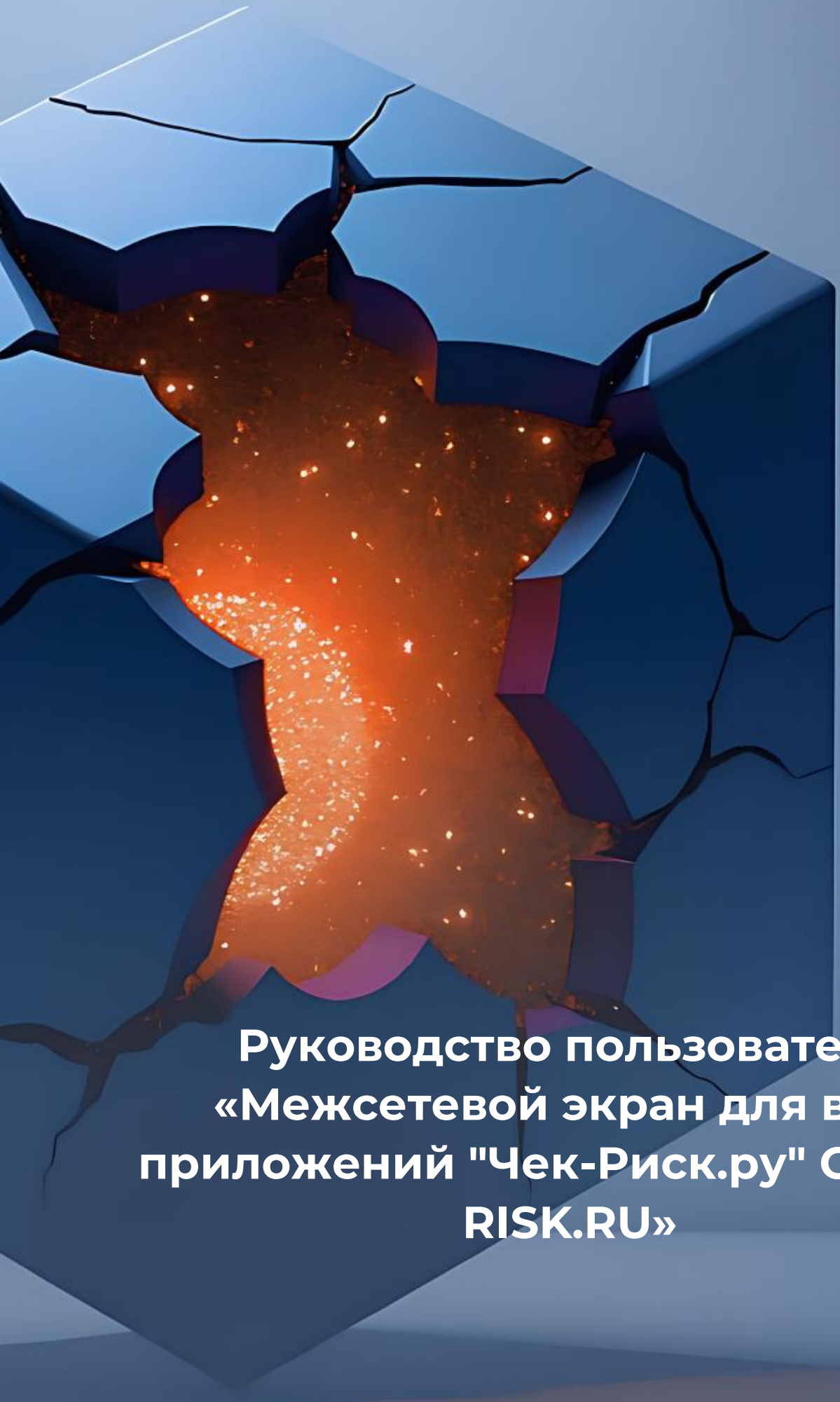
checkriskru_bot sales@check-risk.ru

CHECK RISK



Руководство пользователя «Межсетевой экран для веб-приложений "Чек-Риск.ру" CHECK-RISK.RU»

Содержание

Термины и определения 7

Общая информация 12

1. Введение 13

1.1 Регистрация аккаунта 13

1.1.1 Устранение возможных проблем 14

1.2 Настройка 2FA аутентификации 15

1.2.1 Как включить 2FA в Check Risk: пошаговая инструкция 15

1.2.2 Что такое 2FA и почему это важно 17

1.2.3 Решение проблем и восстановление доступа 18

1.3 Временная блокировка атак 19

1.3.1 Возможные причины и сроки блокировки 19

1.3.2 Обжалование временной блокировки 20

1.3.3 Восстановление доступа после блокировки 20

1.4 Постоянная блокировка атак 21

1.4.1 Причины блокировки 21

1.4.2 Что означает блокировка 22

1.4.3 Как подать апелляцию 22

1.5 Восстановление доступа к аккаунту 24

1.5.1 Если вы забыли логин 24

1.6 Удаление аккаунта 24

1.6.1 Как отправить запрос на удаление аккаунта 24

1.6.2 Что происходит после удаления аккаунта 25

2. Начало работы 26

2.1 Описание выделенной инфраструктуры 26

2.1.1 Порядок взаимодействия и параметры конфигурации 26

2.1.2 Ограничения и допуски 26

2.1.3 Отказоустойчивость и производительность 27
2.2 Настройка кастомных страниц WAF 27
2.2.1 Порядок настройки 29
2.2.2 Рекомендации по содержанию и защите: 31
2.3 Анти DDOS 32
2.4 Режимы работы 33
2.4.1 Доступные режимы 34
2.4.2 Рекомендуемые практики при переключении 36
2.5 Проверка работы WAF 37
2.6 Добавление SSL сертификата 38
2.7 Требования к квалификации сотрудников 40
2.7.1 Администратор безопасности WAF 41
2.7.2 Аналитик WAF (оператор мониторинга) 41
2.7.3 Оператор реагирования на инциденты 41
2.7.4 Аудитор/наблюдатель 41
2.8 Расчет количества QPS 42
2.9 Обновление фидов 43
2.9.1 Системы автоматического на основе фидов 44
2.10 Верификация приложения 44
2.10.1 Порядок подтверждения прав 45
2.11 Генерация SSL сертификата 46
2.11.1 Порядок генерации 47
2.12 Добавление приложения 49
2.13 Настройка входящего трафика на сервер для работы с WAF 50
2.13.1 Принцип работы 50
2.13.2 Установка скрипта 50
2.13.3 Проверка скачивания и применения списка 54

2.13.4 Автообновление списка через systemd timer ... 55
2.13.5 Закрытие прямого доступа ... 57
2.14 Получение реального IP-адреса пользователя за WAF ... 57
2.14.1 Включите передачу заголовков на стороне WAF ... 58
2.14.2 Настройка сервера на обработку X-Forwarded-For ... 58
2.14.3 Nginx учет реального IP из X-Forwarded-For ... 58
2.14.4 Apache (httpd) Учет реального IP из X-Forwarded-For (mod_remoteip) 59
3. Управление угрозами ... 60
3.1 Инструкция по подключению источника Check Risk WAF с PT SIEM ... 60
3.1.1 Подгрузка пакета KB ... 61
3.1.2 Добавление пакета в текущий набор установки ... 62
3.1.3 Установка пакета в SIEM ... 62
3.1.4 Создание задачи по сбору событий по протоколу Syslog ... 62
3.1.5 Ограничение пула адресов ... 64
3.1.6 Проверка поступления и нормализации событий ... 64
3.2 Настройка дашборда KUMA для событий Check Risk WAF ... 65
3.2.1 Инструкция ... 66
3.3 Описание полей событий syslog ... 68
3.3.1 Общая «обёртка» сообщения ... 69
3.3.2 Формат type: "access" (журнал запросов) ... 70
3.3.3 Формат type: "audit" (события безопасности) ... 71
3.4 Передача логов атак по Syslog ... 74
3.4.1 Настройка в «Глобальные настройки безопасности» ... 75
3.4.2 Готовые правила нормализации событий Check Risk WAF ... 75
3.5 Добавление угрозы в исключение ... 76
3.6 Фильтрация угроз ... 79
3.7 Инструкция по созданию виджета для Check Risk WAF в MaxPatrol SIEM ... 81

3.7.1 Добавление фильтра для WAF ... 82
3.7.2 Создание группировки по полю object.type ... 83
3.7.3 Предпросмотр и сохранение виджета ... 83
3.7.4 Добавление виджета на дашборд ... 84
3.8 Настройка нормализации событий Check Risk WAF в SIEM KUMA ... 85
3.8.1 Инструкция по установке ... 85
3.8.2 Добавление нового коллектора ... 86
3.9 Анти-Бот система ... 90
3.9.1 Порядок настройки и применения ... 90
3.9.2 Поведение при работе с токеном ... 92
3.10 Рекомендации и лучшие практики ... 93
3.11 Карточка угрозы ... 96
3.11.1 Добавление IP-адреса в группу ... 98
3.11.2 Добавление URL в карточку приложения и выпуск правила ... 99
3.11.3 Экспорт и воспроизведение запроса ... 100
3.11.4 Практические рекомендации по применению ... 101
3.12 Управление угрозами ... 101
3.12.1 Порядок работы ... 102
4. Правила безопасности ... 105
4.1 Проверка работоспособности правила ... 105
4.2 Добавление IP адреса в черный список ... 107
4.3 Настройка разрешающего правила ... 108
4.3.1 Области проверки и операторы ... 109
4.3.2 Рекомендованные сценарии настройки ... 110
4.4 Настройка правил ... 111
4.4.1 Доступные области и ключевые операторы ... 112
4.4.2 Пример практических примеров конфигураций ... 113

4.5 Настройка запрета по гео-локации GeoIP 114
4.6 Добавление IP адреса в белый список 116
4.6.1 Порядок добавления IP-адреса в белый список 116
4.7 Настройка блокирующего правила 117
4.7.1 Порядок настройки 118
4.7.2 Примеры конфигураций 119
Контакты службы поддержки 121

Термины и определения

В настоящий документ введены термины и сокращения, указанные в таблице 1.

Термин	Определение
HTTP	Hyper Text Transfer Protocol – (протокол передачи гипертекста) – протокол прикладного уровня передачи данных в виде текстовых сообщений.
HTTPS	Hyper Text Transfer Protocol Secure – расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных.
OWASP Top 10 2021	Список из 10-и самых опасных векторов атак на веб-приложения: A01:2021- Нарушение контроля доступа (англ. Broken Access Control) A02:2021 - Утечка чувствительных данных (англ. Sensitive Data Exposure) A03:2021- Внедрение кода (англ. Injection). A04:2021- Небезопасный дизайн (англ. Insecure Design) A05:2021- Неправильная конфигурация (англ. Security Misconfiguration) A06:2021-Уязвимые и устаревшие компоненты (англ. Vulnerable and Outdated Components) A07:2021- Ошибки идентификации и аутентификации (англ. Identification and Authentication Failures) A08:2021- Нарушение целостности данных и программного обеспечения (англ. Software and Data Integrity Failures) A09:2021- Журнал безопасности и сбои мониторинга (англ.

Термин	Определение
	Security Logging and Monitoring Failures) A10:2021- Подделка запросов со стороны сервера или же SSRF (англ. Server-Side Request Forgery)
SSH	Secure Shell — «безопасная оболочка», сетевой протокол прикладного уровня, позволяющий производить удалённое управление.
SSL	Secure sockets layer — уровень защищённых сокетов — криптографический протокол, который подразумевает более безопасный сетевой доступ к веб-приложениям.
SQL	Structured query language — «язык структурированных запросов» — формальный непроцедурный язык программирования, применяемый для создания, модификации и управления данными в произвольной реляционной базе данных, управляемой соответствующей системой управления базами данных (СУБД).
TCP/IP	Transmission Control Protocol/Internet Protocol – стек сетевых протоколов разных уровней модели сетевого взаимодействия, включает в себя протоколы четырех уровней: прикладного, транспортного, сетевого, канального.
TLS	Transport Layer Security — безопасность транспортного уровня, как и его предшественник SSL.
Атака	Попытка использования уязвимости приложения, возникающей за счет несевершенности кода, модулей, библиотек, используемого программного обеспечания и направленная на неправомерное взаимодействие, получение информации, нарушение порядка и правил обработки данных, обход авторизации, повышение прав и т.д.

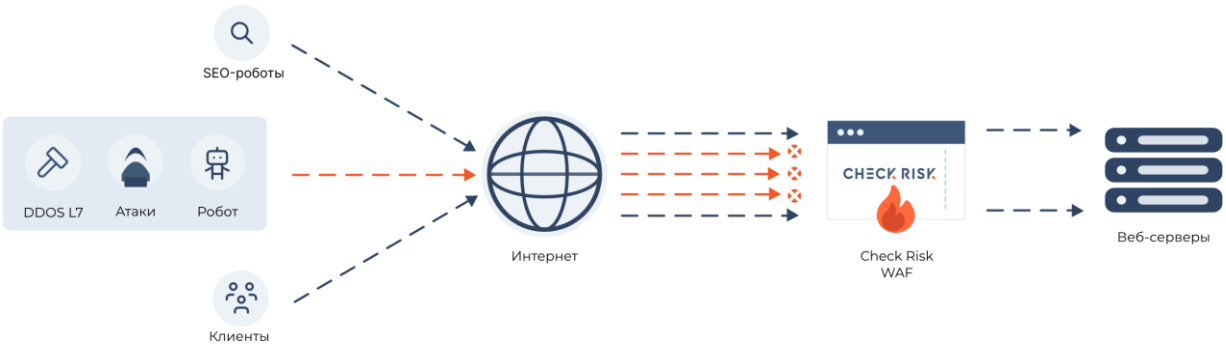
Термин	Определение
БД	База данных.
Система	Комплексное решение, включающее следующие подсистемы: ✓ обнаружения атак; ✓ динамического анализа (поиск уязвимостей); ✓ подтверждения уязвимостей; ✓ управления и отчетности.
Подсистема	Встроенный модуль системы, отвечающий за часть функционала системы.
Веб-консоль управления	Графический интерфейс пользователя. Предназначен для управления системой (администрирование системы, настройка конфигурации, анализ объектов и т. п.). Работает как веб-приложение и не требует установки на компьютер.
Веб-приложение	Программное обеспечение, осуществляющее взаимодействие по HTTP протоколу с браузерами: прием запросов, поиск указанных файлов и передача их содержимого (текст, контент).
Доступность информации	Свойство информации, обеспечивающее возможность получения к ней доступа и её использования.
ИБ	Информационная безопасность.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информация ограниченного доступа	Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, а также в соответствии с нормативными документами Заказчика, которые устанавливают степень конфиденциальности используемой информации.

Термин	Определение
Инцидент информационной безопасности	Одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес-операций или представляющих угрозу для безопасности информационной.
Исполнитель	Исполнитель определяется по результатам проведенного конкурса и всех необходимых закупочных мероприятий.
Канал передачи данных	Среда, состоящая из технических средств передачи данных, программного обеспечения и протоколов передачи данных.
Канал сбора данных	Среда сбора данных, состоящая из технических средств сбора данных, средств программного обеспечения и протоколов передачи данных.
Категория	Элемент классификатора, соответствующий определенной предметной области (например, грифы секретности или термины проекта). Содержит либо перечень категорий (подкатегорий), либо перечень терминов, характерных для данной категории.
Объект защиты	Набор веб-приложений
ОС	Операционная система.
ПО	Программное обеспечение.
Событие информационной безопасности	Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики безопасности информационной или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
Уязвимость	Недостаток в программном коде или в настройках веб-приложений, использование которого, приводит к нарушению целостности веб-приложений и некорректной работе.

Термин	Определение
Целостность информации	Свойство информации, обеспечивающее сохранность заранее определенного вида и качества этой информации.

Общая информация

ПО «Межсетевой экран для веб-приложений "Чек-Риск.ру" CHECK-RISK.RU» (далее – Check Risk) — платформа информационной безопасности класса SaaS, объединяющая в себе облачный WAF уровня L7, антибот систему, Анти-DDoS систему на уровнях L3, L4, L7. Решение предназначено для защиты веб-сайтов, API и внешних сервисов.



Единая облачная платформа Check Risk обеспечит быстрое внедрение защитных мер, минимизирует поверхность атаки внешнего сетевого периметра за счёт фильтрации на уровне приложений и обеспечивает непрерывный контроль за уязвимостями. Бесплатные утилиты позволяют оперативно выполнить базовую проверку активов и упростить работу ITsc, IT специалистам.

Преимущества и особенности ПО:

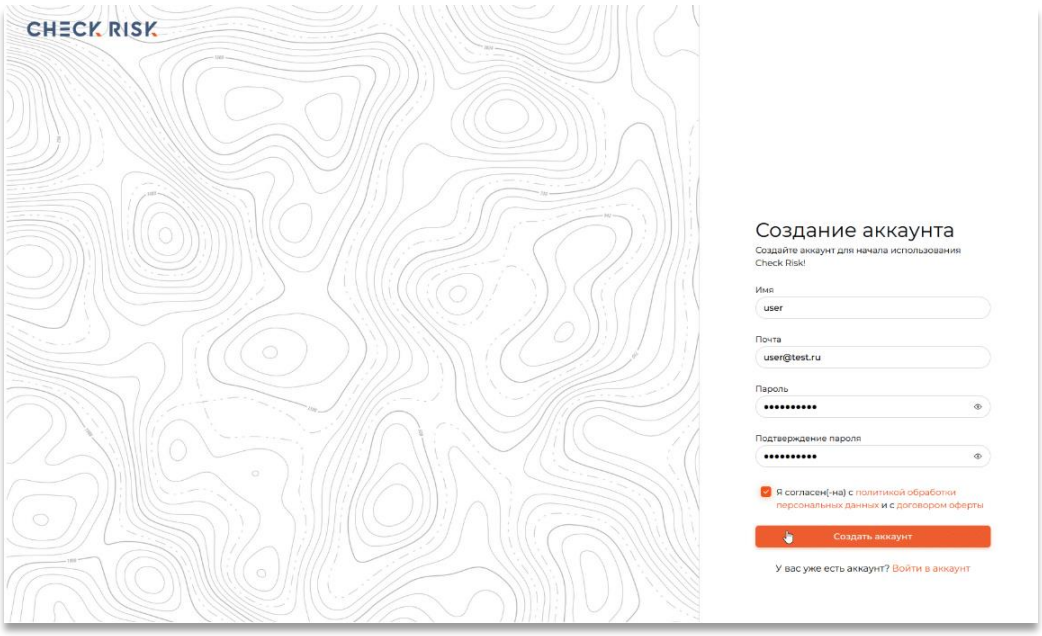
- Быстрое подключение и запуск облачной WAF-защиты. Пользователь подключает защищаемые веб-ресурсы в сервис и получает готовую к работе защиту без установки на своей стороне.
- Защита веб-ресурсов внешнего периметра. В сервисе поддерживается защита публичных веб-приложений, включая сайты и порталы.
- Защита форм, API и административных разделов. Пользователь может применять защиту к критичным компонентам веб-приложений (формы, API, админ-панели).
- Управление политиками и правилами защиты. Пользователь включает и управляет политиками и правилами WAF-защиты для обработки HTTP(S)-трафика.

- Защита от актуальных веб-угроз. Сервис предназначен для противодействия атакам на веб-приложения (в т.ч. из перечня OWASP Top 10), а также эксплойтам.
- Противодействие DDoS-атакам и вредоносному бот-трафику. Пользователь получает механизмы блокирования атакующего трафика, включая DDoS и вредоносных ботов.

1. Введение

1.1 Регистрация аккаунта

Чтобы начать работу с платформой Check Risk, необходимо зарегистрировать аккаунт. Процесс регистрации прост и занимает всего пару минут.



После регистрации необходимо подтвердить указанный email, чтобы активировать аккаунт и получить полный доступ к функционалу платформы. Для подтверждения аккаунта выполните следующие действия:

1. Откройте почтовый ящик, который вы указали при регистрации (если письма нет во «Входящих», проверьте папку «Спам»).
2. Найдите письмо от команды Check Risk и откройте его. В тексте письма будет содержаться специальная ссылка для активации вашего аккаунта.
3. Перейдите по этой ссылке, чтобы подтвердить аккаунт. После перехода в браузере должно появиться уведомление об успешной активации аккаунта.

После успешного подтверждения аккаунта вы сможете войти на платформу, используя свой email и пароль, и приступить к работе с сервисом.

1.1.1 Устранение возможных проблем

Если у вас возникли сложности при регистрации или подтверждении аккаунта, воспользуйтесь следующими рекомендациями:

Письмо для подтверждения не пришло.

Проверьте папку «Спам» в вашем почтовом ящике — письмо подтверждения могло попасть туда. Убедитесь, что при регистрации вы правильно указали адрес электронной почты (без опечаток). Подождите несколько минут, так как доставка письма может занять 5–10 минут. Если письмо так и не пришло, запросите повторную отправку письма или обратитесь в поддержку.

Ссылка для подтверждения не работает.

Если при нажатии на ссылку из письма активация аккаунта не происходит, скопируйте эту ссылку вручную и вставьте её в адресную строку браузера (важно скопировать ссылку полностью). Если ссылка оказалась недействительной (например, истёк срок её действия), запросите новое письмо для подтверждения аккаунта или свяжитесь со службой поддержки.

Не удаётся завершить регистрацию.

Проверьте, что все обязательные поля формы заполнены корректно. Убедитесь, что придуманный пароль соответствует требованиям безопасности (например, содержит не менее 8 символов). Если система сообщает, что такой email уже зарегистрирован, воспользуйтесь функцией «Восстановление пароля» для входа вместо создания нового аккаунта. Если возникают другие ошибки при регистрации, попробуйте повторить попытку немного позже или обратитесь в службу поддержки.

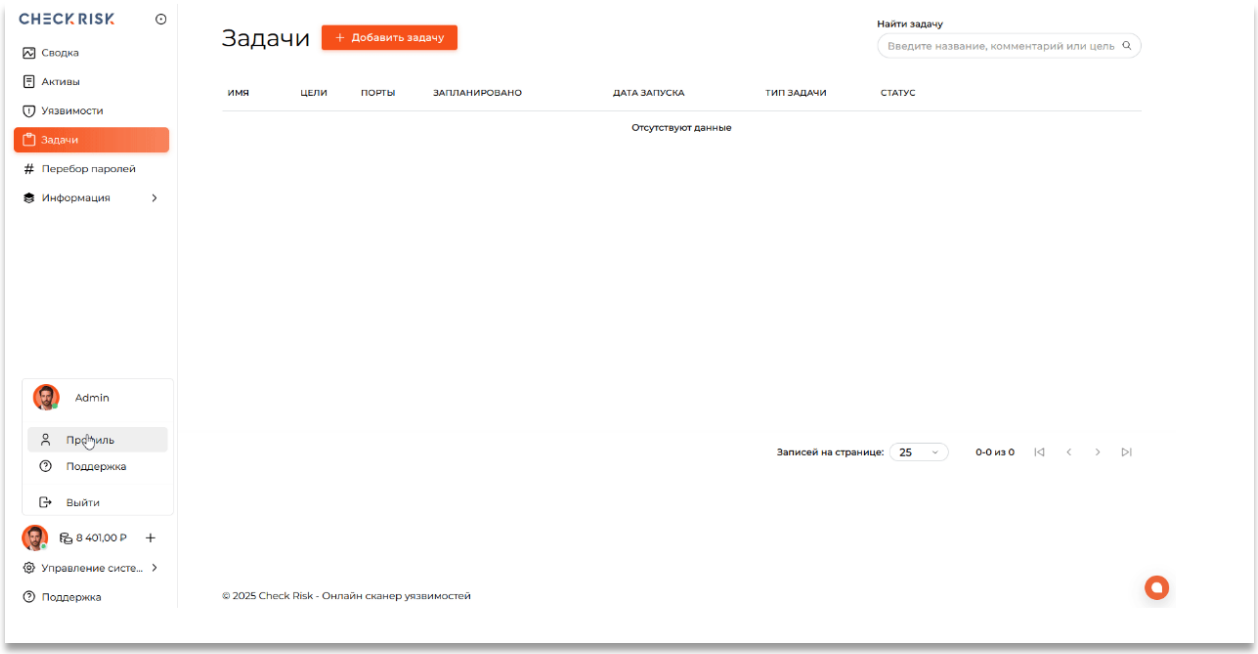
1.2 Настройка 2FA аутентификации

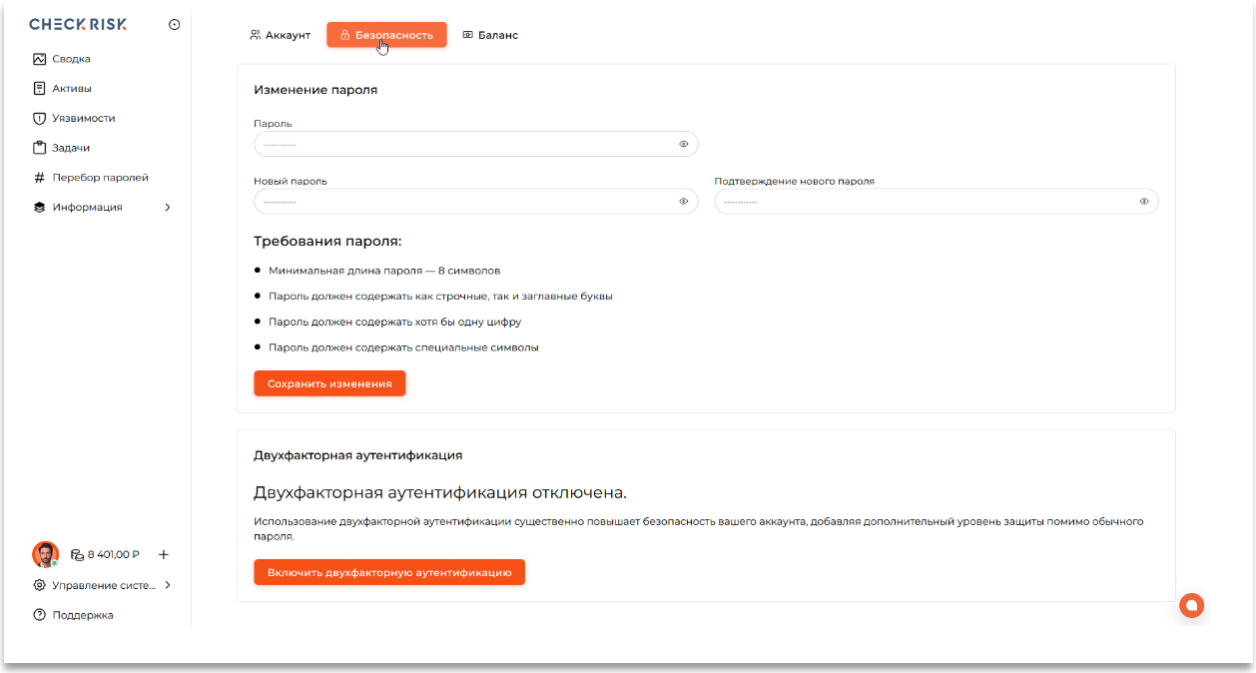
Двухфакторная аутентификация (2FA) — это дополнительный уровень защиты вашего аккаунта. С 2FA для входа на Check Risk требуется не только пароль, но и одноразовый код с вашего мобильного телефона. Это существенно повышает безопасность: даже если злоумышленник узнает ваш пароль, без второго фактора он не сможет получить доступ к аккаунту.

1.2.1 Как включить 2FA в Check Risk: пошаговая инструкция

> Прежде чем начать, убедитесь, что на вашем смартфоне установлено приложение-аутентификатор (например, Google Authenticator или Authy), доступное бесплатно в App Store и Google Play. Эти приложения генерируют одноразовые коды, необходимые для 2FA.

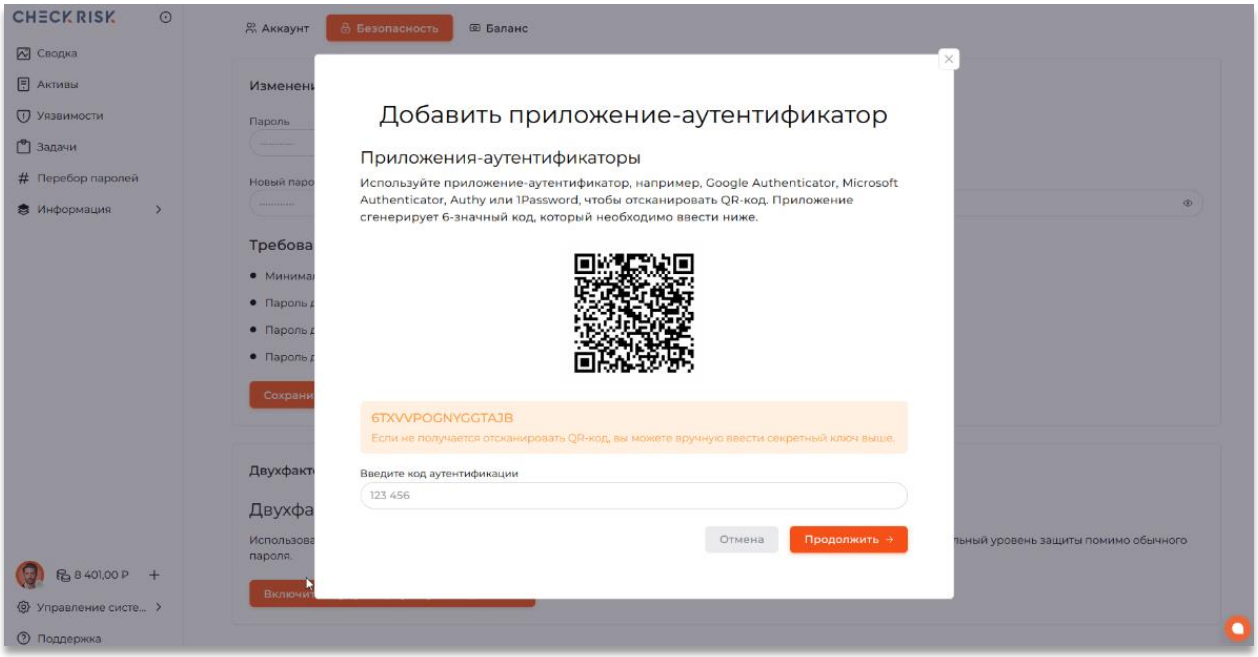
1. **Войдите в свой аккаунт Check Risk.** Перейдите на сайт Check Risk и авторизуйтесь с помощью своего логина и пароля.
2. **Откройте настройки безопасности.** В панели управления нажмите на аватар пользователя и откройте раздел «Профиль». В разделе профиль перейдите во вкладку Безопасность.





3. **Начните включение 2FA**. Нажмите кнопку «Включить двухфакторную аутентификацию». На экране появятся QR-код и секретный ключ для настройки 2FA.

4. **Отсканируйте QR-код через приложение-аутентификатор.** Запустите на смартфоне приложение Google Authenticator или Authy. Нажмите кнопку добавления нового аккаунта (значок «+») и выберите вариант «Сканировать QR-код». Наведите камеру телефона на QR-код, отображённый на странице Check Risk, чтобы привязать ваш аккаунт.



5. **Получите и введите код подтверждения.** После успешного сканирования в приложении-аутентификаторе появится шестизначный одноразовый код для Check Risk. Введите этот код в соответствующее поле на сайте и нажмите «Продолжить» для завершения подключения 2FA.
6. **Сохраните резервные коды.** Если сервис предоставит резервные коды восстановления, сохраните их в надёжном месте (например, выпишите на бумагу и храните офлайн). Резервные коды пригодятся, если вы потеряете доступ к приложению-аутентификатору — с их помощью можно будет войти в аккаунт.
7. **Завершение настройки.** После ввода кода и сохранения резервных ключей двухфакторная аутентификация будет активирована. Теперь при каждом входе в аккаунт вам понадобится вводить одноразовый код из приложения-аутентификатора вдобавок к основному паролю.

1.2.2 Что такое 2FA и почему это важно

2FA (двухфакторная аутентификация) добавляет ко входу в систему второй шаг проверки, обычно с помощью вашего смартфона. При активации 2FA вы вводите

пароль, а затем подтверждаете личность вводом специального кода из приложения на телефоне. Такой подход обеспечивает:

- ✓ **Дополнительную защиту:** никто, кроме вас, не сможет войти в аккаунт, даже если пароль стал известен посторонним.
- ✓ **Безопасность данных:** снижается риск взлома аккаунта и утечки конфиденциальной информации.
- ✓ **Удобство и контроль:** вы всегда получаете уведомление (код) на телефон при попытке входа, что позволяет своевременно обнаружить несанкционированный доступ.

Мы настоятельно рекомендуем всем пользователям включить 2FA на Check Risk для максимальной защиты аккаунта.

1.2.3 Решение проблем и восстановление доступа

При настройке и использовании 2FA могут возникнуть вопросы или сложности. Ниже приведены советы, которые помогут решить распространённые проблемы:

Код не принимается: убедитесь, что вводите актуальный код из приложения. Коды обновляются каждые ~30 секунд, поэтому важно вводить их своевременно, пока текущий код не сменился на новый. Также проверьте правильность времени на вашем смартфоне — если часы неточно идут, код может не совпадать. В Google Authenticator на Android есть функция синхронизации времени (в настройках приложения), при необходимости воспользуйтесь ею.

Не удаётся отсканировать QR-код: если камера не распознаёт QR-код, попробуйте увеличить яркость экрана монитора. Также убедитесь, что приложению-аутентификатору разрешён доступ к камере в настройках телефона. В качестве альтернативы можно добавить аккаунт вручную: скопируйте секретный ключ (он отображается рядом с QR-кодом) и в приложении выберите опцию ввода ключа вручную.

Потерян телефон или удалено приложение: если вы сменили или потеряли устройство с аутентификатором, используйте ранее сохранённые резервные коды для входа. После входа с помощью резервного кода сразу отключите 2FA в настройках аккаунта или привяжите новое устройство. Если резервных кодов нет, обратитесь в службу поддержки — после проверки ваших

данных специалисты помогут восстановить доступ к аккаунту (например, отключат 2FA, чтобы вы смогли войти и настроить её заново).

Ошибка при включении 2FA: если во время настройки произошла ошибка (например, QR-код не сгенерировался или код подтверждения не принимается), перезагрузите страницу и попробуйте начать процесс заново. Убедитесь, что используете последнюю версию приложения-аутентификатора. При повторяющихся сбоях свяжитесь с поддержкой для проверки технических неполадок.

Всегда храните резервные коды в безопасном месте и никому их не сообщайте. Помните, что служба поддержки Check Risk никогда не попросит у вас пароль или коды 2FA. Будьте бдительны и не передавайте подобную информацию третьим лицам.

1.3 Временная блокировка атак

Временная блокировка аккаунта — это краткосрочное ограничение доступа к вашему профилю на Check Risk. В течение периода блокировки вы не сможете войти в систему или пользоваться сервисом. Это не удаление аккаунта и не постоянный бан: все ваши данные сохраняются, и по истечении срока блокировки доступ автоматически восстанавливается. Такая мера служит для защиты пользователей и системы от несанкционированных действий или несерьёзных нарушений правил.

1.3.1 Возможные причины и сроки блокировки

Существуют разные причины, по которым аккаунт может быть временно заблокирован. Ниже перечислены основные ситуации и типичные сроки такой блокировки:

- ✓ **Многократный неверный ввод пароля.** Если вы несколько раз подряд ввели неправильный пароль, система может временно заблокировать ваш аккаунт (15 минут) для защиты от подбора пароля и несанкционированного доступа. Например, если вы забыли пароль и подряд попробовали несколько неверных вариантов, вход будет приостановлен на короткое время.
- ✓ **Подозрительная активность или попытка взлома.** Необычные действия в аккаунте могут привести к блокировке на (до 24 часов). Это происходит, если система заподозрит, что аккаунтом пытается воспользоваться

злоумышленник. Например, резкий всплеск запросов к сервису с вашего профиля или вход с незнакомого устройства может вызвать временную блокировку для проверки безопасности.

- ✓ **Небольшое нарушение правил сервиса.** При несоблюдении условий использования (особенно впервые и, если нарушение не грубое) аккаунт может быть приостановлен на 1–3 дня. Блокировка служит предупредительной мерой. Например, запуск сканирования ресурсов, которые запрещены правилами Check Risk, или иное некорректное использование сервиса может повлечь блокировку аккаунта на пару дней.
- ✓ **Превышение лимитов или чрезмерная нагрузка.** Автоматические алгоритмы могут временно заблокировать аккаунт на несколько часов, если вы сильно превысили обычные лимиты использования или создаёте повышенную нагрузку на систему. Такое может случиться, если за короткий промежуток времени запущено слишком много одновременных проверок безопасности.

> ! Имейте в виду, что повторные нарушения могут привести к более длительной блокировке. В случае серьёзных или систематических нарушений возможна перманентная блокировка аккаунта (без возможности восстановления доступа через данный аккаунт).

1.3.2 Обжалование временной блокировки

Если вы считаете, что блокировка произошла по ошибке или уже, устранили причину нарушения, вы можете обжаловать решение. Для этого свяжитесь с нашей службой поддержки (например, через форму обратной связи на сайте или по электронной почте), указав детали случившегося. Наша команда оперативно рассмотрит обращение и поможет восстановить доступ, если блокировка действительно была наложена неправомерно или вопрос успешно решён. Учтите, что при краткосрочных блокировках (несколько минут или часов) иногда быстрее дождаться автоматического снятия ограничения, чем завершится рассмотрение жалобы.

1.3.3 Восстановление доступа после блокировки

По окончании срока блокировки доступ к аккаунту возобновляется автоматически. Вам не нужно повторно регистрироваться – просто войдите в систему со своими учетными данными, как обычно. Все функции сервиса снова

станут доступны. Если причиной блокировки был неверный пароль, убедитесь, что теперь вводите правильный пароль (при необходимости воспользуйтесь функцией восстановления пароля).

1.4 Постоянная блокировка атак

Check Risk может заблокировать аккаунт пользователя для обеспечения безопасности сервиса и его пользователей. Обычно блокировка происходит при обнаружении нарушений правил или подозрительной активности.

Если Вы только что зарегистрировались и не можете войти в аккаунт, сначала убедитесь, что завершили процесс регистрации (например, подтвердили адрес электронной почты — см. анимацию ниже). Если регистрация выполнена правильно, но аккаунт всё равно заблокирован, значит система выявила определённые причины для блокировки. Ниже описаны возможные причины, значение блокировки и порядок подачи апелляции.

1.4.1 Причины блокировки

Нарушение условий использования. Аккаунт может быть заблокирован за серьёзное нарушение пользовательского соглашения. Например, попытки использовать Check Risk для нелегального сканирования чужих ресурсов без разрешения владельцев или для деятельности, нарушающей закон и правила сервиса. Такие действия рассматриваются как недопустимые и ведут к немедленной блокировке.

Подозрительная активность. Система автоматически мониторит аномальное поведение аккаунтов. В случае выявления подозрительной активности (например, необычно большого числа запросов за короткий период, попыток обхода лимитов или входа в систему из непривычных геолокаций) аккаунт может быть заблокирован в целях безопасности. Такая превентивная мера помогает предотвратить возможные угрозы — например, компрометацию аккаунта или злоупотребление ресурсами сервиса.

Создание нескольких аккаунтов. Запрещается регистрировать более одного аккаунта для обхода ограничений или получения дополнительных бесплатных возможностей. Если система обнаружит связанные между собой дублирующие аккаунты, все они могут быть заблокированы без предупреждения.

Грубые нарушения и злоупотребления. В случаях грубых или повторных нарушений блокировка, как правило, носит перманентный характер. К таким нарушениям относятся попытки взломать сам сервис Check Risk, умышленное нанесение вреда другим пользователям, и использование сервиса в целях, противоречащих принципам безопасности. В подобных ситуациях доступ блокируется во избежание угроз для платформы и её пользователей.

1.4.2 Что означает блокировка

Блокировка аккаунта означает, что Вы не можете пользоваться сервисом. При попытке входа в личный кабинет Вы увидите уведомление о блокировке, и доступ к функционалу Check Risk будет ограничен.

Сканирование во время блокировки невозможно. Ранее сохранённые данные (например, отчёты о проверках и настройки проектов) остаются в системе, но недоступны до снятия блокировки. Блокировка действует на неопределённый срок (до решения вопроса) — сама по себе она не отменяется со временем, требуется вмешательство поддержки для её снятия.

1.4.3 Как подать апелляцию

Апелляция — это запрос на пересмотр решения о блокировке аккаунта. Если Вы считаете блокировку ошибочной или уже устранили нарушения, выполните следующие шаги, чтобы подать апелляцию:

- ✓ **Свяжитесь с технической поддержкой.** Отправьте обращение через онлайн-чат на нашем сайте или на электронную почту support@check-risk.ru. В теме сообщения укажите, что речь идёт об апелляции блокировки аккаунта.

- ✓ **Предоставьте информацию и объяснения.** В тексте обращения опишите ситуацию. Обязательно укажите адрес электронной почты, на который зарегистрирован аккаунт, и подробно объясните, почему, по Вашему мнению, блокировка неверна или как Вы исправили нарушение. Чем полнее и честнее будет информация, тем проще специалистам разобраться в Вашей ситуации.
- ✓ **Ожидайте ответ.** Специалисты нашей поддержки рассмотрят запрос индивидуально. Обычно на это требуется несколько рабочих дней. После проверки Вы получите от нас письмо с результатом рассмотрения. Если апелляция удовлетворена, аккаунт будет разблокирован. Если в разблокировании отказано, мы поясним причины отказа.

> ! Не пытайтесь зарегистрировать новый аккаунт, чтобы обойти блокировку. Такие действия нарушают правила сервиса. Все повторные аккаунты, созданные с целью обхода блокировки, также будут обнаружены и заблокированы. Подобные попытки обхода ограничений могут негативно повлиять на рассмотрение Вашей апелляции.

1.5 Восстановление доступа к аккаунту

Возникли проблемы со входом в аккаунт Check Risk? Ниже вы найдете рекомендации, что делать, если вы забыли логин или потеряли доступ к электронной почте, указанной при регистрации.

1.5.1 Если вы забыли логин

Попробуйте войти по адресу электронной почты. Введите адрес электронной почты, который вы использовали при регистрации, в поле для логина на странице входа. Адрес электронной почты используется в качестве логина, и вы сможете успешно войти в систему.

Воспользуйтесь восстановлением пароля. Если войти по email не получилось, нажмите на ссылку «Забыли пароль?» на странице авторизации и укажите адрес электронной почты, привязанный к вашему аккаунту. На этот адрес придёт письмо с инструкциями по сбросу пароля. Выполнив инструкции из письма, вы сможете задать новый пароль и восстановить доступ к аккаунту. В письме также может быть указан ваш логин.

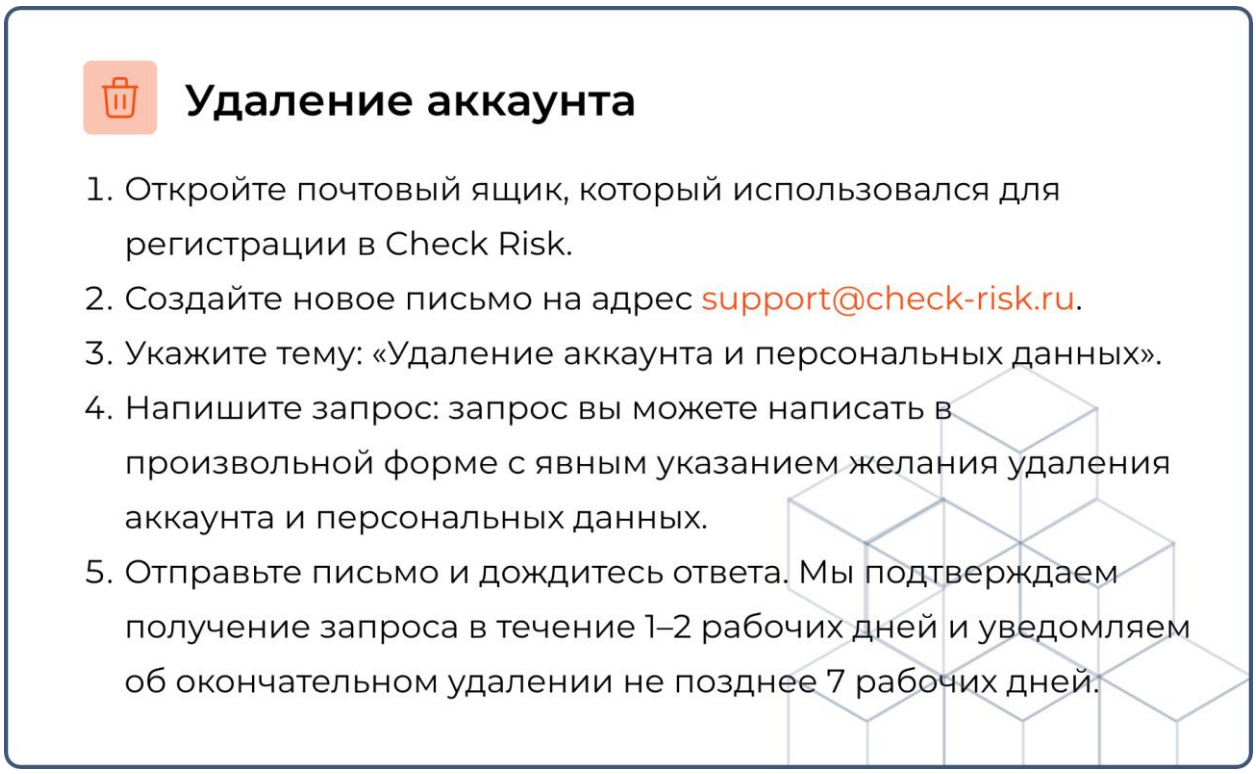
Обращение в службу поддержки (при отсутствии доступа). Если вы не можете войти в аккаунт (например, забыли пароль, а сбросить его через старый email не получается), свяжитесь с нашей службой поддержки. Мы поможем подтвердить, что аккаунт принадлежит вам, и привяжем к нему новый адрес электронной почты, чтобы вы снова получили доступ к своему профилю.

1.6 Удаление аккаунта

Если Вы решили удалить свой аккаунт на платформе Check Risk, Вы можете сделать это, отправив соответствующий запрос. Мы понимаем важность Вашей конфиденциальности и действуем строго в рамках законодательства о персональных данных (Федеральный закон № 152-ФЗ «О персональных данных»). Ниже вы найдете простую пошаговую инструкцию по удалению аккаунта, объяснение последствий этого действия и гарантии соблюдения конфиденциальности.

1.6.1 Как отправить запрос на удаление аккаунта

Чтобы удалить аккаунт, выполните следующие шаги:



1.6.2 Что происходит после удаления аккаунта

Безвозвратное удаление данных: Все данные, связанные с Вашим аккаунтом (например, личная информация, email, результаты сканирования), будут полностью удалены из нашей системы и не подлежат восстановлению. Это означает, что информация об аккаунте исчезнет без возможности возврата.

Отсутствие доступа: после удаления аккаунта Вы не сможете войти в Check Risk с использованием Ваших прежних учётных данных (логина и пароля) или каким-либо образом восстановить удалённый аккаунт. Если в будущем Вы решите снова воспользоваться сервисом, потребуется зарегистрировать новый аккаунт.

Сроки выполнения запроса: Ваш запрос на удаление обрабатывается как можно быстрее. Как правило, процесс занимает не более 7 рабочих дней с момента обращения – это соответствует требованиям законодательства. Вы будете уведомлены, когда удаление аккаунта завершено.

Соответствие законодательству: Удаление аккаунта и уничтожение персональных данных проводится в строгом соответствии с Федеральным законом № 152-ФЗ «О персональных данных». Это гарантирует соблюдение Ваших прав, а также полную конфиденциальность и законность всех действий с данными.

2. Начало работы

2.1 Описание выделенной инфраструктуры

В данном разделе представлено описание выделенной инфраструктуры WAF SaaS, предоставляемой всем клиентам с типом лицензии «Коммерческая». Материал предназначен для специалистов по информационной безопасности и сетевых администраторов, которые планируют эксплуатацию сервиса в выделенном контуре, а также для лиц, принимающих решения по емкости каналов связи и режимам отказоустойчивости.

2.1.1 Порядок взаимодействия и параметры конфигурации

Состав выделенной инфраструктуры

Балансировщики трафика уровня L4/L7: один или несколько экземпляров. Базовая пропускная способность каждого балансировщика от 1 Гбит/с, варианты 10 и 100 Гбит/с доступны по согласованию.

Узлы WAF в виде виртуальных серверов (KVM): не менее двух экземпляров, географически разделены по двум разным (облачным) ЦОД. Базовая пропускная способность сетевых интерфейсов каждого узла от 1 Гбит/с, варианты 10 и 100 Гбит/с доступны по согласованию.

Сетевая логическая модель

Выделение изолированного периметра (VPC/VLAN) для сервисных подсетей.

Назначение выделенных публичных и/или приватных IP-адресов для балансировщиков; маршрутизация трафика от клиентов к балансировщикам, далее к узлам WAF и далее к исходным приложениям Заказчика.

Возможность публикации сервисов с TLS-терминацией на балансировщиках либо пробросом TLS до узлов WAF (режимы по согласованию с Вашими требованиями).

2.1.2 Ограничения и допуски

Фактическая пропускная способность ограничивается выбранными параметрами и характеристиками внешних подключений Заказчика.

Расширенные сценарии фильтрации DDoS и отдельные требования к криптоконфигурации (например, mTLS, версии и наборы шифров) настраиваются по согласованию и могут требовать дополнительного согласования времени внедрения.

Наименования элементов интерфейса и расположение пунктов меню могут незначительно отличаться в зависимости от версии портала.

Выделенная инфраструктура обеспечивает сетевую изоляцию, предсказуемую производительность и повышенную отказоустойчивость за счет распределения по двум независимым ЦОД. Предусмотрены варианты наращивания емкости каналов и расширения числа компонентов без перерывов в работе.

2.1.3 Отказоустойчивость и производительность

Распределение трафика между узлами WAF в активном режиме с постоянными проверками доступности (health checks).

Автоматическое переключение при деградации канала или узла; поддержка сценариев обслуживания без простоя при соблюдении оговоренных окон изменений.

Масштабирование по горизонтали за счет увеличения числа балансировщиков и/или узлов WAF в пределах согласованных лимитов.

2.2 Настройка кастомных страниц WAF

В данном разделе доступны настройки кастомных служебных страниц, которые возвращает WAF SaaS при блокировании запросов или при ошибках шлюза. Это позволяет сохранить единый стиль коммуникации, предоставить пользователю понятное объяснение, а службе поддержки — быстро сопоставить инцидент с конкретным запросом.

Поддерживаются следующие типы страниц:

1. «Атака обнаружена (403)»
2. «Лимит запросов (429)»
3. «Анти-бот проверка (468)»
4. «Ошибка шлюза (502)»
5. «Шлюз не отвечает (504)»

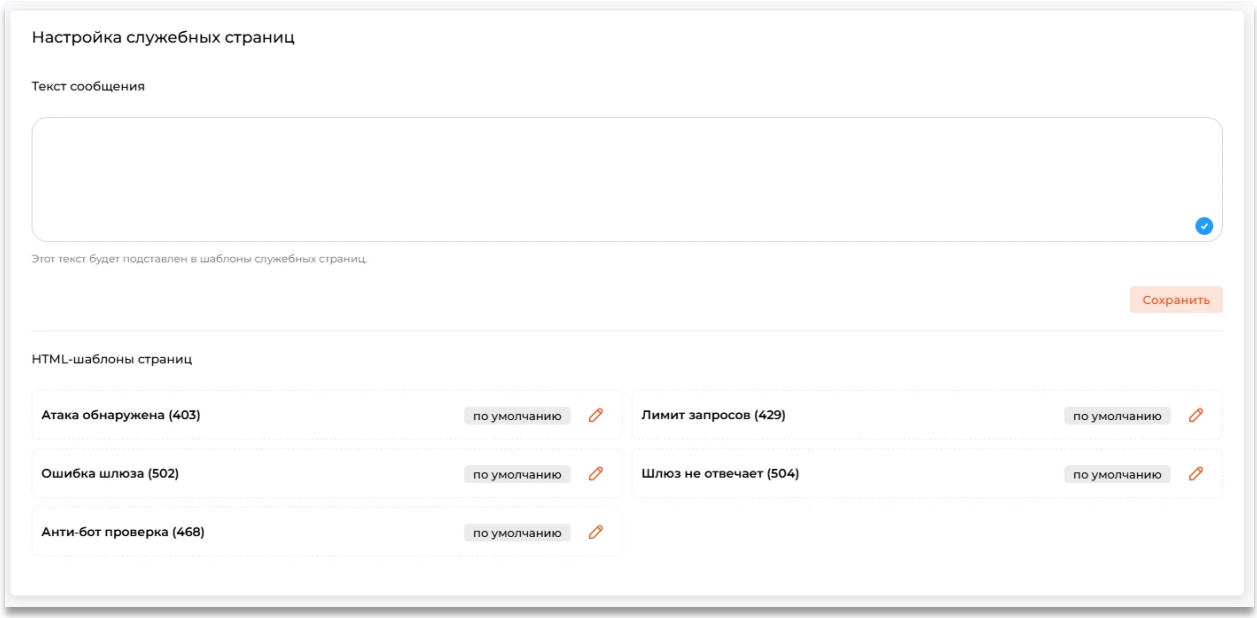
В шаблонах доступны переменные:

{{REQUEST_ID}} — уникальный идентификатор заблокированного запроса

{{SERVER_ID}} — идентификатор узла, вернувшего страницу

{{MESSAGE}} — универсальный текст, который Вы задаёте в поле «Текст сообщения» и используете в любом шаблоне

Рекомендация: рекомендуется держать страницы минималистичными, без внешних скриптов и трекеров, с директивой noindex, nofollow, и обязательно отображать REQUEST_ID для ускорения расследований инцидентов.

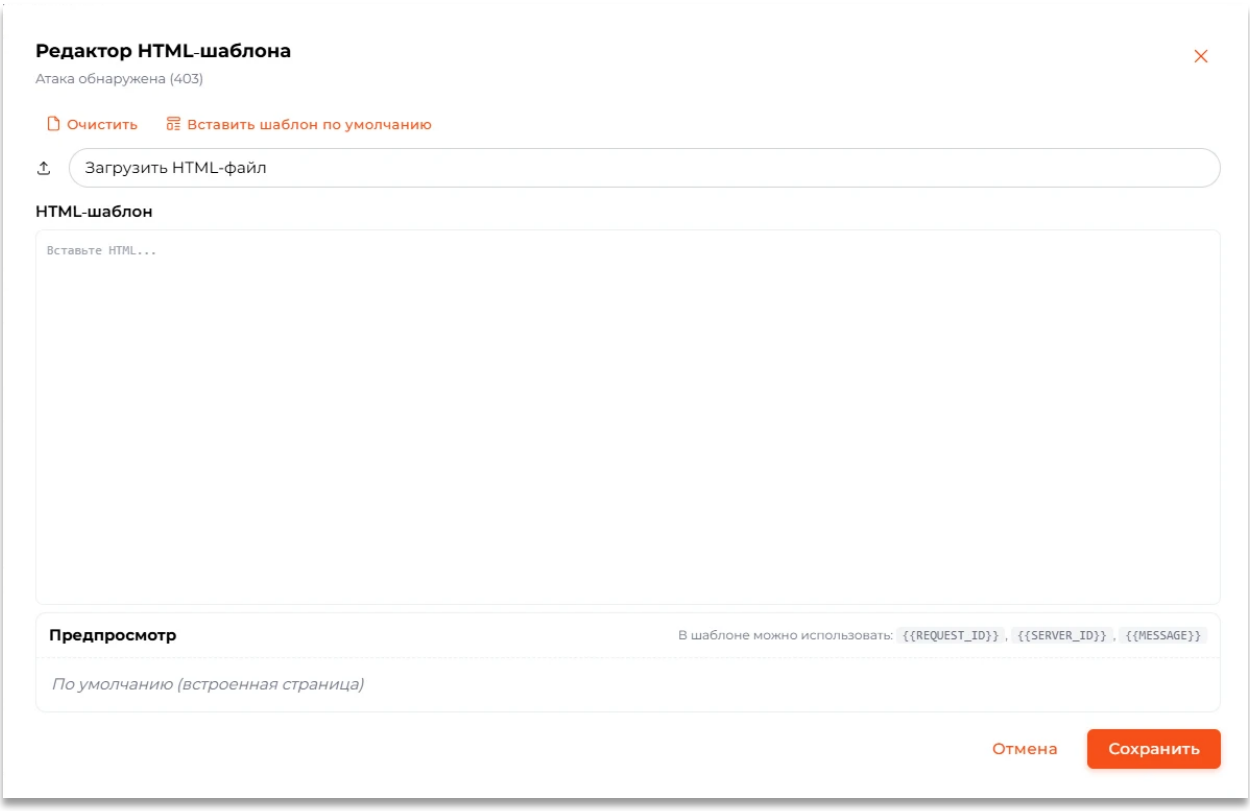


2.2.1 Порядок настройки

Для формирования единого сообщения введите текст в поле «Текст сообщения». Этот текст будет автоматически подставляться в выбранные Вами HTML-шаблоны через переменную {{MESSAGE}}. Нажмите «Сохранить», чтобы зафиксировать изменения.

Для редактирования конкретной служебной страницы откройте соответствующий шаблон через иконку редактирования. В появившемся редакторе доступны операции:

1. «Вставить шаблон по умолчанию» — загрузить базовый, безопасный макет
2. «Загрузить HTML-файл» — импортировать собственный файл
3. «Очистить» — начать с пустого поля
4. «Сохранить» — применить изменения

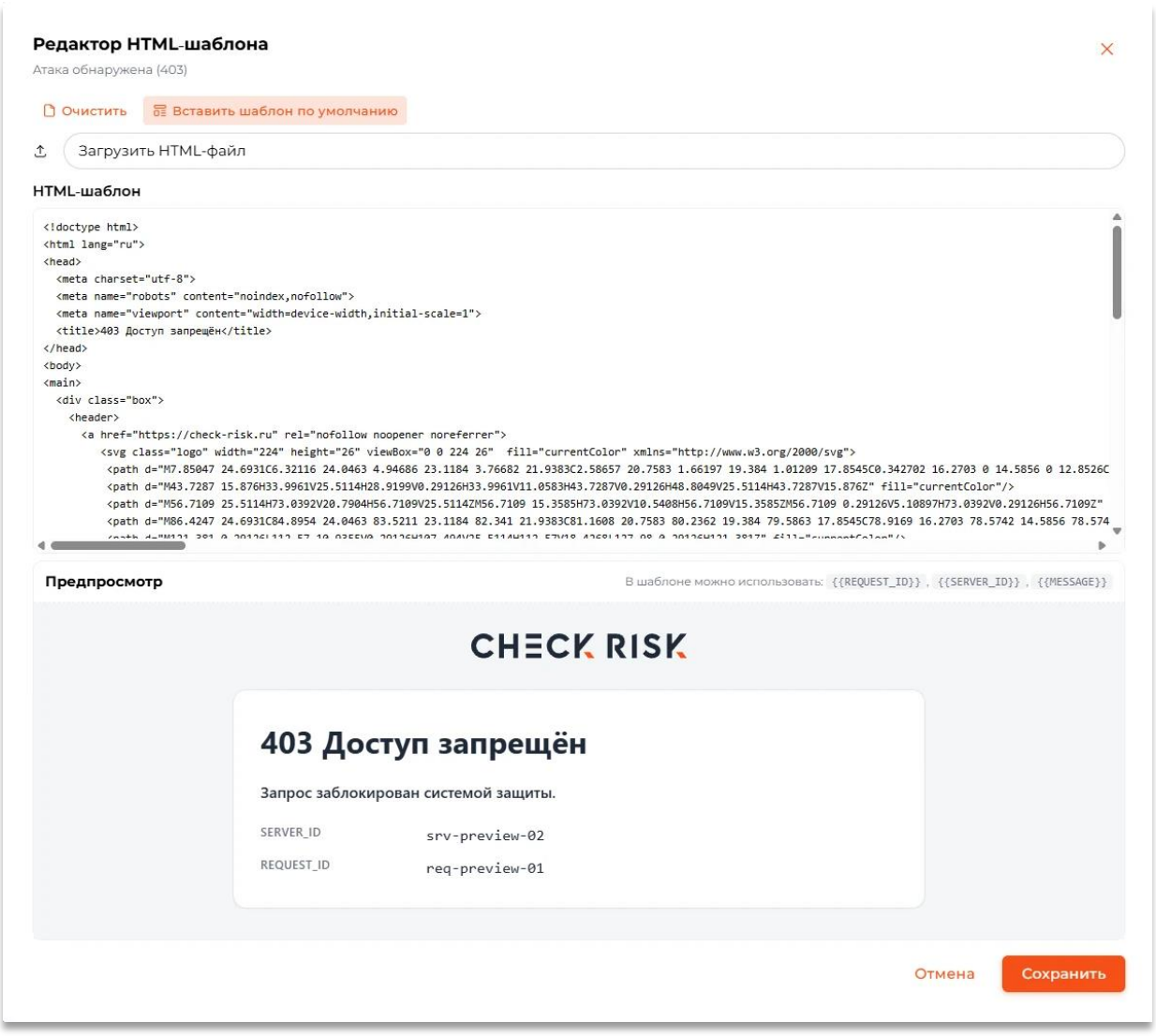


Ниже приведён минимальный пример безопасного HTML кода для страницы блокировки. Используйте его как основу и адаптируйте под фирменный стиль. Внутренние стили предпочтительнее внешних подключений.

```
<!doctype html>
<html lang="ru">
<head>
    <meta charset="utf-8">
    <meta name="robots" content="noindex,nofollow">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Доступ ограничен</title>
    <style>
        body {margin: 0; font-family: system-ui, -apple-system, Segoe UI, Roboto, Arial, sans-serif; background: #f6f7f9}
        .box {max-width: 760px; margin: 8vh auto; background: #fff; padding: 32px; border-radius: 12px; box-shadow: 0 4px 20px rgba(0,0,0,.06)}
        h1 {margin:0 0 12px}
        .kvs {display: grid; grid-template-columns: 140px 1fr; gap: 6px 16px; margin-top: 16px; font-size:14px; color: #555}
        .muted {color: #666; margin: 6px 0 0}
    </style>
</head>
<body>
    <main class="box">
        <h1>Доступ ограничен</h1>
        <p class="muted">{{MESSAGE}}</p>
        <div class="kvs">
            <div>SERVER_ID</div><div>{{SERVER_ID}}</div>
            <div>REQUEST_ID</div><div>{{REQUEST_ID}}</div>
```

```
        </div>
    </main>
</body>
</html>
```

Используйте предпросмотр внизу окна редактора, чтобы мгновенно проверить итоговый вид страницы без выполнения запроса к защищаемому ресурсу.



2.2.2 Рекомендации по содержанию и защите:

✓ Не включать на страницы внешние скрипты, пиксели и виджеты, которые могут нарушить политику безопасности или замедлить отдачу

✓ Не раскрывать подробные версии ПО, внутренние доменные имена и прочие элементы, повышающие риск атак

✓ Сохранять единообразный текст для всех шаблонов через {{MESSAGE}}, а в заголовке страницы явно указывать причину блокировки

✓ Поддерживать доступность: понятные заголовки, контрастный текст, читаемые сообщения об ошибке

Для возврата к безопасной базе используйте «Вставить шаблон по умолчанию». Хранение и публикация шаблонов выполняются на стороне WAF; приложение не участвует в отдаче страницы, что исключает утечки из бэкенда.

Кастомные служебные страницы повышают прозрачность защиты и уменьшают нагрузку на поддержку. Зафиксируйте единый текст через {{MESSAGE}}, включите REQUEST_ID и SERVER_ID для быстрого трейсинга, держите вёрстку лёгкой и автономной. При изменениях актуализируйте шаблоны для всех соответствующих кодов, чтобы пользователи всегда получали предсказуемое и информативное сообщение.

2.3 Анти DDOS

В данном разделе представлена функциональность защиты от распределённых атак DDOS на уровне приложений (L7: HTTP/HTTPS). Цель защиты — автоматически выявлять и подавлять аномальные шаблоны запросов, перегружающих веб-приложение, без вмешательства со стороны пользователя. Механизмы включают адаптивные лимиты запросов, поведенческую аналитику, динамические челленджи и блокировку источников.

> ! Функция активна для всех клиентов по умолчанию. отключение не предусмотрено политикой сервиса. Ваша зона ответственности — корректно подключить приложение к WAF, контролировать телеметрию и при необходимости задавать исключения (allowlist) для доверенных источников.

Система работает в автоматическом режиме, но необходим мониторинг работы системы с размещенным приложением. Доступны следующие элементы мониторинга:

Графики нагрузки. Показаны QPS/ RPS по времени, доля отклонённых запросов, пики по URI, методам и кодам ответа. Рекомендуется сверять пики с окнами деградации на стороне бэкенда.

Источники атаки. Агрегируются топ IP, подсети и ASN, а также страны и автономные системы. Для каждого источника указывается применённая реакция.

Журнал решений. Фиксируются детектированные сигнатуры и эвристики: всплески по не кешируемым URI, попытки обхода кэша, аномальный User-Agent, невалидные токены, частые 4xx/5xx, «burst»-паттерны и замедленные соединения.

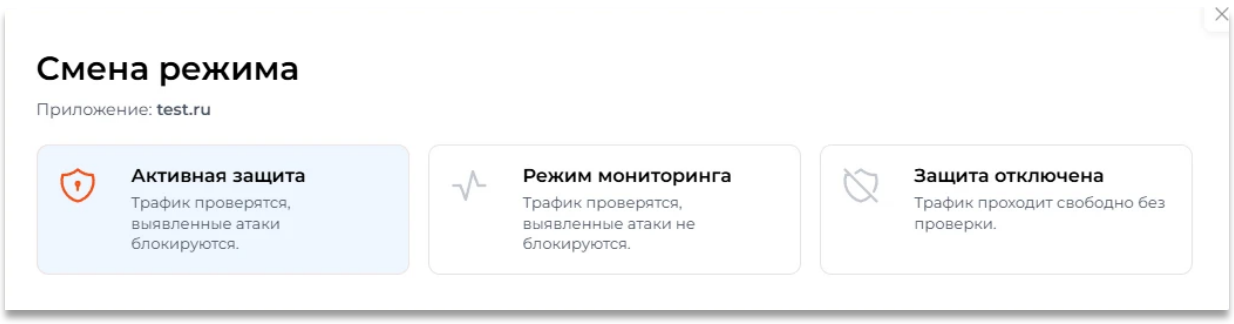
> **Примечание:** в случае если происходит блокировка "чистого" трафика, необходимо добавить исключения для пропуска доверенного трафика. Доступно добавление безопасных источников по IP/подсети/ASN, а также по путям и методам. Исключения применяются моментально и приоритетнее автоматических правил. Используйте ТОЛЬКО при полной уверенности в

Защита L7 включена и работает постоянно, настройка выключения недоступна. Ваша задача — обеспечить корректное подключение приложений к WAF, отслеживать телеметрию и аккуратно управлять исключениями. При признаках деградации производительности на стороне бэкенда сопоставьте временные окна с журналом решений и графиками нагрузки. При сохранении проблемы создайте тикет в службу поддержки с указанием домена, интервала времени и примеров запросов.

> **Примечание:** настройка в рамках описанных процедур обеспечивает устойчивость к прикладным DDoS без нарушения доступности легитимного трафика.

2.4 Режимы работы

В данном разделе описаны режимы работы WAF в составе сервиса и их влияние на обработку L7-трафика приложений. Режим определяет политику реагирования на обнаруженные события безопасности и порядок фиксации телеметрии.



2.4.1 Доступные режимы

Защита: запросы анализируются в реальном времени, вредоносные действия блокируются согласно активным политикам. Все срабатывания и параметры запроса фиксируются в журналах.

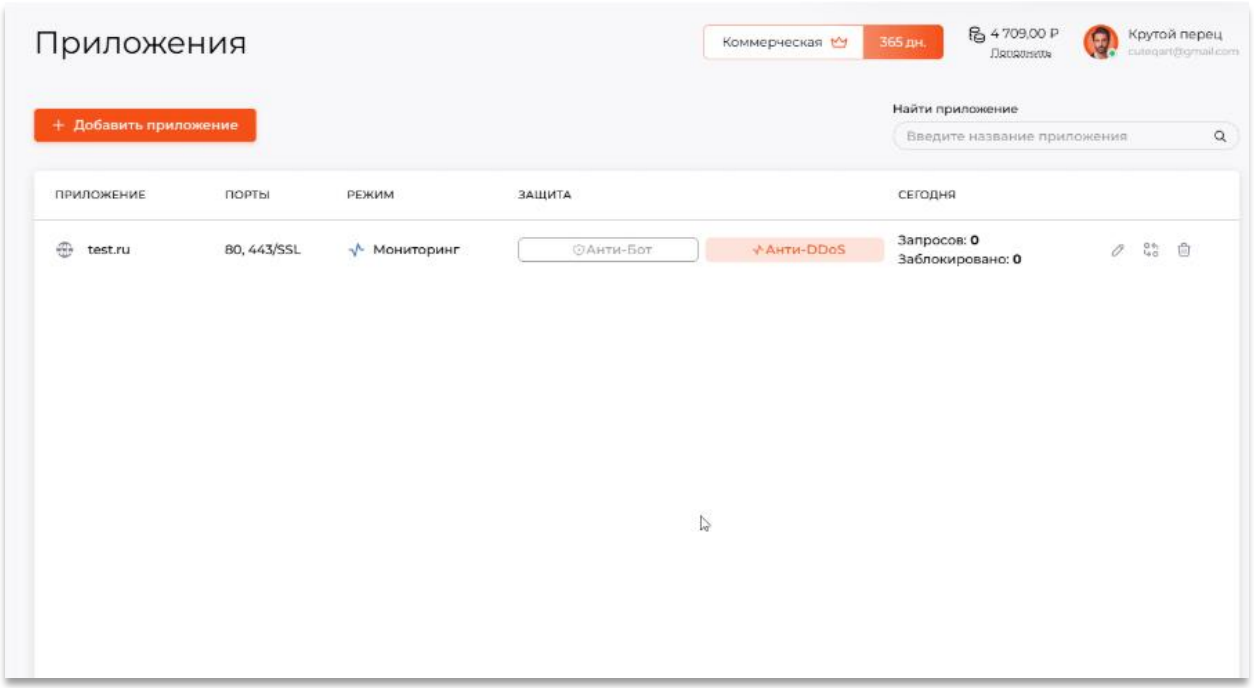
Мониторинг: запросы проходят без блокировки, но полностью анализируются. Срабатывания правил сохраняются в журналах и доступны в разделе событий. Режим предназначен для безопасной обкатки правил и исключений.

Отключен: анализ и реагирование WAF не выполняются. Запросы передаются бэкенду без проверки; журналы WAF по приложению не пополняются. Используется только при отладке инцидентов и кратковременных технических работах.

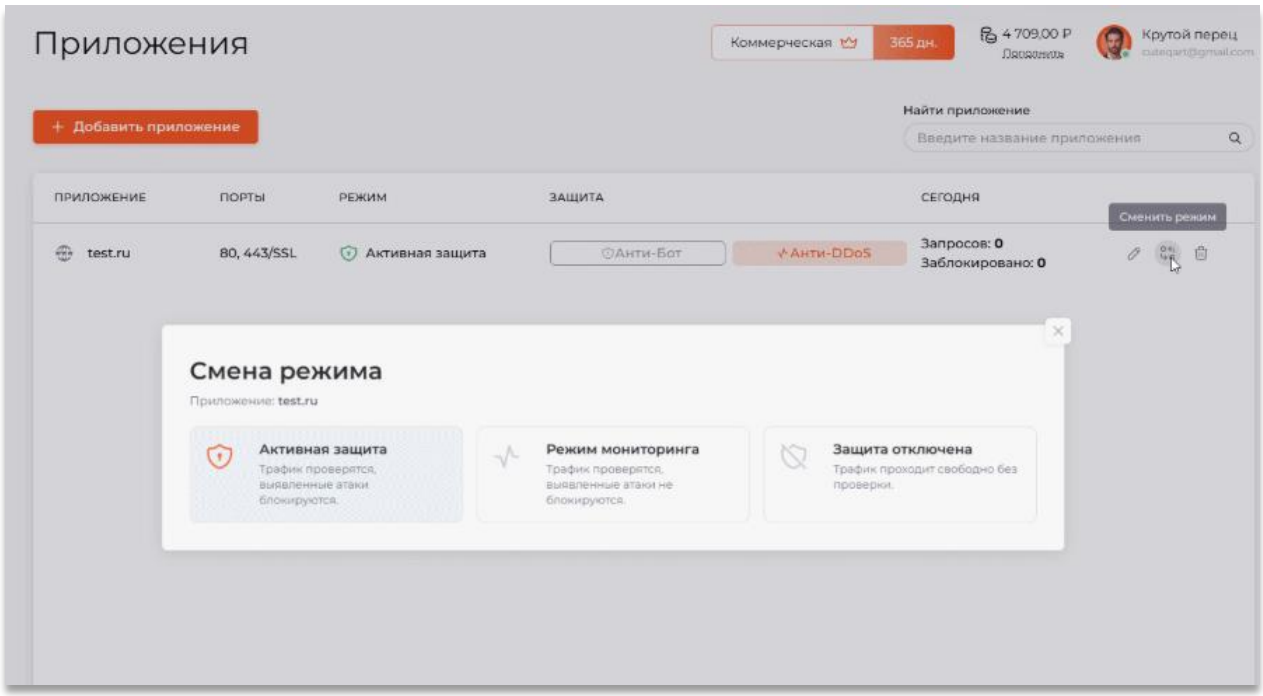
> **Примечание:** управление модулями «Анти-бот» и «Анти-DDoS» выполняется отдельно от переключения режима WAF.

Для изменения режима необходимо, чтобы приложение было добавлено в систему. Переключение осуществляется в разделе перечня приложений.

Для переключения режима необходимо выполнить следующие действия:



1. Откройте раздел с перечнем приложений. Найдите нужное приложение в таблице.
2. В панели управления приложением нажмите на кнопку «Сменить режим». В появившемся окне изменения режиме, выберете необходимый Вам режим защиты: «Защита», «Мониторинг» или «Отключен».



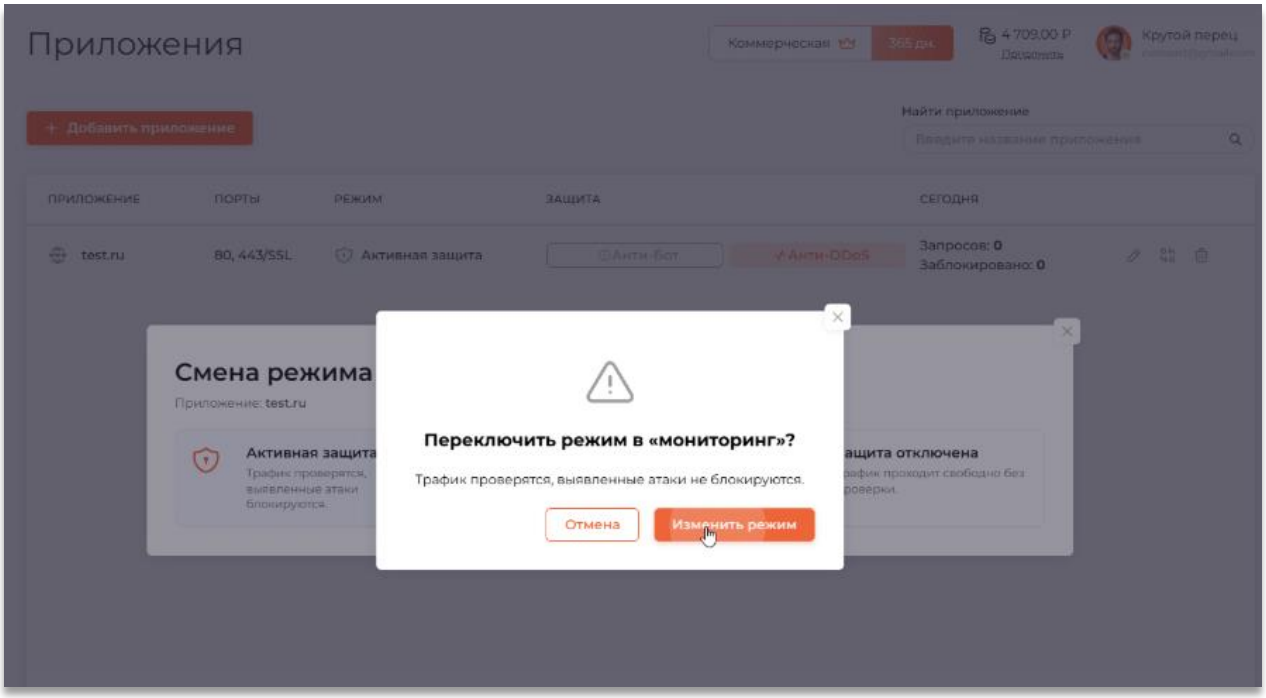
3. Подтвердите применение. Через короткое время новый режим отобразится в интерфейсе, а события начнут фиксироваться в соответствии с выбранной политикой.

2.4.2 Рекомендуемые практики при переключении

- ✓ Перед вводом в боевой контур используйте «Мониторинг» для оценки ложных срабатываний, настройки исключений и верификации маршрутов.
- ✓ После валидации политик переводите приложение в «Защита» для блокирования атак и активного реагирования.
- ✓ Режим «Отключен» применяйте только точечно и на минимальное время; по завершении работ возвращайте «Защита» или «Мониторинг».

> **Примечание:** убедитесь, что в карточке приложения обновился индикатор режима и началось появление событий телеметрии.

> **Примечание:** проверьте в журнале событий появление записей в соответствии с выбранным режимом.



Корректный выбор режима позволяет сбалансировать доступность и безопасность. «Мониторинг» снижает риск ложных блокировок при внедрении, «Защита» обеспечивает немедленное пресечение атак, «Отключен» допустим исключительно как временная мера. После каждого переключения проверяйте

журналы и метрики приложения, чтобы подтвердить ожидаемое поведение трафика.

2.5 Проверка работы WAF

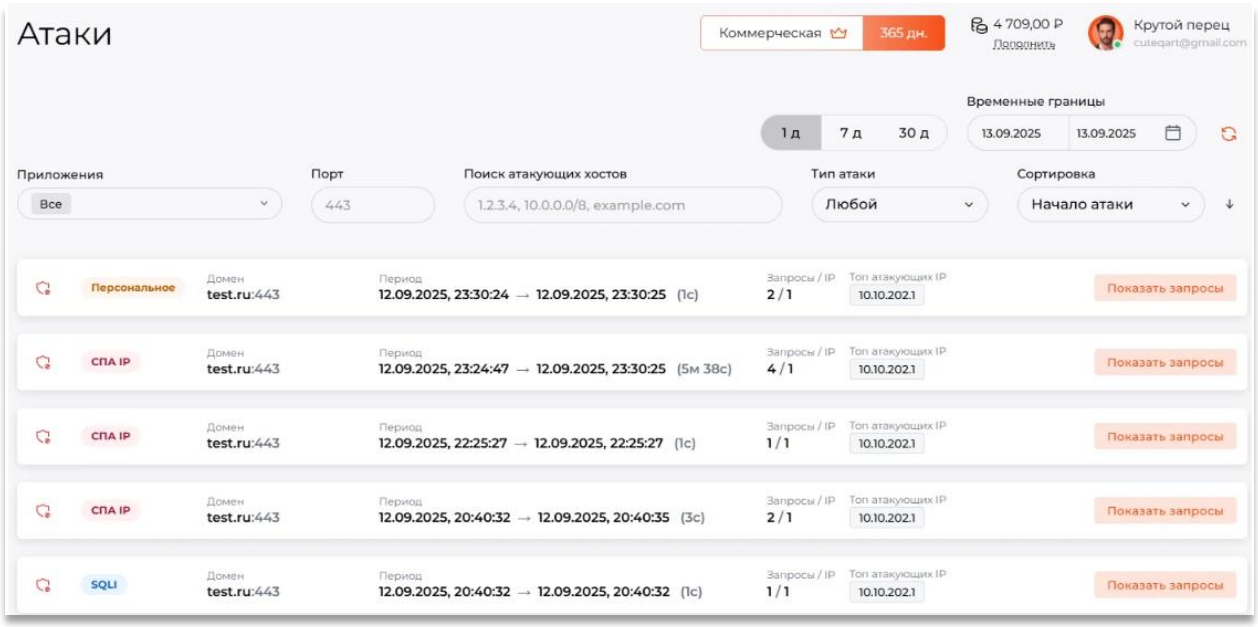
В данном разделе представлена инструкция проверки работоспособности WAF, которая позволит провести тестирование работоспособности после внедрения. Цель проведение проверки — быстрое подтверждение прохождения трафика через WAF, правила срабатывают корректно, а метрики и журналы фиксируют события.

> **Внимание:** перед началом тестирования убедитесь, что домен добавлен и активен, политика назначена, сертификат привязан.

Тестирование работоспособности системы и активной защиты происходит в 7 этапов:

Цель проверки	Как выполнить	Ожидаемый результат
Приложение под защитой	Откройте карточку приложения и проверьте статусы: Активно, WAF включен, режим политики Блокирование или Мониторинг	Статусы отображаются корректно, приложение связано с нужной политикой
Трафик проходит через WAF	`curl -I https://ВАШ_ДОМЕН/`	В ответе присутствуют характерные заголовки WAF или CDN, реальный IP бэкенда не раскрывается
XSS (базовый)	`curl -I "https://ВАШ_ДОМЕН/?q=<script>alert(1)</script>"`	В Блокирование код 403 или страница блокировки с Request ID, в Мониторинг успешный ответ и запись события в журналах
SQLi (базовый)	`curl -I "https://ВАШ_ДОМЕН/?id=' OR 1=1--"`	Блокировка или запись события с категорией SQLi, фиксируется параметр `id`
Path Traversal	`curl -I "https://ВАШ_ДОМЕН/download?file=../../etc/passwd"`	Блокировка или запись события с категорией Path Traversal, фиксируется параметр `file`
Сигнатуры инструментов	`curl -I -H "User-Agent: sqlmap/1.7" "https://ВАШ_ДОМЕН/"`	Блокировка или логирование запроса как автоматизированного клиента при включенной защите от ботов
Дашборд отражает тесты	Обновите дашборд, установите диапазон времени, часовую зону и фильтр по приложению	Счетчики Заблокировано, Обнаружено и связанные графики отражают проведенные тесты

Корректная работа WAF подтверждается возвратом кода ответа 403 или страницей блокировки с Request ID для атакующих запросов в режиме



Рекомендуется сохранить Request ID и время каждого теста для последующей корреляции и регрессионных проверок после релизов и изменения политик.

Блокирование, а также появлением соответствующих записей в журналах и изменением метрик на дашборде.

2.6 Добавление SSL сертификата

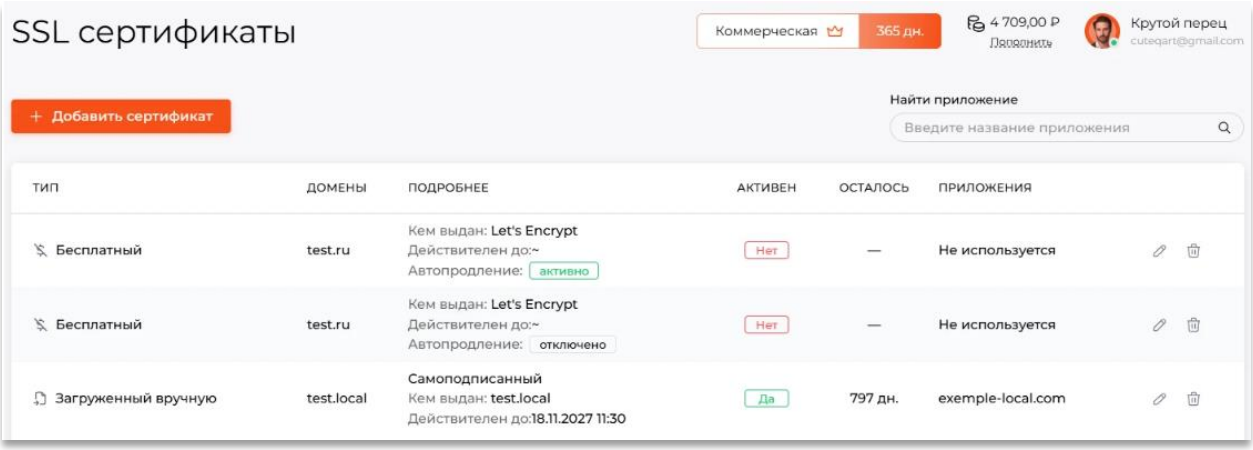
В данном разделе выполняется загрузка и хранение пар ключей SSL шифрования трафика между Вашими пользователями и приложениями, защищаемыми WAF. Поддерживается добавление сертификата и соответствующего приватного ключа из отдельных файлов в форматах .crt и .key. Функциональность предназначена для размещения собственных валидных сертификатов, для использования в настройках приложений.

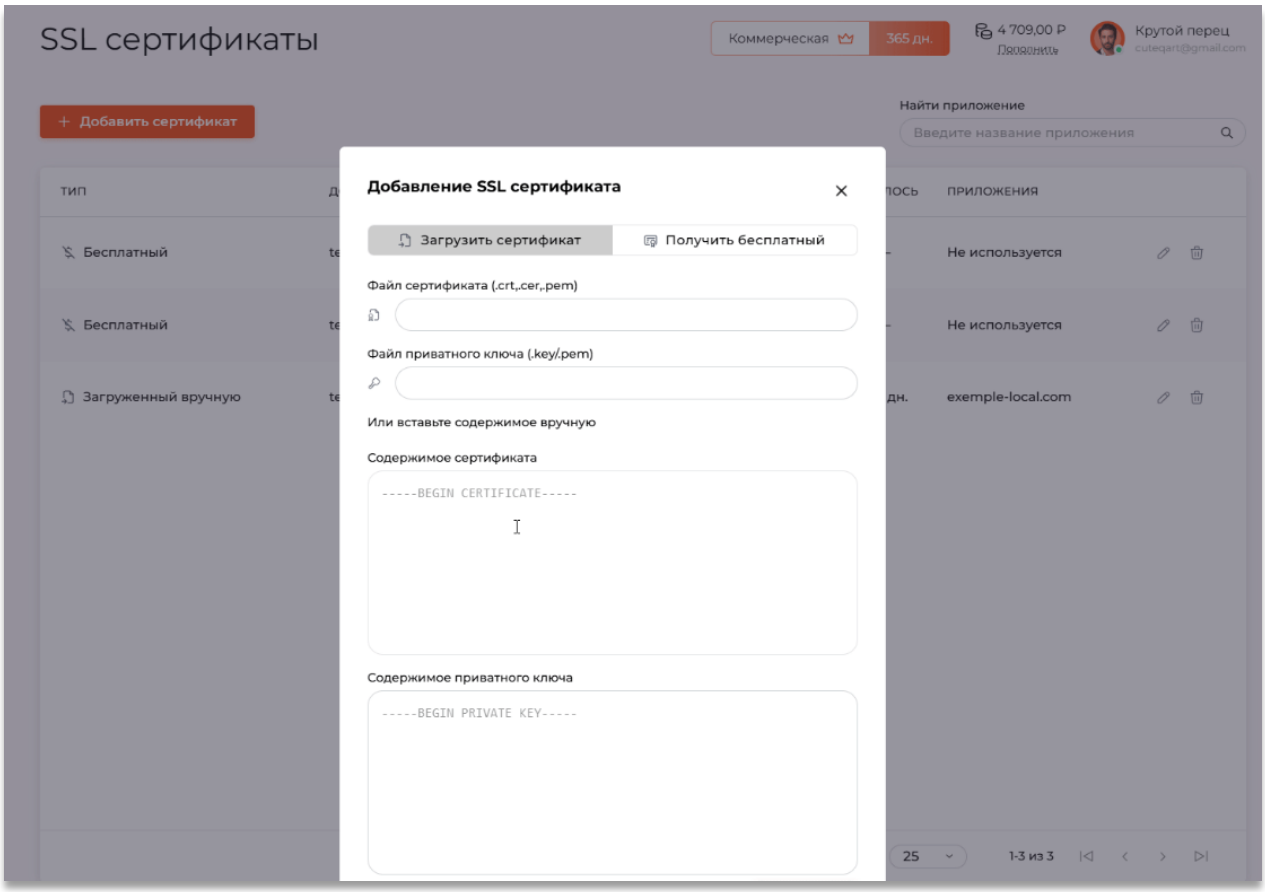
Порядок добавления

1. Для добавления сертификата нажмите в верхнем меню раздела кнопку «Добавить сертификат».
2. В открывшемся окне «Добавление SSL сертификата» доступна вкладка «Загрузить сертификат».
3. После заполнения полей нажмите «Добавить». Сертификат появится в перечне и станет доступен для привязки к необходимым доменам приложений.

- ✓ «SSL сертификат». Вставьте содержимое файла сертификата в кодировке PEM или воспользуйтесь кнопкой «Получить SSL сертификат из файла» и укажите файл с расширением .crt. Допустимо размещение полной цепочки: конечный сертификат, затем промежуточные центры сертификации.
- ✓ «Приватный ключ». Вставьте содержимое приватного ключа в формате PEM или воспользуйтесь кнопкой «Получить приватный ключ из файла» и укажите файл с расширением .key. Ключ должен соответствовать загружаемому сертификату по паре ключей и быть без парольной фразы, поскольку поле для ввода пароля не предусмотрено.

Примечание: вкладка «Получить сертификат» предназначена для альтернативного получения сертификата внутри системы. Используйте ее при наличии соответствующих регламентов и только для задач, где это допустимо политикой безопасности Вашей организации.





Рекомендация: проверяйте соответствие доменных имен в поле CN/SAN параметрам приложения и включать цепочку промежуточных сертификатов для корректной валидации клиентами. Перед загрузкой убедитесь, что используете актуальные криптографические параметры и что приватный ключ сформирован для того же алгоритма, что и сертификат.

2.7 Требования к квалификации сотрудников

В данном разделе устанавливаются минимальные требования к квалификации сотрудников, которым предоставляется доступ к функциональности WAF SaaS и к операциям сопровождения. Цель — обеспечить безопасную эксплуатацию сервиса, корректную настройку политик, своевременное реагирование на инциденты и соблюдение регуляторных требований. Ответственность за соответствие требованиям несут руководитель подразделения информационной безопасности и владельцы приложений, использующих защиту WAF.

2.7.1 Администратор безопасности WAF

- ✓ Глубокое понимание сетевой и веб-модели: L3–L7, HTTP/1.1–3, TLS 1.2/1.3
- ✓ Настройка и валидация правил/исключений WAF, управление режимами block/challenge/log
- ✓ Интеграция журналов с SIEM, знание форматов JSON/CEF и ретенции

2.7.2 Аналитик WAF (оператор мониторинга)

- ✓ Тестирование влияния политик на доступность и производительность
- ✓ Аналитик WAF (оператор мониторинга)
- ✓ Триаж событий и классификация FP/TP по серьёзности
- ✓ Построение выборок и отчётов, владение запросами к журналам
- ✓ Идентификация атак по сигнатурам и поведенческим индикаторам
- ✓ Оформление обоснованных заявок на исключения
- ✓ Контроль метрик качества: блок-рейт, FP-рейт, латентность

2.7.3 Оператор реагирования на инциденты

- ✓ Оператор реагирования на инциденты
- ✓ Применение временных мер: challenge, rate limit, точечное блокирование
- ✓ Активирование DDoS-профилей и режимов деградации без простоя
- ✓ Эскалация по матрице, взаимодействие с владельцами сервисов
- ✓ Быстрый откат конфигурации и возврат к стабильному состоянию

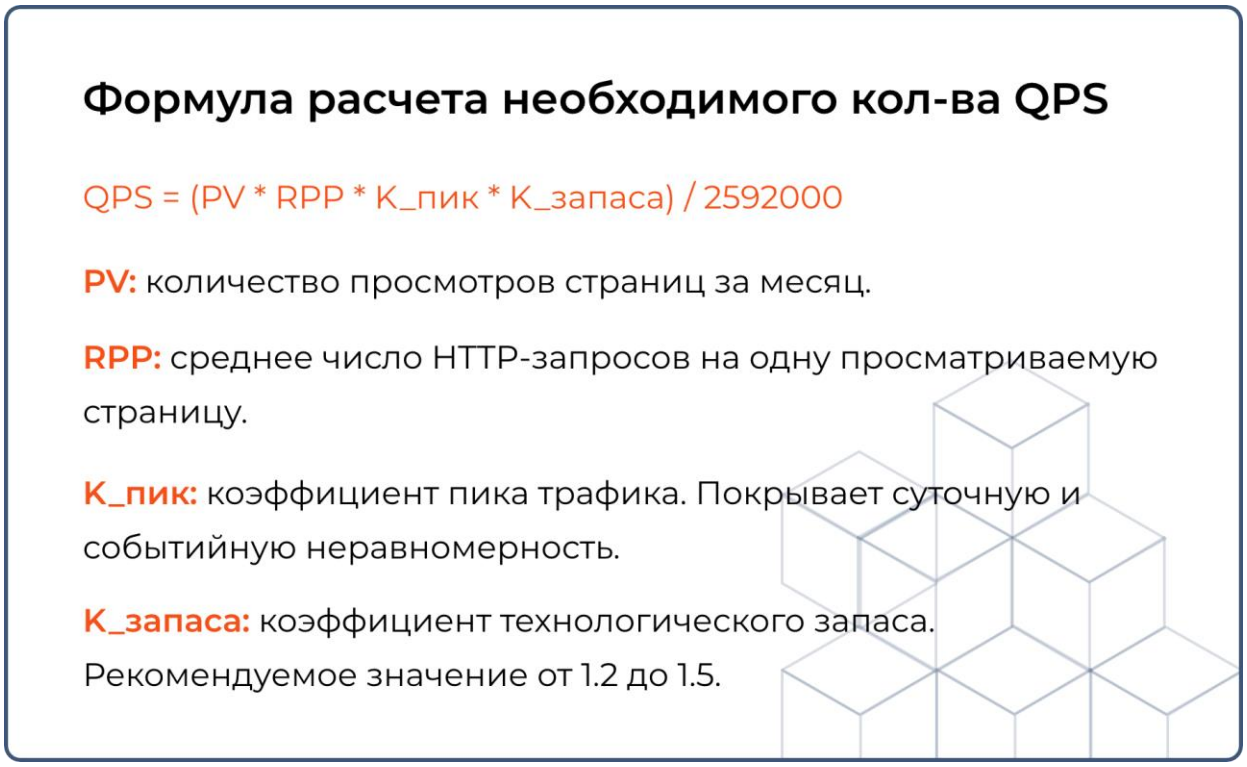
2.7.4 Аудитор/наблюдатель

- ✓ Аудитор/наблюдатель
- ✓ Формирование доказательной базы по контролям ИБ
- ✓ Проверка соответствия прав принципу наименьших привилегий
- ✓ Оценка полноты/целостности/ретенции журналов
- ✓ Подготовка отчётности для внутренних и внешних проверок
- ✓ Знание применимых регуляторных требований и корпоративных политик

В данном разделе фиксируются критерии допуска и поддержания квалификации. Рекомендуется проводить переаттестацию не реже одного раза в 12 месяцев либо после существенных изменений в политиках или архитектуре защиты.

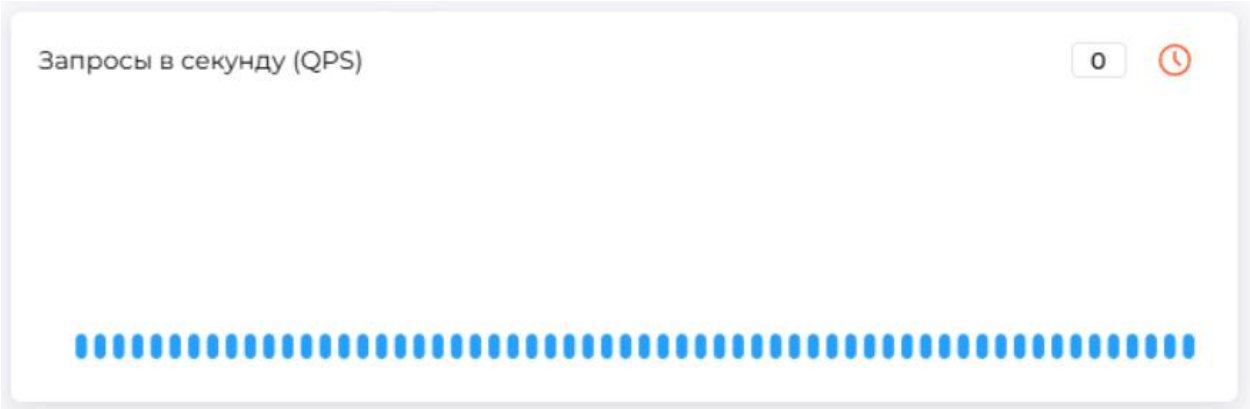
2.8 Расчет количества QPS

В данном разделе описан порядок определения требуемой квоты QPS для WAF SaaS. QPS интерпретируется как количество HTTP(S) запросов в секунду, которые подсистемы фильтрации обязаны обрабатывать без деградации времени отклика и качества защиты. Корректный расчет QPS позволяет выбрать тариф, предотвратить ложные ограничения на пике трафика и обеспечить запас на всплески, ботов и технические операции.



Фактическую нагрузку на приложение Вы можете просмотреть в разделе "Сводка" в разделе "Запросы в секунду (QPS)".

Примечание: при получении данных выполняются нормализация форматов, дедупликация, назначение приоритетов источникам и оценка надежности данных. Это позволяет уменьшить количество ложных срабатываний и обеспечить предсказуемое применение политик.



Важные уточнения:

- ✓ RPP зависит от архитектуры фронтенда, наличия SPA, степени бандлинга, кэширования на уровне CDN и браузера, а также от того, где именно включен WAF относительно цепочки доставки.
- ✓ Доля ботов и сканеров может увеличивать нагрузку. Если аналитика очищена от ботов, закладывайте дополнительный запас.
- ✓ Для API-сервисов удобнее оперировать RPM и 95-м процентилем RPS из логов, далее применять K_запаса и округлить.

2.9 Обновление фидов

В данном разделе описываются принцип механизма обновления фидов угроз в WAF SaaS в автоматическом режиме без участия пользователя. Цель модуля состоит в поддержании актуальной модели рисков для блокировки и ограничивания вредоносной активности. Система автоматически и регулярно получает индикаторы компрометации из множества бесплатных и коммерческих источников, а также обогащает их собственными данными о текущих атаках. Поддерживаются типовые артефакты угроз: IP-адреса и подсети, домены и URL, сигнатуры ботов и сканеров, C2, характеристики клиентских отпечатков, паттерны запросов приложения.

> **Примечание:** при получении данных выполняются нормализация форматов, дедупликация, назначение приоритетов источникам и оценка надежности данных. Это позволяет уменьшить количество ложных срабатываний и обеспечить предсказуемое применение политик.

2.9.1 Системы автоматического на основе фидов

СПА (Система Предотвращения Атак) IP: данная система представляет собой агрегированную само обновляющуюся базу вредоносных и опасных IP адресов, которая обновляется каждую минуту. Блокировка угроз происходит в автоматическом режиме.

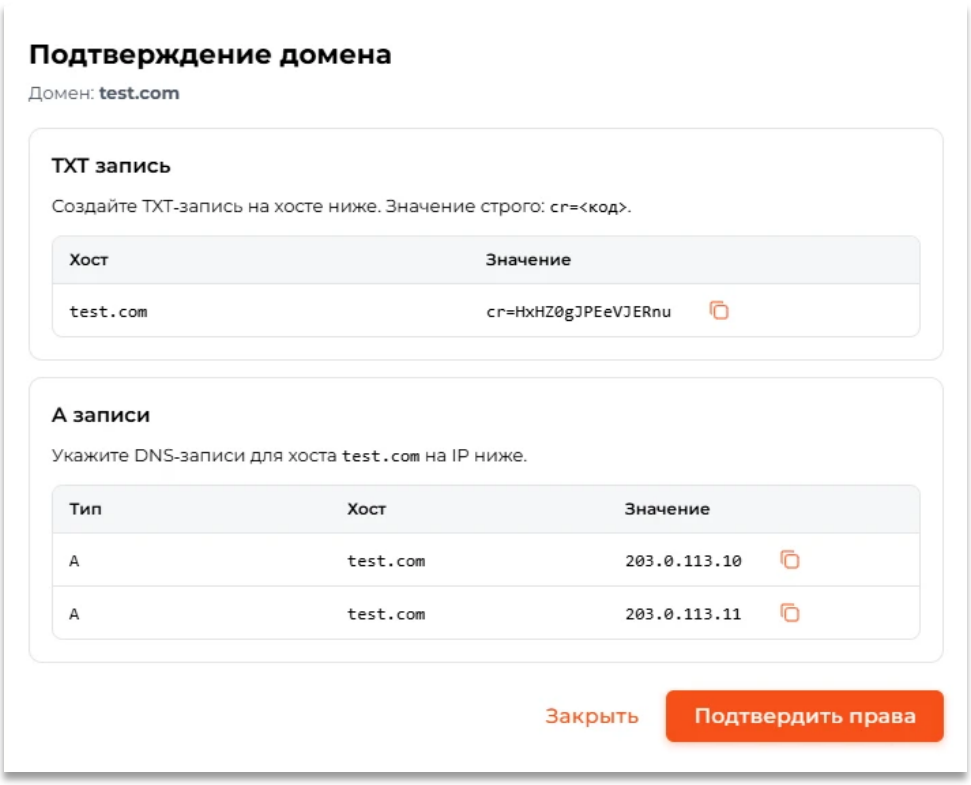
СПА (Система Предотвращения Атак) User Agent: данная система представляет собой агрегированную само обновляющуюся базу вредоносных и опасных User Agent приложений, которая обновляется каждую минуту. Блокировка угроз происходит в автоматическом режиме.

> **Примечание:** если вам по какой-либо причине необходимо предоставить доступ до вашего приложения IP адреса или User Agent приложения, которое блокирует СПА, то вам необходимо создать разрешительное правило.

В результате эксплуатации данного механизма Вы получаете непрерывно актуализируемый набор индикаторов угроз, объединяющий данные внешних провайдеров и внутреннюю телеметрию атак.

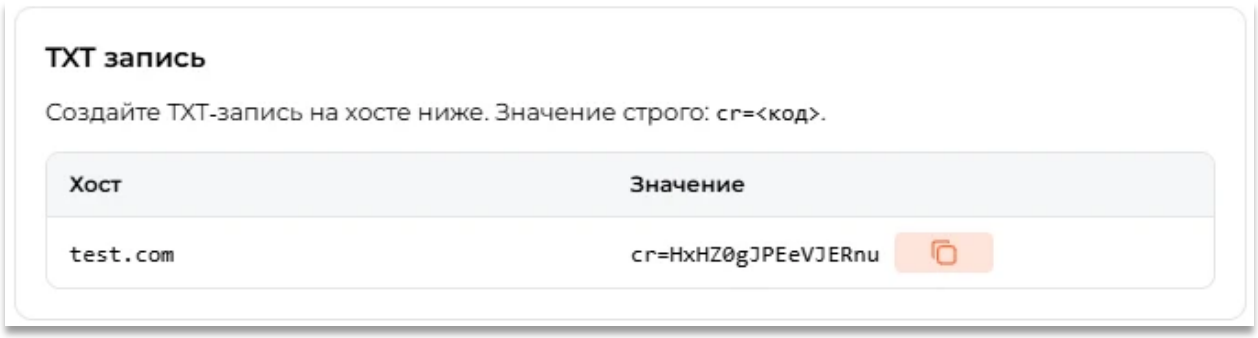
2.10 Верификация приложения

В данном разделе описывается порядок подтверждения прав на домен для добавления веб-приложения в WAF SaaS. Подтверждение выполняется посредством размещения TXT-записи в DNS с точным значением формата cr=<key-16>. Процедура проводится однократно для корневого домена. Поддомены любого уровня подтверждать не требуется: после успешной верификации домена добавление приложений на его поддоменах доступно без дополнительных проверок.



2.10.1 Порядок подтверждения прав

Перед настройкой приложения, необходимо провести проверку приложения для подтверждения доступа. Для подтверждения нажмите на кнопку в верхнем меню «Добавить приложение». В открывшемся заполните URL адрес сайта, после в окне отобразится уникальный ключ в формате cr=<key-16>. Скопируйте значение без изменений и следуйте шагам ниже.



- ✓ Откройте панель управления DNS у Вашего регистратора или провайдера хостинга.
- ✓ В зоне проверяемого домена создайте новую запись типа TXT. Имя записи оставьте пустым или укажите символ @ (это соответствует корневому домену).

- ✓ В поле значения вставьте строку, полученную в окне добавления приложения. Пример корректного значения. Пример: cr=9f1a2b3c4d5e6f70

> **Внимание:** некоторые панели требуют обрамлять значение двойными кавычками.

- ✓ Сохраните запись. Дождитесь распространения изменений в DNS. Время зависит от TTL и политики провайдера.
- ✓ После успешной проверки статус домена изменится на «Подтверждено».
- ✓ После успешной верификации домена Вы можете завершить добавление приложения и переходить к следующим этапам внедрения WAF SaaS:
- ✓ Для перенаправления трафика под WAF Вам необходимо по аналогии с инструкцией разместить в "A" запись IP адрес(а) для добавленного приложения (домен/поддомен).

После переключения трафика Вы можете перейти к настройке политик защиты, привил и настроек безопасности.1

> **Внимание:** если проверка не проходит, проверьте точность значения, видимость TXT-записи с внешних DNS-резолверов и дождитесь полного обновления кэшей, затем повторите попытку.

2.11 Генерация SSL сертификата

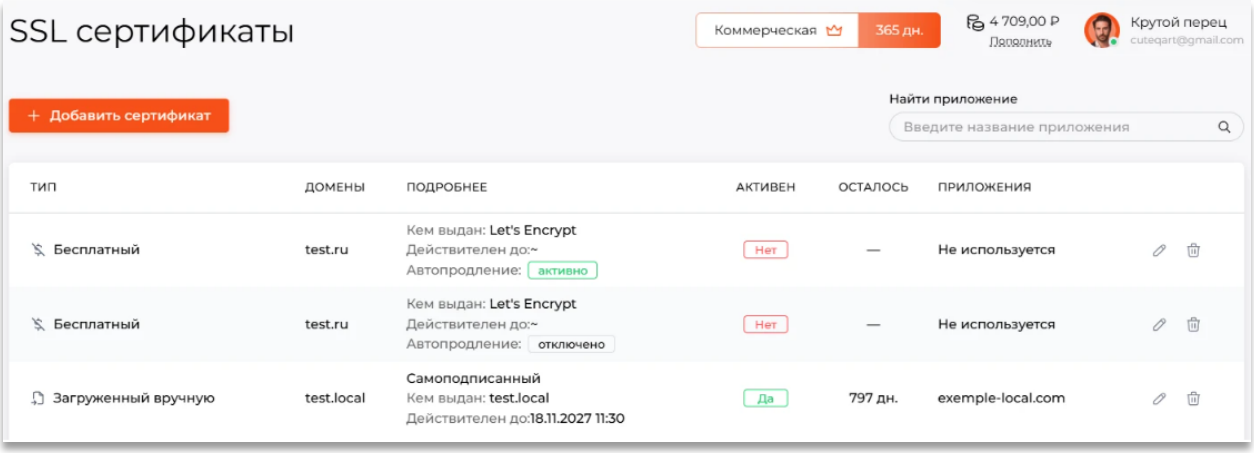
В данном разделе описывается получение бесплатного доверенного SSL-сертификата от Let's Encrypt для доменного имени, по которому публикуется Ваше приложение за WAF SaaS. Сертификат выпускается на основании

указанного доменного имени и после успешной проверки владения доменом появляется в реестре сертификатов автоматически. Срок действия выпускаемого сертификата составляет 30 дней.

Таки же присутствует возможность активировать последующее продление SSL сертификата, которое выполняется в автоматическом режиме за 3 дня до окончания действия SSL сертификата. Замена сертификата в конфигураторе приложения происходит автоматически.

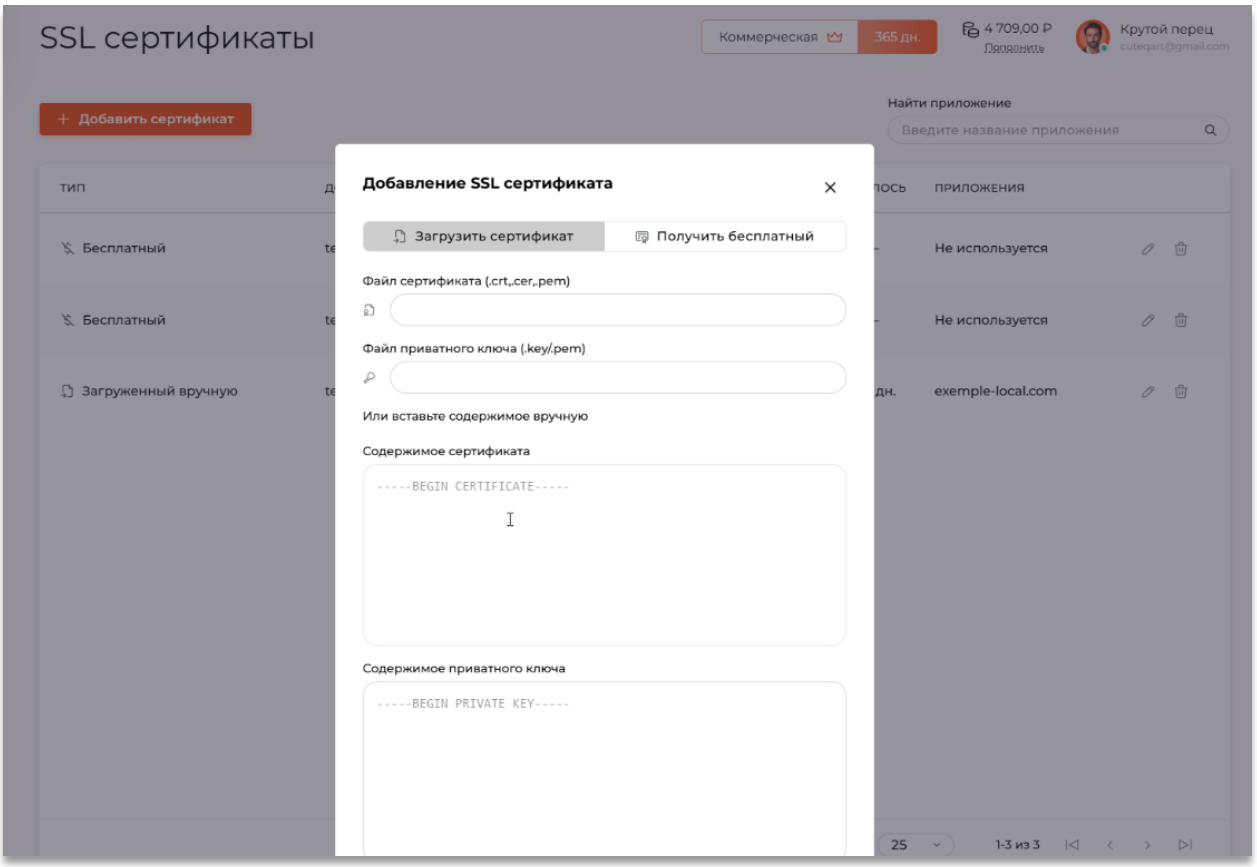
2.11.1 Порядок генерации

Для запуска выпуска сертификата необходимо воспользоваться интерфейсом раздела «SSL сертификаты».2.12 Добавление приложения



Выполните следующие действия в рабочем окне:

- ✓ Нажмите кнопку «Добавить сертификат» в верхнем меню.
- ✓ В открывшемся окне «Добавление SSL сертификата» выберите режим «Получить сертификат».
- ✓ Укажите доменное имя в поле «Домен» в формате FQDN, без протокола и пути, например: app.example.com.
- ✓ Нажмите «Добавить» для получения сертификата.



После отправки запроса сервис автоматически инициирует процедуру проверки владения доменом и выпуска сертификата. При успешном завершении операции в таблице появится новая запись. В списке отображаются ключевые поля: «Тип», «Домены», «Подробнее» (издатель и сроки действия), «Приложения». Для контроля статуса и параметров сертификата используйте ссылку в колонке «Подробнее».

Примечание: срок действия сертификата, выпущенного через данный механизм, равен 30 дням. Система инициирует продление заблаговременно, без участия пользователя.

В результате выполнения описанных действий Вы получаете действующий SSL-сертификат Let’s Encrypt сроком на 30 дней, автоматически добавленный в реестр сертификатов и готовый к назначению приложениям.

Рекомендация: периодически проверяйте блок «Подробнее» для контроля актуальности и подтверждать, что сетевые и DNS-параметры не препятствуют автоматическому продлению.

2.12 Добавление приложения

В данном разделе описывается процедура регистрации актива (веб-приложения) в WAF. Регистрация актива необходима для выпуска публичных точек входа, привязки доменного имени, выбора TLS-сертификата, задания портов публикации и указания целевых upstream-узлов, куда будет проксироваться трафик из периметра WAF. Операция выполняется под учетной записью с правами на управление приложениями и предполагает наличия прав управления DNS-записями домена.

Для добавления актива нажмите на кнопку в верхнем меню «Добавить приложение». В открывшемся окне «Добавление приложения» выполните настройку полей, как показано ниже.

Домен

Укажите FQDN без протокола и пути. Допускаются маски поддоменов (например, *.example.ru), а также одиночные домены (example.com). Используйте маску только при реальной необходимости. Убедитесь, что позже сможете направить A/AAAA/CNAME домена на адрес, предоставленный WAF.

Порты

Задайте перечень публикаций. По умолчанию доступны 80 и 443. Поле «SSL» у порта включает TLS-терминацию на стороне WAF. Рекомендуется оставлять 443 с включенным «SSL» и использовать 80 только для переадресации на HTTPS или технологических задач (например, валидация домена). Кнопка «Добавить порт» используется для объявления дополнительных слушателей. Иконка корзины справа удаляет соответствующий порт.

SSL сертификат

Выберите сертификат, соответствующий указанному домену или его wildcard-варианту. Рекомендуется использовать полную цепочку (leaf + intermediate). Для портов с активированным «SSL» сертификат обязателен.

Обратный прокси

Укажите адрес целевого узла в формате http://IP:порт. Путь не поддерживается, маршрутизация осуществляется только по хосту и порту (это явно указано в поле подсказки). Убедитесь, что источник трафика для Вашего origin ограничен сетевыми правилами и принимает соединения только от адресов WAF.

Добавить upstream

При необходимости добавьте несколько upstream-адресов. Удаление отдельного адреса выполняется иконкой корзины справа.

Комментарий

Необязательное поле для служебной пометки актива (назначение, владелец, окно обслуживания).

Сохранение изменений

Проверьте корректность домена, порта и выбранного сертификата, после чего нажмите «Добавить». Кнопка «Отмена» прерывает операцию без сохранения.

После добавления актива он появится в списке приложений. Для корректной работы необходимо актуализировать A-записи DNS домена, указать предоставленные Вам адреса WAF и проверить доступность upstream-узлов из периметра сервиса.

> **Рекомендация:** хорошей практикой является включение принудительного использования HTTPS, активировать HSTS в политиках безопасности и ограничить прямой доступ к origin-серверам с внешних сетей, оставив вход только через WAF по средством соединения точка-точка.

2.13 Настройка входящего трафика на сервер для работы с WAF

2.13.1 Принцип работы

Мы используем связку ipset + iptables:

- ✓ Скрипт регулярно скачивает Ваш персональный список IPv4 WAF по URL.
- ✓ Складывает адреса в ipset-набор waf_allow4.
- ✓ Обновляет цепочку iptables WAF_ALLOW и ставит переход в INPUT в самое начало.
- ✓ Далее создаётся правило DROP для портов приложения, чтобы прямой доступ в обход WAF был закрыт.

2.13.2 Установка скрипта

- ✓ **Зависимости**

```
sudo apt update
sudo apt install -y curl ipset iptables
```

✓ **Создайте файл скрипта**

Создайте файл:

```
sudo nano /usr/local/sbin/waf-ips-update.sh
```

Вставьте тело скрипта и заполните настройки:

- Укажите ваш URL списка в URL="..."
- Укажите порты, которые должны быть доступны только через WAF, в PORTS="..." (пример: 80 443)
-

```
#!/usr/bin/env bash
set -Eeuo pipefail
PATH="/usr/sbin:/usr/bin:/sbin:/bin"

# ====== SETTINGS ======
URL=""                    # IP/CIDR per line, comments allowed
PORTS="80 443"            # TCP ports (can be "80,443")
# ======================

LOCKDIR="/run/waf-ips-update.lock"
SET="waf_allow4"
TMP="waf_allow4_tmp"
CHAIN="WAF_ALLOW"

die(){ echo "ERROR: $*" >&2; exit 1; }
```

```
[[ ${EUID:-$(id -u)} -eq 0 ]] || die "run as root (sudo)"
command -v curl >/dev/null 2>&1 || die "missing: curl"
command -v ipset >/dev/null 2>&1 || die "missing: ipset"
command -v iptables >/dev/null 2>&1 || die "missing: iptables"

# lock to prevent concurrent runs
mkdir "$LOCKDIR" 2>/dev/null || exit 0

tmp="$(mktemp)"
cleanup(){ rm -f "$tmp"; rmdir "$LOCKDIR" 2>/dev/null || true; }
trap cleanup EXIT

# normalize ports
PORTS="${PORTS//,/ }"

# download and ensure HTTP 200
code="$(curl -sS -L --connect-timeout 10 --max-time 45 -o "$tmp" -w "%{http_code}"
"$URL" || echo 000)"
[[ "$code" == "200" ]] || die "URL must return HTTP 200 (got $code)"

# prevent HTML instead of IP list
if head -c 200 "$tmp" | tr -d '\000' | grep -qiE '<!doctype|<html'; then
  die "downloaded content looks like HTML, not an IP list"
fi

# iptables wait (if supported)
IPT_WAIT=()
```

```
iptables -w 1 -L >/dev/null 2>&1 && IPT_WAIT=(-w 5)

# ipset
ipset create "$SET" hash:net family inet -exist
ipset create "$TMP" hash:net family inet -exist
ipset flush  "$TMP"

# fill temporary set and ensure it is not empty
valid=0
while IFS= read -r line || [[ -n "$line" ]]; do
  line="${line%%#*}"
  line="${line//$'\r'/}"
  for tok in $line; do
    [[ -z "$tok" ]] && continue
    if ipset add "$TMP" "$tok" -exist 2>/dev/null; then
      valid=$((valid+1))
    fi
  done
done < "$tmp"

(( valid > 0 )) || die "no valid IPv4 IPs/CIDRs found (not applying)"

# atomic swap
ipset swap "$TMP" "$SET"
ipset flush "$TMP"

# iptables: dedicated chain + jump at top of INPUT
```

```
iptables "${IPT_WAIT[@]}" -N "$CHAIN" 2>/dev/null || true
iptables "${IPT_WAIT[@]}" -F "$CHAIN"

for p in $PORTS; do
  [[ "$p" =~ ^[0-9]{1,5}$ ]] || die "bad port: $p"
  (( p>=1 && p<=65535 )) || die "bad port: $p"
  iptables "${IPT_WAIT[@]}" -A "$CHAIN" -p tcp --dport "$p" -m set --match-set "$SET" src -j ACCEPT
done
iptables "${IPT_WAIT[@]}" -A "$CHAIN" -j RETURN

# ensure exactly one jump in INPUT at the top
while iptables "${IPT_WAIT[@]}" -C INPUT -j "$CHAIN" >/dev/null 2>&1; do
  iptables "${IPT_WAIT[@]}" -D INPUT -j "$CHAIN" || break
done
iptables "${IPT_WAIT[@]}" -I INPUT 1 -j "$CHAIN"

echo "OK: updated from $URL (ports: $PORTS, entries: $valid)"
```

Сделайте скрипт исполняемым

```
sudo chmod +x /usr/local/sbin/waf-ips-update.sh
```

2.13.3 Проверка скачивания и применения списка

✓ **Запуск**

```
sudo /usr/local/sbin/waf-ips-update.sh
```

Успешный пример вывода:

OK: updated from https://... (ports: 80 443, entries: 123)

✓ **Проверка ipset**

sudo ipset list waf_allow4

Внутри должны быть IP/подсети из вашего списка.

✓ **Проверка iptables**

sudo iptables -S WAF_ALLOW

sudo iptables -L INPUT -n --line-numbers | head -n 30

Ожидаемая логика:

- В INPUT в самом начале стоит переход в WAF_ALLOW
- В WAF_ALLOW есть правила ACCEPT на нужные порты для источников из waf_allow4, затем RETURN

2.13.4 Автообновление списка через systemd timer

Создайте файл сервиса обновления

nano /etc/systemd/system/waf-ips-update.service

[Unit]

Description=Update WAF IPv4 allowlist

Wants=network-online.target

After=network-online.target

[Service]

Type=oneshot

ExecStart=/usr/local/sbin/waf-ips-update.sh

Создайте таймер, который будет запускать сервис обновления списка

nano /etc/systemd/system/waf-ips-update.timer

[Unit]

Description=Periodic WAF allowlist update

[Timer]

OnBootSec=1min

OnUnitActiveSec=10min

Persistent=true

Unit=waf-ips-update.service

[Install]

WantedBy=timers.target

Примените найтсройки:

sudo systemctl daemon-reload

sudo systemctl enable --now waf-ips-update.timer

Проверка:

systemctl status waf-ips-update.timer

journalctl -u waf-ips-update.service -n 50 --no-pager

2.13.5 Закрытие прямого доступа

Скрипт добавляет allow для IP WAF. Чтобы запретить прямой доступ, добавьте DROP для портов приложения после jump в WAF_ALLOW.

Пример для 80,443:

```
sudo iptables -I INPUT 2 -p tcp -m multiport --dports 80,443 -j DROP
```

включайте DROP только после того, как убедились, что WAF реально проксирует трафик на ваш сервер и скрипт успешно подтягивает список IP.

Проверка порядка:

```
sudo iptables -L INPUT -n --line-numbers | head -n 30
```

Откат (удалить по номеру строки N из вывода):

```
sudo iptables -D INPUT N
```

2.14 Получение реального IP-адреса пользователя за WAF

После смены DNS-записей на адреса WAF пользователи вашего сайта больше не подключаются к вашему серверу напрямую.

Все входящие запросы приходят от IP-адресов WAF-узлов, поэтому ваш сервис видит не IP клиента, а IP WAF.

Чтобы передавать на ваш сервер реальный IP-адрес и порт клиента, используйте стандартные заголовки семейства X-Forwarded.

2.14.1 Включите передачу заголовков на стороне WAF

В панели управления WAF включите опцию передачи клиентских параметров подключения.

После активации этой настройки WAF начнёт автоматически добавлять к каждому запросу, перенаправляемому на ваш сервер, следующие заголовки:

- ✓ X-Forwarded-For — реальный IP-адрес клиента;

2.14.2 Настройка сервера на обработку X-Forwarded-For

Заголовки X-Forwarded-* нельзя считать достоверными, если к origin-серверу можно подключиться напрямую в обход WAF: клиент сможет подставить любые значения и “подменить” свой IP.

> Доверие к 0.0.0.0/0 допустимо только после того, как вы ограничили доступ через firewall и разрешили входящие подключения к веб-серверу только с IP WAF. **Инструкция:** https://check-risk.ru/help-center/server_firewall_setup

2.14.3 Nginx учет реального IP из X-Forwarded-For

Добавьте в конфигурацию (контекст http или нужный server блок):

```
# Вариант "доверять всем" — ТОЛЬКО если firewall пускает на сервер только WAF:
set_real_ip_from 0.0.0.0/0;

real_ip_header X-Forwarded-For;
real_ip_recursive on;
```

После этого $remote_addr и стандартные access-логи Nginx будут содержать реальный IP клиента (из X-Forwarded-For).

2.14.4 Apache (httpd) Учет реального IP из X-Forwarded-For (mod_remoteip)

Включите модуль mod_remoteip, затем добавьте настройки, в деректию apache conf.d/remoteip.conf или в виртуальный хост:

```
a2enmod remoteip && systemctl reload apache2

RemoteIPHeader X-Forwarded-For

# Вариант "доверять всем" — ТОЛЬКО если firewall пускает на сервер только WAF:

RemoteIPTrustedProxy 0.0.0.0/0
```

Перезагрузите Apache:

```
systemctl reload apache2
```

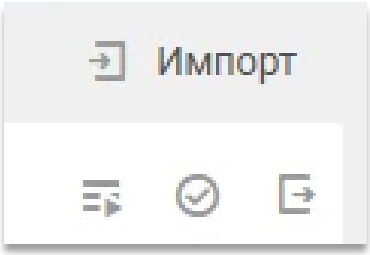
3. Управление угрозами

3.1 Инструкция по подключению источника Check Risk WAF с PT SIEM

В данном разделе представлена развёрнутая инструкция по установке правил нормализации для интеграции Check Risk WAF с PT MaxPatrol SIEM. Цель инструкции — обеспечить специалистов информационной безопасности чётким алгоритмом действий для корректного импорта пакета нормализации, его интеграции в систему, настройки сбора событий и проверки результата.

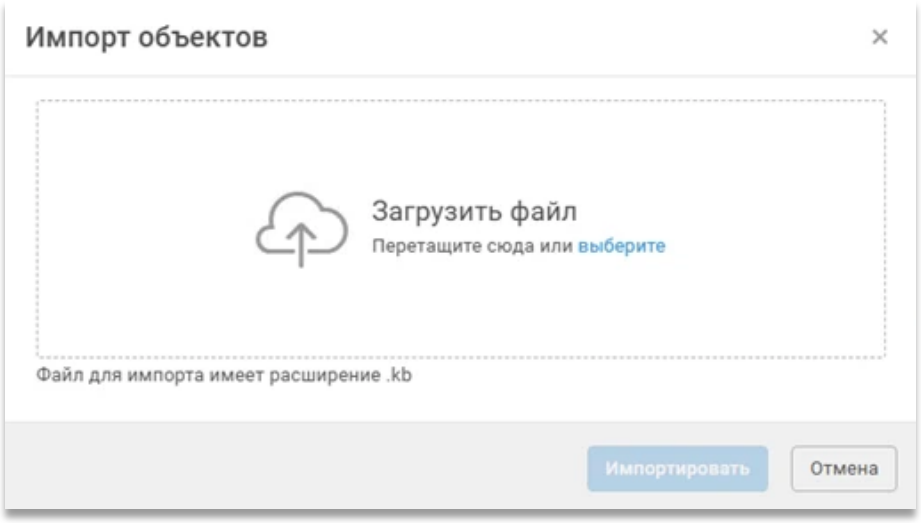
Правильная установка правил нормализации гарантирует, что события от Check Risk WAF будут интерпретироваться SIEM в структурированном виде. Это позволит использовать их для построения дашбордов, настройки корреляционных правил, а также анализа инцидентов.

Перейдите в раздел Knowledge Base в веб-интерфейсе MaxPatrol SIEM. В верхнем меню будет доступна функция импорта, предназначенная для загрузки пакетов знаний, включающих правила нормализации, справочники и дополнительные объекты.

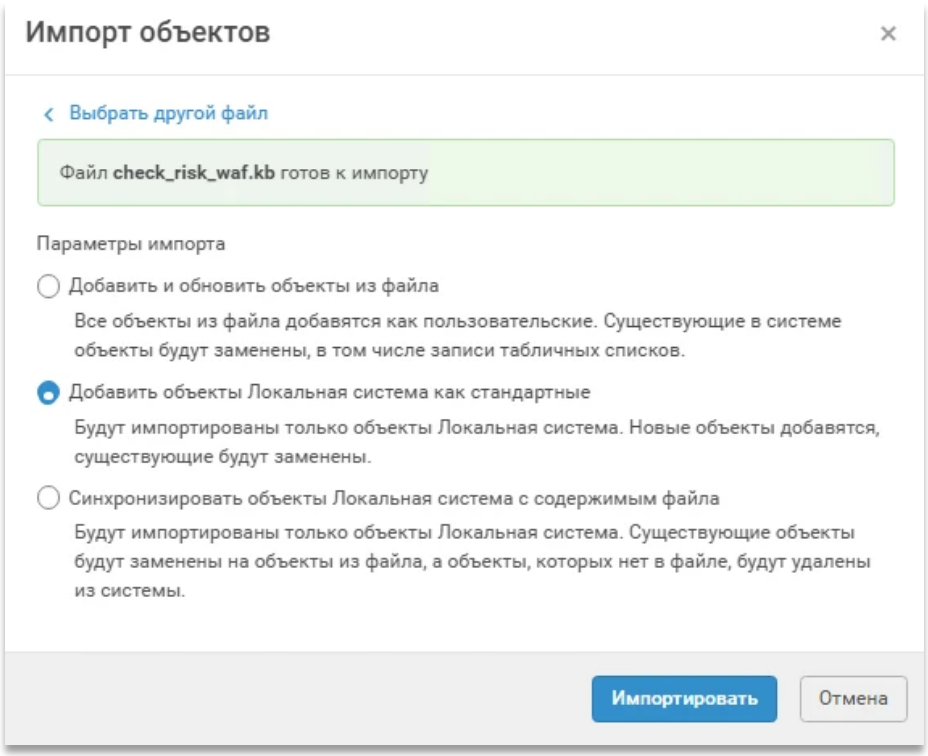


3.1.1 Подгрузка пакета KB

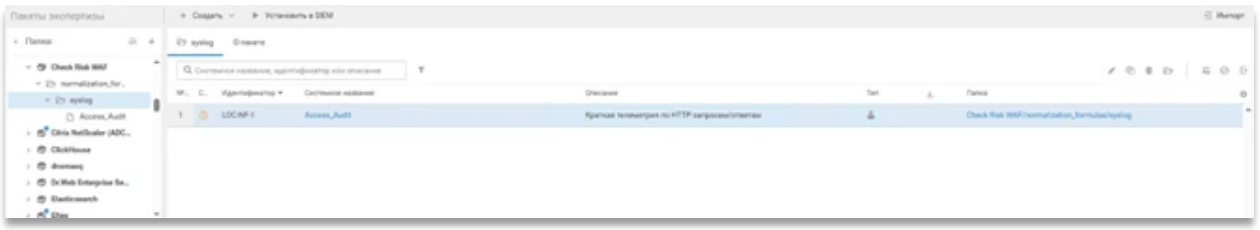
После выбора функции импорта откроется окно для загрузки пакета. Укажите файл пакета KB, предоставленный поставщиком Check Risk.



На этапе загрузки необходимо выбрать вариант: добавить объекты Локальная система как стандартные.



При успешном импорте в списке появится пакет Check Risk WAF, что будет подтверждением корректной загрузки.

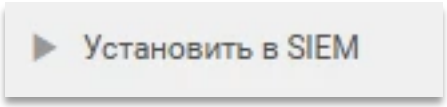


3.1.2 Добавление пакета в текущий набор установки

Для того, чтобы правила нормализации стали частью Вашей активной конфигурации, необходимо добавить импортированный пакет в набор установки. Для этого выделите соответствующее правило и используйте значок выбора набора для установки. Данный шаг позволяет управлять тем, какие пакеты будут применяться в рабочей среде.

3.1.3 Установка пакета в SIEM

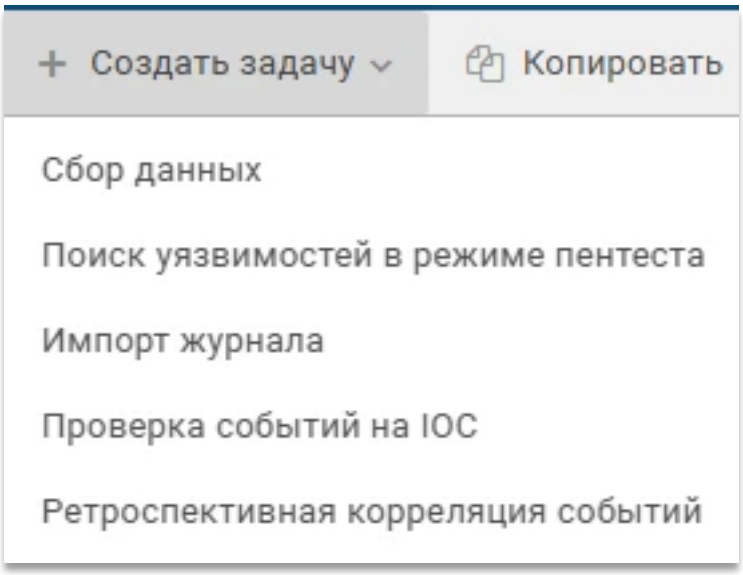
После того, как пакет был добавлен в набор, необходимо провести установку. Выберите созданный набор установки и запустите процедуру развёртывания. В ходе выполнения операции система проверит корректность объектов и добавит их в рабочую базу знаний.



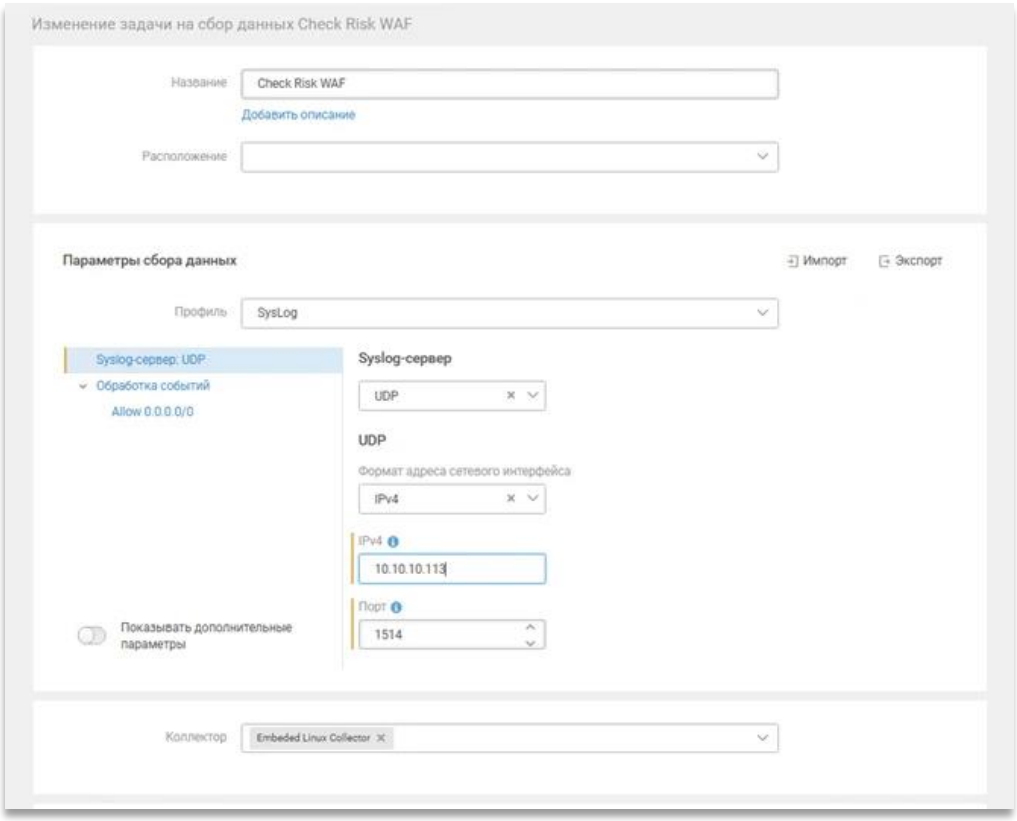
Рекомендуется дождаться завершения процесса и удостовериться в отсутствии ошибок в журнале установки.

3.1.4 Создание задачи по сбору событий по протоколу Syslog

Чтобы события от Check Risk WAF начали поступать в SIEM, необходимо настроить задачу сбора данных. Для этого создайте задачу типа Сбор данных с профилем Syslog

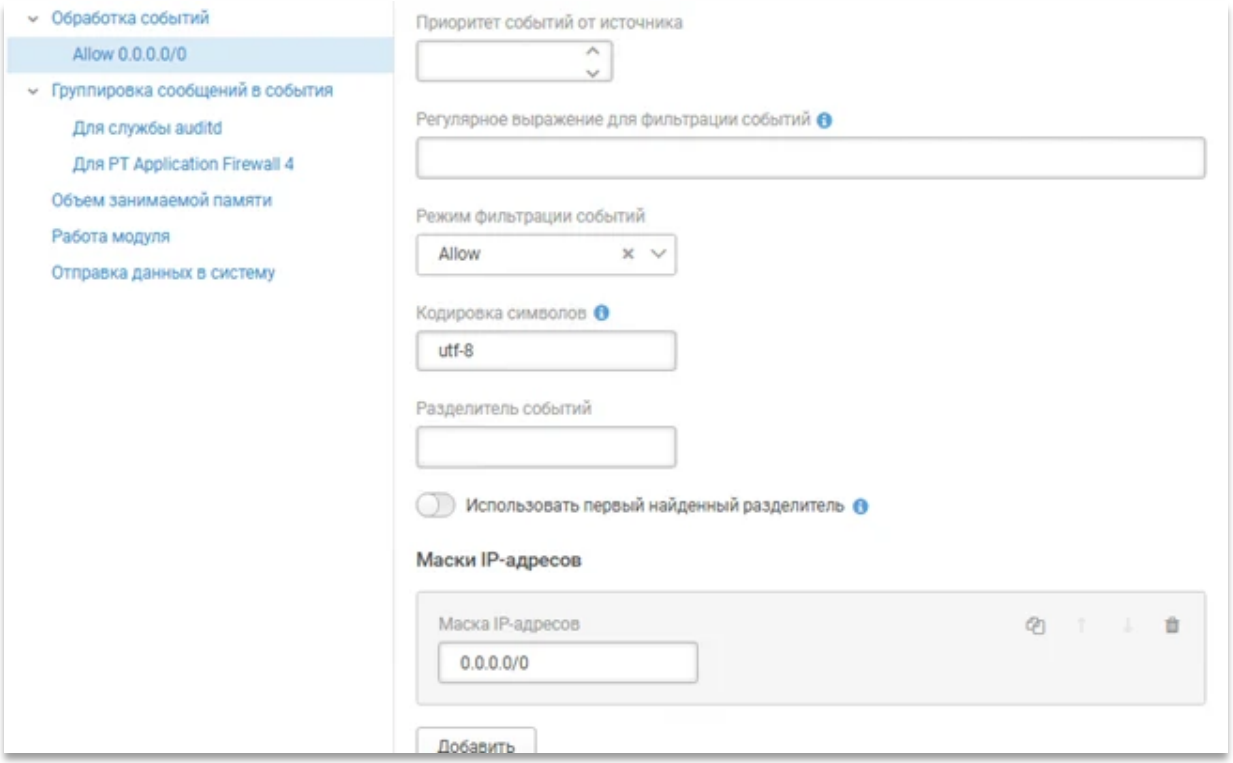


Укажите адрес получателя (IP-адрес Коллектора), протокол передачи (UDP), а также порт. По умолчанию используется стандартный порт 514, однако при необходимости можно задать нестандартное значение.



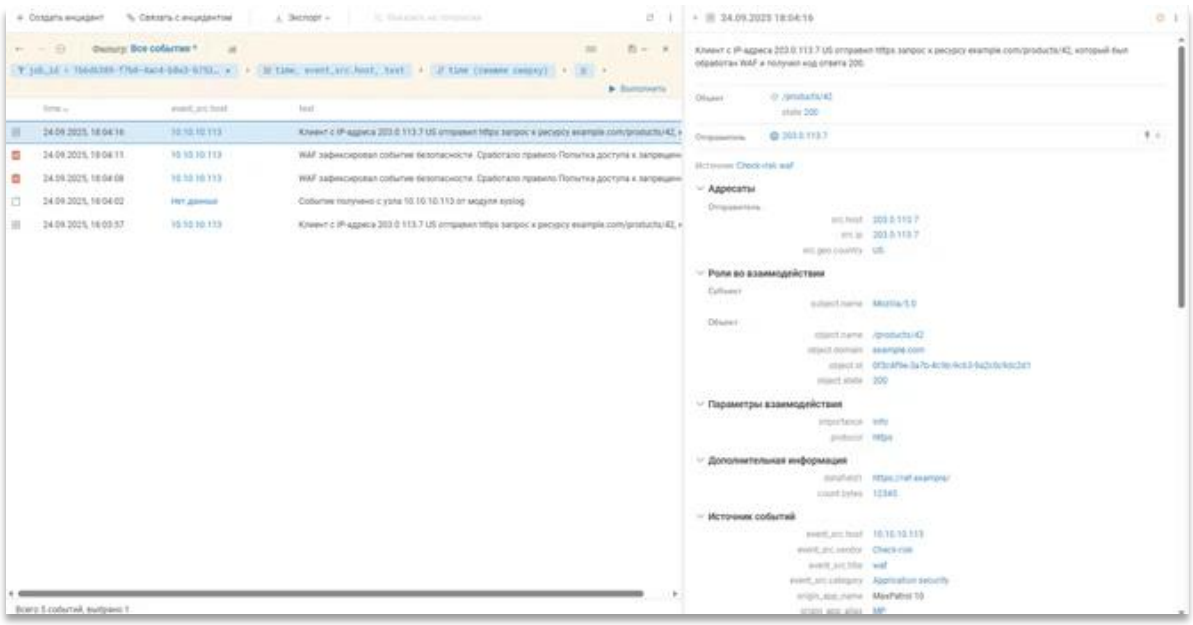
3.1.5 Ограничение пула адресов

С целью повышения уровня безопасности и исключения приёма событий от посторонних источников рекомендуется ограничить пул IP-адресов, с которых допускается приём сообщений. Настройка выполняется на этапе конфигурации задачи или средствами сетевых фильтров.



3.1.6 Проверка поступления и нормализации событий

Для проверки корректности работы задачи дважды кликните по её названию в списке. В открывшемся окне используйте кнопку «Найти события».



Если Вы видите события с корректно заполненными полями (например, источник события, IP-адрес, дата и время, уникальный идентификатор), значит, правило нормализации было установлено правильно и SIEM корректно интерпретирует поступающие данные.

В данной инструкции представлена полная последовательность действий по интеграции Check Risk WAF с PT MaxPatrol SIEM. Следуя описанным шагам — от импорта пакета знаний и его установки до создания задачи сбора и проверки нормализации — Вы обеспечите надёжную и корректную обработку событий.

Корректно установленный пакет нормализации позволит использовать события WAF в механизмах корреляции, настраивать оповещения, формировать отчёты и проводить расследования инцидентов в единой системе.

Если в процессе импорта или установки возникают ошибки, рекомендуется проверить версию пакета и совместимость с текущей версией SIEM, а также обратиться в техническую поддержку.

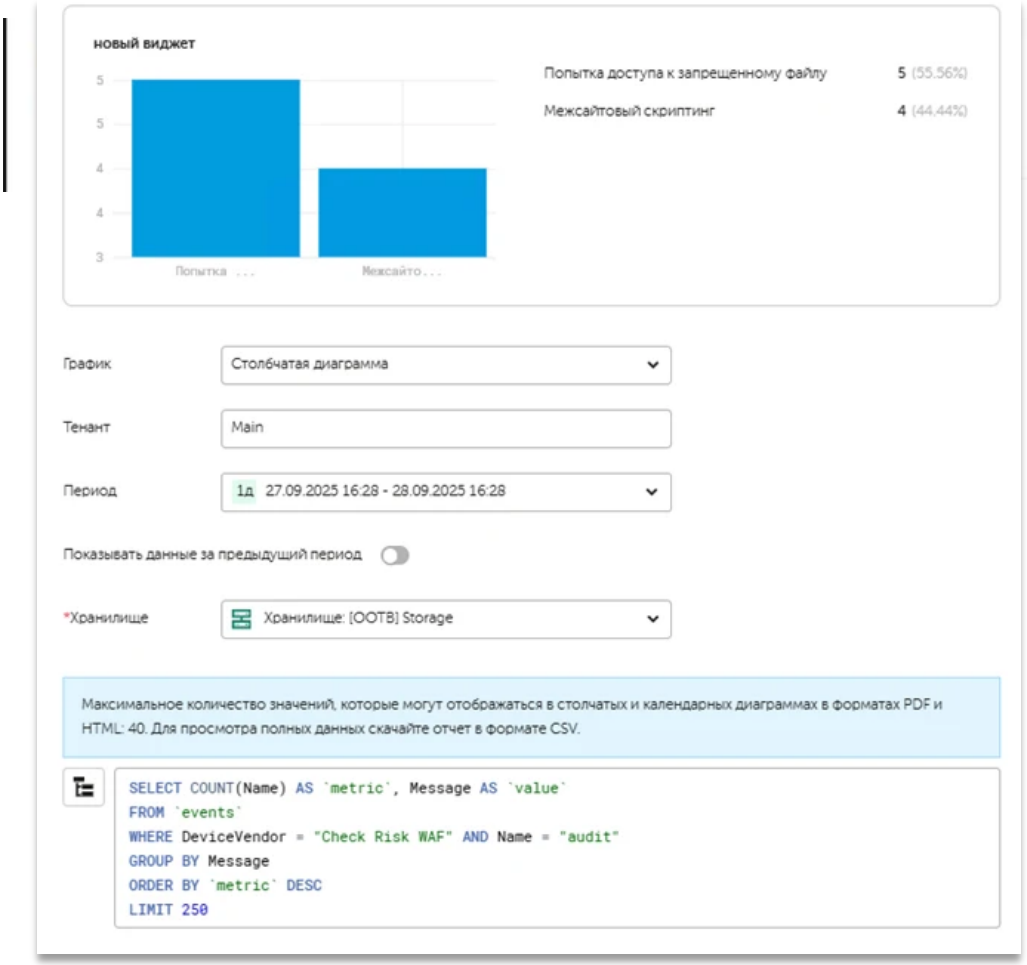
3.2 Настройка дашборда KUMA для событий Check Risk WAF

В данном разделе рассматривается процедура добавления виджета для отображения событий от Check Risk WAF в системе KUMA. Данный функционал позволяет в режиме реального времени визуализировать и анализировать события безопасности, поступающие от WAF, что повышает эффективность мониторинга и позволяет оперативно выявлять аномалии. Создание виджета

предоставляет возможность использовать гибкие фильтры и запросы для построения информативных дашбордов, отражающих актуальное состояние защищаемой инфраструктуры.

3.2.1 Инструкция

Для начала Вам необходимо выбрать актуальный тенант, в котором будет создан новый виджет. Далее создать новый макет и присвоить понятное название,



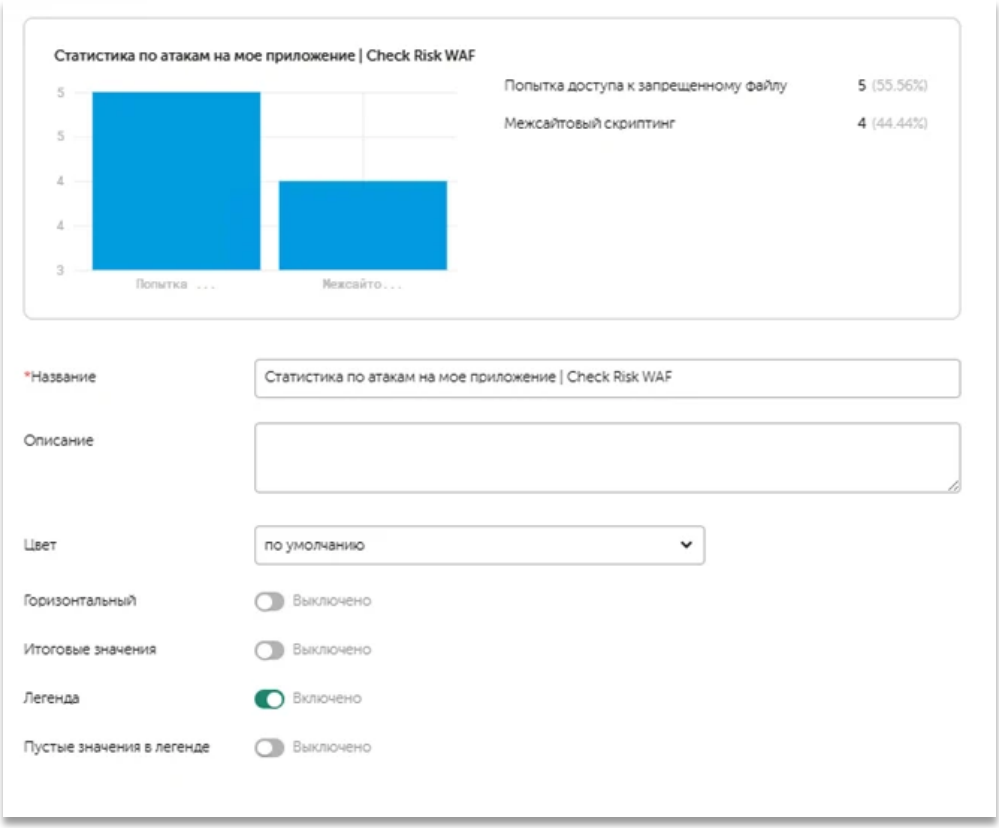
например Check Risk WAF. Инициировать процедуру добавления нового виджета, воспользовавшись кнопкой «Добавить виджет». В открывшемся списке типов необходимо остановить выбор на варианте «События».

В открывшейся форме конфигурации заполните поля в соответствии с представленным примером. Обратите внимание, что запрос SQL-запроса должен быть внесён в поле запроса без изменений.

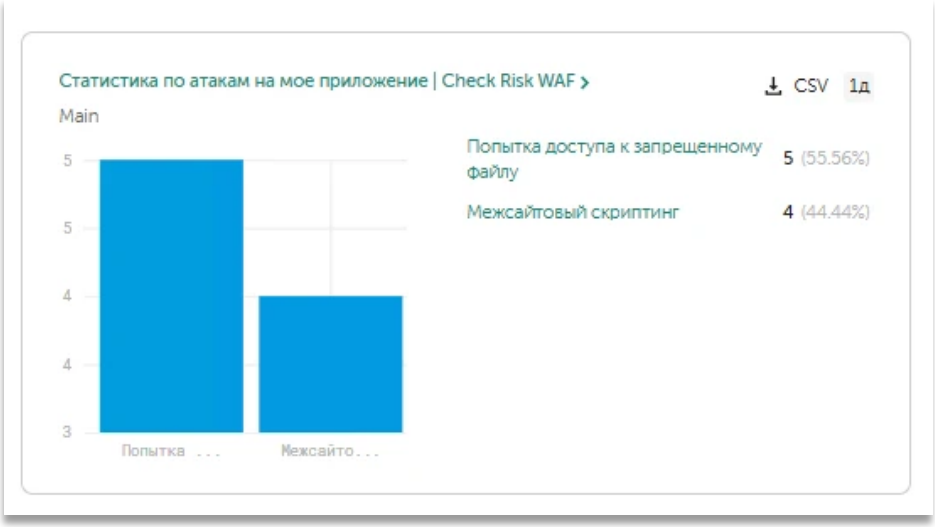
Запрос:

```
SELECT COUNT(Name) AS `metric`, Message AS `value`
FROM `events`
WHERE DeviceVendor = "Check Risk WAF" AND Name = "audit"
GROUP BY Message
ORDER BY `metric` DESC
LIMIT 250
```

После внесения запроса укажите название виджета, убедитесь, что все обязательные параметры заполнены, и подтвердите действие нажатием на кнопку «Добавить». На финальном этапе сохраните настройки.



Для проверки корректности выполненных действий убедитесь, что на дашборде появился новый виджет, отображающий данные в соответствии с заданным запросом.



В данной инструкции была рассмотрена пошаговая процедура создания и добавления виджета для отображения событий от Check Risk WAF в KUMA. В результате выполнения описанных действий Вы получили визуальный элемент, позволяющий отслеживать и анализировать сработки в наглядной форме.

Корректно настроенный дашборд с подобными виджетами повышает эффективность мониторинга, ускоряет обнаружение инцидентов и обеспечивает прозрачность работы систем защиты.

3.3 Описание полей событий syslog

В данном разделе формализуются состав, типы и семантика полей событий WAF для передачи по syslog и последующей интеграции с Вашими SIEM/SOAR и хранилищами логов. События описываются единым JSON-объектом в кодировке UTF-8; тип события определяется полем type; поля с неизвестными значениями опускаются; метки времени имеют формат ISO-8601 в UTC с суффиксом Z. Эти требования обеспечивают детерминированный парсинг и корректную корреляцию на стороне принимающей системы.

Вы можете настроить приём сообщений syslog от сервиса WAF и выполнить маппинг полей в Вашей SIEM, руководствуясь нижеприведённой спецификацией. Для первичной валидации корректности парсинга

целесообразно включить журналирование на тестовой витрине и сопоставить извлекаемые поля type, event_time, action, rule_ids, client_ip, domain, uri, status.

Ключевые положения формата

- ✓ Каждое событие — ровно один JSON-объект в UTF-8.
- ✓ Для различения типов событий используется поле type.
- ✓ Поля с неизвестными значениями опускаются, null не передаётся.
- ✓ Метки времени — ISO-8601 UTC с суффиксом Z (например, 2025-09-15T12:34:56Z).

Транспорт и кадрирование

- ✓ UDP (RFC 5426): передаётся один JSON-объект целиком; возможна фрагментация/усечение при больших размерах.
- ✓ TCP (RFC 6587, octet-counted): кадрирование в виде "<длина> <JSON>".
- ✓ TLS (RFC 5425): идентично TCP, но по защищённому каналу; рекомендуется для продакшн-интеграций.
- ✓ Ретраи при сетевых ошибках отсутствуют; доставка best-effort.

3.3.1 Общая «обёртка» сообщения

Поле	Тип	Обяз.	Описание
type	string	да	Вид события. Возможные значения: "access", "audit".
event_time	string	да	Время события в формате ISO-8601 (UTC), например 2025-09-15T12:34:56Z.

3.3.2 Формат type: "access" (журнал запросов)

Назначение: краткая телеметрия HTTP-запросов и ответов.

Поле	Тип	Обяз.	Пример	Описание
website_uuid	string	да	"0f3c4f9e-3a7b-4c9b-9c63-9a2c0c9dc2d1"	Идентификатор сайта/приложения (UUID).
domain	string	нет	"example.com"	Хост из запроса.
client_ip	string	нет	"203.0.113.7"	IP клиента.
scheme	string	нет	"https"	Протокол прикладного уровня: http/https (эвристика).
uri	string	да	"/products/42"	Путь без query-строки.
status	number	нет	200	HTTP-код ответа.
bytes_sent	number	нет	12345	Объём ответа в байтах.
country	string	нет	"US"	ISO-3166-1 alpha-2, если определена страна клиента.
user_agent	string	нет	"Mozilla/5.0 ..."	User-Agent запроса.
referer	string	нет	"https://ref.example/"	Referer без query (может отсутствовать).

Пример события access


```
{
  "type": "access",
  "event_time": "2025-09-15T12:34:56Z",
  "website_uuid": "0f3c4f9e-3a7b-4c9b-9c63-9a2c0c9dc2d1",
  "domain": "example.com",
  "client_ip": "203.0.113.7",
  "scheme": "https",
  "uri": "/products/42",
  "status": 200,
  "bytes_sent": 12345,
  "country": "US",
  "user_agent": "Mozilla/5.0",
  "referer": "https://ref.example/"
}
```


Гарантии и поведение для access:

- ✓ uri всегда без query-строки.
- ✓ При большом размере события могут быть опущены факультативные поля (например, user_agent).
- ✓ Отсутствующие/невычислимые поля опускаются.

3.3.3 Формат type: "audit" (события безопасности)

Назначение: фиксация срабатывания правил/политик и итогового действия по запросу.

Поле	Тип	Обяз.	Пример	Описание
website_uuid	string	да	"0f3c4f9e-3a7b-4c9b-9c63-9a2c0c9dc2d1"	Идентификатор сайта/приложения (UUID).

domain	string	нет	"example.com"	Хост из запроса.
client_ip	string	нет	"203.0.113.7"	IP клиента.
scheme	string	нет	"https"	Протокол прикладного уровня: http/https (эвристика).
uri	string	да	"/products/42"	Путь без query-строки.
status	number	нет	200	HTTP-код ответа.
bytes_sent	number	нет	12345	Объём ответа в байтах.
country	string	нет	"US"	ISO-3166-1 alpha-2, если определена страна клиента.
user_agent	string	нет	"Mozilla/5.0 ..."	User-Agent запроса.
referer	string	нет	"https://ref.example/"	Referer без query (может отсутствовать).

Структура элементов messages:

```
{
 "message": "...краткое пояснение...",
 "details": {
  "ruleId": 941100,            // число или null для кастомного правила
  "reference": "...опционально...",  // может отсутствовать
  "ruleCustomUuid": "...uuid..."     // присутствует только у кастомного правила
 }
```

}

Пример события audit:

{
"type": "audit",
"event_time": "2025-09-15T12:34:56Z",
"website_uuid": "0f3c4f9e-3a7b-4c9b-9c63-9a2c0c9dc2d1",
"server_id": "7b1b2c3d-4e5f-6789-aaaa-bbbbccccdddd",
"unique_id": "1700000000:abc123",
"domain": "example.com",
"client_ip": "203.0.113.7",
"protocol": "https",
"uri": "/login",
"status": 403,
"country": "US",
"messages": [
{
"message": "SQLi pattern detected",
"details": { "ruleId": 942100, "reference": "ARGS:q", "ruleCustomUuid": null }
}
],
"rule_ids": [942100],
"custom_rule_uuids": [],
"action": "BLOCK"
}

Гарантии и поведение для audit:

✓ action принимает одно из значений: BLOCK (запрос отклонён) или MONITORING (запрос пропущен, событие зафиксировано).

- ✓ request ограничен по длине и предварительно фильтруется от служебных/вспомогательных заголовков.
- ✓ rule_ids и custom_rule_uuids содержат уникальные значения.

Данный раздел фиксирует единый формат событий WAF в syslog: один JSON-объект на событие, строгая типизация через type, временные метки в ISO-8601 UTC, отсутствие передач null, а также поддерживаемые транспорты и особенности доставок. Для обеспечения корректной аналитики в Ваших системах рекомендуется ориентироваться на приведённые схемы полей, примеры и поведенческие гарантии по каждому типу события.

3.4 Передача логов атак по Syslog

В данном разделе описывается порядок настройки передачи журналов инцидентов веб-приложений (логи атак WAF) во внешние системы по протоколу Syslog с использованием TCP или UDP. Поддерживается шифрование канала передачи с применением TLS.

> **Внимание:** функция доступна в рамках тарифа «Коммерческая».

Основные особенности:

Передаются только события, классифицированные WAF как атаки (обнаруженные и/или заблокированные);

- ✓ Доступны варианты доставки по TCP/UDP, а также TLS-шифрование канала;
- ✓ Параметры включаются в «Глобальные настройки безопасности» и при необходимости переопределяются в «Локальные настройки безопасности» для отдельных сайтов/политик;
- ✓ Предуготовленные правила нормализации для SIEM систем: KUMA (Kaspersky Unified Monitoring and Analysis Platform) и PT SIEM.

Порядок настройки передачи событий

Настройка пересылке логов предусмотрено как "Глобальной" (Единой политикой для всех приложений) так и "локальной" (Точечной настройки политики приложения).

3.4.1 Настройка в «Глобальные настройки безопасности»

1. Откройте «Глобальные настройки безопасности» и перейдите к блоку отправки событий во внешние системы "Syslog/SIEM".
2. Включите функцию отправку логов;
3. Укажите получателя: адрес или FQDN и порт (по умолчанию обычно используется 514 для UDP/TCP или 6514 для TLS; конкретное значение определяется Вашими корпоративными стандартами);
4. Выберите протокол доставки: UDP, TCP или TLS. Для TLS задайте требования проверки сертификата: проверка цепочки, CN/SAN, при необходимости включите взаимную аутентификацию (mTLS) и загрузите клиентский сертификат;
5. Сохраните изменения.

3.4.2 Готовые правила нормализации событий Check Risk WAF

В рамках комплекта поставки нашей системы, предусмотрены готовые системы нормализации для SIEM систем, которые готовы к работе "Из коробки".

SIEM система	Описание	Версия	URL правила нормализации	Проверочная сумма MD5
KUMA (Kaspersky Unified Monitoring and Analysis Platform)	Готовое правило нормализации для SIEM KUMA, которое обеспечивает полноценный парсинг события атак, полученный по протоколу syslog.	1.0	https://check-risk.ru/siem/check_risk_waf_kuma_v1_0	817A21371E703EDE0A605270CD827434
Positive Technologies : SIEM	Готовое правило нормализации для PT SIEM, для дальнейшей интеграции в базу данных PTKB, которое обеспечивает полноценный	1.0	https://check-risk.ru/siem/check_risk_waf_pt_v1_0.kb	43906E81EA2DA86DEC503813A0AB1D53

	парсинг события атак, полученный по протоколу syslog.			

URL правила нормализации вы можете скачать на нашем сайте https://check-risk.ru/help-center/syslog-attack-logs-waf.

Внимание: перед установкой правила нормализации ВСЕГДА сверяйте проверочную сумму md5!

Передача логов атак по Syslog предназначена для безопасного и надежного экспорта инцидентов WAF во внешние системы мониторинга и расследования. Возможности включаются на глобальном уровне с опциональным переопределением на уровне отдельных сайтов, поддерживается шифрование TLS, а для ускорения интеграции предоставлены готовые правила нормализации для KEDR и PT VIEM.

Рекомендация: хорошей практикой является включение принудительного использования HTTPS, активировать HSTS в политиках безопасности и ограничить прямой доступ к origin-серверам с внешних сетей, оставив вход только через WAF по средством соединения точка-точка.

3.5 Добавление угрозы в исключение

В данном разделе описывается порядок создания правила-исключения для разрешения конкретного легитимного трафика, который был ошибочно классифицирован как угроза (ложное срабатывание). Исключение создается в виде правила с действием «Разрешить», ограниченного по приложению, URL и иным признакам, чтобы не ослаблять защиту всего веб-ресурса. Конструктор правил поддерживает объединение условий внутри группы по логике И, а между группами по логике ИЛИ, а также имеет переключатель инверсии результата «НЕ» для редких случаев, когда необходимо обратить итог проверки.

(СКРИНШОТ)

Порядок действий

Для добавления исключения нажмите на пиктограмму "Щиток +". Исключения создаются в контексте выбранного правила сработки приложения.

Рекомендуемый рабочий сценарий:

- ✓ Откройте раздел "Уязвимости" и найдите событие, вызвавшее ложное срабатывание. В поле URL нажмите на пиктограмму "Щиток +".

- ✓ В форме «Добавление правила» задайте действие «Разрешить», в поле «Приложения» выберите соответствующий сайт, затем добавьте условия, которые минимально точно описывают легитимный запрос. Конструктор поддерживает области проверки: Приложения, URL и Путь URL, Хост, Заголовок, GET-параметры, POST-параметры, Тело запроса, HTTP-метод, а также соответствующие операторы сравнения: Равно, Не равно, Содержит, Не содержит, Начинается с, Регулярное выражение, Существует/Не существует для параметров и заголовков. Для метода доступны значения из стандартного набора: GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS, TRACE, CONNECT.

- ✓ Внутри Группы условий #1 добавляйте признаки через «Добавить условие (И)», чтобы все они выполнялись одновременно. Если требуется несколько вариантов запроса, используйте «Добавить группу (ИЛИ)». Переключатель «Инвертировать результат (НЕ)» по умолчанию отключайте; он предназначен для специфических случаев и в типовой задаче исключения не применяется.

- ✓ Пример узкого исключения для заблокированного запроса из журнала:

  Приложения → Равно → test.local

  URL → Равно → /?id=1%20OR%2... (используйте точное значение из журнала или более строгий вариант через Путь URL + параметр)

  HTTP-метод → Равно → POST

- ✓ При необходимости добавьте точечные условия по заголовкам или параметрам (GET/POST) с оператором Равно.

- ✓ Убедитесь, что переключатель «Включено» активен, и сохраните правило кнопкой «Добавить». Поле описания рекомендуется заполнить контекстом: источник запроса, номер инцидента, срок пересмотра. Модель правила поддерживает флаг enabled и действие allow|deny; для исключения следует использовать allow.

(СКРИНШОТ)

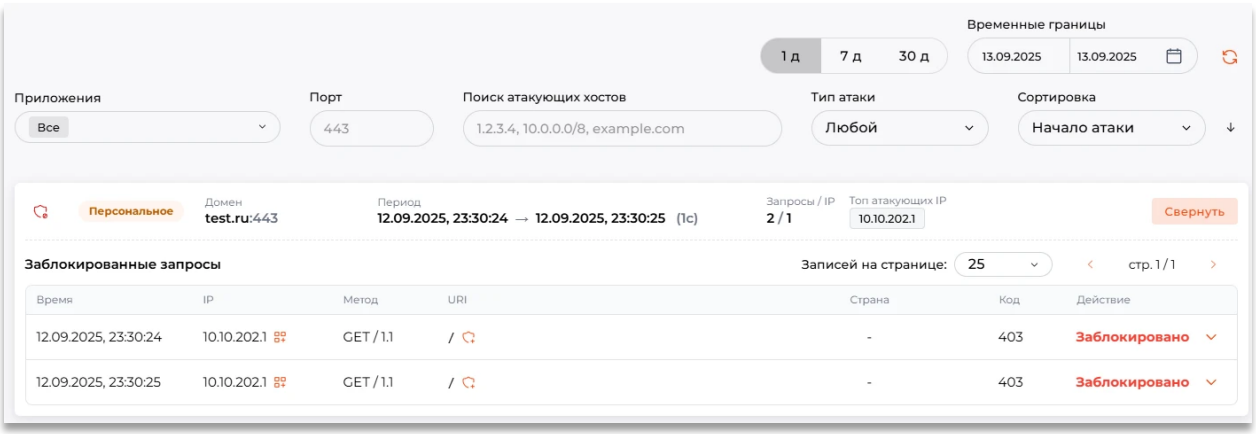
В целях минимизации рисков следует придерживаться следующих практик:

- ✓ Ограничивайте область действия исключения по приложению, точному пути и методу.
- ✓ Не объединяйте в одном правиле несвязанные случаи. Для разных вариантов используйте отдельные группы "ИЛИ" или отдельные правила. Логика конструктора: внутри группы условия связаны "И", группы объединяются при помощи "ИЛИ". Глобальная инверсия через «НЕ» используется только при необходимости.
- ✓ После публикации проверьте журнал трафика: целевой запрос должен проходить без статуса 403, при этом иные атаки продолжат блокироваться. При появлении побочных эффектов сразу сузьте условия или отключите правило.

Данный порядок позволяет оперативно устранять ложные срабатывания без деградации уровня защиты и обеспечивает управляемость исключений на уровне конкретных признаков запроса.

3.6 Фильтрация угроз

Раздел предназначен для оперативной фильтрации и анализа зафиксированных атак в WAF SaaS. Здесь Вы определяете срез событий по приложениям и портам, ограничиваете временные границы, отбираете конкретные типы атак, находите источники по IP или подсети и переходите к детальному разбору каждого запроса. Раздел показывает фактическую обработку трафика, код ответа сервера и сработавшее правило, что позволяет быстро классифицировать инцидент, подтвердить блокировку и выявить ложные срабатывания.



Раздел отображает:

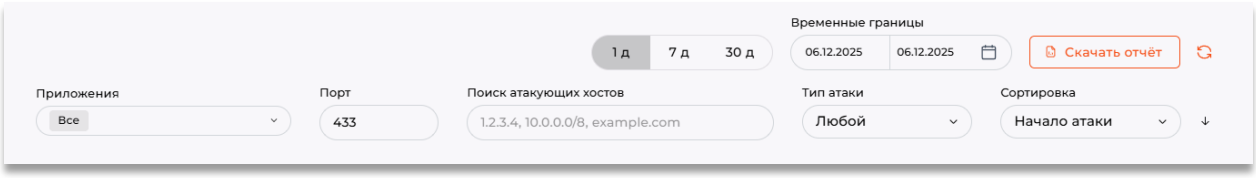
- ✓ Панель фильтров с параметрами Приложения, Порт, Поиск атакующих хостов, Тип атаки, Сортировка и временные границы;
- ✓ Список карточек атак с краткой сводкой по домену, периоду, количеству запросов и «топ атакующих IP»;
- ✓ Таблицу заблокированных запросов с полями Время, IP, Метод, URI, Код и Действие;
- ✓ Детальную карточку запроса с «Сырым HTTP-запросом», вкладками Raw, Заголовки, Тело, cURL, а также блоком «Правила» с указанием сработавшей сигнатуры, например «SQL Injection Attack Detected via libinjection» с идентификатором.

Примечание: для корректной работы фильтров у Вас должно быть добавлено хотя бы одно приложение. Добавление выполняется из верхнего меню по кнопке «Добавить приложение».

Перейдите в раздел «Атаки». Используйте панель фильтров в верхней части экрана для уточнения выборки.

Выбор области анализа:

1. В поле «Приложения» задайте нужное приложение или оставьте «Все» для сводного просмотра по всем доменам, защищаемым WAF.



2. В поле «Порт» выберите целевой порт. По умолчанию отображается 443.
3. В блоке «Временные границы» укажите интервал в формате дата и время начала и окончания. Это исключает шум и ускоряет разбор.
4. В поле «Тип атаки» отберите интересующие категории, например SQLi или LFI. Положение «Любой» оставляет все типы.
5. В поле «Поиск» атакующих хостов» введите одиночный IP, диапазон или подсеть в CIDR. Допускается ввод нескольких значений через запятую.
6. В поле «Сортировка» используйте порядок «Начало атаки» для инцидента-ориентированного обзора.

Работа со списком атак

- ✓ Ориентируйтесь на строку статуса, где виден домен, период атаки и индикатор активности. Например, пометка «Атака в процессе» сигнализирует об идущем событии.
- ✓ Нажмите «Показать запросы», чтобы раскрыть таблицу заблокированных обращений. В обзоре отображаются время, IP-адрес источника, HTTP-метод, URI, код ответа и действие. Для заблокированных обращений код, как правило, 403, а в столбце «Действие» указано «Заблокировано».
- ✓ Управляйте пагинацией параметром «Записей на странице», чтобы не пропускать разрозненные попытки одного источника.

Детальный разбор запроса

1. Откройте карточку запроса для просмотра технических артефактов. В блоке «Сырой HTTP-запрос» доступны вкладки:

- ✓ Raw для точной реконструкции запроса вместе со стартовой линией POST / HTTP/1.1;
- ✓ «Заголовки» для проверки аномалий в User-Agent, Content-Type, X-Forwarded-For и др.;
- ✓ «Тело» для инспекции полезной нагрузки;
- ✓ cURL для быстрой репродукции запроса в тестовой среде.

2. Используйте действия «Показать сырой JSON», «Копировать URL» и «Копировать», чтобы экспортировать артефакты в систему тикетов или SIEM. При необходимости примените «Скачать», если доступна выгрузка.

3. В блоке «Правила» изучите сигнатуру, сработавшую на запрос. Указывается тип атаки и движок детектирования. Например, «SQL Injection Attack Detected via libinjection» с идентификатором правила. Это помогает классифицировать инцидент и обосновать блокировку.

4. Сверяйте поле «Топ атакующих IP» для быстрой атрибуции источника и последующей агрегации событий по адресу.

Раздел обеспечивает строгую фильтрацию событий и полноту артефактов для расследования: от верхнеуровневых фильтров до показа исходного HTTP-трафика и сигнатуры детекта. Рекомендуется фиксировать результаты анализа в системе учёта инцидентов, проводить репродукцию спорных запросов в изолированной среде и поддерживать синхронизацию времени между WAF и журналами приложений.

3.7 Инструкция по созданию виджета для Check Risk WAF в MaxPatrol SIEM

В данном разделе представлена подробная инструкция по добавлению виджета со сработками правил Check Risk WAF в интерфейсе PT MaxPatrol SIEM. Основное назначение виджета заключается в визуализации информации о событиях WAF в удобной графической форме. Использование подобного

инструмента позволяет специалисту оперативно отслеживать распределение событий, контролировать активность и выявлять аномалии.

Перейдите в раздел «События»:

Откройте веб-интерфейс MaxPatrol SIEM и перейдите в раздел "События". В данном разделе представлена лента всех поступающих логов, которые уже были нормализованы. Именно отсюда формируются фильтры и группировки, которые затем можно преобразовать в виджет.

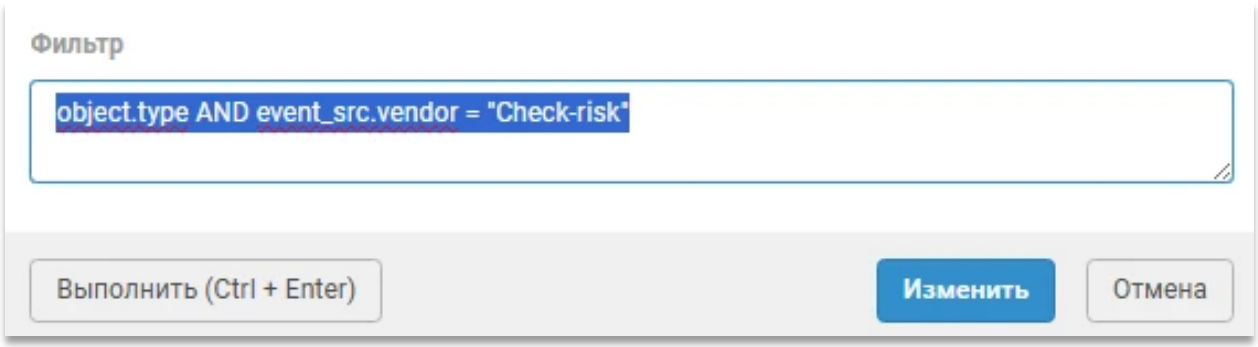
Скриншот

3.7.1 Добавление фильтра для WAF

> object.type AND event_src.vendor = "Check-risk"

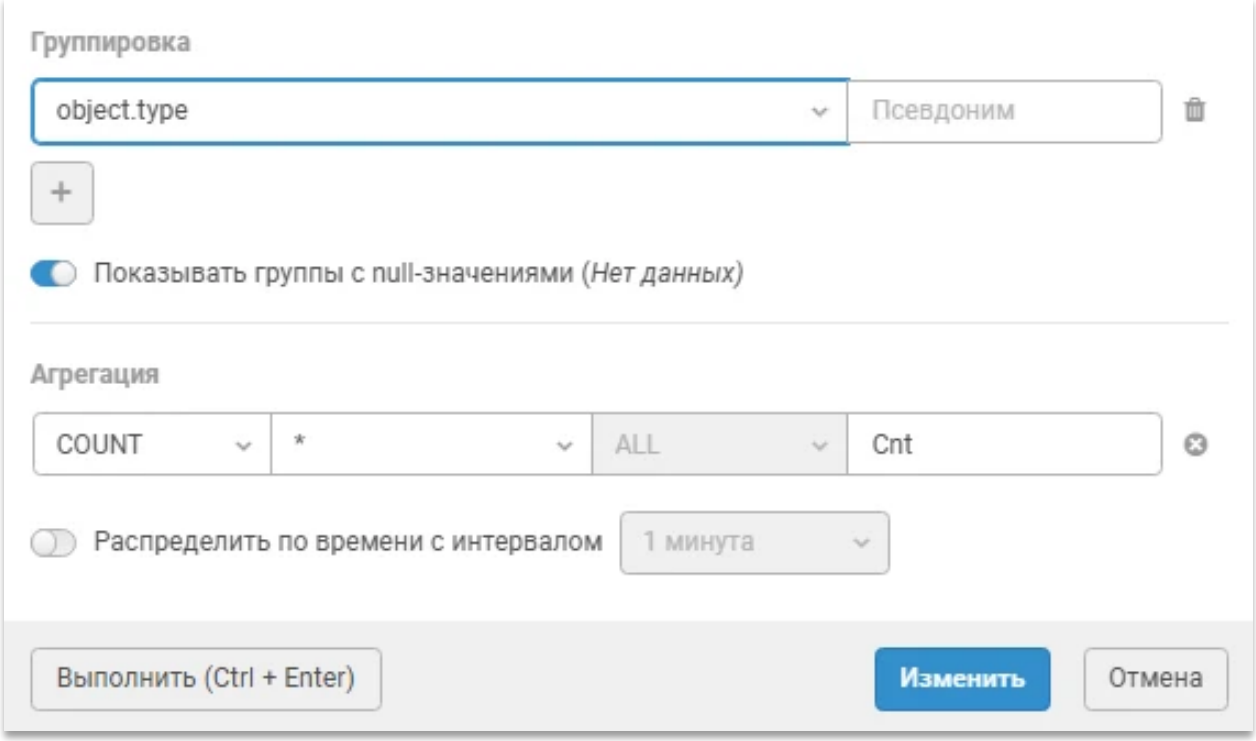
В панели фильтрации укажите условие:

Это условие позволит отобразить только события, поступающие от Check Risk WAF, и исключит лишние записи. Таким образом, Вы получите выборку исключительно по интересующим объектам.



3.7.2 Создание группировки по полю object.type

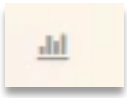
Для наглядного отображения данных примените группировку по полю object.type. Данный параметр позволит классифицировать события по их типу,



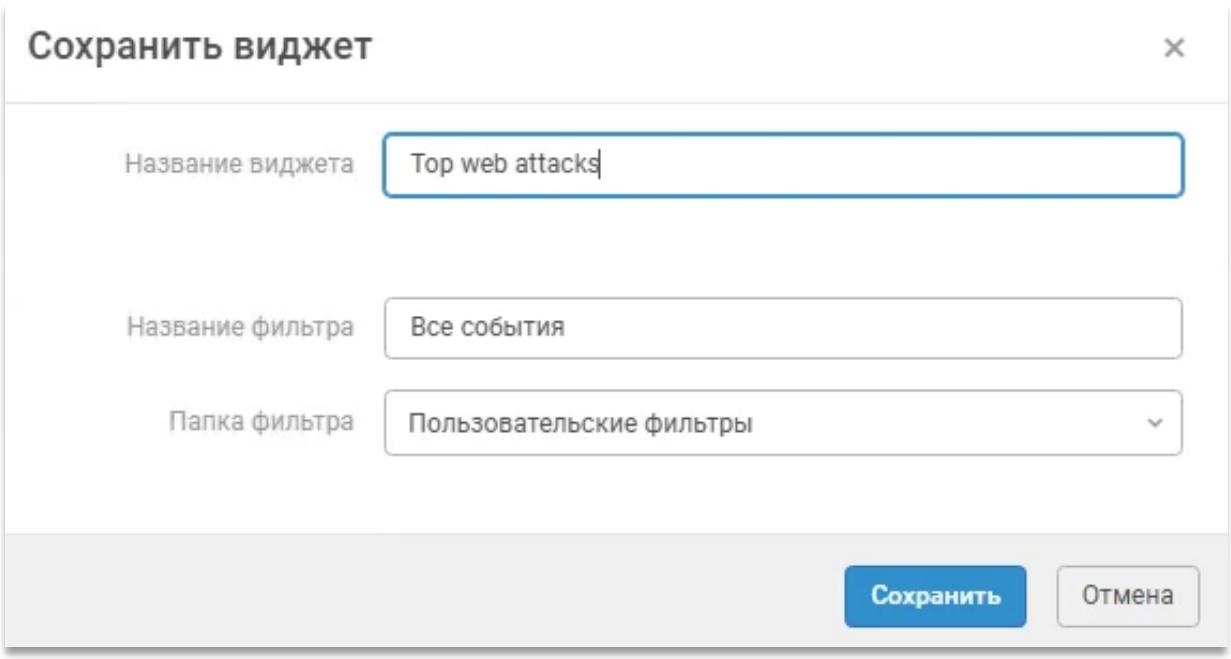
что обеспечит более удобный анализ при построении визуализации.

3.7.3 Предпросмотр и сохранение виджета

Нажмите на кнопку "Посмотреть виджет".



В появившемся окне выберите тип отображения — столбчатая диаграмма. Такой вариант наглядно демонстрирует соотношение типов событий. После выбора сохраните виджет для последующего использования.



3.7.4 Добавление виджета на дашборд

На главной странице перейдите к разделу "Дашборды". Вы можете либо создать новый дашборд (нажав на плюсик), либо открыть существующий, где доступно место для размещения нового элемента.

Нажмите на кнопку Добавить виджет, после чего выберите ранее созданный виджет со сработками правил WAF. Подтвердите добавление.

Скриншот

Если на дашборде появился виджет с данными по сработкам правил Check Risk WAF, значит, все действия выполнены правильно, и система корректно визуализирует события.

Скриншот

В данной инструкции была рассмотрена пошаговая процедура создания и добавления виджета для отображения событий от Check Risk WAF в MaxPatrol SIEM. В результате выполнения описанных действий Вы получили визуальный

элемент, позволяющий отслеживать и анализировать сработки в наглядной форме.

Корректно настроенный дашборд с подобными виджетами повышает эффективность мониторинга, ускоряет обнаружение инцидентов и обеспечивает прозрачность работы систем защиты.

3.8 Настройка нормализации событий Check Risk WAF в SIEM KUMA

В данном разделе приводится пошаговая инструкция по добавлению правила нормализации событий от Check Risk WAF в SIEM KUMA. Целью данного раздела является обеспечение корректного приёма, парсинга и маршрутизации логов WAF в KUMA посредством импорта нормализатора и настройки коллектора. Инструкция рассчитана на инженера по информационной безопасности или администратора KUMA и содержит практические указания, необходимые для интеграции, проверяемые действия и контрольные точки состояния коллектора после установки.

3.8.1 Инструкция по установке

Импорт правила нормализации

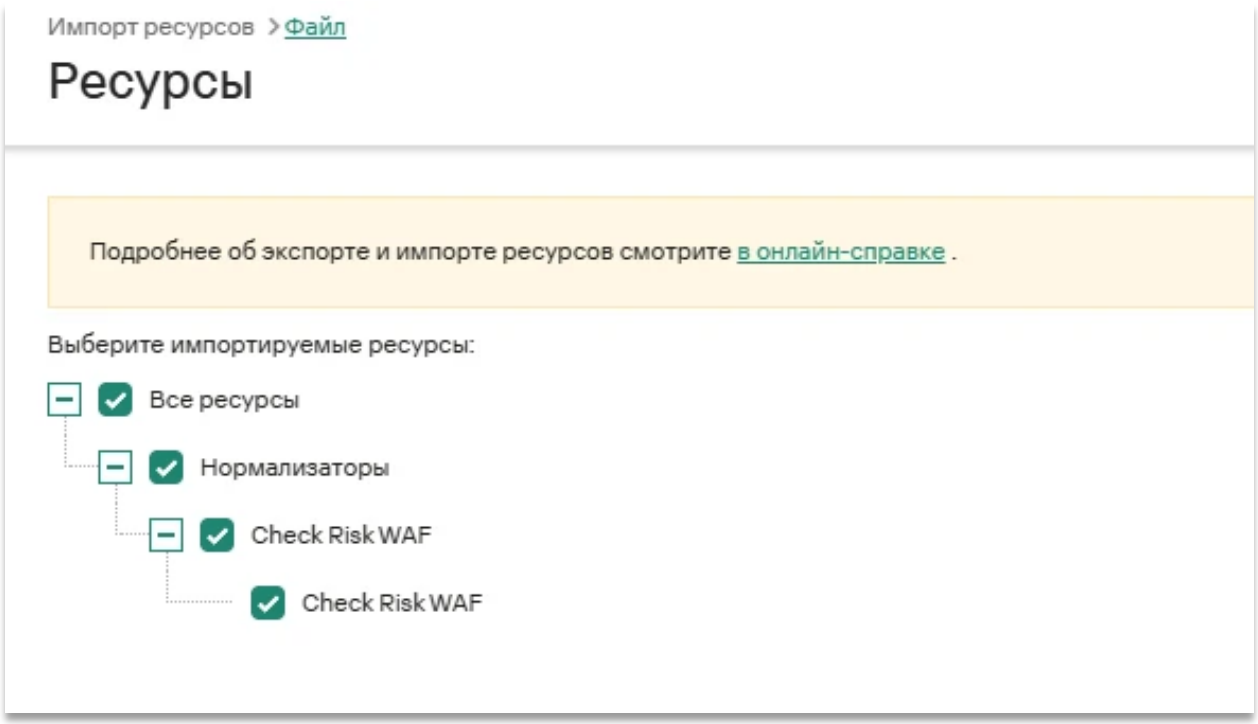
Перейдите в раздел «Ресурсы и сервисы», затем откройте подраздел «Нормализаторы». Нажмите кнопку «Импортировать ресурсы» в интерфейсе.

СКРИН

В диалоге импорта выберите целевой тенант (по умолчанию — main). В качестве источника импорта укажите «файл». В поле пароля введите q123123Q!q123123Q!. Выберите файл с именем check-risk-waf для загрузки.

СКРИН

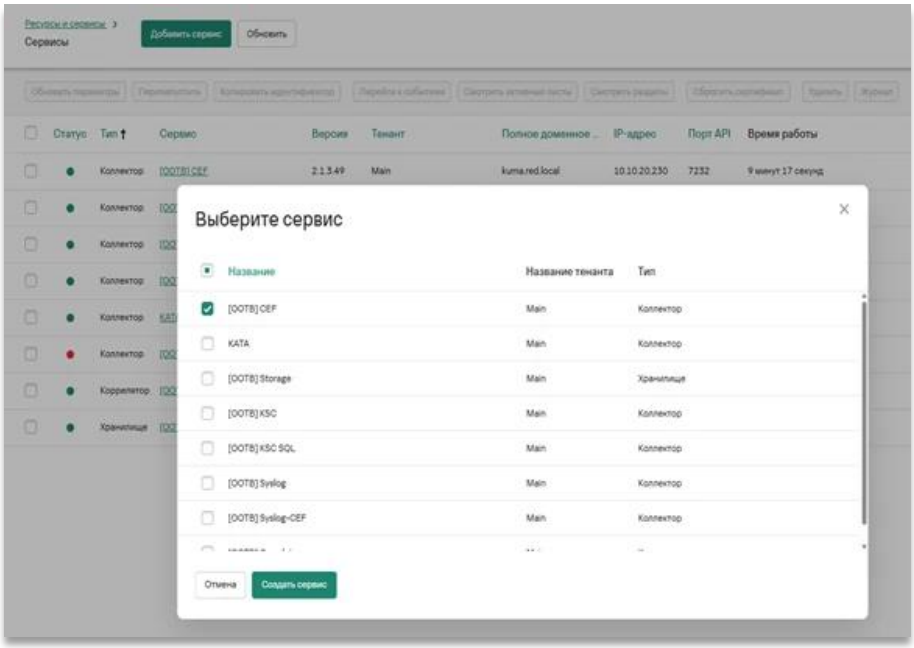
Отметьте все ресурсы, предназначенные для импорта, и подтвердите импорт нажатием кнопки «Импортировать».



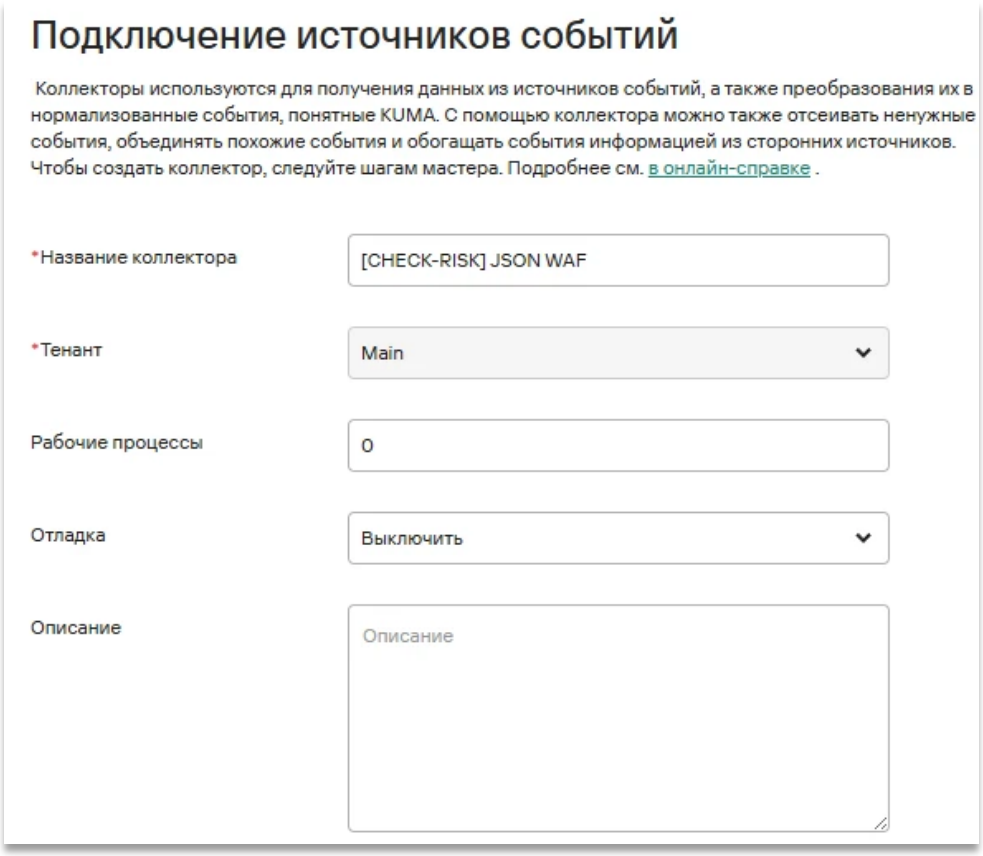
После успешного импорта в выбранном тенанте появится раздел Check Risk Waf с загруженным правилом нормализации. Убедитесь, что правило доступно для выбора в списке нормализаторов.

3.8.2 Добавление нового коллектора

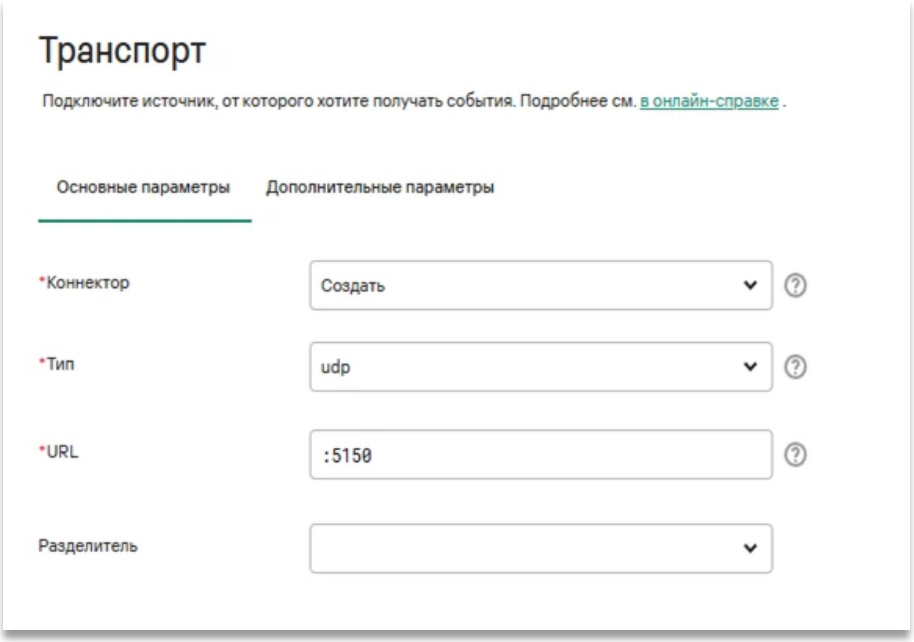
1. Перейдите в раздел «Ресурсы и сервисы», затем откройте «Сервисы».
2. Нажмите «Добавить сервис» и в списке шаблонов выберите [OOTB] CEF как основу, затем нажмите «Создать».



Откройте созданный сервис-коллектор для редактирования. Измените название на удобное для вас, например [CHECK-RISK] JSON WAF.



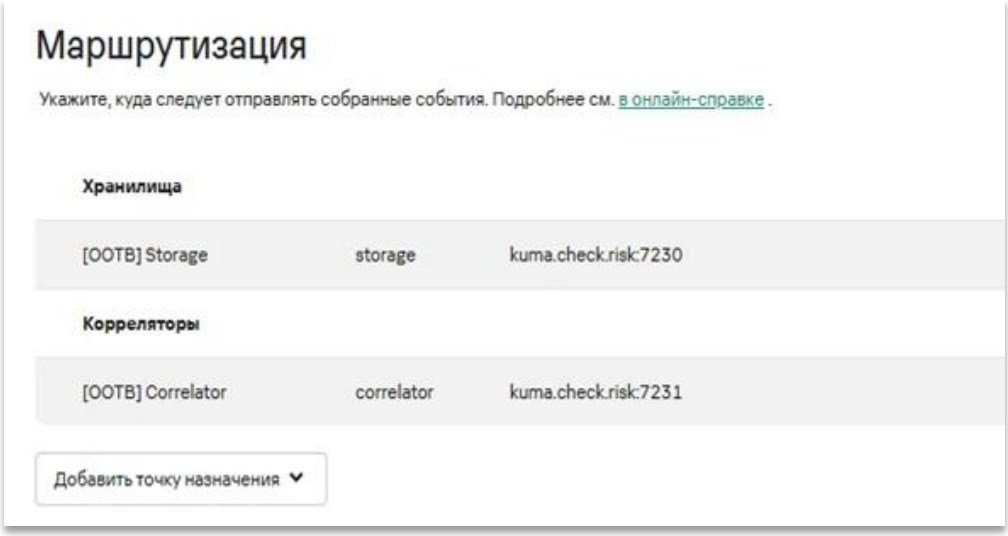
На вкладке «Транспорт» укажите транспортный протокол UDP и назначьте свободный порт для приёма сообщений. Убедитесь, что порт не занят другими сервисами.



На вкладке «Парсинг событий» в поле выбора нормализатора укажите ранее импортированный нормализатор Check Risk Waf.

СКРИН

На вкладке «Маршрутизация» проверьте, что у коллектора указан корректный путь к хранилищу и коррелятору. При необходимости добавьте дополнительные точки назначения.



При необходимости на вкладке «Проверка параметров» сохраните команду установки коллектора, которая будет показана для запуска на целевом сервере. Сохраните настройки коллектора нажатием «Сохранить коллектор».

СКРИН

Подключитесь к серверу, на которое будет устанавливаться коллектор, по SSH от имени root и выполните ранее сохранённую команду установки. Пример команды (в вашем окружении FQDN, идентификатор и порт будут отличаться; используйте значения, сгенерированные интерфейсом KUMA):

/opt/kaspersky/kuma/kuma collector --core https://kuma.check.risk:7210 --id 72faff01-5b10-4aed-bc9d-bf510f5c4b1c --api.port 7237 --install

После выполнения команды при необходимости выполните перезагрузку коллектора через интерфейс KUMA, выбрав нужный коллектор и нажав «Перезагрузить».

Контроль успешной установки: в интерфейсе «Активные сервисы» коллектор должен приобрести зелёный статус «работает».

СКРИН

Проведите тестовую отправку логов из Check Risk WAF на указанный UDP-порт и убедитесь, что события корректно проходят через нормализатор и поступают в назначенные точки хранения/корреляции. Для верификации используйте просмотр входящих событий в KUMA и/или логи коллектора.

Пример корректно нормализованного события безопасности:

СКРИН

Пример корректно нормализованного события доступа к ресурсу:

СКРИН

В данной инструкции представлена полная последовательность действий по интеграции Check Risk WAF с KUMA. Следуя описанным шагам — от импорта правила и его установки до создания коллектора и проверки нормализации — Вы обеспечите надёжную и корректную обработку событий.

Корректно установленный пакет нормализации позволит использовать события WAF в механизмах корреляции, настраивать оповещения, формировать отчёты и проводить расследования инцидентов в единой системе.

Если в процессе импорта или установки возникают ошибки, рекомендуется проверить версию пакета и совместимость с текущей версией SIEM, а также обратиться в техническую поддержку.

3.9 Анти-Бот система

В данном разделе описывается механизм противодействия автоматизированным запросам, имитирующим действия реальных пользователей. Анти-Бот система анализирует поведение клиента и предъявляет проверку, по результатам которой выдается криптографически защищенный токен. Наличие валидного токена позволяет проходить защиту без повторных проверок в течение заданного срока.

Модуль настраивается точечно: можно включить защиту для всего трафика либо ограничить применение правилами по атрибутам запроса.

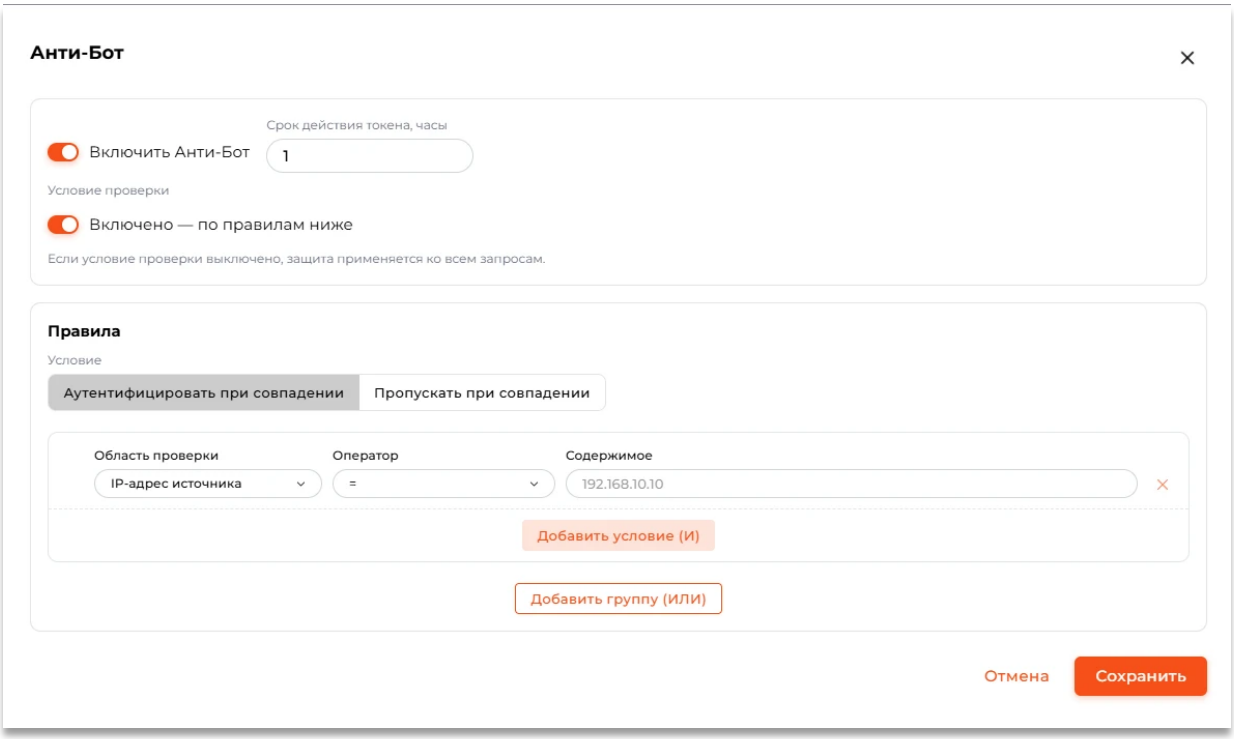
Ключевые цели механизма:

- ✓ Снижение нагрузки от сканеров, парсеров и скриптов массового перебора;
- ✓ Защита форм аутентификации, корзины и платежных маршрутов;
- ✓ Сохранение доступности легитимного трафика за счет гибкой логики исключений.

3.9.1 Порядок настройки и применения

Для активации защиты используйте переключатель «Включить Анти-Бот». После включения модуль начинает предъявлять проверку клиентам, не имеющим действующего токена. Параметр «Срок действия токена, часы» задает TTL выданного токена. Допустимый диапазон составляет от 1 до 168 часов.

> **Рекомендация:** рекомендуем выбирать минимально достаточное значение: Для публичных разделов обычно достаточно 8–24 часов; Для высокорисковых маршрутов целесообразно 1–4 часа.



При необходимости ограничьте область применения проверки. Для этого активируйте «Условие проверки». Если данное условие выключено, защита применяется ко всем входящим запросам без исключения. При включенном условии становятся доступны правила.

В блоке «Правила» определите логику работы модуля:

- ✓ переключатель «Условие» задает режим:

  — «Аутентифицировать при совпадении» означает, что проверка будет предъявляться только трафику, соответствующему заданным правилам;

  — «Пропускать при совпадении» означает, что совпавший трафик исключается из проверки.

- ✓ конструктор условий использует группы, объединенные отношениями «И» внутри группы и «ИЛИ» между группами. Это позволяет составлять как узкие, так и широкие фильтры.

- ✓ поле «Область проверки» определяет атрибут запроса. Наиболее востребованы: IP-адрес источника, заголовки клиента (например: User-Agent), путь URI, страна/ASN, наличие авторотационного заголовка.

- «Оператор» определяет тип сравнения. В простых сценариях достаточно «=».

- «Содержимое» содержит значение для сравнения. Пример:

  Область проверки — «IP-адрес источника», Оператор — «=», Содержимое — «192.168.10.10» (пример). Такое правило адресно применит или снимет защиту для указанного узла.

- используйте элементы «Добавить условие (И)» для уточнения в пределах группы и «Добавить группу (ИЛИ)» для альтернативных ветвей.

После составления правил сохраните изменения кнопкой «Сохранить».

3.9.2 Поведение при работе с токеном

- успешное прохождение проверки сопровождается выдачей токена, который передается клиентом в последующих запросах (как cookie или служебный заголовок, в зависимости от реализации);
- при истечении срока действия токена проверка предъявляется повторно;
- при удалении cookie или запрете их использования клиент будет получать проверку каждый раз, пока не будет выдан новый токен.

В данном разделе приведены принципы работы и порядок конфигурирования Анти-Бот системы, включая выпуск и срок действия токена, управление областью применения и конструирование правил.

Рекомендация: рекомендуем начинать с ограниченного набора условий и постепенно расширять покрытие, отслеживая метрики отказов и производительность.

Внимание: при обнаружении негативного влияния на легитимный трафик временно используйте режим «Пропускать при совпадении» для спорных источников и корректируйте признаки до достижения стабильного уровня защиты.

3.10 Рекомендации и лучшие практики

В данном разделе приведены практики по работе с настройкой правил исключений, которые позволят добавлять исключения так, чтобы пропустить трафик при ложном срабатывании и не ослабить защиту защищаемого приложения.

Ниже представлен перечень правил оптимизации настроек правил исключений и описание лучших практик их использования.

Минимизируйте область действия исключения

- ✓ Привязывайте правило к конкретному приложению и домену. Для этого используйте область проверки «Приложения» и по возможности «Хост» с оператором «Равно».
- ✓ Уточняйте путь и метод. Комбинируйте «Путь URL» или «URL» с оператором «Равно» либо «Начинается с», и добавляйте «HTTP-метод» со значением GET/POST/.... Такой подход исключает лишние совпадения.
- ✓ Не расширяйте границы совпадения без необходимости. Операторы «Содержит» и «regex» применяйте только тогда, когда точное сравнение невозможно. Для чувствительных маршрутов используйте точные пути и параметры.

Работайте адресно с параметрами и заголовками

- ✓ Для GET/POST-параметров и заголовков всегда указывайте имя поля в «sub_k» и подбирайте строгие операторы сопоставления. При необходимости используйте «Существует/Не существует» для валидации самого факта наличия поля.
- ✓ Устанавливайте значения так, как они видны в журнале: с учётом кодирования (%2F, %20 и т. п.). Это исключит расхождения при проверке «Равно».

Корректно комбинируйте условия

- ✓ Помните о логике конструктора: внутри группы условия связаны "И", между группами действует "ИЛИ". Стройте правило так, чтобы каждая группа описывала один допустимый вариант запроса.
- ✓ Переключатель «Инвертировать результат (НЕ)» используйте только при явной необходимости инверсия усложняет проверку и повышает риск охватить лишний трафик.

Избегайте чрезмерно общих исключений

- ✓ Не применяйте шаблоны, охватывающие весь путь, домен или тело запроса. Предпочитайте «Равно» вместо «Содержит», «Начинается с» вместо широких регулярных выражений. Это критично для исключений, связанных с типовыми атаками в параметрах.
- ✓ Для сложных случаев разбивайте исключение на несколько независимых групп "ИЛИ" или на отдельные правила, чтобы упростить аудит и откат.

Проверяйте результат и пересматривайте исключение

- ✓ После публикации проверяйте журнал событий: целевой запрос должен пройти без кода 403, а попытки эксплуатации уязвимостей по схожим маршрутам оставаться заблокированными. Используйте точные индикаторы из журнала для валидации.
- ✓ Устанавливайте регламент пересмотра исключений. Ложноположительные срабатывания обычно устраняются в приложении, после чего исключение следует сузить или удалить.

Ниже приведены короткие примеры в формате «Проблема → Решение»:

Проблема: блокируется единичный POST-запрос по точному URL из журнала инцидентов.

Решение: в конструкторе создайте правило с действием «Разрешить» и одной группой условий:

Приложения → Равно → нужный сайт; URL → Равно → значение из журнала (включая кодирование %); HTTP-метод → Равно → POST. Включите правило. Дополнительных операторов не требуется.

Проблема: CORS preflight (OPTIONS) ошибочно классифицируется как угроза.

Решение: одна группа условий: HTTP-метод → Равно → OPTIONS; Заголовок → «Origin» → оператор «Существует»; Заголовок → «Access-Control-Request-Method» → оператор «Существует». Действие «Разрешить».

Проблема: веб-хук от внешнего провайдера режется на уровне WAF, хотя источники IP доверенные.

Решение: одна группа условий: Путь URL → Равно → /webhook/provider; HTTP-метод → Равно → POST; IP-адрес источника → Равно → перечислите официальные IP провайдера. Действие «Разрешить».

Проблема: технический эндпойнт /admin/healthz нужен только из офисной сети, всё остальное должно блокироваться.

Решение: одна группа условий: Путь URL → Равно → /admin/healthz; HTTP-метод → Равно → GET; IP-адрес источника → оператор «В CIDR» → 10.10.0.0/16. Действие «Разрешить».

Проблема: один и тот же POST-эндпойнт корректно принимает два допустимых Content-Type. Первый проходит, второй блокируется.

Решение: используйте две группы условий, объединённых логикой ИЛИ:

первая группа: Приложения = сайт, Путь URL = /api/checkout, Метод = POST, Заголовок Content-Type = application/json;

вторая группа: те же признаки, но Content-Type = application/vnd.api+json. Кнопка «Добавить группу (ИЛИ)» доступна в конструкторе.

Проблема: ложное срабатывание на GET-параметр limit, когда значение в допустимом диапазоне 1–100.

Решение: одна группа условий: Путь URL → Равно → /api/search; Метод → Равно → GET; GET-параметры → имя limit → оператор «Регулярное выражение» → шаблон, ограничивающий значения 1–100.

Проблема: доступ к тестовому эндпойнту должен быть разрешён только из группы корпоративного VPN.

Решение: одна группа условий: Путь URL → Равно → /internal/test; Метод → Равно → POST; IP-адрес источника → оператор «В группе IP» → выберите нужную группу.

Проблема: в исключении ошибочно охватывается слишком широкий диапазон, из-за чего риск проницаемости повышен.

Решение: сузьте правило: предпочитайте операторы «Равно» и «Начинается с» для URL/Путь URL, исключите «Содержит» и избыточные регулярные выражения; не используйте инверсию «НЕ», если это не строго необходимо.

Проблема: требуется временно разрешить конкретный запрос, сохранив возможность быстрого отката.

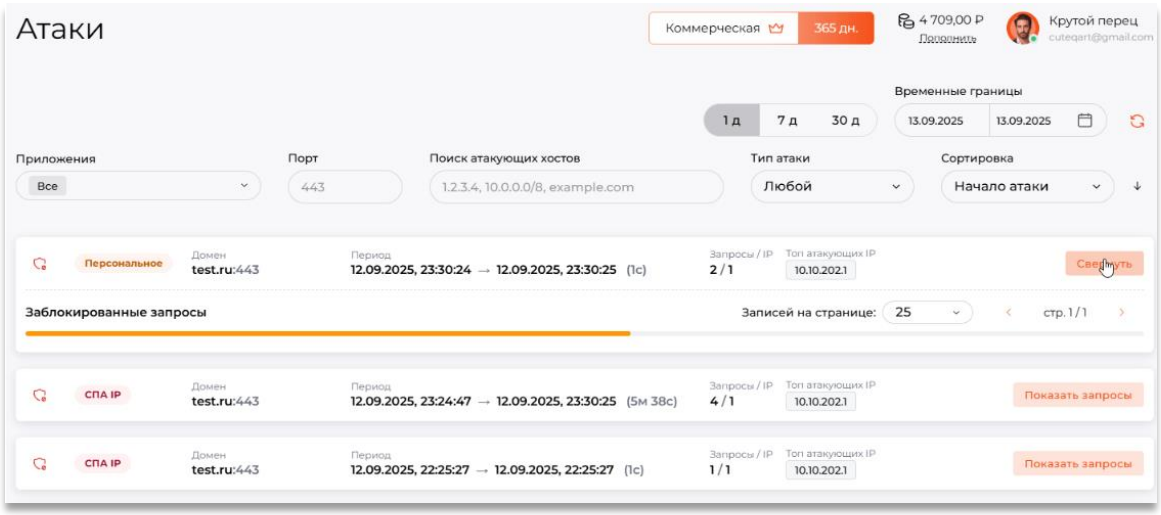
Решение: создайте отдельное правило с уникальным именем и описанием, установите действие «Разрешить», добавьте минимальный набор условий в одной группе, включите флаг «Включено». Для альтернативных вариантов запроса используйте дополнительные группы «ИЛИ», а не расширяйте одну группу.

> **Внимание:** Будьте предельно внимательны при создании правил исключения. ВСЕГДА проверяйте работоспособность, и анализируйте созданные исключения(е). Некорректно созданное(ные) правила могут существенно ослабить защиту приложения.

Данные примеры опираются на поддерживаемые области проверки и операторы конструктора правил, а также на механику групп «И»/ «ИЛИ» и доступные методы HTTP для формирования правил исключений.

3.11 Карточка угрозы

Карточка угрозы предназначена для оперативного анализа событий веб-приложения, зафиксированных WAF SaaS, быстрого принятия контрмер без переключения между разделами. В одном окне доступна техническая сводка по запросу, сработавшему правилу (с указанием сигнатуры и идентификатора), структурированные артефакты запроса, а также прикладные действия: добавление исходного IP-адреса в группу и формирование правила для конкретного URL и метода.

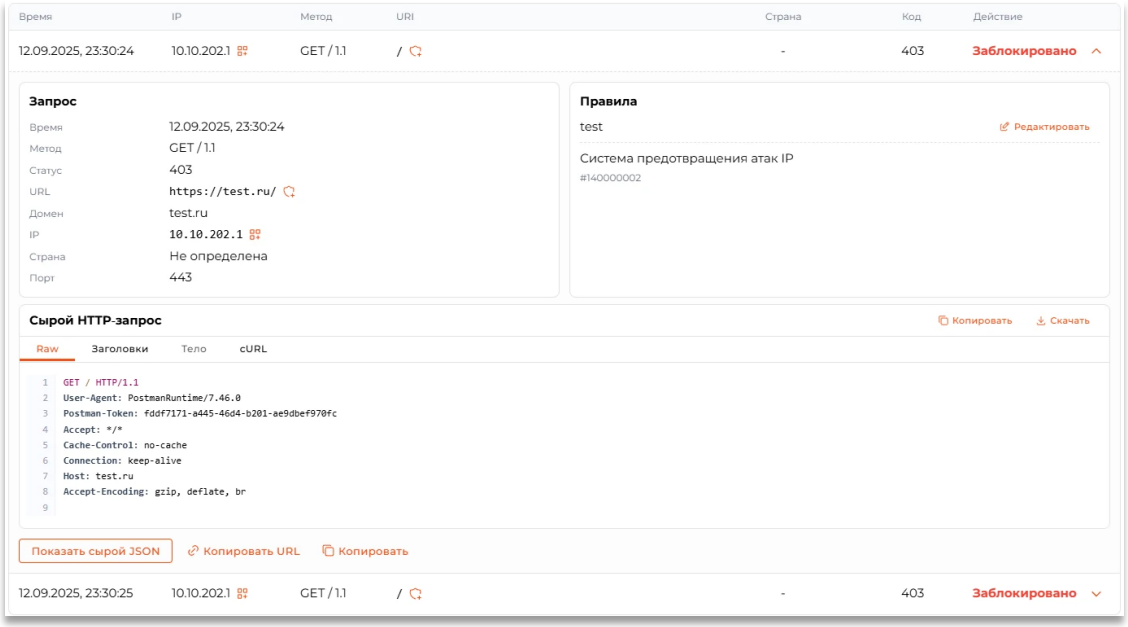


Для открытия карточки угрозы выберите запись в журнале событий безопасности или в перечне заблокированных запросов. Откроется детальная форма с двумя колонками: атрибуты события и контекст правила детектирования.

Что отображается в карточке

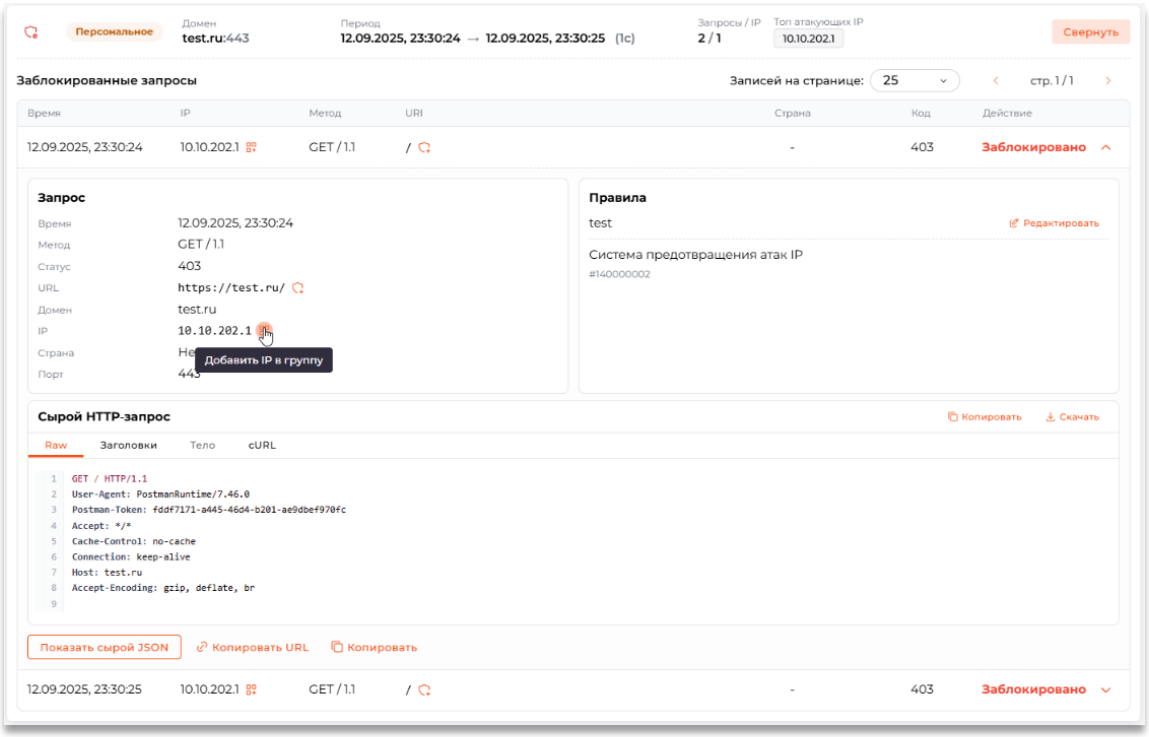
- ✓ Технические атрибуты запроса: дата и время, домен/приложение, IP клиента, порт, протокол, HTTP-метод, код ответа сервера.
- ✓ URL запроса целиком, включая строку запроса: рядом доступна иконка копирования для передачи артефакта в буфер обмена.
- ✓ Информация о сработавшем контроле: название и источник правила, идентификатор сигнатуры (например, SQL Injection via libinjection, ID 942100), уровень воздействия.

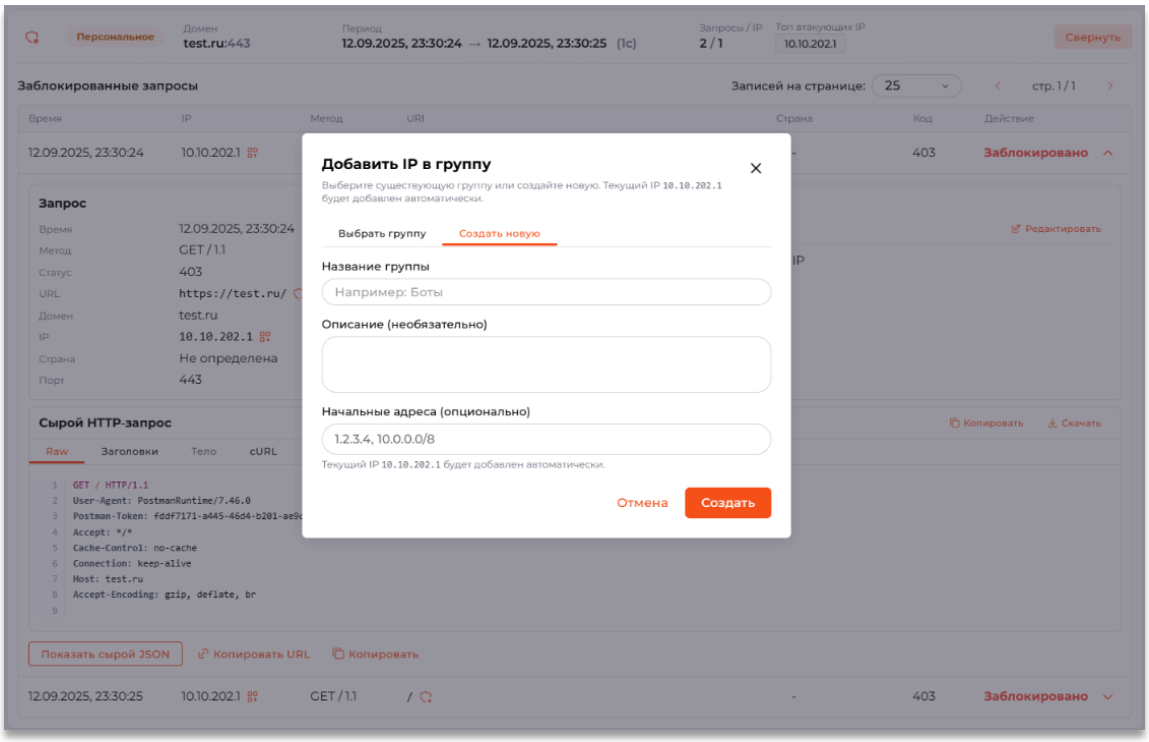
  Сырые данные запроса в нескольких представлениях: Raw, Заголовки, Тело (если присутствует), готовая команда cURL и JSON-представление события. Это позволяет быстро воспроизвести запрос, приложить артефакты к тикету и провести локальную валидацию.



3.11.1 Добавление IP-адреса в группу

- ✓ В области атрибутов события используйте контекстную команду «Добавить IP в группу».
- ✓ В открывшемся окне выберите существующую группу из справочника или переключитесь на вкладку создания новой группы.
- ✓ При создании новой группы заполните наименование и, при необходимости, описание; при желании укажите диапазоны адресов. Текущий IP будет добавлен автоматически.
- ✓ Сохраните изменения. Группа сразу доступна в политиках WAF, списках блокировки/наблюдения и отчетах.

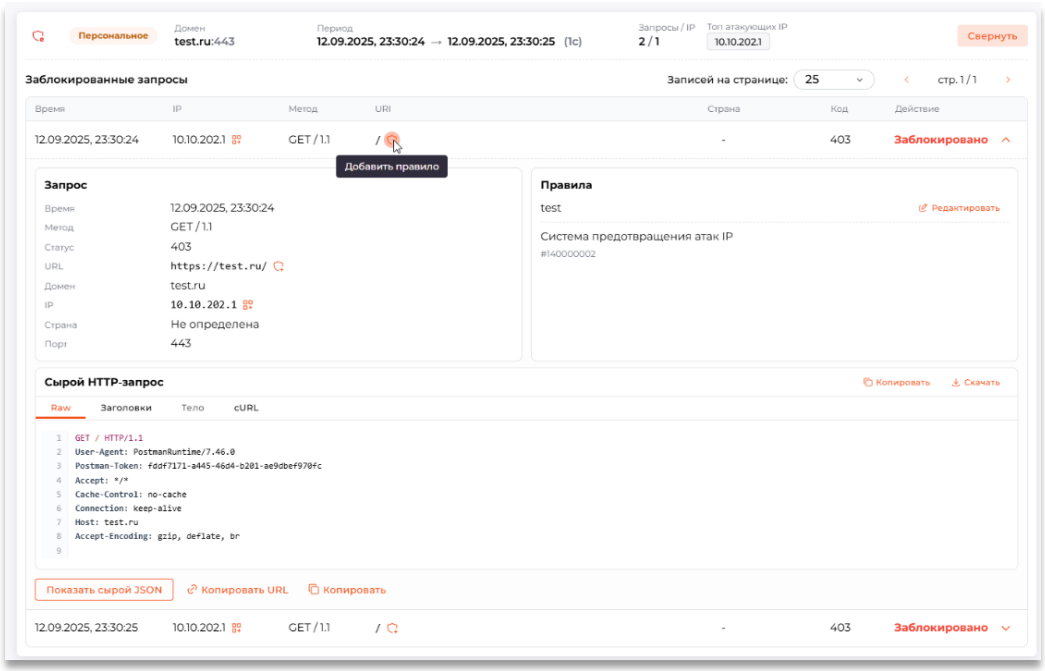


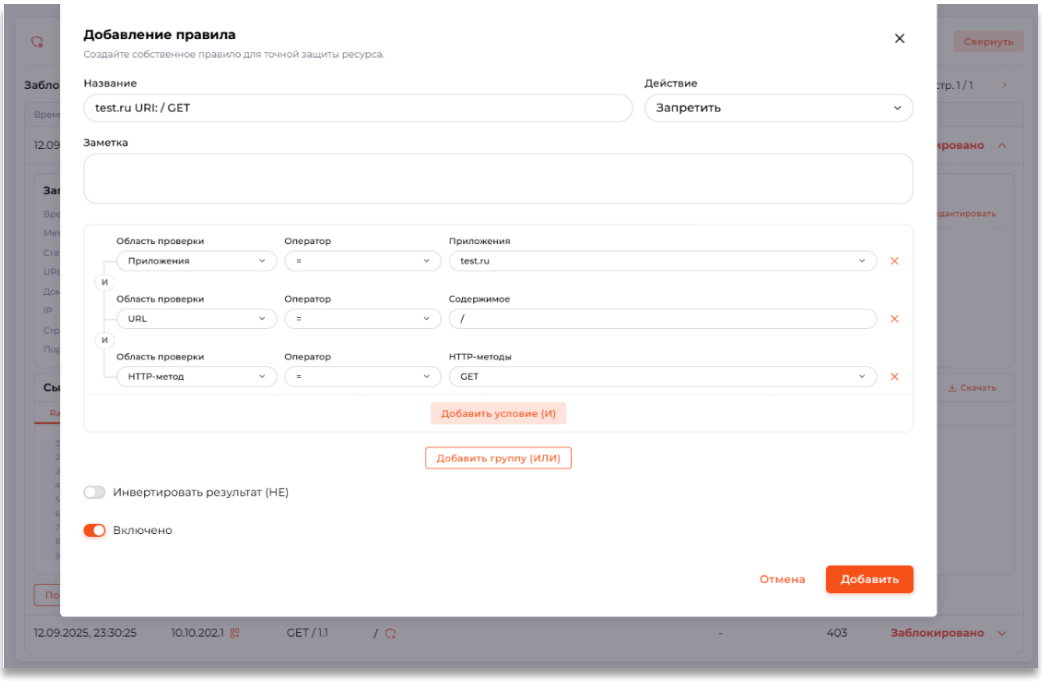


3.11.2 Добавление URL в карточку приложения и выпуск правила

- ✓ Для фиксирования наблюдаемого URL в рамках инвентарной карточки приложения используйте готовые действия карточки угрозы.
- ✓ Для немедленной защиты сформируйте правило непосредственно из карточки угрозы через команду «Добавить правило».

- ✓ В форме создания правила задайте действие «Запретить», укажите приложение, область проверки «URL» со значением из события и при необходимости ограничьте по HTTP-методу.
- ✓ Проверьте, что переключатель «Включено» активен, после чего сохраните правило. Фильтр вступит в силу сразу после публикации.

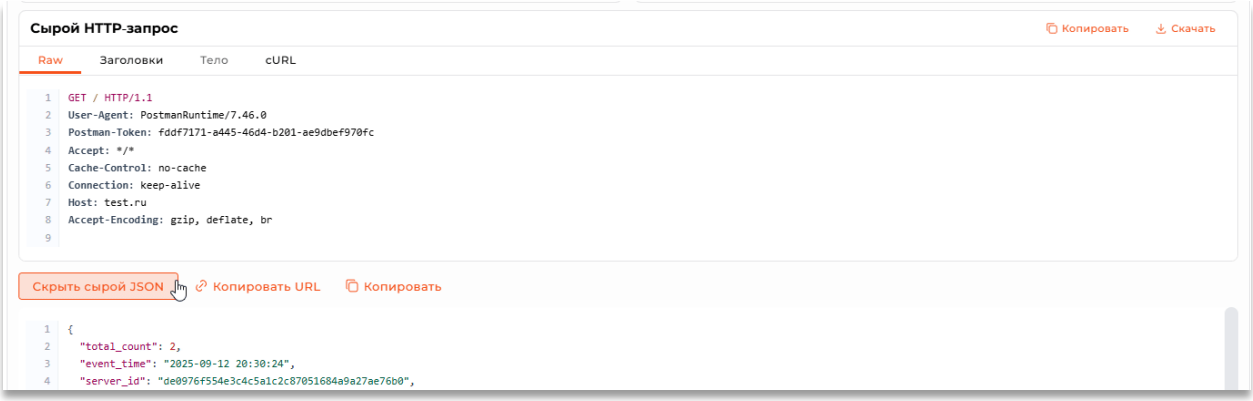




3.11.3 Экспорт и воспроизведение запроса

- ✓ Вкладка cURL содержит готовую команду для лабораторной проверки или воспроизведения инцидента в среде отладки.

- ✓ JSON-блок пригоден для загрузки в систему тикетов и для автоматизированной корреляции в SIEM/SOAR.
- ✓ Используйте иконки копирования/выгрузки для аккуратной передачи артефактов.



3.11.4 Практические рекомендации по применению

- ✓ Добавляйте IP в группу «Блокировка» только при достаточной уверенности; учитывайте NAT, прокси и адреса общих облачных провайдеров.
- ✓ Для повторяющихся атак на один и тот же путь выпускайте правило на уровень «Приложение + URL + Метод» вместо глобальной блокировки сети источника.
- ✓ Перед ужесточением политик сверяйте идентификатор правила детектирования и проверяйте воспроизводимость событием cURL.

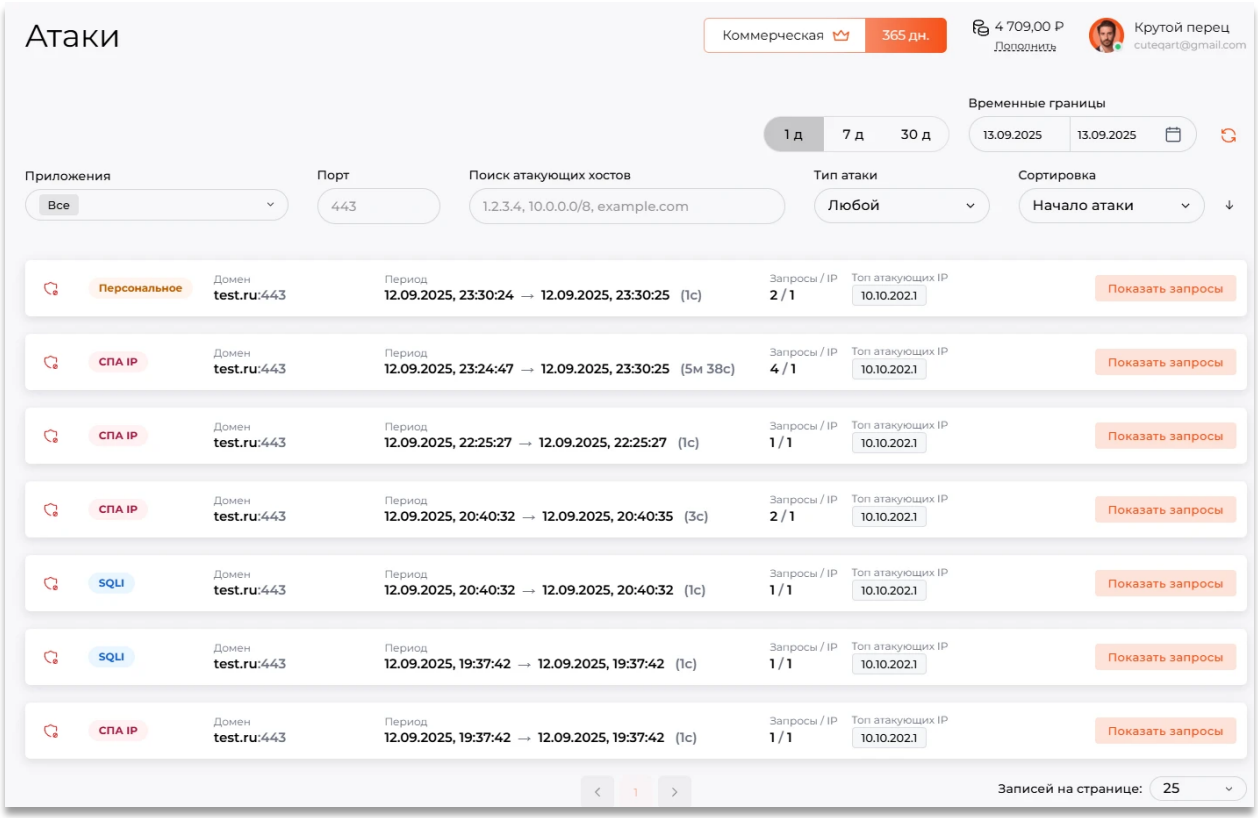
Карточка угрозы объединяет анализ и реагирование: Вы получаете полный контекст события, можете добавить IP в управляемую группу в карточке приложения, а также оперативно выпустить таргетированное правило без выхода из текущего интерфейса.

3.12 Управление угрозами

Данный раздел предназначен для оперативного мониторинга и обработки событий веб-атак, зафиксированных WAF SaaS. В интерфейсе консолидируются детектированные попытки эксплуатации уязвимостей (например, SQLi, LFI и др.), статус реакции WAF, ключевые атрибуты HTTP-запросов, атакующие IP-адреса и временные параметры инцидента.

3.12.1 Порядок работы

Для начала работы выберите приложение(я) и период анализа. Фильтры расположены в верхней панели: «Приложения», «Порт», «Поиск атакующих хостов», «Тип атаки», «Временные границы», «Сортировка». После применения



фильтров отобразится лента инцидентов с группировкой по типам атак и доменам.

Для углубленного анализа откройте карточку интересующей атаки. В карточке отображаются: период активности, домен и порт, «Запросы/IP», «Топ атакующих IP», статус реакции («Заблокировано»). Кнопкой «Показать запросы» раскройте перечень конкретных HTTP-запросов. Для подтверждения природы атаки используйте вкладки блока «Сырой HTTP-запрос»:

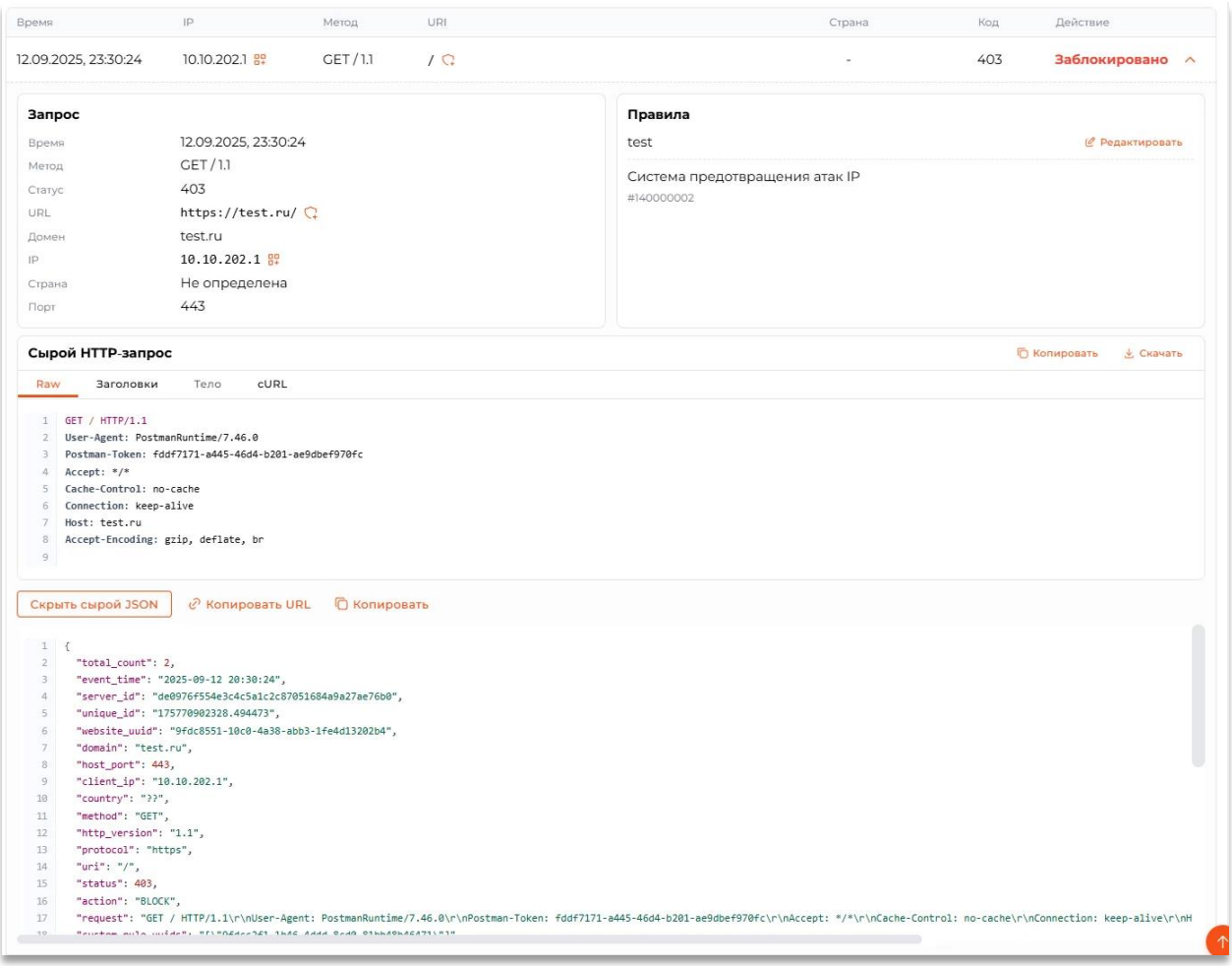
«Raw» для просмотра линии запроса и итоговой сборки пакета.

«Заголовки» для анализа User-Agent, Accept, Cache-Control и иных заголовков, влияющих на трактовку запроса сервером.

«Тело» при наличии POST-данных.

«cURL» для воспроизведения запроса в контролируемой среде

Доступны сервисные действия: «Показать сырой JSON» для экспорта артефактов, «Копировать URL» и «Копировать» для быстрого переноса данных в тикет-систему.



При необходимости сузьте область поиска по атакующему IP через поле «Поиск атакующих хостов». Для анализа динамики используйте пред установки периодов (1 день, 7 дней, 30 дней) или выберите даты вручную в «Временных границах».

Рекомендуется при быстрой оценке угрозы:

- ✓ Проверять соответствие срабатывания содержимому запроса и правилу детекта, указанному в блоке «Правила» (например, «SQL Injection Attack Detected via libinjection»).
- ✓ Сопоставлять количество «Запросов/IP» и «Топ атакующих IP» для выявления автоматизированных кампаний.
- ✓ Экспортировать артефакты (JSON, cURL) для последующей корреляции в SIEM.

- ✓ При повторяющихся источниках использовать смежный функционал портала (раздел «IP-группы») для временной блокировки или создания исключений в соответствии с Вашей политикой.

Раздел «Управление угрозами» обеспечивает полный цикл первичной обработки инцидентов веб-безопасности: обнаружение, верификацию, документирование и передачу на последующие этапы реагирования. Регулярное использование фильтров, детального просмотра сырого трафика и экспорта артефактов позволяет быстро отсекать ложные срабатывания, фиксировать реальные попытки эксплуатации и поддерживать актуальность защитных мер WAF SaaS без снижения доступности приложений.

4. Правила безопасности

4.1 Проверка работоспособности правила

В данном разделе описывается порядок верификации созданных правил WAF, включая проверку корректности логики условий, статуса включения, ожидаемого эффекта на трафик и фиксацию результата в журналах. Правила поддерживают объединение условий внутри группы по логике И, объединение групп по логике "ИЛИ", а также инверсию общего результата через параметр «Инвертировать результат "НЕ"». Действие правила задается как «Разрешить» либо «Запретить», а само правило имеет признак «Включено». Указанные элементы и их семантика соответствуют спецификации конструктора правил.

Для проверки правила выполните следующие действия в интерфейсе и через сетевые запросы.

- ✓ **Убедитесь, что правило сохранено и активно.**
  Проверьте, что правило отображается в перечне, действие соответствует требуемому сценарию, переключатель «Включено» активен.
- ✓ **Просмотрите конфигурацию условия.**
  Откройте карточку правила и проверьте: область проверки, оператор, содержимое значений, состав групп и наличие/отсутствие инверсии результата. Для составных правил подтвердите ожидаемую логику "И" и "ИЛИ".
- ✓ **Выполните тестовые HTTP-запросы из среды, подпадающей под условия.**
  Рекомендуется использовать изолированный источник трафика (VPN-выход, отдельный сервер) с предсказуемым исходящим IP. Базовая проверка статуса ответа:

curl -s -o /dev/null -w '%{http_code}\n' https://<ваш-домен>/

Ожидаемые коды:

Для правил **«Запретить»** — код блокировки приложения (например, 403) либо фирменная страница WAF;

Для правил **«Разрешить»** — успешный код приложения (обычно 200/302).

✓ **Зафиксируйте проверку поведения при альтернативных группах.**

Если правило содержит несколько групп (логика "ИЛИ"), выполните запросы из каждой релевантной среды, чтобы подтвердить, что срабатывает хотя бы одна группа, а лишние группы не влияют на итоговый результат.

✓ **При наличии прокси/CDN проверьте источник IP, который анализирует WAF.**

Убедитесь, что система использует реальный клиентский адрес, а не IP узла CDN. В тестах не полагайтесь на подстановку заголовков со стороны клиента («X-Forwarded-For») без правильно настроенного доверенного списка, иначе результат проверки будет недостоверным.

✓ **Проверьте журналы событий WAF.**

Откройте журнал и убедитесь, что запросы из тестовой среды зафиксированы с указанием действия правила («разрешено» или «запрещено»), совпадает область проверки и оператор, а также отображается ссылка на имя правила.

✓ **Подтвердите отсутствие побочных эффектов.**

Выполните контрольные запросы из легитимных сред, не подпадающих под условия, чтобы убедиться в отсутствии ложных срабатываний.

> ! Рекомендуется хранить артефакты проверки: командные строки, временные IP тестовой среды, отметки из журналов и полученные коды ответов. Для сложных правил документируйте, какие группы и условия обеспечили срабатывание. При изменении набора значений в условиях (например, актуализация подсетей или групп IP) следует повторять проверку по указанной схеме и фиксировать результат в журнале изменений. Логика объединения условий и групп, а также параметр инверсии результата остаются ключевыми точками контроля при каждом цикле проверки

4.2 Добавление IP адреса в черный список

В данном разделе описывается добавление правила, блокирующего трафик с указанных IP-адресов на уровне WAF. Реализация выполняется через действие «Запретить» и условие «IP-адрес источника». Условия внутри одной группы соединяются логикой "И", разные группы объединяются логикой "ИЛИ". При необходимости доступна инверсия результата через параметр «Инвертировать результат "НЕ"». Данная логика соответствует спецификации конструктора правил.

Для добавления IP-адреса в черный список выполните последовательность действий, представленную ниже:

1. Откройте раздел «Правила» и используйте кнопку «Добавить правило». В открывшемся окне в поле «Действие» выберите «Запретить».
2. В группе условий задайте проверку источника:

   Область проверки: «IP-адрес источника».

   Оператор выбирается в соответствии с задачей:

   - ✓ «Равно» для блокировки конкретного IPv4/IPv6.
   - ✓ «В CIDR» для блокировки подсети в формате 192.0.2.0/24 или 2001:db8::/32.
   - ✓ «В группе IP» при использовании заранее подготовленных IP-групп.
   - ✓ «В геолокации» для блокировки стран по ISO-2. Замечание: геолокация по IP является оценочной и не должна рассматриваться как безусловно точная.
3. В поле «Содержимое» укажите адреса или диапазоны. Каждый элемент вводится отдельно. Для «В группе IP» и «В геолокации» выберите значения из выпадающего списка.
4. При необходимости расширьте критерии:
   - ✓ «Добавить условие "И"» для совмещения нескольких проверок в одной группе (все условия должны выполниться).
   - ✓ «Добавить группу "ИЛИ"» для альтернативных наборов условий (достаточно выполнения одной группы).
5. Не используйте переключатель «Инвертировать результат "НЕ"», если требуется классический черный список. Инверсия применяется для специфических сценариев исключения и в типовой конфигурации не нужна.

6. Убедитесь, что переключатель «Включено» активен, затем сохраните изменения кнопкой «Добавить».

> Рекомендуется указывать минимально необходимый набор адресов и подсетей, збегать широких масок без необходимости, регулярно актуализировать IP-группы и верифицировать правило на тестовой среде. При использовании прокси или CDN убедитесь, что в правилах учитывается реальный клиентский IP (например, по проксируемым заголовкам, если это предусмотрено инфраструктурой). После применения правила выполните проверку журналов WAF и доступности администраторских интерфейсов с доверенных сетей, чтобы исключить блокировку легитимного трафика.

4.3 Настройка разрешающего правила

В данном разделе описывается порядок настройки разрешающего правила в WAF SaaS. Разрешающее правило применяется к входящим HTTP-запросам и предназначено для безопасного пропуска трафика, который должен игнорироваться механизмами блокировки. Условие считается выполненным, если запрос соответствует хотя бы одной группе условий. Внутри группы условия объединяются логикой "И", между группами используется логика "ИЛИ". При необходимости можно инвертировать параметры привила переключателем «Инвертировать результат "НЕ)».

Для создания разрешающего правила откройте раздел «Правила» и инициируйте создание нового правила. В параметре «Действие» выберите «Разрешить». Введите понятное «Название» и при необходимости заполните «Описание». Откроется форма конструктора условий.

В блоке «Группа условий» задаются проверки. Внутри одной группы все условия должны выполняться одновременно. Для добавления новых проверок внутри группы используйте кнопку «Добавить условие "И"». Для расширения набора альтернативных сценариев разрешения используйте кнопку «Добавить группу "ИЛИ"». Опция «Инвертировать результат "НЕ"» меняет логику итогового совпадения. Переключатель «Включено» активирует правило после сохранения.

В каждой строке условия последовательно укажите область проверки, оператор и значение. Справочная матрица поддерживаемых полей и операторов приведена ниже. Значения можно указывать по одному или нескольким

значением, интерфейс принимает набор значений и трактует их как «любое из». Для заголовков и параметров нужно указать имя поля.

4.3.1 Области проверки и операторы

- ✓ IP-адрес источника. Доступны операторы: «Равно», «Не равно», «Неточное совпадение», «В CIDR», «Не в CIDR», «В группе IP», «Не в группе IP», «В геолокации», «Не в геолокации». Значения: IPv4 или IPv6, сетевые маски CIDR, UUID групп IP и коды стран ISO-2. Доступен выбор «Группа IP» и «Страны».

- ✓ Приложения. Операторы: «Равно», «Не равно». Значения: один или несколько ресурсов из Вашего списка приложений. Список формируется автоматически и доступен в выпадающем меню.

- ✓ URL и Путь URL. Операторы: «Равно», «Не равно», «Содержит», «Не содержит», «Начинается с», «Регулярное выражение». Значения: строки или регулярные выражения.

- ✓ Хост. Операторы: «Равно», «Не равно», «Не чёткое совпадение». Значения: доменные имена.

- ✓ Заголовок, GET-параметр, POST-параметр. Операторы: «Равно», «Не равно», «Содержит», «Не содержит», «Регулярное выражение», «Существует», «Не существует». Обязательно укажите имя поля. Для операторов «Существует» и «Не существует» значение можно не задавать.

- ✓ Тело запроса. Операторы: «Регулярное выражение», «Содержит», «Не содержит». Значения: строки или выражения.

- ✓ HTTP-метод. Операторы: «Равно», «Не равно». Значения: один или несколько из GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS, TRACE, CONNECT.

4.3.2 Рекомендованные сценарии настройки

- ✓ Разрешение по IP или сети: Выберите «IP-адрес источника», оператор «Равно» для конкретных адресов или «В CIDR» для подсети. Укажите адреса или маски. Это корректный способ белого списка для административных зон.

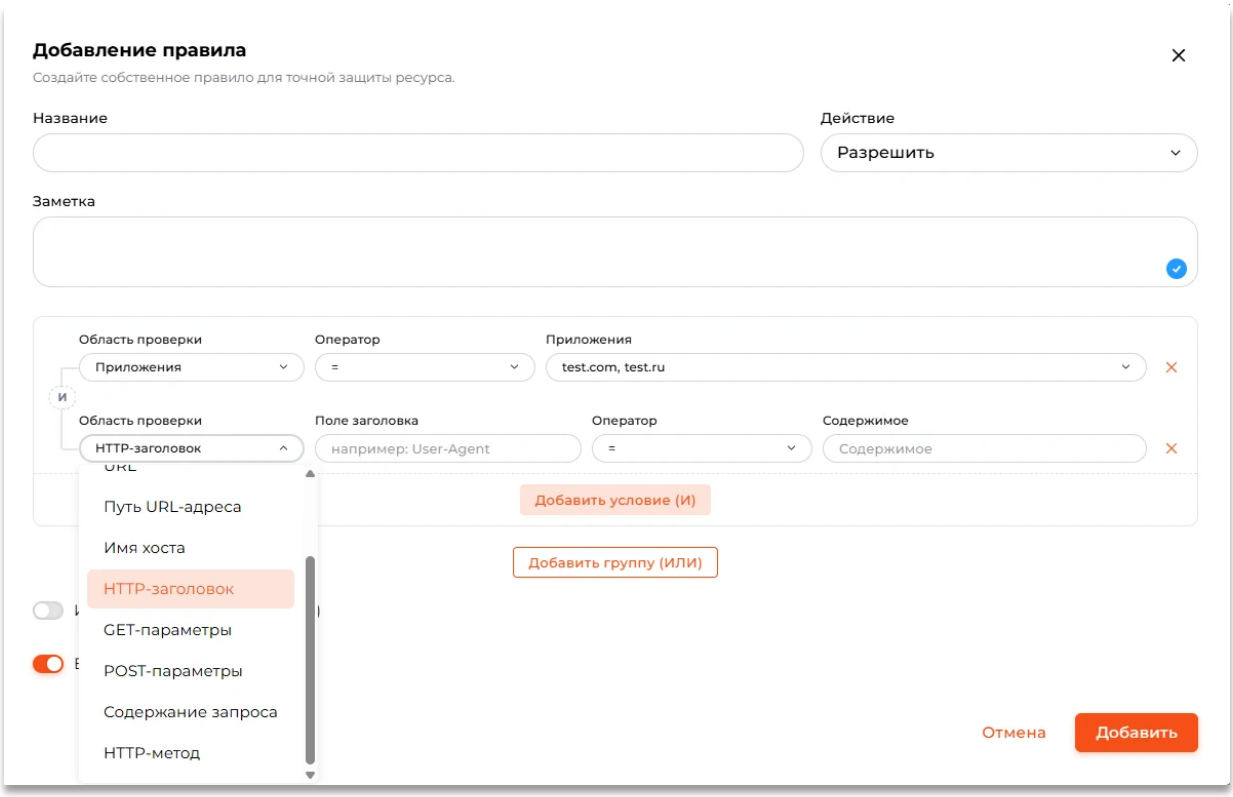
- ✓ Разрешение для доверенной IP-группы: Выберите оператор «В группе IP», затем укажите одну или несколько групп. Используйте этот подход для централизованного управления списками.

- ✓ Разрешение по приложению: Укажите «Приложения», оператор «Равно», затем выберите нужные ресурсы. Подходит для локальной отладки отдельных сайтов.

- ✓ Разрешение по HTTP-методу: Укажите «HTTP-метод» и добавьте, например, «GET» и «HEAD», если требуется пропускать только чтение.

- ✓ Разрешение при наличии конкретного заголовка: Выберите «Заголовок», заполните имя поля, оператор «Существует» и сохраните. Используется для пропуска трафика от доверенного балансировщика.

Для сохранения нажмите «Добавить». После создания правило появится в перечне и может быть включено или отключено переключателем состояния.



Разрешающие правила следует формулировать минимально необходимыми, чтобы не расширять поверхность риска. Рекомендуется использовать точные критерии: IP-адреса, группы IP, конкретные заголовки и методы. Для сложных сценариев объединяйте проверки через «И» внутри группы и разделяйте альтернативы через «ИЛИ» между группами. При использовании инверсии оцените итоговую логику совпадения, так как переключатель «Инвертировать результат (НЕ)» меняет результат проверки целиком. Допускается указывать несколько значений в одном условии, что упрощает поддержку правил без потери прозрачности.

4.4 Настройка правил

В данном разделе настраиваются правила веб-экрана (WAF), определяющие, какие запросы к Вашим приложениям будут разрешены или заблокированы согласно пользовательским правилам. Правило состоит из действия (Разрешить или Запретить), набора условий и их логики объединения.

Условия внутри одной группы проверяются по логике "И", разные группы объединяются по логике "ИЛИ". При необходимости можно инвертировать правила переключателем «Инвертировать результат (НЕ)».

Интерфейс поддерживает добавление и удаление условий и групп, а также выбор областей проверки (IP-адрес источника, URL, заголовки, параметры и другое) и соответствующих операторов совпадения, включая регулярные выражения, CIDR и географию.

Для добавления правила откройте форму «Добавление правила». Укажите имя и выберите действие. Для блокирующей модели используйте «Запретить», для пропускной модели используйте «Разрешить».

Далее задайте логику проверки:

1. В «Группе условий» задайте одно или несколько условий. Кнопка «Добавить условие (И)» добавляет дополнительную проверку внутри группы. Кнопка «Добавить группу (ИЛИ)» создает альтернативную ветку, которая тоже может сработать. Кнопки удаления доступны для условий и для групп.

2. В каждом условии выберите область проверки, оператор и значения. Поле «Содержимое» принимает один или несколько элементов, что интерпретируется как «любой из указанных». Если оператор «Существует» или «Не существует», поле значений не требуется.

3. Переключатель «Инвертировать результат (НЕ)» меняет смысл всей логической конструкции (удобно для исключений). Переключатель «Включено» активирует или временно отключает правило без удаления.

4.4.1 Доступные области и ключевые операторы

✓ IP-адрес источника. Операторы: равно, не равно, неточное совпадение, в CIDR, не в CIDR, в группе IP, не в группе IP, в геолокации, не в геолокации. Для CIDR поддерживаются стандартные маски. Для «группы IP» выбираются заранее созданные группы. Для геолокации используются коды стран ISO-2.

✓ Приложения (сайты). Операторы: равно, не равно. Значения — UUID Ваших приложений.

- ✓ URL и Путь URL. Операторы: равно, не равно, содержит, не содержит, начинается с, регулярное выражение. Регулярные выражения проверяются на стороне сервера.

- ✓ Хост. Операторы: равно, не равно, неточное совпадение.

- ✓ Заголовок, GET-параметр, POST-параметр. Операторы: равно, не равно, содержит, не содержит, регулярное выражение, существует, не существует. Для этих областей обязательно указать имя поля (пример: User-Agent, X-Request-ID или имя параметра).

- ✓ Тело запроса. Операторы: регулярное выражение, содержит, не содержит.

- ✓ HTTP-метод. Операторы: равно, не равно. Поддерживаются стандартные методы (GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS, TRACE, CONNECT).

4.4.2 Пример практических примеров конфигураций

- ✓ Разрешить доступ только из офисных подсетей. Задайте область «IP-адрес источника» с оператором «в CIDR», перечислите нужные подсети. При необходимости добавьте вторую группу по логике ИЛИ для временных IP гостей.

- ✓ Заблокировать попытки доступа к административным разделам. Используйте область «Путь URL» с операторами «начинается с» или «регулярное выражение» для путей вида /admin, /manage.

- ✓ Отсеять запросы без обязательного заголовка. Область «Заголовок», укажите имя заголовка и оператор «существует». Альтернативно инвертируйте итог, чтобы правило сработало на все, кроме запросов с заголовком.

Внимание: перед сохранением проверьте, что в каждой группе присутствует хотя бы одно условие, а в каждом условии корректно заполнены обязательные поля (в том числе имя поля для заголовков и параметров).

После нажатия «Добавить» правило будет создано и, если включено, начнет применяться к трафику.

Рекомендация: мы рекомендуем сначала начинать с правил в режиме «Разрешить» для точечного допуска, затем добавлять блокирующие проверки по мере накопления телеметрии и метрик.

Поддерживайте структуру: одна группа — строгие условия по логике И, дополнительные группы — альтернативные сценарии по логике "ИЛИ". Используйте «Инвертировать результат (НЕ)» для построения исключений без усложнения дерева. Для IP предпочтительнее использовать группы и CIDR, для строковых полей — явные префиксы и регулярные выражения только там, где это действительно необходимо.

4.5 Настройка запрета по гео-локации GeoIP

В данном разделе описывается создание правила, которое блокирует трафик из выбранных стран по данным GeoIP. Проверка выполняется по стране происхождения IP-адреса источника запроса. Для реализации используется действие «Запретить» и оператор «В геолокации» либо «Не в геолокации» в области проверки «IP-адрес источника». Условия в одной группе соединяются логикой "И", разные группы объединяются логикой "ИЛИ". При необходимости возможна инверсия результата через параметр «Инвертировать результат "НЕ"». Указанные операторы и логика подтверждены спецификацией конструктора правил.

Для настройки запрета по геолокации выполните действия, приведенные ниже.

1. Откройте раздел «Правила» и используйте кнопку «Добавить правило». В открывшемся окне в поле «Действие» укажите «Запретить».

2. В группе условий задайте проверку источника:

   Область проверки: «IP-адрес источника».

   Оператор:

   ✓ «В геолокации» чтобы заблокировать список выбранных стран.
   ✓ «Не в геолокации» чтобы заблокировать все страны, кроме выбранных (подходит для «разрешить только...» сценариев).

   Значения стран выбираются из выпадающего списка по привычным наименованиям, при этом в правило сохраняются коды ISO-3166-1 alpha-2.

3. Укажите одну или несколько стран. Каждая страна добавляется отдельным элементом. Для корректной работы допускается смешанное указание нескольких регионов.

4. При необходимости уточните область действия правила:
   ✓ «Добавить условие "И"» чтобы совместить географическую проверку с другими критериями, например «Приложения» или «URL».
   ✓ «Добавить группу "ИЛИ"» чтобы задать альтернативные наборы критериев, например разные страны для разных приложений.

5. Оставьте переключатель «Инвертировать результат "НЕ"» выключенным для типового сценария блокировки по географии. Данный параметр используется для специфических схем и в большинстве случаев не требуется.

6. Убедитесь, что переключатель «Включено» активен, затем сохраните изменения кнопкой «Добавить».

Рекомендуется комбинировать GeoIP с дополнительными условиями (например, «Приложения», IP-группы, точные CIDR), чтобы минимизировать риск ложных блокировок. Следует учитывать, что точность геолокации ограничена: прокси, VPN, мобильные операторы и облачные площадки могут изменять определяемую страну. При использовании CDN либо обратного прокси

необходимо убедиться, что WAF анализирует реальный клиентский IP (например, по доверенным заголовкам), иначе геолокация будет применяться к адресу узла CDN.

> **Внимание:** после включения правила рекомендуется проверить журналы WAF и базовую доступность пользовательских сценариев из допустимых регионов, прежде чем распространить правило на продуктивную среду.

4.6 Добавление IP адреса в белый список

В данном разделе описывается добавление правила, пропускающего трафик с доверенных IP-адресов без блокировки со стороны WAF. Механизм реализуется через действие «Разрешить» и условие проверки «IP-адрес источника». Условия внутри одной группы объединяются логикой И, разные группы объединяются логикой "ИЛИ". Дополнительно доступна инверсия результата проверки через параметр «Инвертировать результат "НЕ"».

4.6.1 Порядок добавления IP-адреса в белый список

Для добавления IP-адреса в белый список выполните действия, описанные ниже:

1. Откройте раздел «Правила» и используйте кнопку «Добавить правило». В появившемся окне задайте действие «Разрешить».

2. В блоке «Группа условий» настройте проверку.

   Область проверки: «IP-адрес источника».

   Оператор выбирайте в зависимости от задачи:

   - ✓ «Равно» когда требуется разрешить конкретный IPv4 или IPv6.
   - ✓ «В CIDR» когда нужно разрешить подсеть в формате 10.0.0.0/8 или 2001:db8::/32.
   - ✓ «В группе IP» когда используются заранее подготовленные группы адресов.
   - ✓ «В геолокации» когда допускается доступ из выбранных стран по ISO-2.

3. В поле «Содержимое» укажите один или несколько значений. Каждое значение вводится отдельным элементом. Допустимы записи одиночных IP и сетей CIDR. Для «В группе IP» и «В геолокации» выбирайте элементы из выпадающего списка.

4. При необходимости расширьте правило:
   - ✓ «Добавить условие "И"» когда нужно одновременно учесть несколько критериев в одной группе.
   - ✓ «Добавить группу "ИЛИ"» когда допускаются альтернативные наборы критериев.

   Пример: одна группа для конкретных IP, другая группа для служебной подсети.

5. Оставьте переключатель «Инвертировать результат "НЕ"» выключенным. Этот режим предназначен для исключающих сценариев и в контексте белого списка обычно не применяется.

6. Убедитесь, что переключатель «Включено» активен, затем сохраните изменения кнопкой «Добавить».

> ! Рекомендуется ограничивать белые списки минимально необходимыми диапазонами и конкретными адресами, регулярно актуализировать группы IP, а также проверять поведение на тестовой среде перед переносом в продуктив. После добавления правила проконтролируйте журналы WAF, чтобы убедиться, что запросы с разрешенных адресов проходят без ложных блокировок и что побочных эффектов не наблюдается.

4.7 Настройка блокирующего правила

В данном разделе описан порядок создания и включения блокирующих правил WAF SaaS с действием «Запретить». Правило сопоставляет входящий HTTP-трафик с набором условий. Логика объединения условий в правиле, следующая: условия внутри одной группы соединяются по логическому "И", разные группы соединяются по логическому "ИЛИ". При необходимости Вы

можете инвертировать общий результат срабатывания переключателем «Инвертировать результат (НЕ)».

Области проверки включают IP-адрес источника, приложения, URL, путь URL, хост, заголовки, GET и POST-параметры, тело запроса, а также HTTP-метод. Доступные операторы зависят от выбранной области, например для IP поддерживаются точное сравнение, проверка по CIDR, группы IP и геолокация, для параметров и заголовков доступны «Содержит», «Не содержит», «Регулярное выражение» и проверки наличия, для метода доступны «Равно» и «Не равно».

4.7.1 Порядок настройки

Для добавления блокирующего правила нажмите кнопку «Добавить правило». В открывшемся окне укажите понятное имя, в поле «Действие» выберите «Запретить», после чего соберите условия в конструкторе. Используйте «Добавить условие (И)» для добавления нового критерия внутри группы и «Добавить группу (ИЛИ)» для альтернативных веток. Переключатель «Инвертировать результат (НЕ)» применяйте только если необходимо обратить итоговую логику сопоставления. Завершите конфигурацию кнопкой «Добавить» и убедитесь, что переключатель «Включено» активен.

При выборе области проверьте допустимые операторы и требования к значениям:

- ✓ Для «IP-адрес источника» доступны: «Равно», «Не равно», «Неточное совпадение», «В CIDR», «Не в CIDR», «В группе IP», «Не в группе IP», «В геолокации», «Не в геолокации». Значения вводятся в формате IP, CIDR, UUID группы IP либо ISO-2-коды стран.

- ✓ Для «Заголовок», «GET-параметры», «POST-параметры» необходимо указать имя поля. Доступны операторы «Равно», «Не равно», «Содержит», «Не содержит», «Регулярное выражение», «Существует», «Не существует».

- ✓ Для «HTTP-метод» поддерживаются «Равно» и «Не равно» с перечислением методов из стандартного набора, включая GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS, TRACE, CONNECT.

4.7.2 Примеры конфигураций

✓ **Блокировка подсетей сканера**

Область проверки: IP-адрес источника. Оператор: «В CIDR». Содержимое: 203.0.113.0/24, 198.51.100.0/24. Действие: «Запретить».

✓ **Блокировка нежелательных методов**

Область проверки: HTTP-метод. Оператор: «Равно». Содержимое: TRACE, CONNECT. Действие: «Запретить».

✓ **Комбинированное правило для административного пути**

Группа условий №1: Путь URL — «Начинается с» — /admin; IP-адрес источника — «Не в CIDR» — 10.0.0.0/8, 192.168.0.0/16.

Действие: «Запретить».

При необходимости добавьте вторую группу через «Добавить группу "ИЛИ"», например альтернативу «Заголовок User-Agent содержит sqlmap».

✓ **Геоблокировка выбранных стран**

Область проверки: IP-адрес источника. Оператор: «В геолокации». Содержимое: ISO-2-коды стран, например CN, BR. Действие: «Запретить».

Для продвинутых сценариев уместно использовать инверсию результата. Например, если требуется заблокировать все, кроме трафика из IP-группы «Корпоративная сеть», соберите группу с «IP-адрес источника» и включите «Инвертировать результат (НЕ)». Итоговая логика: будет заблокирован любой запрос, который не соответствует заданной группе.

> **Внимание:** перед включением правила рекомендуется проверить корректность значений IP и масок CIDR, аккуратно использовать регулярные выражения и избегать чрезмерно широких условий, способных привести к ложным срабатываниям.

Для сложных политик используйте разбиение на несколько групп условий с "ИЛИ", а внутри групп комбинируйте точные критерии по "И". При

необходимости оперативной отмены оставляйте переключатель «Включено» под контролем и применяйте удаление отдельных групп или условий через соответствующие элементы интерфейса.

Контакты службы поддержки

Если решить проблему самостоятельно не удалось, свяжитесь со службой поддержки Check Risk. Специалисты поддержки помогут вам завершить регистрацию и ответят на любые вопросы:

- ✓ Электронная почта: support@check-risk.ru — отправьте письмо с описанием проблемы и указанием вашего аккаунта.
- ✓ Онлайн-чат: на сайте Check Risk для оперативной связи со специалистом поддержки на сайте https://check-risk.ru/.

Хотите быть уверены, что ваш сайт в безопасности? Check Risk защитит от атак, ботов и утечек данных. Зайдите на сайт и включите защиту уже сегодня!