



ул. Ольховская, д. 4, корп. 2

г. Москва, 105066

+7 499 110-25-34

info@bi.zone

www.bi.zone

Руководство пользователя BI.ZONE Brand Protection



Оглавление

Термины и сокращения	4
Описание решения	6
Функциональные возможности	6
Направления отслеживания угроз.....	7
Мошенничество	7
Утечки информации	8
Инфополе	10
Технические характеристики.....	10
Архитектура	10
Доступ	10
Отказоустойчивость	10
Безопасность	11
Логирование	11
Быстрый старт	12
Регистрация.....	12
Ввод данных о компании	13
Описание разделов	15
Дашборд	15
Новости	17
Угрозы	18
История изменения статусов	19
Вложения к объекту	19
Комментарии к объектам.....	20
Получить данные о регистраторе	20
Статусы ресурсов.....	22
Отчеты	23
Профиль	25
Подписки на уведомления.....	25

Смена пароля.....	26
Сценарии действий с объектами	27
Отправить запрос на проверку	27
Действия с объектами в разделах «Запросы», «Фишинг и фрод», «Мобильные приложения», «Закрытые ресурсы»	27
Действия с объектами в разделе «Утечки»	28
Экспорт	29
Построить отчет	30
Различия пакетов	31
FAQ	33
Типовые проблемы.....	37
Техническая поддержка	38

Термины и сокращения

Термин, сокращение	Определение, расшифровка
Заказчик	Клиент, являющийся пользователем платформы
ООО «БИЗон», BI.ZONE	Общество с ограниченной ответственностью «Безопасная информационная зона»
Платформа	Онлайн-платформа BI.ZONE Brand Protection
ПО	Программное обеспечение
СМИ	Средства массовой информации
API	Application programming interface
CERT	Computer emergency response team
CSV	Comma-separated values
DOCX	Формат текстовых документов
FAQ	Frequently asked questions
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
PDF	Portable Document Format
RPO	Recovery Point Objective – максимальный промежуток времени до наступления сбоя, данные за который могут быть утрачены
RTO	Recovery Time Objective – максимальное время для восстановления после сбоя

Термин, сокращение	Определение, расшифровка
SSL	Secure Sockets Layer

Описание решения

Онлайн-платформа BI.ZONE Brand Protection, правообладателем которой является ООО «БИЗон» (далее — BI.ZONE), помогает выполнить следующие задачи:

- предотвратить ущерб репутации компании, наносимый фишинговыми атаками с использованием элементов ее бренда;
- нейтрализовать негативный фон, вызванный действиями поддельных аккаунтов представителей компании в социальных сетях;
- предотвратить распространение нелегитимных приложений, неправомерно использующих бренд компании;
- повысить осведомленность компании о мошеннических схемах и об иных потенциальных угрозах, обсуждаемых на закрытых ресурсах;
- минимизировать последствия утечек корпоративных учетных записей сотрудников компании;
- отслеживать тональность информационного поля бренда и своевременно реагировать на негативные сообщения в СМИ, которые могут повлечь за собой репутационные и финансовые потери.

Функциональные возможности

Платформа предоставляет следующие функциональные возможности:

- **Мониторинг**
Платформа осуществляет автоматизированный круглосуточный мониторинг ресурсов на предмет наличия угроз для компании и бренда. Доступен мониторинг по трем направлениям отслеживания угроз (см. [Направления отслеживания угроз](#)).
- **Досудебная блокировка**
Команда аналитиков BI.ZONE по согласованию с Заказчиком направляет мотивированные обращения регистраторам, хостинг-провайдерам и иным регуляторам с целью досудебной блокировки мошеннических ресурсов, использующих Бренды Заказчика для обмана пользователей.
- **Гибкая настройка**
Для мониторинга и анализа информации Заказчик предоставляет входные данные для настройки инструментов. Входные данные могут включать в себя графические (не более 100) и текстовые (не более 50) товарные знаки,

доменные имена (не более 100), фирменные наименования (не более 100) и другие активы.

- **Ретроспективный анализ**

После предоставления Заказчиком данных для настройки инструментов в платформу подгружается вся информация по обнаруженным ранее индикаторам за предыдущие периоды.

- **Экспертная поддержка**

Команда аналитиков BI.ZONE круглосуточно анализирует поступающую информацию о найденных угрозах. По согласованию с Заказчиком специалисты BI.ZONE могут связываться с потенциальным нарушителем для получения примера данных. А также анализировать открытые источники для выявления взаимосвязей между потенциальными аккаунтами и электронными почтами злоумышленника.

- **Оперативные уведомления**

Команда аналитиков BI.ZONE по согласованию с Заказчиком может оперативно уведомлять уполномоченных Заказчиком лиц по электронной почте или в Telegram.

Направления отслеживания угроз

Платформа позволяет отслеживать угрозы по следующим направлениям:

- Мошенничество;
- Утечки информации;
- Инфополе.

Мошенничество

Направление позволяет выявлять и блокировать мошеннические ресурсы, использующие Бренды Заказчика для обмана пользователей.

Платформа осуществляет круглосуточный мониторинг интернета для обнаружения фишинговых, вредоносных и прочих мошеннических ресурсов, использующих стилистику и символику Заказчика. Мониторинг осуществляется автоматически, без необходимости участия Заказчика.

Выявление доменных имен, использующих элементы Брендов Заказчика

Платформа осуществляет ежедневный анализ зарегистрированных доменных имен в 1118 доменных зонах (.com, .ru, .su, .рф, .com, .net, .org, .info, .top, .loan, .biz,

.хуз и проч.), чтобы оперативно выявлять имена, использующие элементы Брендов Заказчика. База доменов ежедневно пополняется из различных источников, в том числе от операторов зон, регистраторов, ICANN, реестров HTTPS-сертификатов и других источников. На текущий момент в базе содержится более 1 миллиарда зарегистрированных доменных имен. Платформа осуществляет ежедневное сканирование более 20 миллионов веб-ресурсов.

Само по себе создание подобного домена не нарушает правил регистрации. Однако в дальнейшем эти домены могут использоваться для фишинга, мошенничества и других атак, поэтому они вносятся в список на мониторинг для регулярной проверки на наличие неправомерного контента.

Выявление нелегитимных мобильных приложений

Платформа позволяет выявлять мобильные приложения, неправомерно использующие бренд компании, распространяющиеся в официальных магазинах мобильных приложений (Apple AppStore, Google Play Store, Samsung Galaxy Store, Huawei AppGallery, Xiaomi Mi GetApps, Amazon Appstore), а также на неофициальных ресурсах.

Выявление поддельных аккаунтов и групп в социальных сетях

Платформа осуществляет поиск поддельных групп, аккаунтов топ-менеджеров и представителей Заказчика в социальных сетях. Мониторинг производится в более чем 15 крупнейших российских и мировых социальных сетях, включая ВКонтакте, Одноклассники, Facebook, Twitter, Instagram, TikTok, LinkedIn, Reddit, Tumblr, YouTube и других.

Утечки информации

Направление позволяет Заказчику своевременно узнавать о возможных утечках данных компании, включая данные аутентификации, сведения о доступе к информационным системам, информацию, содержащую коммерческую тайну и иную чувствительную информацию. При обнаружении утечек платформа оперативно уведомляет об этом Заказчика и предоставляет имеющиеся контекстные данные.

Поиск утечек чувствительной информации в открытых источниках

Платформа осуществляет выявление скомпрометированных данных и чувствительной информации о Заказчике в открытых источниках, включая:

- Сайты и форумы;

- Средства массовой информации;
- Социальные сети;
- Специализированные группы в социальных сетях и мессенджерах.

Поиск утечек чувствительной информации на теневых ресурсах

Платформа осуществляет постоянный мониторинг специализированных форумов и закрытых групп, в том числе на ресурсах даркнета, в которых могут быть опубликованы базы данных Заказчика или базы сторонних компаний, содержащие чувствительную информацию о сотрудниках Заказчика. Например, корпоративные учетные записи, имена и должности сотрудников и проч.

Поиск утечек чувствительной информации на ресурсах для обмена данными

Платформа осуществляет выявление записей, содержащих чувствительную информацию о Заказчике (логины, пароли, фрагменты исходного кода программ и проч.), на ресурсах для обмена данными и репозиториях, таких как github.com, pastebin.com и др.

Поиск потенциальных угроз на закрытых ресурсах

Платформа анализирует сообщения в закрытых группах и на теневых ресурсах интернета для выявления информации, которая может быть связана с ущербом для Заказчика. К ней могут относиться описания мошеннических схем, объявления о поиске инсайдеров и т. д.

Мониторинг Telegram

Платформа ежедневно сканирует более 150 тысяч публикаций в более чем 2000 специализированных каналах и чатах в мессенджере Telegram. Сканирование осуществляется для выявления мошеннических схем или иной чувствительной информации, касающейся Заказчика. По просьбе Заказчика шаблоны мониторинга могут быть изменены.

Мониторинг торговых площадок и площадок онлайн-объявлений

Платформа осуществляет мониторинг более 15 торговых площадок и площадок онлайн-объявлений.

Инфополе

Направление охватывает мониторинг СМИ, социальных сетей и видеохостингов (YouTube, TikTok, RUTUBE, Likee, YAPPY) что позволяет Заказчику выявлять негативные публикации на ранних стадиях распространения и своевременно реагировать на них.

Для данного направления платформа осуществляет:

- мониторинг и автоматизированную загрузку на платформу BI.ZONE Brand Protection негативных сообщений с упоминанием Брендов Заказчика из СМИ с потенциальным охватом более **1500** пользователей;
- мониторинг и автоматизированную загрузку на платформу BI.ZONE Brand Protection негативных сообщений с упоминанием Брендов Заказчика из социальных сетей и видеохостингов с потенциальным охватом аудитории более **1000** пользователей;
- оперативное уведомление Заказчика о потенциальных информационных атаках и вирусных публикациях.

Технические характеристики

Архитектура

BI.ZONE Brand Protection является облачным решением и не требует размещения в инфраструктуре Заказчика.

Доступ

У BI.ZONE Brand Protection отсутствуют ограничения на количество зарегистрированных учетных записей Заказчика. Для создания дополнительной учетной записи необходимо связаться с представителем BI.ZONE или написать запрос на электронную почту bp@bi.zone.

Отказоустойчивость

Отказоустойчивость платформы обеспечивается командой BI.ZONE.

В таблице ниже перечислены основные параметры отказоустойчивости платформы.

Параметр	Значение
Коэффициент доступности	98,9%
Максимальное время недоступности в год	Не более 96 часов
RPO	Не более 24 часов
RTO	Не более 24 часов
Максимально допустимое количество единовременных пользователей	Без ограничений

Безопасность

Шифрование соединений

Все коммуникации между компонентами платформы и клиентом осуществляются по зашифрованному, защищенному соединению с использованием протокола HTTPS (поддерживается протокол TLS версии 1.2)

Логирование

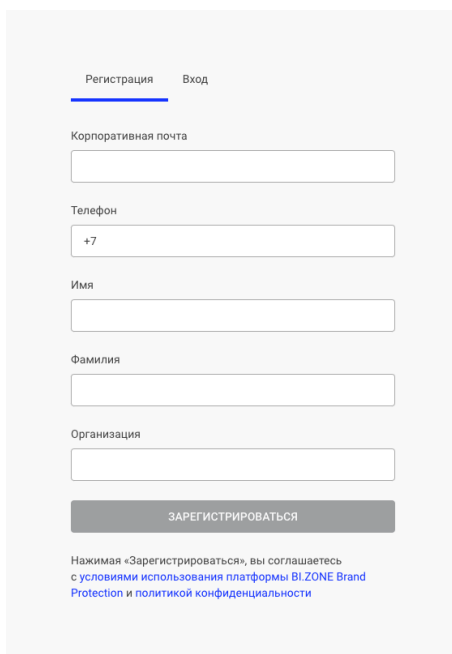
Платформа осуществляет логирование действий пользователей. Каждое событие хранится в течение 6 месяцев в журнале событий.

Быстрый старт

Регистрация

Для регистрации на сайте br.bi.zone вам потребуется заполнить 5 полей (рис. 1):

- корпоративная почта (необходимо регистрироваться на корпоративные почтовые адреса);
- контактный номер телефона;
- имя;
- фамилия;
- организация (наименование вашей компании).



Регистрация Вход

Корпоративная почта

Телефон

Имя

Фамилия

Организация

ЗАРЕГИСТРИРОВАТЬСЯ

Нажимая «Зарегистрироваться», вы соглашаетесь с условиями использования платформы BI.ZONE Brand Protection и политикой конфиденциальности

Рис. 1. Форма регистрации

Если у вас возникли технические или другие проблемы с регистрацией на платформе, вы можете обратиться в службу поддержки, написав на почтовый адрес br@bi.zone.

Ввод данных о компании

При первом заходе после регистрации пользователя платформа выведет окно с запросом о вводе данных о компании (рис. 2). Указанная информация необходима нам для настройки инструментов поиска данных.

Данные организации ✕

Официальный сайт *

Платформа выполнит поиск сайтов, использующих атрибутику вашего бренда

Домен, к которому привязана корпоративная почта

Платформа выполнит поиск утечек учетных записей, связанных с корпоративной почтой. Можно указать несколько доменов, через запятую

Другие официальные ресурсы организации

Сайты, аккаунты и группы в социальных сетях.
Данные ресурсы мы не будем считать фишинговыми или мошенническими

IP-адреса

Мы будем выявлять упоминания ваших IP-адресов в качестве целей для атак. Вы можете указать несколько адресов через запятую или тире

Ключевые слова *

Рекомендуем использовать слова, содержащие следующую информацию:
Название бренда;
Названия бонусных программ;
Названия продуктов;
и тд.

Комментарий


 После сохранения будет выполнена бесплатная разовая проверка. Будьте внимательны при заполнении.

Рис. 2. Форма ввода данных о компании

Необходимо заполнить следующие поля:

- **Сайт организации.**
- **Домен, к которому привязана корпоративная почта** (платформа выполнит поиск утечек учетных записей, связанных с указанным доменом. Пользователь может указать несколько почтовых доменов через запятую).
- **Другие официальные ресурсы** (сайты, аккаунты и группы в социальных сетях. Данные ресурсы попадут в whitelist, мы не будем считать их мошенническими).
- **IP-адреса** (данная информация необходима для настройки инструмента, который будет выявлять упоминания ваших IP-адресов в качестве целей для атак. Пользователь может указать несколько адресов через запятую или тире).
- **Ключевые слова** (рекомендуем использовать слова, содержащие название бренда, названия бонусных программ, продуктов и т. д. Данная информация используется для выявления объявлений о вашей компании на теневых ресурсах).
- **Комментарий** (дополнительная информация и пожелания, которые нам необходимо учесть при настройке инструментов).

После прохождения пользователем этапа ввода данных о компании мы начнем настройку наших инструментов для поиска информации. Как только данные будут добавлены, вам на почту придет уведомление. Обычно первые результаты работы наших инструментов становятся доступны к просмотру в течение часа после регистрации.

Описание разделов

Дашборд

У пользователя есть возможность просмотра статистики в разделе **Дашборд**. Данные на виджетах представлены в трех форматах:

1. Динамика по обнаружению (рис. 3).

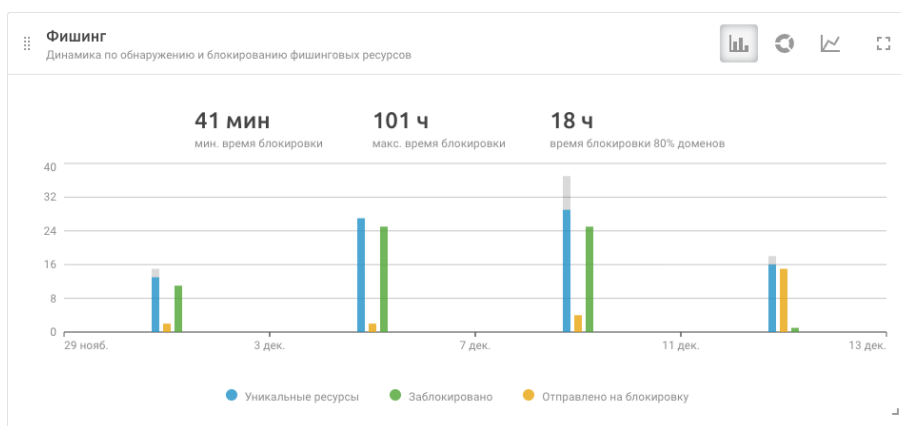


Рис. 3. Динамика по обнаружению

2. Статистика по обнаружению (рис. 4).

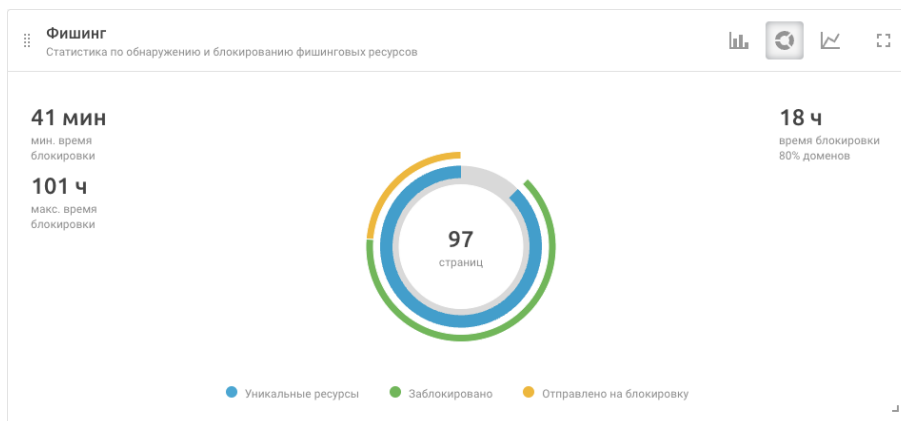


Рис. 4. Статистика по обнаружению

3. Динамика по времени блокировки (рис. 5).

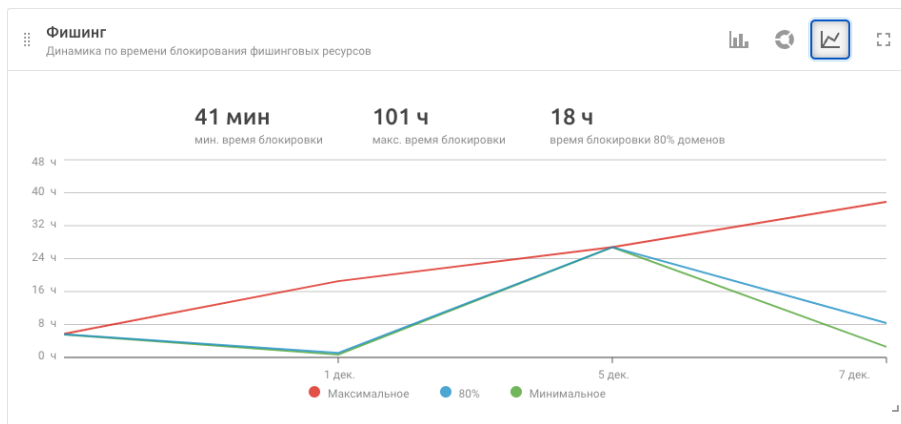


Рис. 5. Динамика по времени блокирования

У пользователя есть возможности настройки даты, отображения конкретной услуги (фишинг, мошеннические ресурсы, утечки и т. д.) (рис. 6).

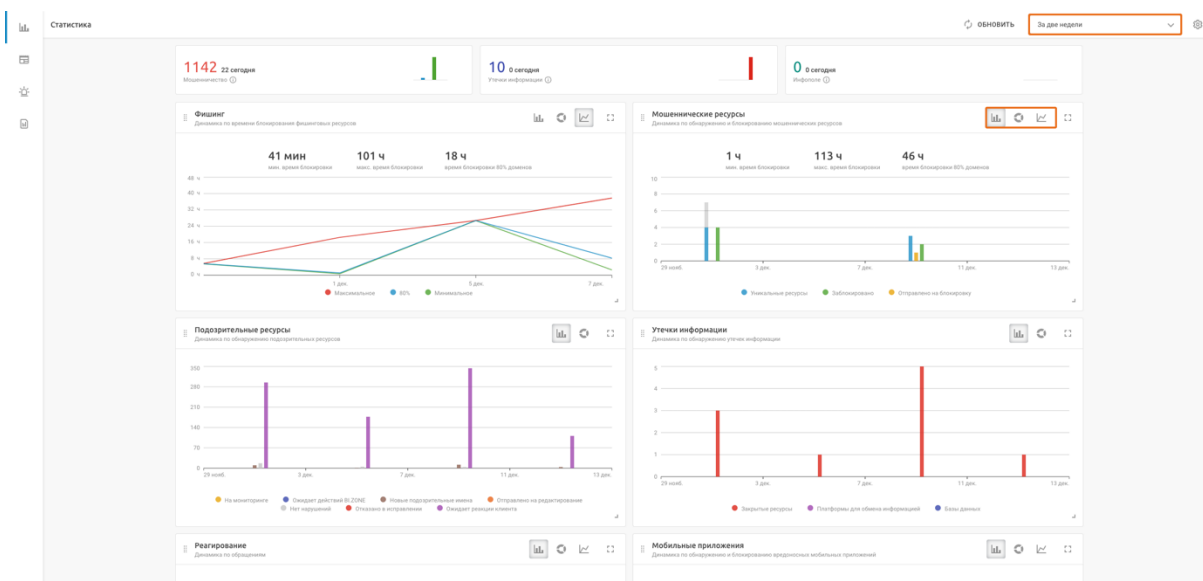


Рис. 6. Фрагмент раздела с дашбордами

Новости

На платформе существует раздел **Новости** (рис. 7). В нем команда наших аналитиков публикует новости о найденных скомпрометированных базах данных.

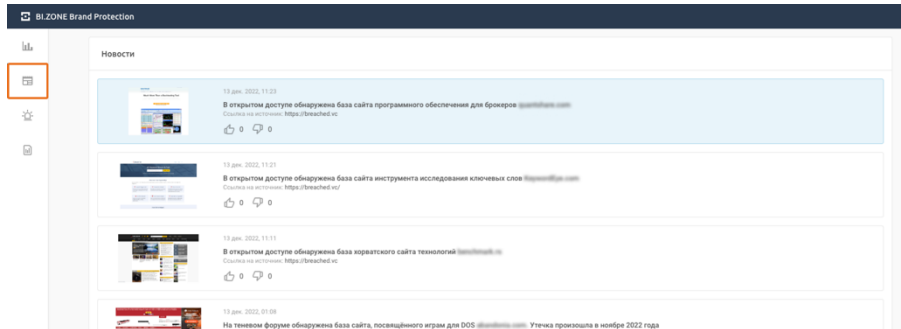


Рис. 7. Раздел новостей

В карточке с новостью (рис. 8) вы можете увидеть краткое описание:

- сервис, откуда произошла утечка;
- какие столбцы в ней были;
- количество строк;
- источник, в котором мы нашли данную базу;
- дата публикации.

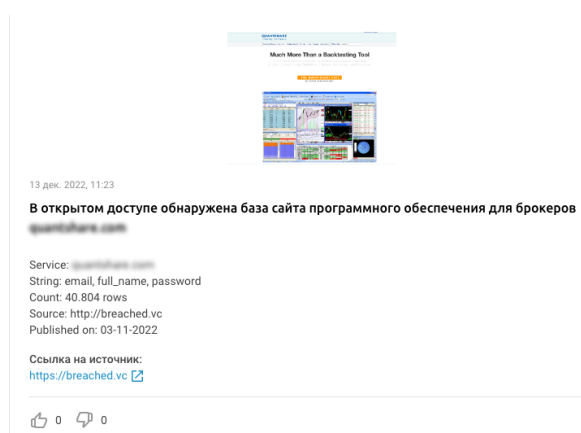


Рис. 8. Карточка новости

Угрозы

На платформе есть возможность настройки фильтров для поиска. Вы можете выбрать интересующие вас источники, статусы, категории индикаторов (**Phishing**, **Malware**), а также в качестве фильтра использовать тег. Например, чтобы посмотреть все сработки инструмента по поиску скомпрометированных данных в GitHub, вам следует использовать в качестве фильтра тег **Coderover** (рис. 9).

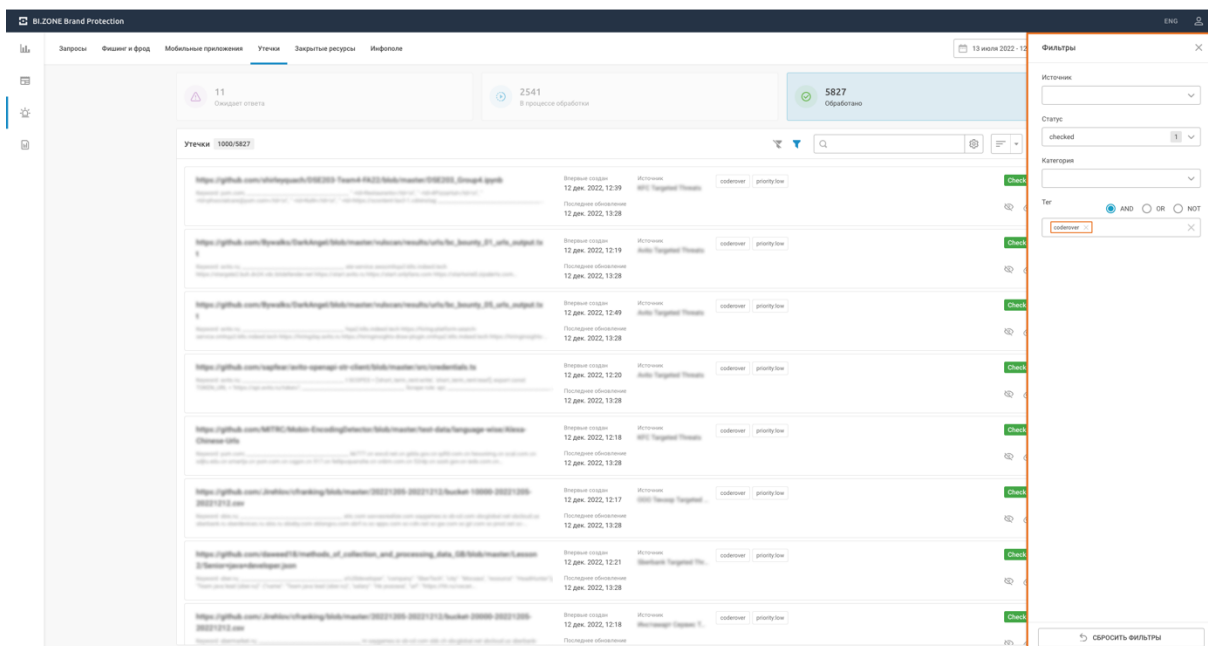


Рис. 9. Фильтры поиска

История изменения статусов

При работе с объектами у пользователя есть возможность просмотреть историю изменения статусов. Для этого надо выбрать конкретный объект и нажать кнопку «История изменения статусов» (рис. 10).

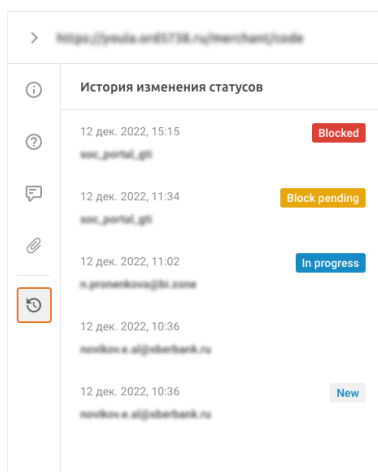


Рис. 10. История изменения статусов

В появившемся окне пользователь увидит историю изменения статуса (кто, когда изменил) у интересующего объекта.

Вложения к объекту

У пользователя есть возможность просматривать скриншот к объекту, а также запросить новый скриншот. Для этого надо выбрать соответствующий раздел и нажать кнопку **Запросить скриншот** (рис. 11).

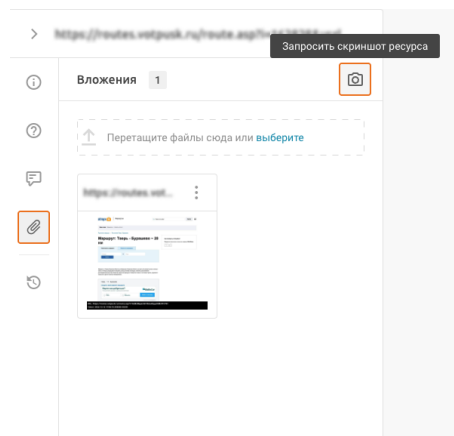


Рис. 11. Запрос скриншота

Комментарии к объектам

В некоторых случаях специалистам BI.ZONE может потребоваться дополнительная информация об объекте или у заказчика может появиться дополнительная информация либо вопросы о каком-то объекте. Данную информацию можно передать через комментарии к объекту. Чтобы оставить комментарий, надо выбрать соответствующий раздел в карточке объекта и нажать на *плюс* (рис. 12).

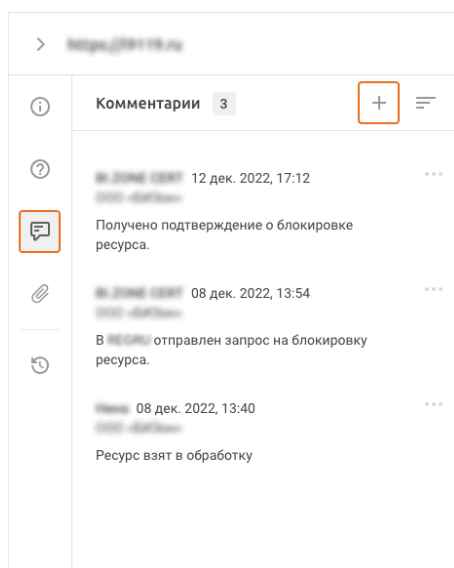


Рис. 12. Окно добавления комментария

После того как текст комментария будет введен, следует нажать кнопку **Добавить**.

Получить данные о регистраторе

Пользователь платформы может запросить данные о регистраторе определенного объекта в разделе **Фишинг и фрод**. Для этого выберите соответствующий раздел в карточке объекта.

Статусы ресурсов

Статусы на платформе разделены на 4 блока состояния потенциальных угроз для бренда:

1. **Ожидает ответа** — в данный блок попадают домены или другие типы IoC в статусе **Waiting for customer**. Если домен находится в этом статусе, значит, мы ждем от заказчика подтверждения/опровержения легитимности.
2. **В процессе обработки** — в данный блок попадают все новые домены, а также домены, которые находятся на этапе отправки жалобы. Статусы, используемые в данном блоке: **New, In progress, In communication, Waiting for support, Correcting**.
3. **Отслеживается** — в данном разделе находятся домены, стоящие на мониторинге, и те домены, на которые мы отправили жалобы. Статусы, используемые в данном блоке: **Block pending, Monitoring, Delegation restored**.
4. **Обработано** — в данный раздел попадают домены, заблокированные регистратором/хостинг-провайдером, легитимные домены, а также домены, для досудебной блокировки которых недостаточно оснований. Статусы в данном блоке: **No violations, Legitimate, Blocked, No content, Irrelevant, Edited, Correction denied**.

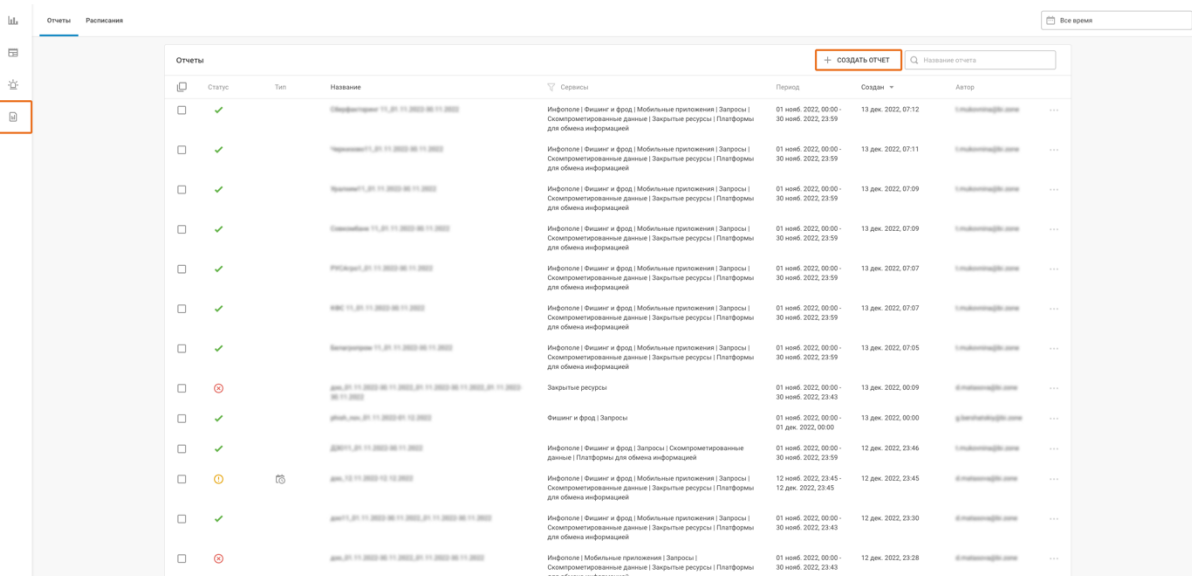
Описание статусов:

- **Waiting for customer** — ожидает действий заказчика (подтвердить/опровергнуть легитимность ресурса).
- **New** — все новые потенциальные угрозы для бренда.
- **In progress** — данный статус означает, что специалисты взяли домен в работу (то есть на него будет отправлена жалоба).
- **In communication** — домен находится в статусе обсуждения с заказчиком или регистратором (используется очень редко).
- **Waiting for support** — домен ожидает действий со стороны специалиста BI.ZONE.
- **Correcting** — отправлен запрос на исправление информации на сайте / удаление товарного знака.
- **Block pending** — отправлена жалоба на домен.
- **Monitoring** — домены, на которых может появиться фишинговый/мошеннический контент.

- **Delegation restored** — делегирование восстановлено. Данный статус выставляется доменам, которые устранили нарушение и попросили о восстановлении.
- **No violations** — ссылки не содержат фишинговый или мошеннический контент, основания для досудебной блокировки домена отсутствуют.
- **Legitimate** — легитимные/официальные домены.
- **Blocked** — домен заблокирован.
- **No content** — контент отсутствует: ссылки попали на платформу уже заблокированными, на ресурсе отсутствуют контент и визуальный образ.
- **Irrelevant** — актуально для источников по базам данных.
- **Edited** — информация на сайте исправлена.
- **Correction denied** — запрос на исправление информации на сайте отклонен.

Отчеты

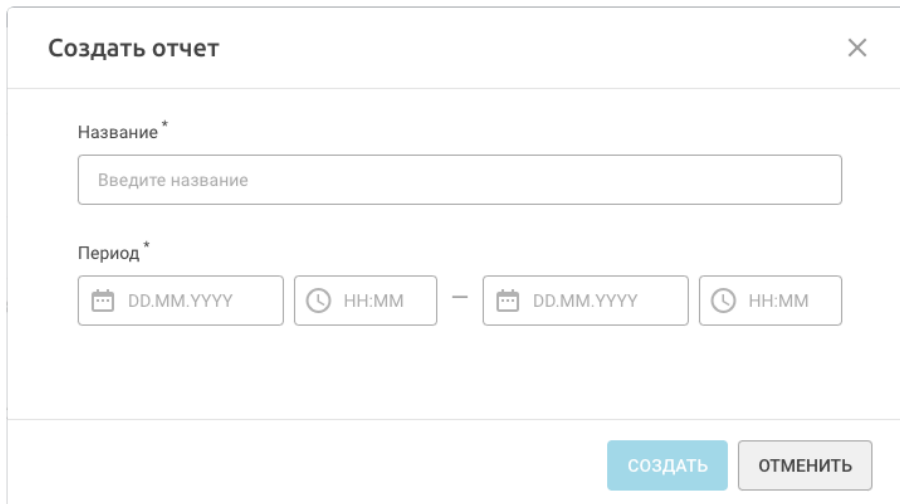
У заказчика есть возможность самостоятельно в любой момент времени создать отчет. Для этого на платформе надо перейти на вкладку **Отчеты** (рис. 15) и нажать кнопку **Создать отчет**.



Статус	Тип	Название	Сервисы	Период	Создан	Автор
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:12	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:11	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:09	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:09	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:07	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:07	...
✓	Инцидент	Инцидент 11.201.2022.00.00-30.11.2022	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	13 дек. 2022, 07:05	...
⊘	Закрытые ресурсы	...	Закрытые ресурсы	01 нояб. 2022, 00:00-30 нояб. 2022, 23:43	13 дек. 2022, 00:09	...
✓	Фишинг и фрод	...	Фишинг и фрод Запросы	01 нояб. 2022, 00:00-01 дек. 2022, 00:00	13 дек. 2022, 00:00	...
✓	Инцидент	...	Инцидент Фишинг и фрод Запросы Скомпрометированные данные Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:59	12 дек. 2022, 23:46	...
⊘	Инцидент	...	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	12 нояб. 2022, 23:45-12 дек. 2022, 23:45	12 дек. 2022, 23:45	...
✓	Инцидент	...	Инцидент Фишинг и фрод Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:43	12 дек. 2022, 23:30	...
⊘	Инцидент	...	Инцидент Мобильные приложения Запросы Скомпрометированные данные Закрытые ресурсы Платформы для обмена информацией	01 нояб. 2022, 00:00-30 нояб. 2022, 23:43	12 дек. 2022, 23:28	...

Рис. 15. Вкладка с отчетами

В появившемся окне (рис. 16) будет предложено выбрать дату, за которую вы хотите сформировать отчет, а также дать название отчету.



Создать отчет

Название *

Введите название

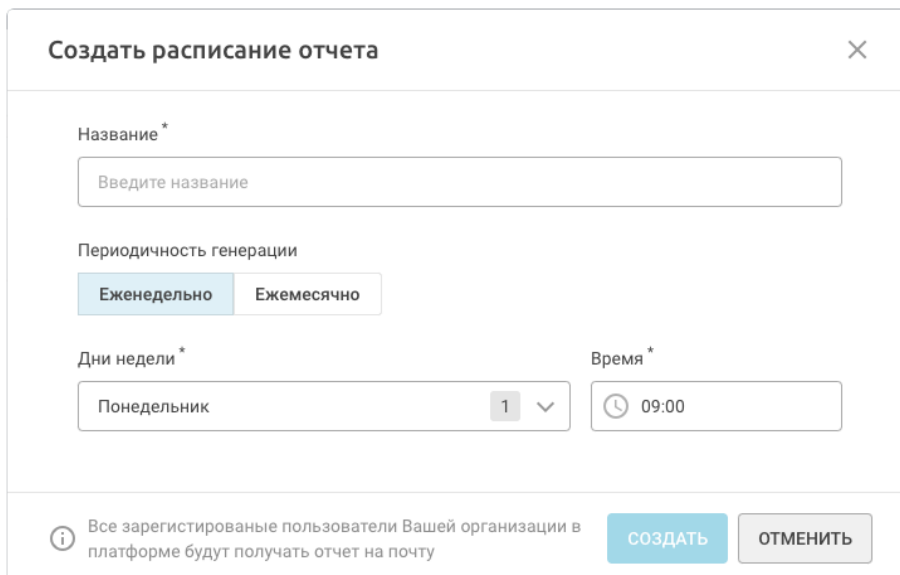
Период *

DD.MM.YYYY HH:MM — DD.MM.YYYY HH:MM

СОЗДАТЬ ОТМЕНИТЬ

Рис. 16. Окно создания отчета

Также на странице формирования отчета вы можете открыть вкладку **Расписание** (рис. 17) и задать расписание отчета. По заданным критериям отчет будет формироваться в автоматическом режиме.



Создать расписание отчета

Название *

Введите название

Периодичность генерации

Еженедельно Ежемесячно

Дни недели * Время *

Понедельник 1 09:00

Все зарегистрированные пользователи Вашей организации в платформе будут получать отчет на почту

СОЗДАТЬ ОТМЕНИТЬ

Рис. 17. Вкладка для задания расписания

Все зарегистрированные пользователи вашей организации будут получать отчет в назначенное время.

Профиль

Изменение персональных данных пользователей, смена пароля и настройка подписок на уведомления возможны на странице личного профиля (рис. 18).

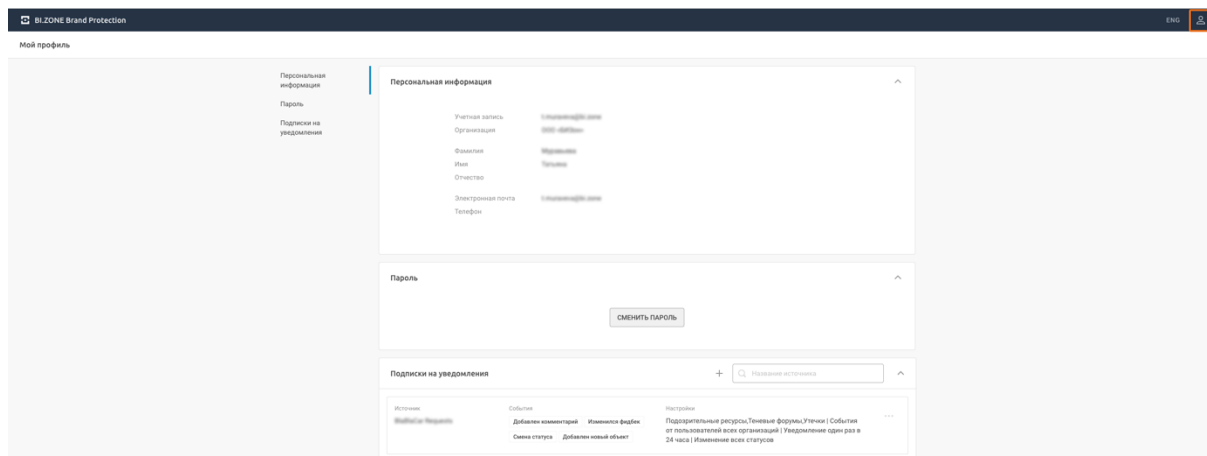


Рис. 18. Страница личного профиля

Подписки на уведомления

Настройка уведомлений происходит на странице профиля. Вы можете настроить уведомления по интересующим вас сервисам (скомпрометированные данные, платформы для обмена информацией, мобильные приложения, фишинг и фрод, закрытые ресурсы, запросы, инфополе).

По умолчанию мы подписываем новых пользователей на обновления по всем сервисам и событиям. У пользователя есть возможность выбрать конкретное событие (смена статуса, добавление новых потенциальных угроз для бренда, добавление комментария), также можно подписаться на изменение определенных статусов. Платформа позволяет настроить частоту уведомлений и тип

интересующих вас уведомлений (например, присылать события от пользователей вне организации) (рис. 19).

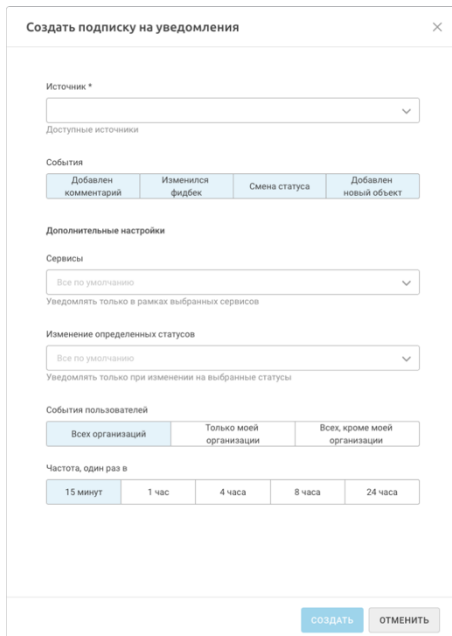


Рис. 19. Создание подписки на уведомления

Также есть возможность настроить частоту уведомлений: раз в 15 минут, раз в час или раз в 24 часа.

Смена пароля

В профиле пользователя у вас есть возможность сменить пароль согласно нашей парольной политике (рис. 20). В форме для ввода нового пароля вы увидите подсказки, которые помогут установить пароль согласно нашим политикам.

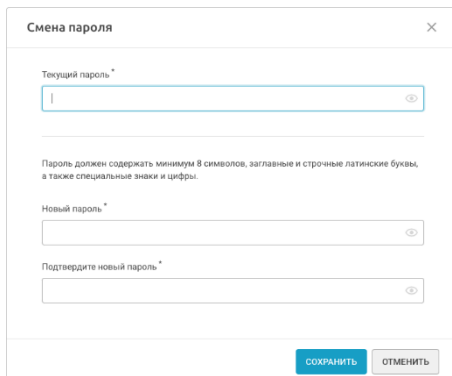


Рис. 20. Форма смены пароля

Сценарии действий с объектами

Отправить запрос на проверку

У пользователей платформы есть возможность отправить ресурсы для проверки специалистами круглосуточной смены. Необходимо нажать кнопку **Создать запрос** (рис. 21). Внести ссылки на ресурсы, которые вызывают вопросы. Также можно оставить комментарий с дополнительной информацией, которая поможет специалисту вынести вердикт.

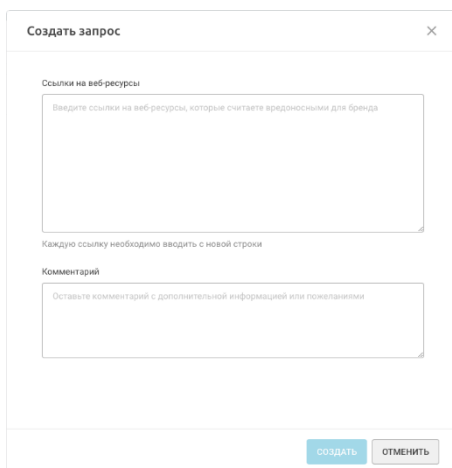


Рис. 21. Форма создания запроса на проверку

Действия с объектами в разделах «Запросы», «Фишинг и фрод», «Мобильные приложения», «Закрытые ресурсы»

При проверке потенциальных угроз у специалистов смены могут возникать ситуации, когда требуется участие заказчика.

Если у специалиста возникнут вопросы о легитимности домена, он поставит такой домен в статус **Waiting for customer**. Это означает, что мы ожидаем от заказчика вердикта по домену. Заказчику доступны кнопки **Заблокировать**, **Нарушений нет** и **Мониторинг** (спрятана под кнопкой с тремя точками) (рис. 22). После того как вы

нажмете одну из кнопок, специалист обработает индикатор соответствующим образом.

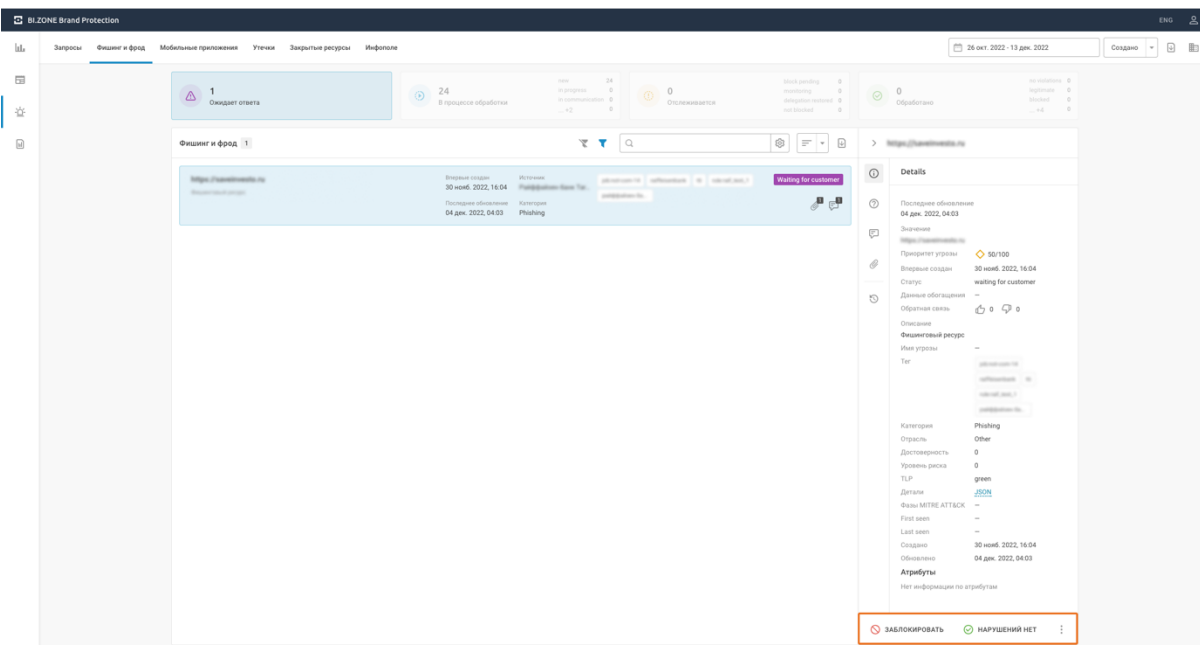


Рис. 22. Ожидание вердикта от заказчика

Действия с объектами в разделе «Утечки»

В разделе **Утечки** пользователь может отметить проверенные угрозы нажатием кнопки **Отметить как просмотренное** (рис. 23).

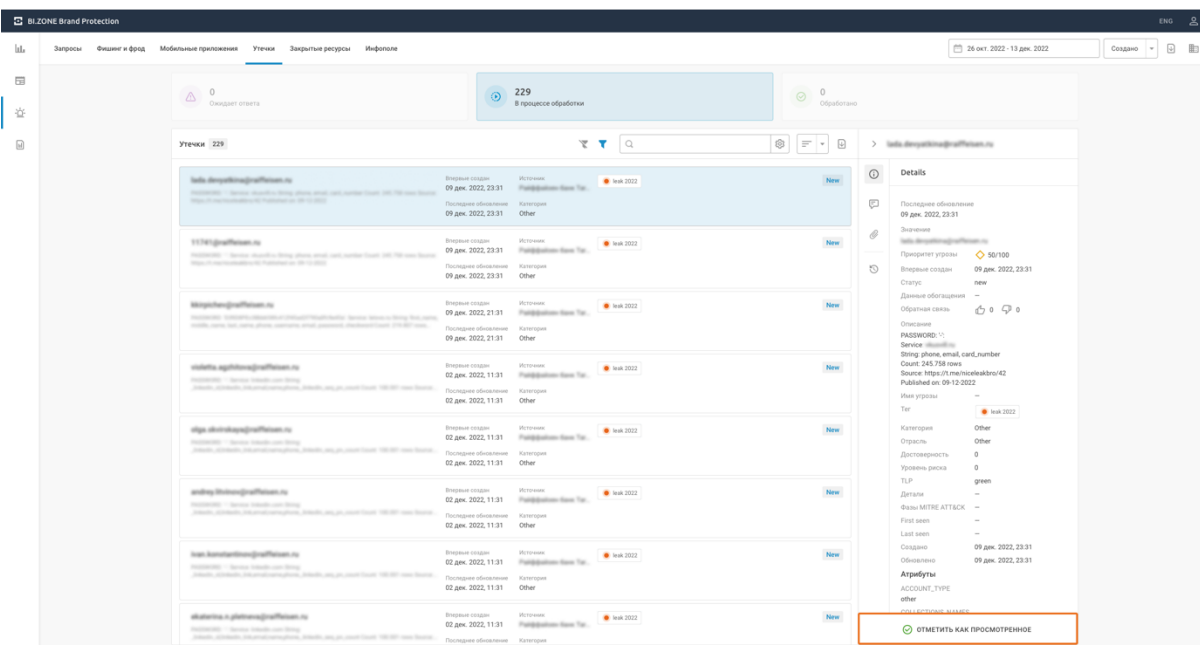


Рис. 23. Окно с кнопкой для отметки просмотренной угрозы

Экспорт

На платформе присутствует возможность сделать экспорт данных в двух вариантах:

1. Нажав на кнопку экспорта в верхнем правом углу экрана, вы сможете экспортировать данные по всем сервисам с определенным фильтром по дате (на рис. 24 — за все время).

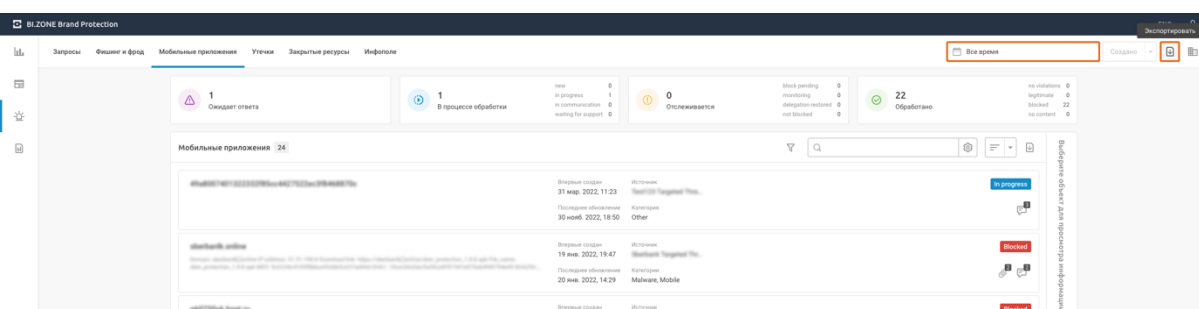


Рис. 24. Экспорт данных по всем сервисам

2. Пользователь платформы может сделать экспорт данных по определенному сервису за определенную дату (например, получить список загруженных потенциальных угроз с фишинговым контентом за определенную дату) (рис. 25).

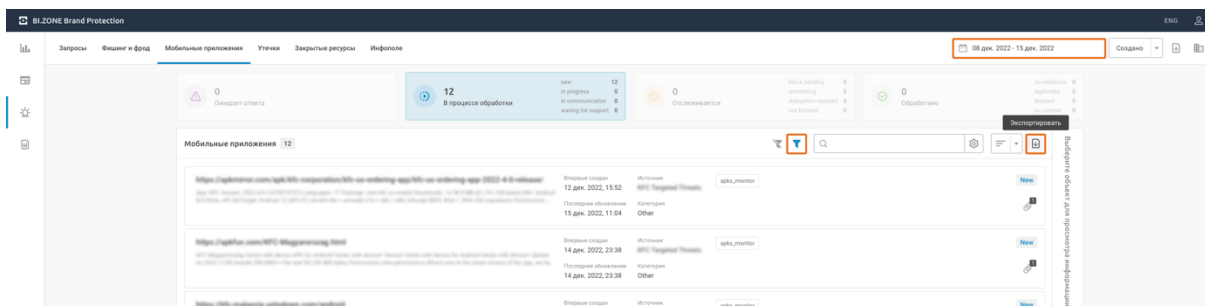


Рис. 25. Экспорт данных по определенному сервису

При нажатии кнопки **Экспортировать** (рис. 26) у пользователя появится возможность выбрать конкретные экспортируемые поля (значение, тип (данных), источник, статус, описание и т. д.). Файл экспортируется в формате CSV.

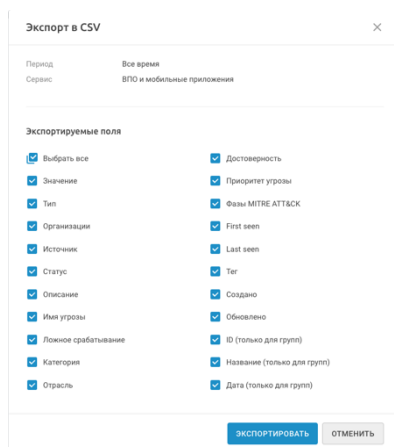


Рис. 26. Выбор экспортируемых полей

Построить отчет

Платформа BI.ZONE Brand Protection позволяет выгружать отчеты в режиме реального времени, создавать расписание их генерации и составлять список получателей. Отчеты создаются автоматически в форматах PDF и DOCX. В отчеты могут быть включены следующие разделы:

1. Краткое описание результатов.
2. Фишинговые и другие мошеннические ресурсы.
3. Подозрительные доменные имена.
4. Мошеннические аккаунты в социальных сетях.
5. Сообщения о мошеннических схемах, продажах баз данных и об иной информации о заказчике из закрытых ресурсов.
6. Скомпрометированные корпоративные учетные данные.
7. Ссылки на ресурсы для обмена информацией с фрагментами кода, логинами и паролями.
8. Негативные сообщения с упоминанием заказчика в СМИ.
9. Негативные сообщения с упоминанием заказчика в социальных сетях.
10. Описание мер, принятых для устранения угроз и рисков.

Различия пакетов

Возможно подключение расширенной лицензии на данное ПО.

Расширенная лицензия по направлению «Мошенничество» включает:

- обработку ПО результатов поиска в рамках направления «Мошенничество» 24/7/365;
- проверку всего потока обнаруженных мошеннических ресурсов;
- блокировку неограниченного количества обнаруженных фишинговых и мошеннических ресурсов.

Расширенная лицензия по направлению «Утечки информации» включает:

- обработку ПО результатов поиска в рамках направления «Утечки информации» 24/7/365;
- информирование о критических угрозах;
- выгрузку информации о threat actor (авторе публикации / злоумышленнике / мошеннике);

Расширенная лицензия по направлению «Инфополе» включает:

- обработку ПО результатов поиска в рамках направления «Инфополе» 24/7/365;
- сбор информации о первоисточнике;
- аналитическую справку по информационным поводам один раз в месяц.

Основное отличие от обычной лицензии заключается в том, что все найденные потенциальные угрозы обрабатываются нашей круглосуточной сменой (рис. 27).

	Самостоятельное управление	Экспертная поддержка
Доступ ко всем модулям	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Круглосуточный мониторинг и реагирование	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Модуль «Мошенничество»		
Ручная проверка мошеннических ресурсов	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ручная проверка мошеннических ресурсов	10 в месяц	Без ограничений
Модуль «Утечки информации»		
Коммуникация со злоумышленниками, включая запрос образца данных	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Анализ профиля злоумышленника	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Модуль «Инфополе»		
Ручная проверка информационного потока	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Поиск и анализ первоисточника	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Аналитический срез по информационным поводам	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Рис. 27. Сравнение лицензий

FAQ

В каких случаях мы можем заблокировать сайт?

Мы можем направить запрос на досудебную блокировку домена. Если он нарушает правила регистрации домена либо правила хостинг-провайдера — домен будет заблокирован.

Согласно документу «Правила регистрации доменных имен в доменах .RU и .РФ», компетентная организация (а BI.ZONE имеет такой статус) вправе направить мотивированное обращение регистратору домена с целью его блокировки, если подтвердятся случаи:

- фишинга;
- действий по заражению сайта вредоносным ПО либо управлением ботнетом;
- распространения порнографических изображений несовершеннолетних.

Если факт нарушений подтвердится, регистратор заблокирует домен. Если сайт/домен не нарушает правил регистрации и/или правил использования услуг хостера, заблокировать такой сайт будет проблематично. Однако команда BI.ZONE использует все возможные легальные рычаги, чтобы добиться блокировки сайта с нарушениями.

Также у BI.ZONE есть эскалационный лист организаций, куда мы можем дополнительно направить жалобу для блокировки домена, если на наше первичное обращение нет реакции. Например:

1. Регистратору.
2. Хостинг-провайдеру.
3. Владельцу домена верхнего уровня (например, есть ответственный за доменную зону .shop).
4. Компании, выпустившей SSL-сертификат, с просьбой отозвать его.
5. CERT (группа реагирования на компьютерные инциденты) той страны, где хостится сайт, с просьбой поспособствовать в блокировке. Таким образом мы можем попробовать заблокировать домен, который размещен за рубежом. Наше сотрудничество работает и в обратную сторону, когда коллеги пишут с просьбами помочь заблокировать фишинговый домен, который размещен в России.

6. ICANN (Корпорация по управлению доменными именами и IP-адресами) и др.

И даже если после всех этих действий мы не смогли заблокировать сайт в досудебном порядке, далее заказчик может обратиться в суд. BI.ZONE действует только в рамках досудебного регулирования.

Можем ли мы гарантировать блокировку сайта?

Нет, гарантировать на 100% не можем. Окончательное решение о блокировании сайта принимает хостер/регистратор. Мы со своей стороны гарантируем отправку корректного и мотивированного запроса для организации взаимодействия со всеми ответственными органами.

Стоит отдельно отметить, у нас имеется многолетний опыт взаимодействия с хостерами/регистраторами, и, когда мы пишем обращение с просьбой заблокировать, регистраторы/хостеры понимают, что это не случайное обращение: нас знают и к нашему мнению прислушиваются.

Можно ли забанить клон сайта?

Ответ можно найти выше: если есть достаточные основания.

Как быстро блокируется сайт?

Зависит от многих факторов, в том числе от конкретного регистратора/хостера, а порой и конкретного специалиста, который обрабатывает обращение со стороны регистратора/хостера.

В среднем 80% фишинговых доменов в зоне .ru/.рф блокируется в течение 24 часов. 80% фишинговых доменов в зарубежных зонах блокируется в среднем в течение 48 часов.

Стоит обратить внимание, что не у всех регистраторов/хостеров есть круглосуточная смена. Поэтому, даже если мы максимально оперативно выявили сайт ночью в субботу и направили мотивированное обращение, регистратор/хостер может обработать данный запрос только в понедельник.

То же в случае и с зарубежными сайтами. Иногда на время блокировки ресурса влияет часовой пояс. Если на момент отправки жалобы в стране регистратора/хостера уже ночь, то порой для получения ответа необходимо ждать наступления рабочего дня.

Можем ли мы определить, кто стоит за созданием сайта?

Иногда мы можем получить информацию о регистраторе домена, но чаще всего злоумышленники используют одноразовую почту/телефон для регистрации мошеннических сайтов. Если мы находим конкретную информацию о владельце фишингового домена, нацеленного на вашу компанию, мы обязательно об этом говорим.

Также есть возможность оформить адвокатский запрос, чтобы получить информацию о владельце домена.

Можем ли мы заблокировать конкретную страницу, например в vk.com?

У нас есть партнерское соглашение, а также успешный опыт взаимодействия с администрацией «ВКонтакте» по запросам о неправомерном использовании товарных знаков, а также случаям, когда злоумышленники / бывшие сотрудники выдают себя за официальных представителей компании.

Для направления такого обращения нам необходима доверенность, чтобы доказать VK, что мы имеем право действовать от имени заказчика и в его интересах (чтобы не допустить ошибки и не заблокировать официальный источник). Обычно среднее время реагирования технической поддержки VK составляет до 12 часов.

Можем ли мы заблокировать страницу в Facebook или профиль в Instagram?

У нас есть опыт успешного взаимодействия с администрациями данных ресурсов и блокировки мошеннических аккаунтов.

В некоторых случаях для рассмотрения жалоб необходимо предоставить доверенность на компанию. Но, как правило, если аккаунт действительно мошеннический и выдает себя за представителя компании, то администрация социальной сети идет навстречу и блокирует такую страницу.

Можем ли мы повлиять на выдачу фишингового сайта в поиске?

Если речь идет о рекламной выдаче в поиске, то да, обычно и «Яндекс», и Google идут нам навстречу и убирают мошеннический/фишинговый ресурс из рекламной выдачи.

С «Яндексом» у нас установлены партнерские отношения. А также мы используем партнерский API «Яндекса».

Если это не рекламная выдача, а просто выдача поисковой системы, то здесь могут быть разные ситуации. «Яндекс» и Google, в зависимости от своих алгоритмов, расставляют сайты по рейтингу. И если какой-то сайт без рекламы

смог попасть в топ выдачи, то, вероятнее всего, Google или «Яндекс» будут считать его легитимным. В этой ситуации убрать сайт из поисковой выдачи может быть затруднительно, но, если домен и в самом деле носит мошеннический характер, к нему также может быть предпринят ряд мер.

Можем ли мы отслеживать рекламную выдачу по поиску конкретного слова?

Да. Зачастую мошенники размещают фишинг именно с помощью рекламы.

У нас оформлены партнерские отношения с «Яндексом», и мы используем его API для автоматизированного отслеживания рекламной выдачи по запросу по конкретным словам.

Типовые проблемы

Проблема. Невозможно авторизоваться на платформе.

Решение. В данном случае советуем проверить, правильно ли вы ввели данные для входа. Если в правильности данных вы уверены, попробуйте выполнить восстановление пароля.

Проблема. Не могу сделать скриншот индикатора.

Решение. Данная проблема связана с загрузкой очереди сервиса, отвечающего за снятие скриншотов. Советуем повторить действия по снятию скриншота через некоторое время.

Проблема. Пропали кнопки «Заблокировать»/«Проверено».

Решение. Кнопки для перевода статуса доступны, только если объект не взят в работу специалистом смены. То есть у объекта должен быть статус **New** или **Waiting for customer**.

Проблема. Зашел на платформу и не вижу никаких сработок.

Решение. В таких случаях следует проверить, что в данную минуту у вас не установлены фильтры, ограничивающие вывод результатов. В первую очередь следует обратить внимание на установленные даты. Далее на фильтры по типу, статусу или тегу.

Проблема. Заполнил все данные об организации, но результатов на платформе никаких нет.

Решение. После заполнения данных об организации вам необходимо подождать некоторое время. Это связано с работой наших инструментов. Как только инструменты по поиску завершат свою работу, информация появится на платформе.

Проблема. На странице заглушка «Ничего не найдено». Что это значит?

Решение. Заглушки на странице соответствуют результату:

- **Проверка еще выполняется** — необходимо дождаться, когда наши инструменты обработают.
- **Ничего не найдено** — при проверке не обнаружено нарушений; если при следующих проверках что-то найдется, мы добавим на платформу.

Техническая поддержка

Если у вас возникли проблемы при использовании платформы, сообщите о возникшей проблеме вашему сервис-менеджеру BI.ZONE или обратитесь в службу технической поддержки одним из следующих способов:

- По телефону +7 499 110-25-34 (доб. 2);
- По адресу электронной почты bp@bi.zone.

Техническая поддержка обеспечивается на территории присутствия Заказчика в Российской Федерации, предоставляется круглосуточно и без выходных.

Работоспособность, корректное функционирование и обновление платформы осуществляется компанией BI.ZONE.