

Реализация многофакторной аутентификации на системе управления веб-сайтами Wordpress с защитой от перехвата SMS-сообщений

Исполнитель:

студент гр. 06-211

Козлов А.О.

Руководитель:

Абдуллин Р.М

Цель и задачи

Цель дипломной работы: реализовать двухфакторную SMS-аутентификацию с защитой от автоматизированного анализа содержимого

Основными задачами дипломной работы являются:

1. Изучить и проанализировать существующие методы многофакторной аутентификации.
2. Установить web-сайт на базе CMS Wordpress.
3. Реализовать модуль аутентификации с использованием SMS-сообщений и защитой от автоматизированного анализа сообщений на мобильных устройствах пользователей.

Факторы аутентификации

- Способы аутентификации пользователей различаются прежде всего аутентификационными факторами.
 - Аутентификационный фактор — определенный вид информации, предоставляемый субъектом системе при его аутентификации.
1. Пароль. (знание информации);
 2. Биометрия. (физическая особенность);
 3. устройство аутентификации. (предмет);

Многофакторная аутентификация

- Многофакторная аутентификация — аутентификация, в процессе которой используются аутентификационные факторы нескольких типов.
- Например, пользователь должен предоставить смарт-карту и дополнительно ввести пароль.
- Двухфакторная аутентификация (ДФА) ,так же известна как двухэтапная верификация, является типом многофакторной аутентификации.

Преимущества и недостатки

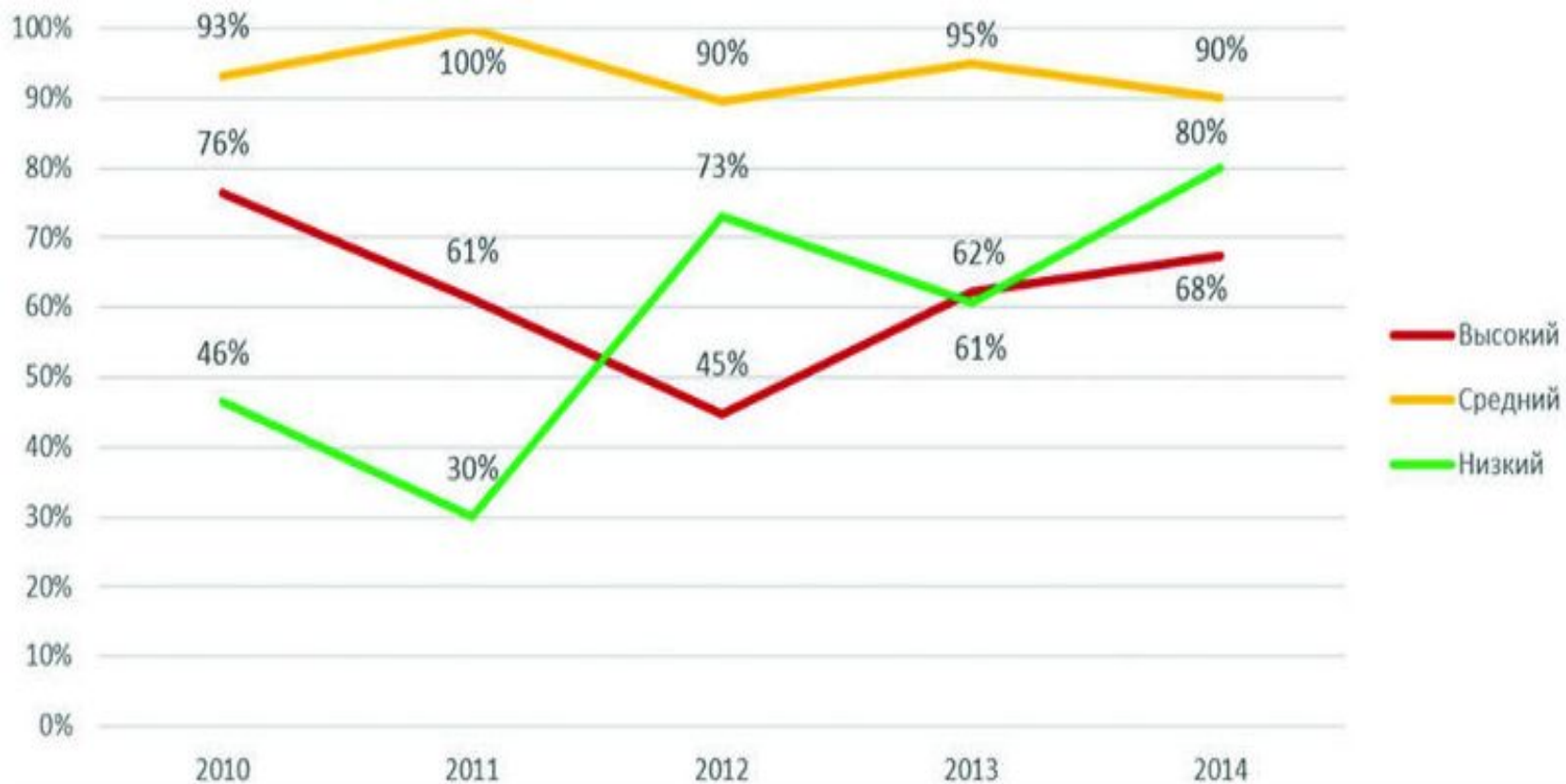
Преимущества:

1. Не нужны дополнительные токены, потому что мобильник всегда под рукой.
2. Код-подтверждения постоянно меняется, а это безопаснее, чем фиксированный логин-пароль.

Недостатки:

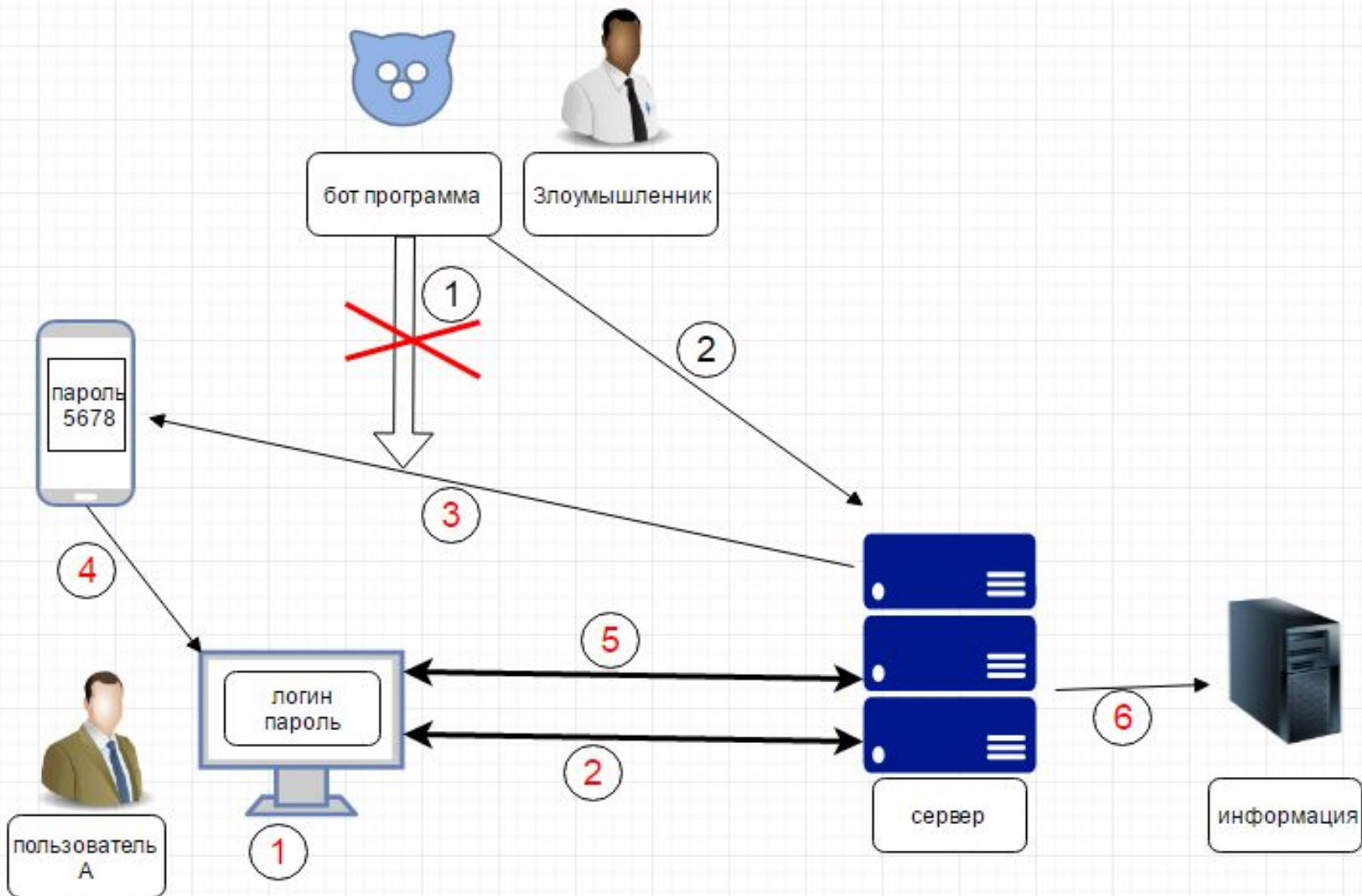
1. Мобильный телефон должен находиться в сети, когда происходит аутентификация, иначе сообщение с паролем просто не дойдет.
2. Вы делитесь с кем-то вашим мобильным телефоном, что влияет на вашу личную жизнь и быть может в будущем на него будет приходить спам.

Доли уязвимых сайтов в зависимости от степени риска уязвимостей

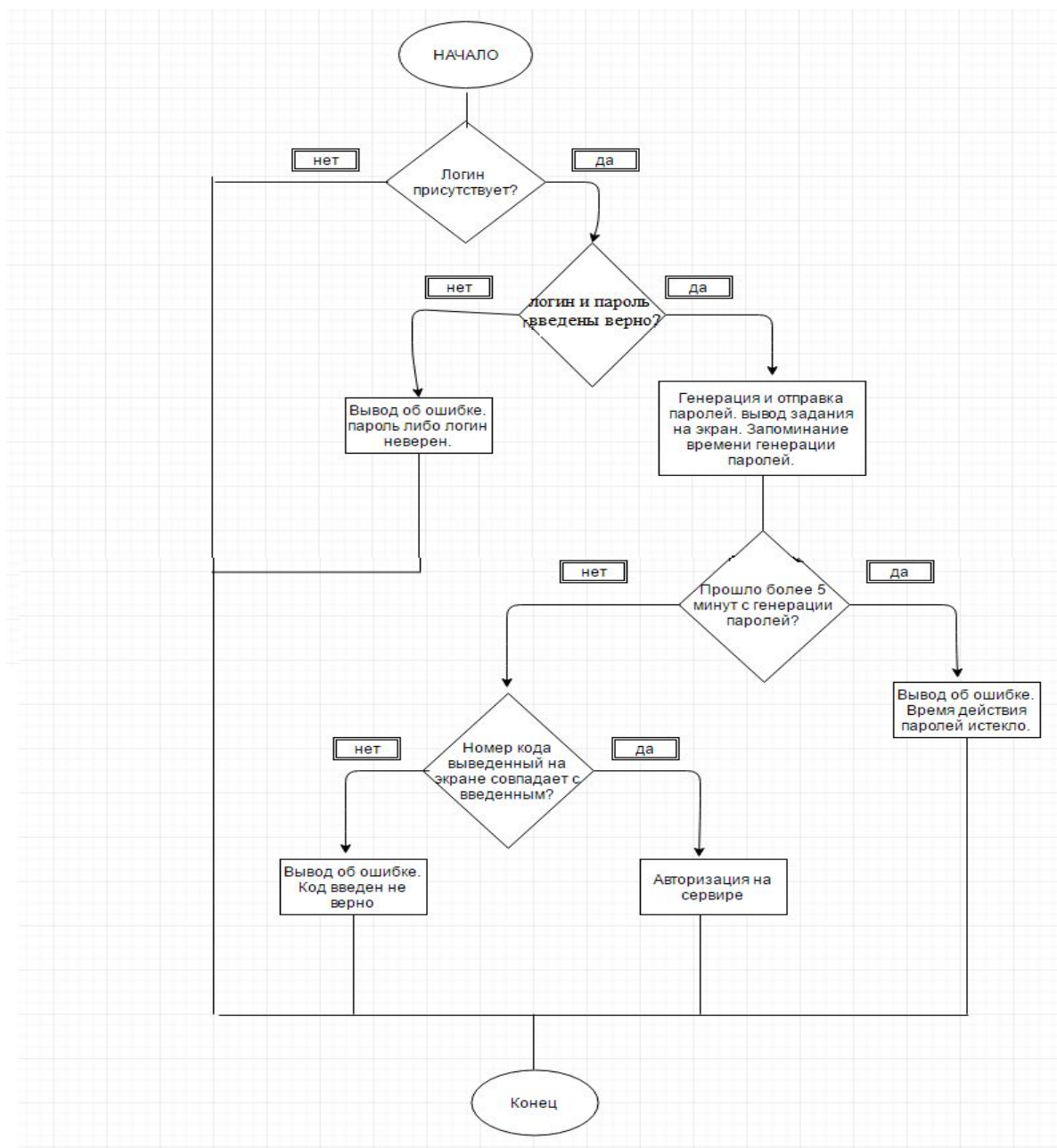


Информация взята с Kaspersky lab

Блок схема перехвата сообщения



Блок схема работы модуля



Выводы модуля об ошибках.

The image displays four screenshots of a WordPress login interface, illustrating error handling and a two-factor authentication (2FA) process.

Top Left Screenshot: Shows the standard login form with the username field containing "admin" and the password field masked with dots. A checkbox for "Запомнить меня" (Remember me) is present, along with a blue "Войти" (Login) button.

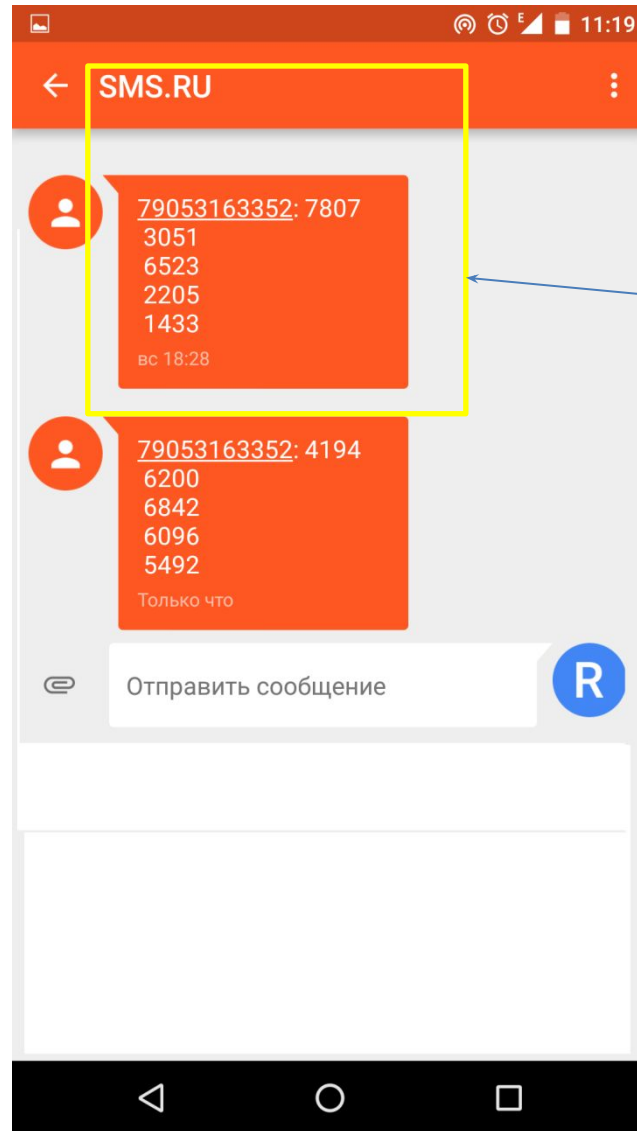
Top Right Screenshot: Shows an error message in a red-bordered box: "ОШИБКА: Введённый вами пароль пользователя admin неверен. [Забыли пароль?](#)" (ERROR: The password you entered for the user admin is incorrect. [Forgot your password?](#)). Below the error, the login form is visible with "admin" in the username field and a masked password field.

Bottom Left Screenshot: Shows the "Двухфакторная аутентификация" (Two-factor authentication) screen. A message in a red-bordered box states: "На ваш номер было отправлено смс с числами, для авторизации введите число №2 XXX-XXX-6080" (An SMS with numbers was sent to your number, for authorization enter the number #2 XXX-XXX-6080). Below this is a text input field labeled "Число №2 из смс" (Number #2 from SMS) and a blue "Вход" (Login) button.

Bottom Right Screenshot: Shows the WordPress logo at the top. Below it, an error message in a red-bordered box reads: "ERROR Неверный код аутентификации." (ERROR Invalid authentication code.). The login form below shows "admin" in the username field and a masked password field, with a "Войти" (Login) button.

Экран мобильного устройства

ПОЛЬЗОВАТЕЛЯ



5 случайно
сгенерированных
чисел

Сравнение с аналогами

<input type="checkbox"/>	Theme My Login Активировать Изменить Удалить	Оформит страницы входа, регистрации и восстановления. Версия 6.4.5 Автор: Jeff Farthing Детали
<input type="checkbox"/>	Two-Factor Authentication - Clockwork SMS Активировать Изменить Удалить	Proper security for your Wordpress site. Text message verification. Версия 1.0.2 Автор: Clockwork Детали
<input type="checkbox"/>	Плагин	Описание

Clockwork

SECURE LOG IN

SMS CODE

ENTER

Two-Factor Authentication - Clockwork SMS

Описание | Установка | Скриншоты | Изменения | FAQ | Отзывы

Клокверский модуль

Редактирование clockwork-two-factor-authentication/clockwork-two-factor.php (неактивен)

Выберите плагин для изменения: Two-Factor Authentication - Clockwork SMS ▾ Выбрать

```
<?php
/*
Plugin Name: Two-Factor Authentication - Clockwork SMS
Plugin URI: http://wordpress.org/extend/plugins/clockwork-two-factor/
Description: Proper security for your Wordpress site. Text message-based two factor authentication for logins.
Version: 1.0.2
Author: Clockwork
Author URI: http://www.clockworksms.com/
*/

/* Copyright 2013, Mediaburst Limited.

Permission to use, copy, modify, and/or distribute this software for any purpose
with or without fee is hereby granted, provided that the above copyright notice
and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT,
OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE,
DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
*/

// Version of the Clockwork plugin in use
```

Документация: Название функции... ▾ Поиск

Обновить файл

Файлы плагинов

- clockwork-two-factor-authentication/clockwork-two-factor.php
- clockwork-two-factor-authentication/css/clockwork.css
- clockwork-two-factor-authentication/js/clockwork_options.js
- clockwork-two-factor-authentication/lib/class-clockwork-plugin.php
- clockwork-two-factor-authentication/templates/user-options.php
- clockwork-two-factor-authentication/templates/required-number-form.php
- clockwork-two-factor-authentication/templates/code-form.php
- clockwork-two-factor-authentication/templates/clockwork-message.php
- clockwork-two-factor-authentication/templates/clockwork_options.js
- clockwork-two-factor-authentication/templates/twofactor_options.js
- clockwork-two-factor-authentication/readme.txt

Наш модуль

Изменение плагинов

Редактирование wp-two-step-auth/index.php (активен)

Выберите плагин для изменения: [TSA] Two Step Authentication

Выбрать

```
<?php
/**
 * Plugin Name: [TSA] Two Step Authentication
 * Description: Двухфакторная аутентификация пользователей
 * Author: Andrey Kozlov
 * Version: 1.0.0
 */

require_once 'helpers.php';

class TSAAuth {

    private static $__instance = null;

    public $api_key = null;

    public static function instance()
    {
        if( ! is_a( self::$__instance, 'TSAAuth' ) ) {
            self::$__instance = new TSAAuth;
            self::$__instance->setup();
        }

        return self::$__instance;
    }
}
```

Файлы плагинов

wp-two-step-auth/index.php

wp-two-step-auth/helpers.php

Документация: Название функции...

Поиск

Внимание: Не рекомендуется вносить изменения в активные плагины. Если ваши изменения приведут к фатальной ошибке, плагин будет автоматически деактивирован.

Заключение

В ходе данной работы были:

1. Изучены и проанализированы существующие методы многофакторной аутентификации;
2. Установлен web-сайт на базе CMS Wordpress по адресу kpfu-students-help.ru;
3. Проведен анализ угроз для систем аутентификации web-сайтов с использованием SMS-сообщений;
4. Реализован модуль аутентификации с использованием SMS-сообщений и защитой от автоматизированного анализа сообщений на мобильных устройствах пользователей;

Спасибо за Внимание

Хронология событий

