

ПРОГРАММНЫЙ ПРОДУКТ
PHISHNET
Руководство администратора

СОДЕРЖАНИЕ

Обозначения и сокращения	3
1. Общие сведения	4
2. Назначение и возможности	5
3. Подготовка к работе	6
4. Неизвестные данные.....	7
5. Управление пользователями	7
6. Вебхуки.....	8

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе используются следующие обозначения и сокращения:

Обозначение (сокращение)	Расшифровка обозначения (сокращения)
JSON	От англ. JavaScript Object Notation — текстовый формат обмена данными, основанный на принципе «ключ–значение». Широко используется для передачи структурированных данных между клиентом и сервером.

1. Общие сведения

PHISHNET (далее – PHISHNET) предназначен для организации, и автоматизация процесса оценки осведомленности пользователей в вопросах информационной безопасности посредством рассылки обучающих электронных писем, эмулирующих вредоносную активность.

Пользовательский интерфейс PHISHNET предоставляет пользователю доступ к выполняемым функциям и обеспечивает визуализацию необходимой информации.

Процедура установки PHISHNET описана в документе «PHISHNET_Установка и настройка ПО».

Настройка и распределение ролей описаны в документе «PHISHNET. Руководство администратора информационной безопасности».

3. Подготовка к работе

Для входа в PHISHNET пользователю необходимо выполнить следующие действия:

- ввести учетные данные (логин и пароль) в окне авторизации (Рисунок 2);
- нажать кнопку «Войти».

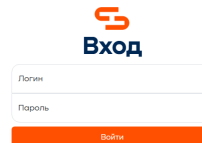


Рисунок 2. Окно авторизации

В результате успешной авторизации на экране отобразится стартовая страница PHISHNET (Рисунок 3).

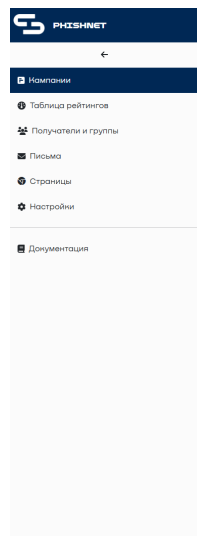


Рисунок 3. Стартовая страница PHISHNET

Главное меню содержит название системы и следующие элементы:



- Раздел «Кампании» предназначен для отображения информации об активных и завершённых кампаниях.
- Раздел «Таблица рейтингов» представляет собой страницу, отображающую рейтинг всех пользователей и групп, которым рассылались письма.
- Раздел «Получатели и группы» предоставляет возможность управлять группами пользователей, которым будут направляться письма в рамках кампаний.
- Раздел «Письма» предоставляет возможность создавать и настраивать письма, которые будут направляться пользователям в рамках обучающих кампаний.

- Раздел «Страницы» предоставляет возможность создавать и управлять шаблонами страниц, которые будут использоваться в фишинговых кампаниях для отображения целевых HTML-страниц пользователям.
- Раздел «Настройки» предназначена для управления и настройки конфигурации система
- Раздел «Документация» содержит документацию системы.

4. Неизвестные данные

На данной странице отображаются данные, полученные в результате отправки формы фишинговой страницы (Рисунок 4). В большинстве случаев отправляемые данные включают параметр `gid` в URL. Если параметр `gid` отсутствует или форма отправлена без каких-либо параметров, такие данные фиксируются и также выводятся на данной странице. Это позволяет отслеживать и анализировать аномальные либо некорректные запросы для дальнейшего контроля и расследования.

Чтобы посмотреть неизвестные данные:

1. В главном меню перейдите в раздел «Неизвестные данные». Откроется страница «Неизвестные данные».
2. Выберите интересующее вас событие и раскройте его кнопкой .
3. Для удаления события используйте кнопку удаления .

Неизвестные данные

На этой странице отображаются данные, отправленные через форму фишинговой страницы. Обычно отправленные данные должны содержать параметр `gid` в URL, однако, если `gid` отсутствует или форма была отправлена без каких-либо параметров, такие данные фиксируются и отображаются здесь. Это позволяет отслеживать и анализировать аномальные или некорректные запросы.











Дата и время ↓↑	Предпросмотр данных	Действия
> 30 августа 2025 г. в 13:11:51	0x[]:androidrogh0st	
> 29 августа 2025 г. в 21:04:04	0x[]:androidrogh0st	
> 29 августа 2025 г. в 21:04:04	0x[]:androidrogh0st	
> 29 августа 2025 г. в 21:04:04	0x[]:androidrogh0st	
> 29 августа 2025 г. в 21:04:04	0x[]:androidrogh0st	
> 28 августа 2025 г. в 06:29:48	0x[]:androidrogh0st	
> 28 августа 2025 г. в 06:29:47	0x[]:androidrogh0st	
> 28 августа 2025 г. в 06:29:47	0x[]:androidrogh0st	
> 28 августа 2025 г. в 06:29:47	0x[]:androidrogh0st	
> 27 августа 2025 г. в 19:30:24	0x[]:androidrogh0st	

Рисунок 4. Стартовая «Неизвестные данные»

5. Управление пользователям

В системе PhishNet предусмотрена поддержка учетных записей пользователей с различными ролями. В настоящее время доступны следующие роли:

- User - роль пользователя, позволяющая выполнять любые действия, за исключением операций системного администрирования (например, управление пользователями, настройка вебхуков и другие административные функции).

- Admin - системная административная роль с полными правами управления всеми возможностями PhishNet.

Чтобы создать пользователя:

1. В главном меню перейдите в раздел «Настройки».
Откроется страница «Настройки».
2. Перейдите в подраздел «Управление пользователями».
3. В открывшемся меню нажмите кнопку «Добавить пользователя»

На странице создания или редактирования учетной записи доступны следующие поля и параметры:

- Логин - уникальный логин пользователя в системе;
- Пароль - пароль для входа в систему;
- Повторите пароль - поле для повторного ввода пароля;
- Пользователь должен задать новый пароль - при следующем входе в систему пользователю будет предложено установить новый пароль;
- Аккаунт заблокирован - параметр, определяющий, может ли пользователь пользоваться функционалом системы;
- Роль - выбор роли пользователя из доступного перечня.

6. Вебхуки

Для получения событий в реальном времени PHISHNET поддерживает возможность настройки вебхуков. При срабатывании событий система будет отправлять HTTP-запросы с JSON-данными на указанный целевой адрес. Формат передаваемого JSON соответствует данным, доступным через API.

Чтобы создать вебхук:

1. В главном меню перейдите в раздел «Настройки».
Откроется страница «Настройки».
2. Перейдите в подраздел «Вебхук».
3. В открывшемся меню нажмите кнопку «Добавить вебхук»

Создавать и редактировать вебхуки могут только пользователи с ролью администратора.

Параметры вебхука:

- Наименование - имя вебхука в системе;
- URL - целевой адрес для отправки данных;
- Секрет - секретная строка для проверки подлинности.
- Активен ? - статус вебхука (включён/выключен).

Каждый запрос вебхука подписывается с использованием алгоритма HMAC-SHA256 на основе всего JSON-тела. Для вычисления подписи используется значение, указанное в поле «Секрет». Подпись передаётся в заголовке «X-Phishnet-Signature», который выглядит следующим образом:

```
POST /webhook HTTP/1.1
Host: localhost:9999
Accept-Encoding: gzip
```

Content-Length: 226

Content-Type: application/json

User-Agent: Go-http-client/1.1

X-Phishnet-Signature:

sha256=2be52d4b83eb7f19b0ecc75ebd6441cefea5512443eb18d38a8beb2e7584a66ccd

Настоятельно рекомендуется установить надёжный секрет и проверять подписи входящих запросов для подтверждения их подлинности и защиты от подмены данных.