

# Техническое задание

## 1. Цель продукта

Система фишинговых рассылок позволяет автоматизировать одно из направлений пентеста, путём проведения массовых отправок писем на группы пользователей от различных отправителей с настраиваемыми параметрами кампании, а также с различными сценариями/оформлениями писем и генерацией ссылок.

## 2. Роли

- **Пользователь** – Работа с кампаниями с полным функционалом.
- **Администратор** – Функционал пользователя, а также возможность создавать пользователей.

## 3. Видение технической доработки продукта

### Лицензирование

Поставка продукта заказчикам, которые выразили желание пилотировать его самостоятельно, должна осуществляться по лицензии на ограниченный функционал и ограниченные сроки.

AS IS:

Лицензирование отсутствует, платформа предоставляется с неограниченным временем действия и полным функционалом.

TO BE:

- Оплаченная лицензия должна поставляться с двумя ограничениями:
  1. Временное – платформа работает с заявленным функционалом время с момента активации (полгода, год, 2 года); За месяц до окончания действия выводится предупреждение о том, что остался месяц. По окончании времени действия, система переходит в ограниченный режим.
  2. Функциональное – количество получателей писем, созданных за всё время (даже если были удалены, то всё равно учитываются) не должно превышать количества, установленного лицензией, и +10%. Закладываются дополнительные 10% от значения, указанных в договоре, которые могут быть использованы для тестовых рассылок, ошибок, новых сотрудников, презентаций и тд. Система выводит предупреждение об израсходовании получателей писем при 100%, но продолжает работать в полном режиме, пока не будут потрачены ещё дополнительные 10%. Когда потрачены 110% система переходит в ограниченный режим.
- Активация лицензии происходит в приветственном/специальном окне по вводу серийного ключа, который владелец продукта генерирует на основе данных получателя продукта и отправляет получателю продукта.
- Превышение ограничений лицензии/отсутствие лицензии позволяет пользоваться продуктом в ограниченном режиме: пропадает возможность создавать компании.

## DETAILS:

- Сервис генерации серийных ключей является оффлайновым приложением, позволяющим:
  - Принимать на вход четыре параметра: имя юридического лица; управляющий параметр времени использования лицензии; управляющий параметр количества получателей рассылки, файл содержащий данные о железе получателя продукта.
  - Генерировать зашифрованный серийный ключ на основе упомянутых выше четырех входных параметров.
    - Серийный ключ является уникальным, не может быть сгенерирован заново.
    - \*Уникальность серийного ключа при неуникальных данных, которые он в себе содержит, должна контролироваться генерирующим приложением или иначе.
  - Расшифровывать серийный ключ, который можно подать на вход, выводя четыре входных параметра для ключа.
  - \*Иметь возможность смены секрета.
- Сервис генерации слепок системы (данных о железе) является оффлайновым приложением/дополнительным сервисом в системе, позволяющим:
  - Запускать сбор информации об устройствах (процессор, видеокарта, материнская плата и тд), установленных на машине, где будет разворачиваться система.
  - На основе собранной информации генерировать файл, который совместим с приложением генерации ключей.
- Система фишинговых рассылок должна:
  - Иметь внутри себя секрет, по которому способна расшифровывать и применять поданный в специальном окне серийный ключ в оффлайн-режиме.
  - \*Иметь возможность смены секрета на стороне поставщика продукта (и не иметь такую возможность на стороне получателя продукта).
  - После активации лицензии выводить информацию в справочной вкладке об:
    - Имени юридического лица.
    - Времени действия лицензии (оставшееся время из времени предусмотренного лицензией или дата начала действия и дата окончания действия).
    - Оставшееся количество получателей писем из количества получателей, предусмотренных лицензией.
  - Не иметь возможности активации/обновления лицензии при повторном вводе действующего/отработанного серийного ключа.
  - Не иметь возможности быть активированной на нескольких машинах посредством контроля на основе собранных данных о железе до генерации ключа.

## Интеграция

Массовая загрузка получателей писем.

AS IS:

Возможен импорт .csv файла в определенном формате со списком получателей.

TO BE:

- Продукт должен дополнительно иметь интеграцию с Active Directory – при наличии требуемых прав и информации у пользователя ПК он сможет в продукте по

нажатию кнопки добавить список получателей, выгрузив контактную книгу Active Directory.

#### DETAILS:

- Подгрузка группы пользователей из AD производится по нажатию кнопки «Импорт из AD».
- \*Возможны дополнительные галочки какую информацию собирать: имя, фамилия, должность, email (email обязательно).

#### Файловые вложения

В рассылке возможно прикрепление файловых вложений с генерацией уникальной ссылки, спрятанной в изображении, для отслеживания открытия файла получателем. Существуют различные шаблоны файлов.

#### AS IS:

Файловые вложения прикрепляются, ссылки не генерируются.

#### TO BE:

- Генерация ссылок в файлах подобно FAQ для GoPhish.

#### Предоставление

Продукт поставляется в цифровом формате.

#### AS IS:

Продукт передается получателю в виде образа виртуальной машины.

#### TO BE:

- Продукт имеет дополнительную возможность быть переданным в качестве дистрибутива с руководством по установке.

#### DETAILS:

- Установка должна быть относительно простой.
- Способ установки/поставки должен предусматривать затрудненность доступа к исходному коду продукта.