

ПРОГРАММНЫЙ ПРОДУКТ
PHISHNET
Руководство пользователя

СОДЕРЖАНИЕ

Обозначения и сокращения	3
Термины и определения	4
1 Введение	5
2 Назначение и возможности	6
3 Подготовка к работе	7
4 Стартовая страница	8
4.1 Кампании	8
4.2 Таблица рейтингов	8
4.3 Получатели и группы	9
4.4 Письма	10
4.5 Страницы	10
4.6 Настройки	12
4.6.1 Настройки - Основные	12
4.6.2 Настройки - Лицензия	12
4.6.3 Настройки – Профили отправителя	13
4.6.4 Настройки – Доменные имена	13

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе используются следующие обозначения и сокращения:

Обозначение (сокращение)	Расшифровка обозначения (сокращения)
PostgreSQL	Свободная объектно-реляционная система управления базами данных
CSV	Файлы особого типа, которые можно создавать и редактировать в Excel. В CSV-файлах данные хранятся не в столбцах, а разделенные запятыми
HTML	От англ. HyperText Markup Language — язык разметки гипертекста, используемый для создания и структурирования содержимого веб-страниц (текста, изображений, ссылок и других элементов).
URL	От англ. Uniform Resource Locator — единообразный указатель ресурса, адрес, используемый для обозначения местоположения ресурсов в сети Интернет.
LDAP	От англ. Lightweight Directory Access Protocol — облегчённый протокол доступа к каталогам, используется для организации и управления распределёнными директориями с информацией о пользователях, группах и других объектах.
API	Интерфейс прикладного программирования, набор методов и правил для взаимодействия программных компонентов между собой.
SMTP	От англ. Simple Mail Transfer Protocol — протокол передачи почты, используемый для отправки электронных сообщений между серверами электронной почты.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины с соответствующими определениями:

Термин	Определение
Go HTTP Client	Встроенный в стандартную библиотеку Go инструмент для отправки HTTP-запросов и получения HTTP-ответов, поддерживающий настройку таймаутов, прокси, заголовков и прочих параметров сетевых соединений
Rod Browser	Инструмент автоматизации браузеров на языке Go с открытым исходным кодом, позволяющий управлять браузером через протокол Chrome DevTools для выполнения действий, сбора данных и тестирования веб-приложений
VS Code	Кроссплатформенный редактор исходного кода с открытым исходным кодом, разработанный корпорацией Microsoft, поддерживающий множество языков программирования, расширения, отладку и интеграцию с системами контроля версий

1 Введение

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».

2 Назначение и возможности

PHISHNET предоставляет обычному пользователю следующие возможности:

- Создание, настройка и запуск обучающих фишинговых кампаний с возможностью отложенного старта;
- Визуализация результатов кампаний с помощью диаграмм и временных графиков, а также подробная аналитика по каждому пользователю;
- Гибкое создание и настройка шаблонов писем и фишинговых сайтов, включая возможность клонирования существующих сайтов;
- Сбор и хранение данных тестируемых пользователей с поддержкой импорта из CSV;
- Формирование и выгрузка отчетов о результатах кампаний в форматах CSV и XLSX.

3 Подготовка к работе

Для входа в RHISHNET пользователю необходимо выполнить следующие действия:

- ввести учетные данные (логин и пароль) в окне авторизации (Рисунок 1);
- нажать кнопку «Войти».

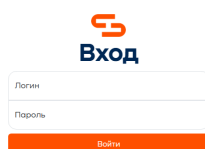


Рисунок 1. Окно авторизации

В результате успешной авторизации на экране отобразится стартовая страница RHISHNET (Рисунок 2).

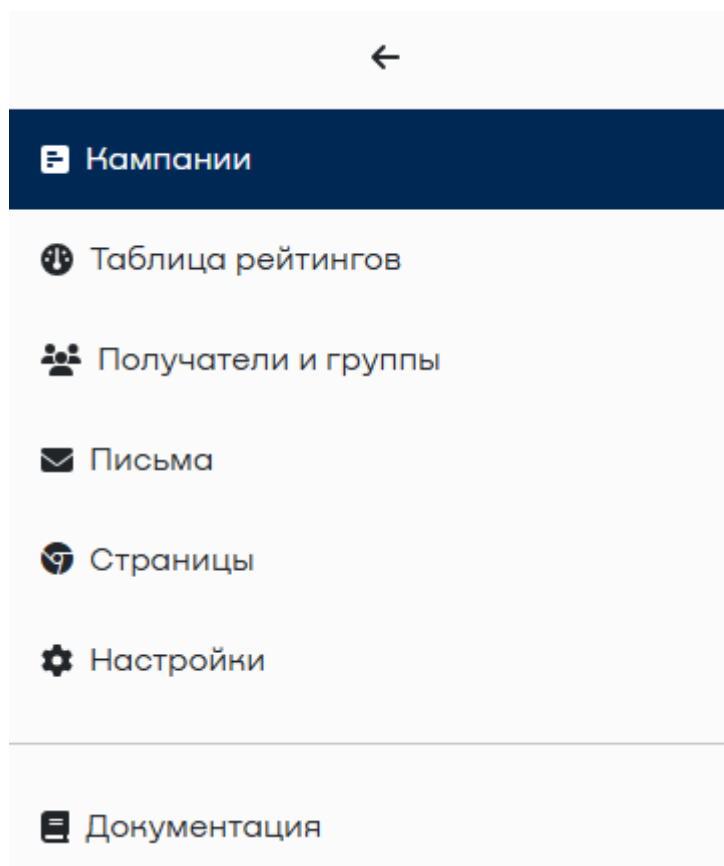


Рисунок 2. Стартовая страница RHISHNET

4 Стартовая страница

Стартовая страница содержит следующие вкладки:

- «Кампании» (см п. 4.1);
- «Таблица рейтингов » (см п. 4.2);
- «Получатели и группы» (см п. 4.3);
- «Письма» (см п. 4.4);
- «Страницы » (см п. 4.5);
- «Настройки» (см п. 4.6);

4.1 Кампании

Страница «Кампании» предназначена для отображения информации об активных и завершённых кампаниях. На странице представлена следующая статистика:

- количество отправленных писем;
- количество открытых писем;
- количество переходов по ссылкам;
- количество полученных данных;
- количество полученных ложных данных.

На странице доступна возможность:

- перейти к просмотру любой активной или завершённой кампании;
- создать новую кампанию с помощью кнопки «Создать кампанию».

4.2 Таблица рейтингов

В рамках каждой фишинговой кампании осуществляется автоматический учёт действий пользователя, влияющих на его рейтинг (Рисунок 3).

Начальный рейтинг пользователя составляет **10.0** баллов. В процессе взаимодействия с фишинговым сценарием рейтинг изменяется следующим образом:

- открытие письма — снижение рейтинга на **0.5** балла;
- переход по ссылке — снижение рейтинга на **0.5** балла;
- ввод данных — снижение рейтинга на **4.0** балла;
- повторный ввод данных — снижение рейтинга на 0.5 балла.

Чем активнее пользователь взаимодействует с фишинговой рассылкой, тем ниже становится его итоговый рейтинг.

Таблица рейтингов

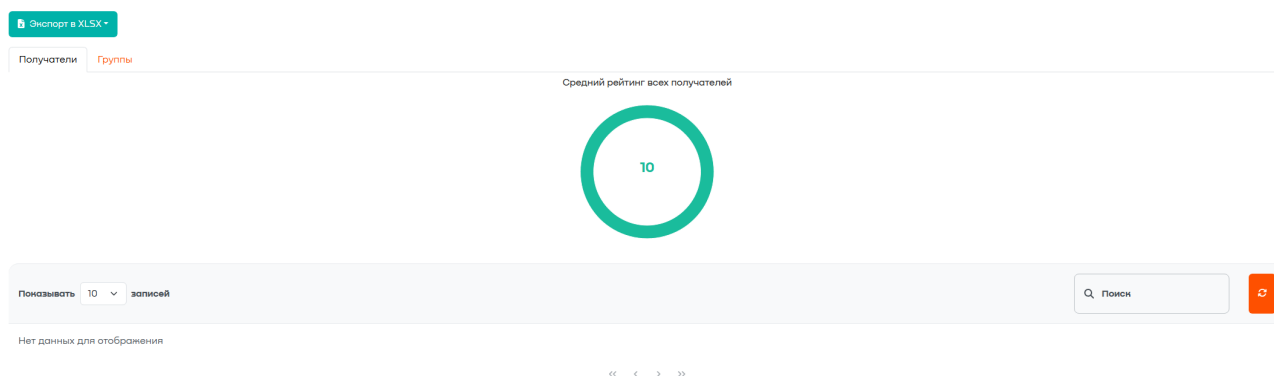


Рисунок 3. Вкладка «Таблица рейтингов»

Пользователь имеет возможность сгенерировать отчёт с рейтингами как по всем пользователям системы, так и отдельно по выбранным группам.

4.3 Получатели и группы

Система RHISHNET предоставляет возможность управлять группами пользователей, которым будут направляться письма в рамках кампаний

Добавление пользователей в группу доступно двумя способами:

- вручную;
- с помощью импорта из файла;

Для создания новой группы выполните следующие действия:

1. Перейдите на страницу «Получатели и группы» в меню навигации.
2. Нажмите кнопку «Добавить группу».
3. В открывшемся диалоговом окне необходимо указать уникальное имя группы и добавить хотя бы одного получателя.

Для ручного добавления пользователя заполните следующие поля:

- Имя;
- Фамилия;
- Электронная почта (обязательное поле);
- Должность;

Для массового добавления пользователей предусмотрен импорт из CSV-файла. CSV-файл должен содержать следующие заголовки:

- Имя;
- Фамилия;
- Электронная почта;
- Должность.

Чтобы выполнить импорт, нажмите кнопку «Импорт получателей», выберите файл и загрузите его. После успешной загрузки данные пользователей отобразятся в диалоговом окне. Для завершения создания группы нажмите кнопку «Сохранить».

4.4 Письма

Система RHISHNET предоставляет возможность создавать и настраивать письма, которые будут направляться пользователям в рамках обучающих кампаний. Экземпляр письма — это содержимое электронных писем, которое направляется получателям в рамках кампаний. Экземпляры могут быть созданы с нуля или импортированы из существующего письма, а также поддерживают прикрепление вложений. Дополнительно в шаблон письма можно добавить отслеживающее изображение для фиксации момента открытия письма пользователем.

Для создания нового экземпляра письма выполните следующие действия:

1. Перейдите на страницу «Письма» в меню навигации;
2. Нажмите кнопку «Добавить письмо»

В открывшемся окне создания/редактирования письма доступны следующие поля:

- Наименование — название письма;
- Отправитель письма — необязательный параметр, который изменяет значение поля «from». Может использоваться для подмены отправителя. Если значение не указано, используется значение из профиля отправителя;
- Тема письма — необязательный параметр, определяющий текст темы письма.
- HTML — HTML-код письма;
- Text — текстовая версия содержимого письма. Если заполнены оба варианта (HTML и Text), приоритет отдаётся HTML-коду;
- «Добавить отслеживание письма» — при активации данного параметра в HTML автоматически добавляется скрипт для отслеживания открытия письма;
- «Вложения письма» — возможность добавить файлы, которые будут прикреплены к письму;

Для переключения между визуальным представлением письма и HTML-кодом нажмите кнопку «HTML редактор». Для предварительного просмотра письма перед отправкой получателям используйте кнопку «Предпросмотр».

Для импорта письма из необработанного контента (например, скопированного через функцию «Просмотр оригинала» в почтовом клиенте) нажмите кнопку «Импортировать письмо» и вставьте соответствующий контент.

4.5. Страницы

Система RHISHNET предоставляет возможность создавать и управлять шаблонами страниц, которые будут использоваться в фишинговых кампаниях для отображения целевых HTML-страниц пользователям.

Шаблоны страниц — это HTML-страницы, которые отображаются пользователям при переходе по фишинговым ссылкам, отправленным в рамках кампании. Шаблоны поддерживают использование переменных, позволяют собирать введённые учётные данные и осуществлять перенаправление пользователей на другой веб-сайт после отправки данных.

RHISHNET автоматически генерирует уникальный идентификатор (параметр RID) для каждого получателя кампании. Этот идентификатор используется для динамической загрузки соответствующей целевой страницы.

Для просмотра результата можно воспользоваться HTML-редактором или запустить тестовую кампанию. При обращении напрямую к слушателю PHISHNET без указания RID будет отображена стандартная страница 404.

PHISHNET позволяет клонировать страницы веб-сайта по указанному URL. Для этого используется инструмент импорта, основанный на Rod Browser, который имитирует поведение реального пользователя (Рисунок 4). В качестве дополнительного метода применяется Go HTTP Client.

Для клонирования страницы выполните следующие действия:

- Нажать кнопку «Импортировать страницу»;
- В открывшемся окне укажите параметры
 1. Наименование страницы — название сохраняемой страницы.
 2. Ссылка — URL исходной страницы для клонирования.
 3. Использовать принудительный импорт — при активации параметра в случае частичного сбоя в Rod Browser используется Go HTTP Client, который может быть более заметен для защитных систем.



Рисунок 4. Меню импорта страницы

Для самостоятельного создания HTML-страницы предусмотрен редактор кода, разделённый на три вкладки:

1. HTML-код — редактор в формате, аналогичном среде разработки (например, VS Code);
2. Поля ввода — отображает все `<input/>` элементы, доступные для редактирования и удаления. Для обновления данных после изменений HTML нажмите кнопку «Обновить», а для сохранения — «Применить изменения»;
3. Предпросмотр страницы — отображает результат редактирования в реальном времени.

PHISHNET по умолчанию активирует опцию «Собирать отправленные данные», позволяя фиксировать введённые пользователями учётные данные.

После отправки данных для снижения подозрительности пользователей предусмотрены следующие варианты перенаправления:

- На внешний веб-сайт — укажите адрес в поле «Перенаправлять на»;
- На контролируемую RHISHNET страницу — установите флаг «Использовать HTML вместо перенаправления по ссылке» и настройте страницу в HTML-редакторе.

В меню управления ресурсами страницы доступны следующие действия:

- копирование URL ресурса;
 - просмотр исходного содержимого;
- удаление ресурса.

4.6. Настройки

Нажав на вкладку «Настройки», вы перейдете на страницу настроек. Данная страница содержит следующие вкладки:

- Основные - содержит основные настройки профиля текущего пользователя;
- Лицензия - содержит информацию о лицензии;
- Профили отправителя - настройка профилей отправителя;
- Доменные имена - настройка доменных имен;
- Конфигурация LDAP - настройка профилей LDAP.

4.6.1. Настройки - Основные

На странице «Основные» доступны следующие функции:

- сброс и копирование ключа API (кнопки «Сбросить» и «Копировать» рядом с полем «Ключ API»);
- выбор языка интерфейса;
- просмотр версии приложения;
- изменение имени пользователя и пароля.

4.6.2. Настройки - Лицензия

На странице «Лицензия» содержится информация о действующей лицензии на ПО RHISHNET используемой на этом сервере. Страница содержит следующую информацию. Информация о лицензии:

- Клиент;
- Продукт;
- Тип подписки;
- Дата выпуска;
- Дата истечения;
- Количество дней до истечения;
- Подлинность лицензии.

Также на странице отображена информация о лимитах и разрешениях доступных для этого сервера:

- Лимит на количество страниц;
- Лимит на количество писем;
- Доступны ли вебхуки;
- Доступен ли LDAP;
- Доступен ли импорт страниц;

- Доступна ли таблица рейтингов;
- Лимит на количество получателей.

4.6.3. Настройки – Профили отправителя

Для отправки электронных писем необходимо настроить данные ретрансляции SMTP, которые называются «Профили отправителя».

Для настройки профиля отправителя выполните следующие действия:

- Перейдите в раздел «Профили отправителя» на боковой панели.
- Нажмите кнопку «Добавить профиль-отправителя».

Важно убедиться, что адрес в поле «SMTP от» является действующим адресом электронной почты.

Проверьте корректность заполнения поля «Хост» в формате хост:порт.

Для проверки работоспособности конфигурации SMTP используйте кнопку «Отправить тестовое письмо».

Меню профиля отправителя содержит следующие поля:

- Наименование профиля отправителя – название профиля, отображаемое в системе.
- SMTP от – электронный адрес, от имени которого будут отправляться письма.
- Хост – SMTP-хост с указанием порта.
- Логин – учетная запись или электронный адрес для подключения к SMTP-серверу.
- Пароль – пароль от учетной записи SMTP.

4.6.4. Настройки – Доменные имена

Страница «Добавление домена» предназначена для добавления доменных имён, используемых при создании компаний (Рисунок 5). Для выбора доменного имени при создании компании необходимо предварительно добавить его в разделе «Добавление домена».

Рекомендуется добавлять только те доменные имена, которые закреплены за IP-адресом сервера, на котором размещен PHISHNET.

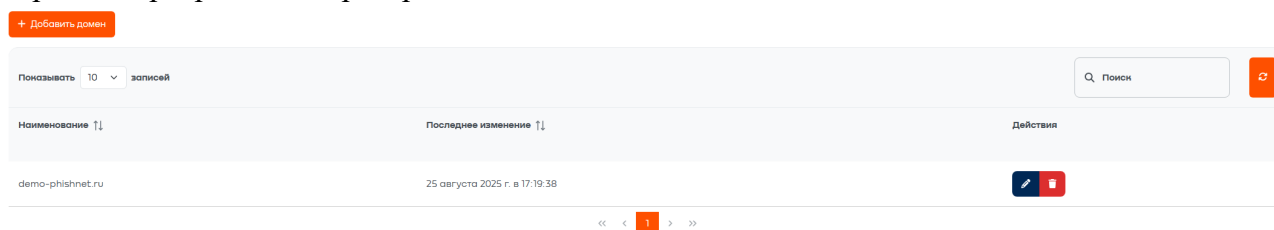


Рисунок 5. Вкладка «Настройки – Доменные имена»