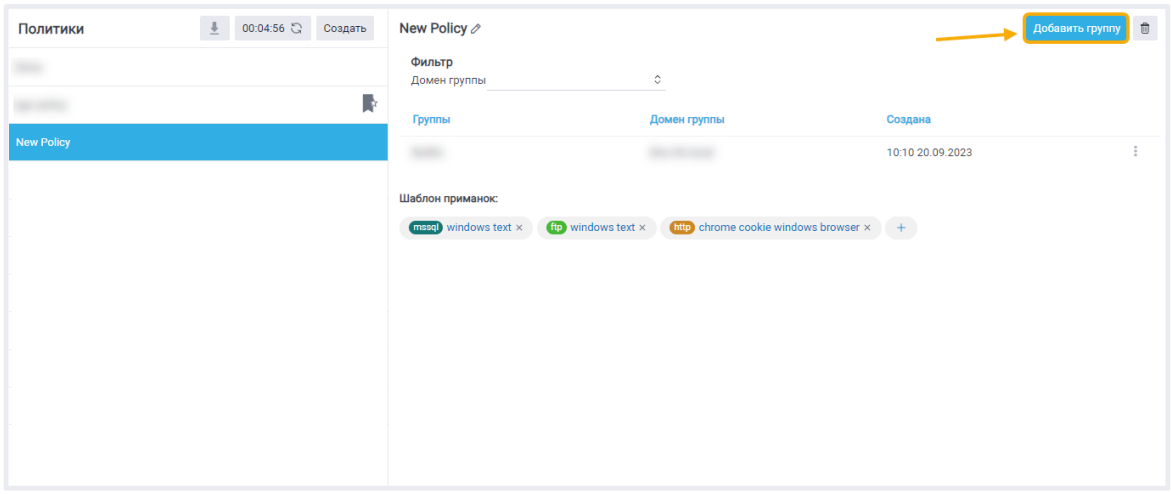
4. Для редактирования названия политики выберите необходимую политику из списка и нажмите на пиктограмму **Редактировать**.
5. В открывшемся окне введите новое название политики и нажмите **Сохранить**.
6. Для удаления политики нажмите на кнопку **Удалить**.



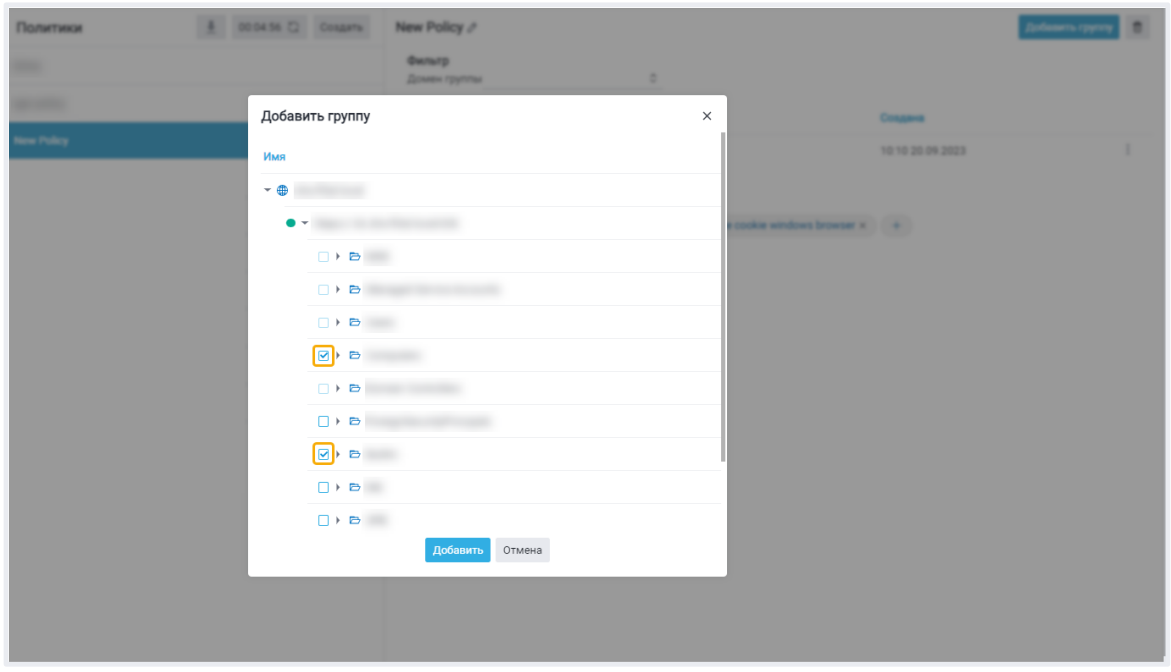
3.4.3 Добавление группы домена

Политика может включать в себя одну или несколько доменных групп. Для добавления новой группы выполните следующие действия:

1. Нажмите на кнопку **Добавить группу**.



2. В открывшемся окне выберите группу домена:



3. Нажмите **Добавить**.

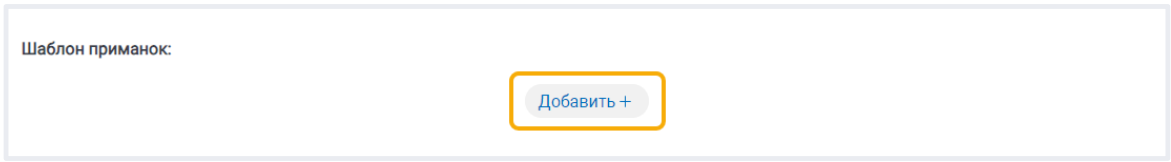
   Новая группа появится в списке групп.

   Для удаления группы домена из Политики нажмите ⋮ → **Удалить**.

3.4.4 Создание шаблона приманок

Для выбранной политики необходимо добавить один или несколько шаблонов приманок, которые будут распространяться на узлы реальной инфраструктуры.

1. Для создания шаблона нажмите кнопку **Добавить**:



2. В открывшемся окне в поле **Приманка** выберите тип ловушки.

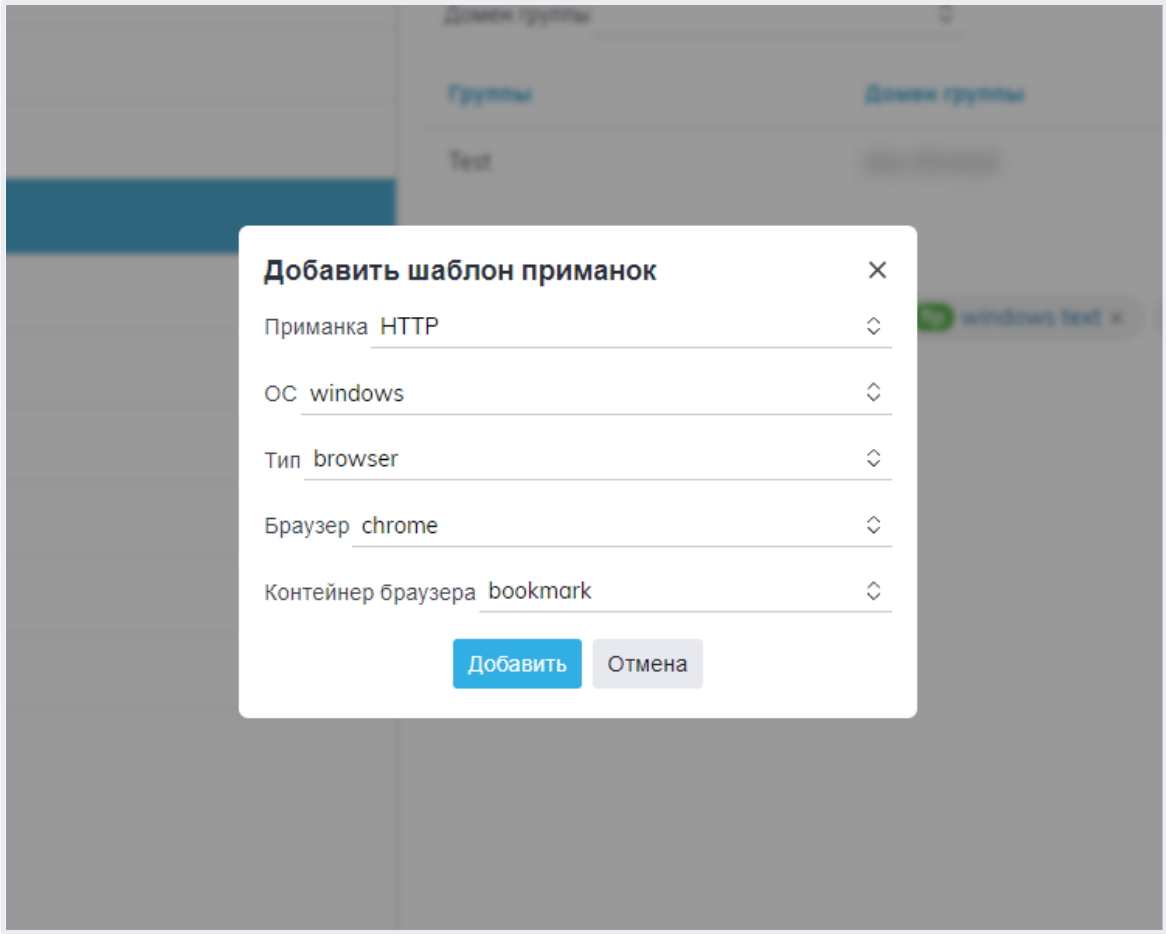
   Доступны следующие типы:

   - **SSH** – "Подключение к серверу"
   - **FTP** – "Файловый сервер"
   - **HTTP** – "Доступ через браузер"
   - **MSSQL** – "База данных Microsoft SQL"
   - **MySQL** – "База данных MySQL"
   - **RDP** – "Подключение к удаленному рабочему столу"
   - **SMB** – "Общая папка"

3. Выберите семейство операционной системы:

   - windows,
   - linux.

4. Выберите **Тип** приманки и при необходимости задайте дополнительные параметры. Например, для приманки HTTP при выборе **Типа** приманки **browser** можно дополнительно настроить параметры **Браузер** и **Контейнер браузера**.



5. Для добавления шаблона нажмите **Добавить**.

Список добавленных шаблонов появится в поле **Шаблон приманок**: