DOI: https://doi.org/10.15688/NBIT.jvolsu.2021.2.1

УДК 004.42
ББК 32.972.53

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРОЕКТОВ НА ОСНОВЕ CMS WORDPRESS

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент, кафедра информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Юрьевич Панин

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBS-161_824661@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Романовна Алеева

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBb-202_156445@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье представлен алгоритм программного комплекса, включающий в себя три основных блока: получение данных и создание резервной копии, обработка информации о системе, применение механизмов защиты. Разработан программный комплекс для обеспечения безопасности веб-проектов на основе CMS WordPress.

Ключевые слова: CMS WordPress, угрозы веб-проектов, средства защиты, механизмы защиты, информационная безопасность.

Для каждой компании-разработчика современных интернет проектов, одной из самых главных задач является именно обеспечение необходимого уровня защиты информации в своем веб-проекте. Когда компания-разработчик интернет проекта стабильно защищает свою информационную систему, она создает надежную и безопасную среду для своей деятельности во всемирной сети. Повреждение, утечка и кража информации с сайта – все это неминуемо приведет к уменьшению уровня доверия к организации в целом, а также к проблемам с законом, а это всегда убытки для каждой компании. Например, могут появиться убытки от плохой репутации компании-разработчика, от отсутствия клиентов, от затрат на возобновление стабильной работы интернет-проекта на основе системы управления контентом WordPress или от потери важной информации, которая содержалась в системе.

Рассмотрим, как обеспечивается работа веб-проекта на основе CMS WordPress с точки зрения информационной безопасности.

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность [1–6]:

– целостность данных – защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных; примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании;

– конфиденциальность информации – незаконное разглашение, утечка, повреждение информации;

– доступность информации для всех пользователей – отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

Нарушение одного из этих аспектов может привести к сбоям в работе, а также невозможности нормальной работы веб-проекта на основе CMSWordPress. На наличие любого из нарушений могут повлиять и внутренние, и внешние угрозы. Учитывая сегодняшнее развитие информационного общества, можно сделать вывод о тенденции к росту количества угроз безопасности.

Полноценная информационная безопасность веб-проекта на основе CMS WordPress предполагает постоянный контроль всех существенных событий и состояний, которые влияют на защиту информации. Причем защита обязана осуществляться постоянно и охватывать весь жизненный цикл данных, то есть от ее поступления или создания до уничтожения или утраты важности и актуальности.

Основными факторами, оказывающими влияние на защиту информации и данных в CMS WordPress, являются:

– большое распространение CMS WordPress по миру;

– автоматизация многих процессов, происходящих в CMS WordPress;

– большое количество компьютерных преступлений, целью которых является именно CMS WordPress;

– тенденция к дальнейшему росту компьютерных преступлений.

Информационная безопасность в веб-проекте на основе CMS WordPress определяется целым сочетанием предпринимаемых мер, которые направлены на безопасность важной информации. Эти меры можно разделить на две группы:

1. Организационные меры.

2. Технические меры.

Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами защиты. Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д. [5].

Задачи систем информационной безопасности компании многогранны. К примеру, это обеспечение надежного хранения данных на различных носителях; защита информации, передаваемой по каналам связи; ограничение доступа к некоторым данным; создание резервных копий и другое.

Полноценное обеспечение ИБ в веб-проекте на основе CMS WordPress реально только при правильном подходе к защите данных. В системе информационной безопасности нужно учитывать все актуальные на сегодняшний день угрозы и уязвимости [6].

Актуальность исследования обусловлена тем, что проблема информационной безо-

пасности интернет проектов, в том числе на CMS WordPress, как на одной из самых распространенных, на сегодняшний день является одной из наиболее значимых в мире. От обеспечения информационной безопасности в веб-проекте на основе CMS WordPress во многом зависит эффективность и прибыльность работы многих интернет-магазинов, порталов и т. д. как в России, так и во всем мире.

Архитектура программного комплекса обеспечения информационной безопасности в веб-проекте на основе CMS WordPress состоит из следующих модулей (рис. 1):

1) пользовательский интерфейс;

2) модуль получения данных и создания резервной копии;

3) модуль обработки информации о системе;

4) модуль применения механизмов защиты.

В модуль получения данных и создания резервной копии происходит сохранение в переменные введенных данных и передачу их в модуль обработки информации о системе, а также резервная копия файлов системы.

В модуле обработки информации о системе происходит обработка введенных на предыдущем этапе данных о наличии в системе сертифицированных механизмов защиты, формируется отчет со списком рекомендаций по защите от актуальных угроз.

В модуле применения механизмов защиты происходит внедрение в код системы таких механизмов защиты, как хеширование паролей согласно ГОСТ Р 34.11-2012 «Стрибог», разграничение доступа согласно ГОСТ Р 50739-95, обеспечение целостности ядра CMS.

Вывод: разработана архитектура программного комплекса, включающая в себя: пользовательский интерфейс, модуль получения данных и создания резервной копии, модуль обработки информации о системе, модуль применения механизмов защиты.

Пользовательский интерфейс (см. рис. 2–4) предназначен для взаимодействия с программой. Он отображает формы для ввода данных пользователем и отображения результатов работы. При разработке пользовательского интерфейса программного комплекса я стремился сделать его наиболее удобным и интуитивно понятным для пользователя. Он состоит из трех окон. В первом окне отображается меню ввода данных о системе и кнопка создания резервной копии. Также в этом окне есть область вывода уведомлений о создании резервной копии. Во втором окне было решено сделать отображение отчета программы о текущих угрозах и необходимости введения некоторых средств и механизмов защиты. А в третьем окне находится меню выбора механизмов защиты для применения. Также в третьем окне отображается отчет о применении выбранных механизмов защиты.

Окно 1

На панели интерфейса имеются:

1) Область показа подсказок по работе с программой.

2) Область ввода данных пользователем.

3) Кнопка ввода данных пользователем.

4) Кнопка завершения работы.

5) Кнопка создания резервной копии.

6) Поле вывода информации о статусе создания резервной копии.

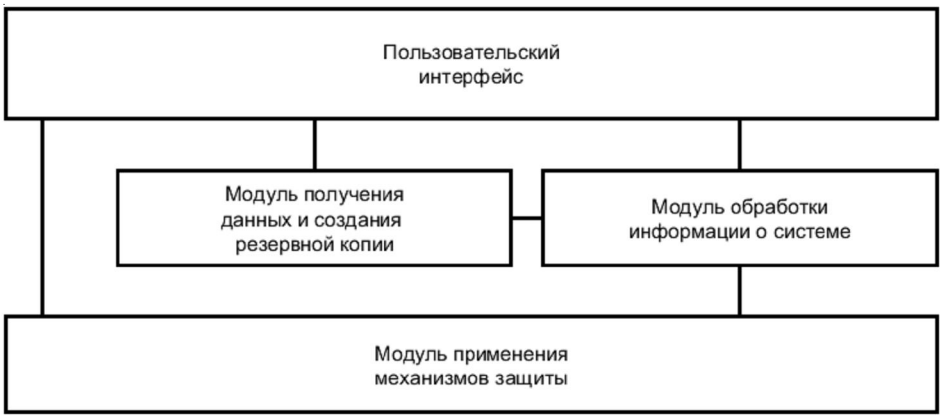

Рис. 1. Архитектура программного комплекса

Окно 2

На панели интерфейса имеются:

1) Область вывода информации об актуальных угрозах и рекомендаций по обеспечению безопасности.

2) Кнопка закрытия текущего окна.

3) Кнопка завершения работы.

4) Кнопка открытия модуля применения механизмов защиты.

Окно 3

На панели интерфейса имеются:

1) Область показа подсказок по работе с программой.

2) Область вывода отчета по примененным механизмам защиты.

3) Поле вывода текущего IP.

4) Меню выбора механизмов защиты.

5) Кнопка запуска модуля применения механизмов защиты.

6) Кнопка закрытия окна.

Вывод: разработан пользовательский интерфейс программного комплекса обеспечения безопасности веб-проектов на основе системы управления контентом WordPress. Были перечислены и описаны все элементы пользовательского интерфейса.

Алгоритм программного комплекса обеспечения безопасности веб-проектов на основе системы управления контентом WordPress состоит из трех основных блоков: получение данных и создание резервной копии, обработка информации о системе и применение механизмов защиты (рис. 5).

Блок-схема модуля получения данных и создания резервной копии представлена на рисунке 6.

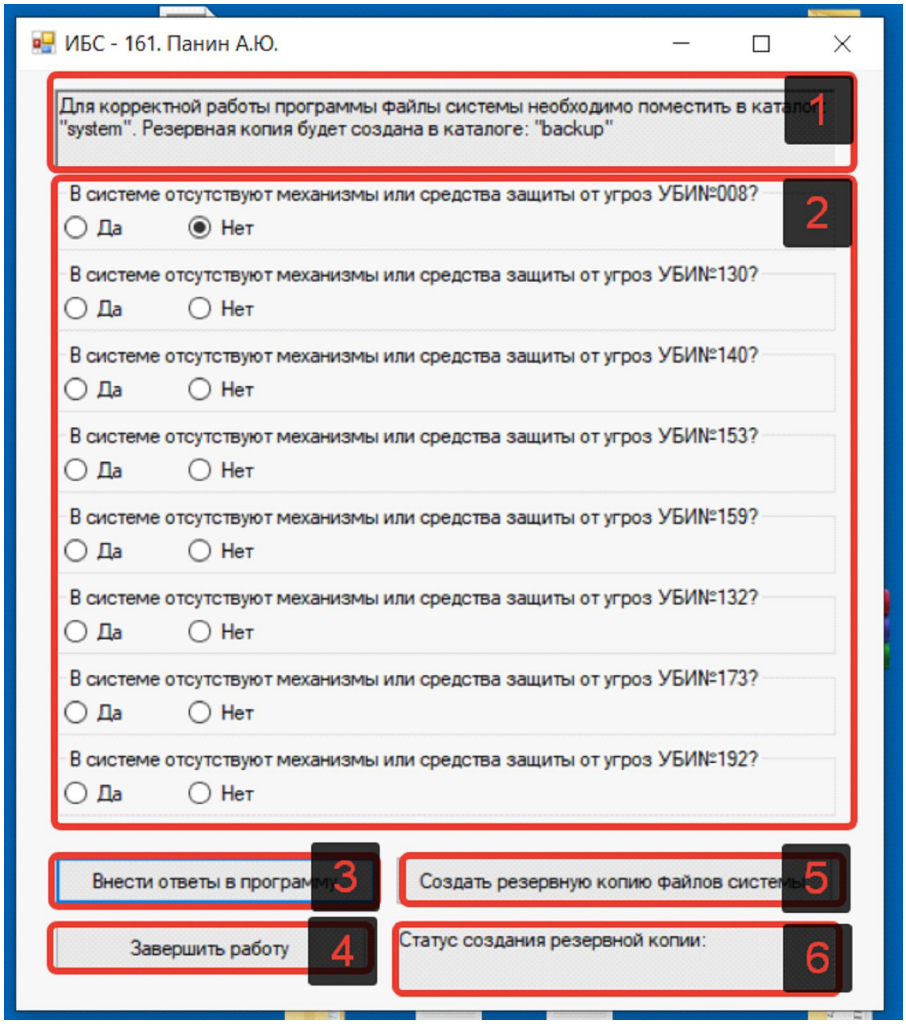

Рис. 2. Пользовательский интерфейс (окно 1)

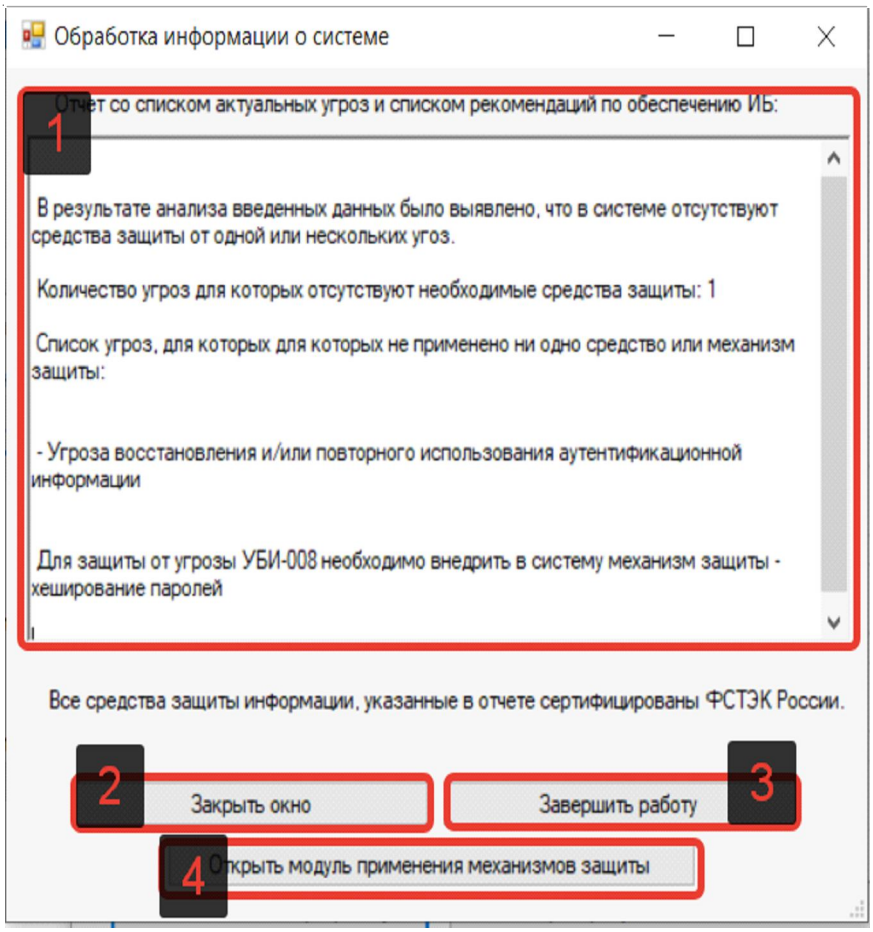

Рис. 3. Пользовательский интерфейс (окно 2)

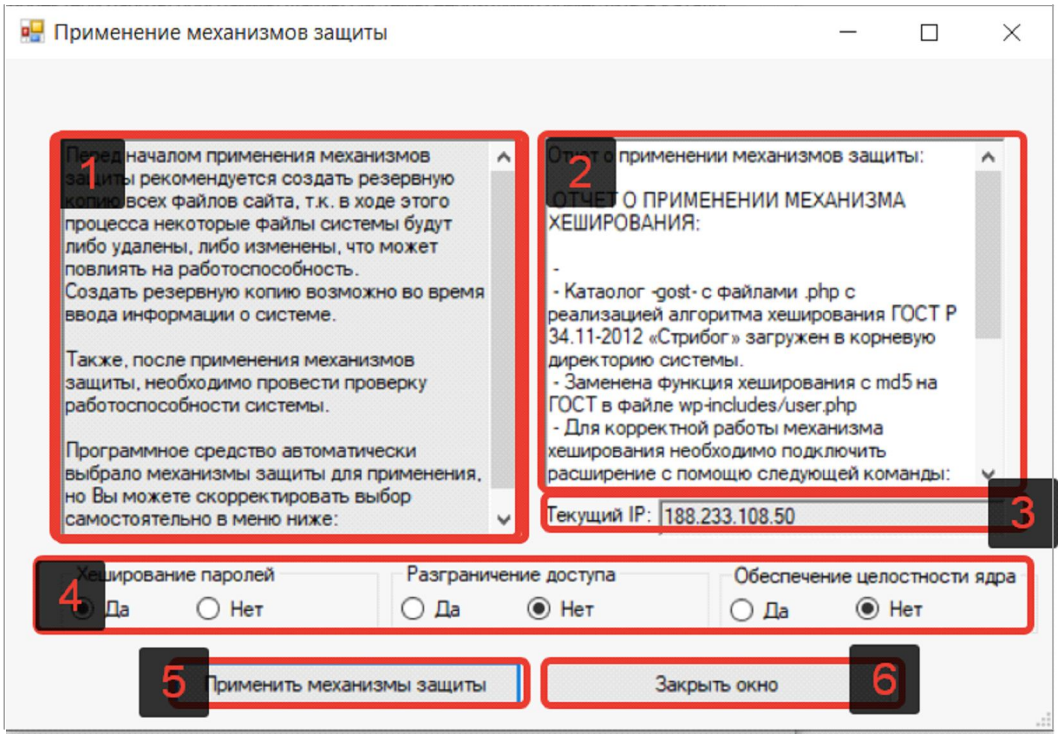

Рис. 4. Пользовательский интерфейс (автоматическая оптимизация безопасности) (окно 3)

Рис. 5. Блок-схема алгоритма программного комплекса повышения безопасности веб-проектов на основе CMS WordPress

Рис. 6. Блок-схема алгоритма модуля получения данных и создания резервной копии

В статье представлен алгоритм программного комплекса, включающий в себя три основных блока: получение данных и создание резервной копии, обработка информации о системе, применение механизмов защиты. На основании отчета о применении механизмов защиты можно сделать вывод о том, что программный комплекс обеспечения безопасности веб-проектов на основе CMS WordPress может определять, какой механизм защиты необходим для защиты от угрозы УБИ-008. Также может быть применен механизм хеширования паролей.

СПИСОК ЛИТЕРАТУРЫ

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е. В. Глинская, Н. В. Чичварин. – М. : Инфра-М, 2018. – 160 с.

2. Гришина, Н. В. Информационная безопасность предприятия : учеб. пособие / Н. В. Гришина. – М. : Форум, 2017. – 159 с.

3. Ковалев, А. А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов : монография / А. А. Ковалев, В. А. Шамахов. – М. : Риор, 2018. – 32 с.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М. : ИД ФОРУМ : НИЦ ИНФРА-М, 2017. – 416 с.

5. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – М. : ДМК, 2017. – 702 с.

6. Ярочкин, В. И. Информационная безопасность : учеб. для вузов / В. И. Ярочкин. – М. : Акад. Проект, 2018. – 544 с.

REFERENCES

1. Glinskaya E.V., Chichvarin N.V. *Informacionnaya bezopasnost' konstrukcij EVM i system: ucheb. posobie* [Information Security of Computer Structures and Systems. Study Guide] .Moscow, Infra-M Publ., 2018. 160 p.

2. Grishina N.V. *Informacionnaya bezopasnost' predpriyatiya: ucheb. posobie* [Information Security of the Enterprise. Study Guide]. Moscow, Forum Publ., 2017. 159 p.

3. Kovalev A.A., Shamahov V.A. *Voennaya bezopasnost' Rossii i ee informacionnaya politika v epohu civilizacionnyh konfliktov: monografia* [Russia's Military Security and Its Information Policy in the Era of Civilizational Conflicts. Monograph]. Moscow, Rior Publ., 2018. 32 p.

4. Shan'gin V.F. *Informacionnaya bezopasnost' komp'yuternyh sistem i setej: ucheb. posobie*

[Information Security of Computer Systems and Networks]. Moscow, ID FORUM Publ., NITs INFRA-M Publ., 2017. 416 p.

5. Shan'gin V.F. *Informacionnaya bezopasnost' i zashchita informacii* [Information Security and Information Protection]. Moscow, DMK Publ., 2017. 702 p.

6. Yarochkin V.I. *Informacionnaya bezopasnost'* [Information Security]. Moscow, Akademicheskiy proekt, 2018. 544 p.

DEVELOPMENT OF A SOFTWARE PACKAGE FOR ENSURING THE SECURITY OF WEB PROJECTS BASED ON CMS WORDPRESS

Yulia S. Bakhracheva

Candidate of Technical Sciences, Associate Professor of the Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksej Yu. Panin

Student, Department of Information Security,
Volgograd State University
IBS-161_824661@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina R. Aleeva

Student, Department of Information Security,
Volgograd State University
IBb-202_156445@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. For every company that develops modern Internet projects, one of the most important tasks is to ensure the necessary level of information protection in its web project. When an Internet project developing company consistently protects its information system, it creates a reliable and secure environment for its activities on the World Wide Web. Damage, leakage, lack and theft of information from the site will inevitably lead to a decrease in the level of trust in the organization as a whole, as well as to problems with the law, which is always a loss for each company. For example, there may be losses from the bad reputation of the developer, the lack of customers, the costs of resuming the stable operation of an Internet project based on the WordPress content management system, or the loss of important information contained in the system. In the paper, an algorithm of the software complex was developed, which includes three main blocks: data acquisition and backup creation, processing of information about the system, and the use of protection mechanisms. A software package has been developed to ensure the security of web projects based on CMS WordPress.

Key words: CMS WordPress, threats to web projects, security tools, security mechanisms, information security.