УДК 004.4/.056

МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ РАЗМЕЩЕНИЯ ПРОТОТИПА ИНТЕГРИРОВАННОЙ СРЕДЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ОТКРЫТЫЙ ДОСТУП В ТЕСТОВОМ РЕЖИМЕ

Абенова Ж.С.

АО «Национальная компания "Казахстан Гарыш Сапары"», Астана, e-mail: zhuza44@mail.ru

Коробочные системы управления взаимоотношениями между предприятиями и заказчиками для информационной поддержки при развитии высокотехнологичной наукоемкой продукции не подходят, так как подобные системы имеют стандартный набор функций и не учитывают потребности конкретных компаний. Поэтому принято решение о создании системы управления интегрированной среды информационного взаимодействия (СУ ИСИВ) для устранения проблем информационного характера в проектных организациях космической отрасли Казахстана. СУ ИСИВ будет разрабатываться с помощью Open Source-технологий, которые имеют открытый исходный код. Однако в силу того, что программы с открытым исходным кодом имеют доступность исходного кода, вопрос безопасности разработки при использовании Open Source-инструментов требует проработки методов повышения уровня безопасности при разработке и эксплуатации СУ ИСИВ. Поэтому в настоящей статье описаны графовые модели несанкционированного доступа в систему контроля доступа и аутентификации, клиентскую и административную панели СУ ИСИВ. Результаты внедрения прототипа СУ ИСИВ в тестовую эксплуатацию показали, что графовые модели помогли определить основные угрозы безопасности в системе ИСИВ и обеспечить функционирование веб-ресурса, разграничить права доступа к файлам системы ИСИВ.

Ключевые слова: open source, модель, веб-ресурс, система управления

METHODS OF IMPROVING THE SAFETY IN THE PREPARATION OF THE PLACING OF A PROTOTYPE OF AN INTEGRATED ENVIRONMENT OF INFORMATION COOPERATION IN OPEN ACCESS IN THE TEST MODE

Abenova Zh.S.

JSC «National Company "Kazakhstan Gharysh Sapary"», Astana, e-mail: zhuza44@mail.ru

The use of packaged systems relationship management between the enterprises and customers to provide information support in the development of hi-tech products are not suitable, since such systems have a standard set of functions and does not take into account the needs of specific companies. For that reason, the decision was taken on creation of control system of the integrated environment of information cooperation (CS IEIC) to resolve the issues of an informational matter in design organizations of space industry of Kazakhstan. The CS IEIC will be developed using Open Source technology that have open source code. However, due to the fact that programs with the open-source code have source code availability, the question of security developments in the use of Open Source tools requires the elaboration of methods to improve the level of safety in the CS IEIC development and operation. Thus, the present article describes graph models of unauthorized access to the access control system and authentication of CS IEIC client and administrative panel. The results of the implementation of CS IEIC prototype in test operation have shown that graph models helped to identify the main security threats in the IEIC system and maintain functionality of a web resource, to differentiate access rights to CS IEIC system files.

Keywords: open source, model, web-resource, control system

В настоящее время представлено большое количество информационных технологий, предназначенных для взаимодействия предприятий и заказчиков/потребителей между собой. Однако подобные системы не подходят для информационной поддержки при развитии высокотехнологичной наукоемкой продукции или проекта в аэрокосмической отрасли Казахстана. Во-первых, использование коробочных систем управления взаимоотношениями предприятий и клиентов представляет собой системы со стандартным набором функций и не учитывает потребности конкретных компаний, и, как правило, нет возможности доработать программный продукт «под себя». Во-вторых, ежегодная стоимость поддержки подобных систем требует больших финансовых затрат на техническое обслуживание, модернизацию и т.д. В-третьих, отсутствует информационная безопасность, так как у разработчика есть полный доступ к вашим данным. Поэтому принято решение о создании веб-ресурса, а именно создании интегрированной среды информационного взаимодействия (ИСИВ) для устранения проблем информационного характера, которые чаще всего возникают в проектных организациях. Основная цель системы управления ИСИВ (СУ ИСИВ) – это обеспечение доступа к единой платформе для получения и обмена информацией от различных источников, централизованное хранение данных, а так-

же возможность реализации ограничений на объем и параметры предоставляемой информации.

СУ ИСИВ будет разрабатываться с помощью Open Source – технологий, которые имеют открытый исходный код. Так как на сегодня одной из выраженных тенденций развития IT-технологий является использование Open Source – инструментов в проектах интеграции промышленности и других сфер народного хозяйства. К примеру, Национальное управление по воздухоплаванию и исследованию космического пространства США (NASA) начиная с 2012 г., рассматривает новую политику по использованию Open Source – технологий в своих разработках[1]. NASA публикует в открытом доступе на сервисе Github для Open Source – пользователей научно-практические разработки [2]. Применение Open Source – технологий дает большие возможности, позволяя экономить финансы и ускорять рабочие процессы, в отличие от платных программных обеспечений (ПО), которые имеют закрытый доступ к исходному коду. Однако в силу того, что программы с открытым кодом наиболее распространены и имеют доступность исходного кода, вопрос безопасности разработок при использовании ПО с открытым кодом требуют проработки методов повышения уровня безопасности при разработке и эксплуатации СУ ИСИВ. Поэтому было принято решение описать с помощью математического аппарата уязвимости системы ИСИВ, которые помогут обеспечить в будущем безопасное функционирование веб-ресурса.

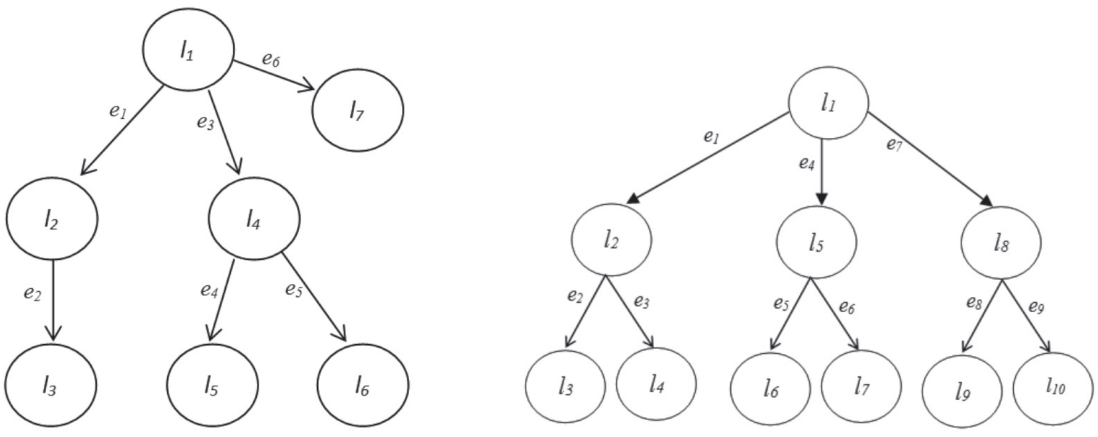
Описание математических моделей СУ ИСИВ

Прототип системы ИСИВ состоит из клиентской и административной частей [3]. Клиентская часть – это собственно веб-портал, который видит посетитель или зарегистрированный пользователь. Административная часть – это панель управления системой ИСИВ, которая отвечает за функционирование веб-ресурса ИСИВ.

Следовательно, для определения уязвимости системы, которой могут воспользоваться злоумышленники для проведения атаки, необходимо составить графовые модели для системы аутентификации и авторизации, административной и клиентской панелей [4].

Опишем графовые модели несанкционированного доступа в систему контроля доступа и аутентификации, клиентскую и административную панели СУ ИСИВ, которые состоят из трех основных множеств: $K = \{k_1, k_2, ..., k_n | n \in N\}$ – множество незащищенности системы, $A = \{a_1, a_2, ..., a_n | n \in N\}$ – множество способов атак на систему, $Z = \{z_1, z_2, z_3, ..., z_n | n \in N\}$ – множество отрицательных воздействий на ИСИВ после совершения атак.

На рис. 1, а, представлена графовая модель G_1, которая описывает способы атак на систему аутентификации и авторизации на основе множеств K, A и Z. $G_1 = \{L; E\}$, где $L = \{l_1, l_2, l_3, ..., l_n\}$, $n = \overline{1, N}$ – множество вершин графа и $E = \{e_1, e_2, e_3, ..., e_m\}$, $m = \overline{1, N}, E \subseteq L$ – множество дуг графа G_1 описывают отношения $M = K \times A \times Z$ [4].



а) *б)*

Рис. 1. а) графовая модель системы аутентификации и авторизации $G_1 = \{L; E\}$, б) графовая модель клиентской стороны $G_2 = \{L; E\}$

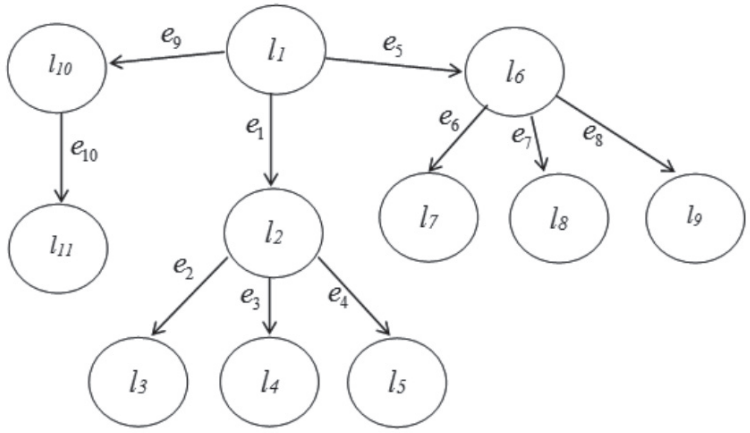


Рис. 2. Графовая модель G_3 = {L; E} административной панели СУ ИСИВ

Модель G_1 раскрывает следующие типы уязвимостей:

– дуга e_1: злоумышленник путем метода перебора имени пользователя, логина и паролей атакует систему аутентификаций и авторизаций;

– дуга e_2: злоумышленник использует функции восстановления пароля;

– дуга e_3: злоумышленник может перехватить сессию пользователя путем угадывания уникального идентификатора сессии (ID);

– дуга e_4: незавершенность сессии позволяет злоумышленнику с помощью похищенного идентификатора сессий получать доступ к файлам или совершать мошеннические действия;

– дуга e_5: «сессия-заглушка», которая периодически соединяется с сервером для предотвращения закрытия сессии;

– дуга e_6: атака направлена на получения доступа к критическим файлам сервера при слабой процедуре аутентификации.

Блок клиентской панели может также содержать уязвимости для совершения атак злоумышленниками. Для описания уязвимостей и возможных способов атак на систему рассмотрен граф $G_2 = \{L;\ E\}$, где $L = \{l_1, l_2, l_3, ..., l_n\}$, $n = \overline{1, N}$ – множество вершин графа, $E = \{e_1, e_2, e_3, ..., e_m\}$, $m = \overline{1, N}, E \subseteq L$ – множество дуг графа G_2, которые описывают отношения $M = K \times A \times Z$, касающиеся структуры клиентской панели ИСИВ. Графовая модель G_2 показана на рис. 1, б, где:

– дуга e_1: атака направлена на получение информации об особенностях реализации протокола http, значении cookies, сообщениях об ошибках, определении структуры каталогов, браузера и интерфейса веб-приложения на стороне пользователя;

– дуга e_2: данный тип атак используется для создания фальшивых веб-страниц, включающих формы входа в систему;

– дуга e_3: злоумышленник посылает серверу сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа;

– дуга e_4: атака направлена на получения доступа к файлам, директориям вне директорий веб-сервера;

– дуга e_5: злоумышленник выполняет межсайтовое выполнение сценариев;

– дуга e_6: CSRF-атака использует функции браузера, позволяющие автоматически отправлять ID с каждым GET или POST-запросом к веб-приложению;

– дуга e_7: атака направлена на использование функций веб-приложений с целью обхода механизмов разграничения доступа;

– дуга e_8: SQL-атаки направлены на веб-сервер, создающие запросы к базе данных на основе, вводимых данных пользователем;

– дуга e_9: атаки, которые позволяют злоумышленнику передать исполняемый код для выполнения его на стороне веб-сервера.

Для описания возможных способов атак и уязвимостей административной панели системы ИСИВ рассмотрен граф $G_3 = \{L;\ E\}$ $L = \{l_1, l_2, l_3, ..., l_n\}$, $n = \overline{1, N}$ – множество вершин графа, $E = \{e_1, e_2, e_3, ..., e_m\}$, $m = \overline{1, N}$ – множество дуг графа G_3, описывающие $M = K \times A \times Z$. Графовая модель G_3 показана на рис. 2:

– дуга e_1: сканирование, направленное на определение типа операционной системы (ОС) и компонентов веб-сервера;

– дуга e_2: атака направлена на получение доступа к скрытым данным или функциональным возможностям системы;

– дуга e_3: злоумышленник использует функции поиска для получения доступа к файлам за пределами корневой директории веб-ресурса;

– дуга e_4: уязвимость в виде индексации директорий может возникнуть при ошибке конфигурации;

– дуга e_5: атака направлена на нарушение функционирования и доступности веб-ресурса, на отказе в обслуживании веб-ресурса;

– дуга e_6: недостаточное противодействие автоматизации;

– дуга e_7: следующий вид атак направлен на ОС веб-сервера путем манипуляций входными данными;

– дуга e_8: злоумышленник создает запросы поверх транспортных протоколов интернета (TCP/UDP);

– дуга e_9: злоумышленник изменяет путь исполнения программы путем перезаписи данных памяти системы;

– дуга e_{10}: следующий вид атаки модифицирует путь исполнения программы методом перезаписи областей памяти с помощью функции форматирования символьных переменных.

Методы внедрения прототипа СУ ИСИВ на предприятии в открытый доступ в период тестовой эксплуатации

Первым делом были изучены совокупность взаимосвязанных мероприятий и задачи предприятия, касающиеся взаимодействия сотрудников предприятия с внешними организациями в рамках информационного сопровождения при совместной работе по перспективным проектам и при реализации внутрикорпоративных коммуникаций. В результате в прототип СУ ИСИВ перенесены следующие основные процессы деятельности предприятия:

– предоставление участникам полной и оперативной информации касательно реализации перспективных проектов;

– информирование участников проектов о новых дополненных данных по перспективным проектам;

– обсуждение проблемных вопросов при решении задач по проектам;

– формирование рабочих задач, сроков, а также назначение ответственных для решения задач.

В итоге на этапе внедрения прототипа системы ИСИВ в открытый доступ были сформулированы специфические задачи функционирования прототипа СУ ИСИВ в рамках формирования единой площадки по перспективным проектам. К ним относятся:

– создание раздела «Каталоги», который является архивом данных по проектам;

– создание панели инструментов по управлению проектами, где можно добавлять задачи и назначать ответственных и т.д.;

– создание раздела «Обсуждение» для коллективного обсуждения по решению задач.

Для управления проектами в единой площадке были созданы следующие права доступа в систему ИСИВ [5]: «Руководитель проекта», «Заместитель руководителя проекта», «Менеджер проекта», «Члены проекта», «Наблюдатели», «Администраторы».

Результаты внедрения СУ ИСИВ в период тестовой эксплуатации в открытый доступ

В период тестовой эксплуатации в открытом доступе обязательно проверяются у пользователей доступы к служебным файлам, каталогам, а также проводятся проверки защиты всех критически важных разделов административной панели от внешнего воздействия [6].

Из графовой модели G_1 можно отметить, что основные направления угроз безопасности пользователей, связаны с раскрытием пароля путем подбора пароля и получения доступа к БД пользователей. Основными способами борьбы с подбором паролей являются запрет на установку пользователям «слабых» паролей и ограничение количества попыток авторизации в единицу времени [7, 8].

Также из графовых моделей G_2, G_3 видно, что еще одной из важных уязвимостей системы является индексация системы ИСИВ [7, 8]. Так как СУ ИСИВ реализована с помощью Open Source – технологий и имеет открытый исходный код, злоумышленнику провести атаку несложно, зная версию, дату обновления расширений, а также номера установленного пакета исправлений исходных кодов. Поэтому необходимо скрыть факт использования Open Source – инструментов и устранить их отличительные черты функционирования для затруднения поиска типовых уязвимостей.

К примеру, в период тестовой эксплуатации прототипа СУ ИСИВ выявлен уязвимый файл, позволяющий провести индексацию веб-ресурса – robots.txt. Поскольку содержит список каталогов, запрещенных для индексации поисковыми машинами. Поэтому необходимо запретить прямой доступ к файлам *.xml, *.txt, *.sql, *ini, которые могут быть использованы для определения версии установленных расширений ПО.

Заключение

Тестовая эксплуатация прототипа СУ ИСИВ показала существенное сокращение времени обмена данными между сотрудни-

ками и внешними пользователями системы, наличие доступа к необходимой актуальной информации 24 часа в сутки независимо от географического положения субъекта. В ходе эксплуатации были выявлены недостатки и уязвимости, которые были устранены.

Методами, применяемыми в процессе внедрения прототипа СУ ИСИВ в тестовую эксплуатацию, являются изучение взаимодействия сотрудников предприятия с внешними организациями и внутрикорпоративных коммуникаций, а также применение математических моделей для определения уязвимостей в системе аутентификации и авторизации, административной и клиентской панелей. Модели $G_1 = \{L;\ E\}$, $G_2 = \{L; E\}$, $G_3 = \{L; E\}$ помогли определить основные направления угроз безопасности в системе ИСИВ и обеспечить безопасное функционирование веб-ресурса, разграничить права доступа к файлам системы ИСИВ в период тестовой эксплуатации.

В ходе проведенной работы были сделаны следующие основные выводы:

1. В период тестовой эксплуатации необходимо обязательное строгое разграничение прав доступа к файлам СУ ИСИВ, пока не будут устранены выявленные уязвимости.

2. В период тестовой эксплуатации обязательно запретить самостоятельную регистрацию новых пользователей. Такая процедура обеспечивает дополнительную защиту, так как СУ ИСИВ будут пользоваться только «проверенные» пользователи, имеющие непосредственное отношение к работам по проектам в данной системе.

3. Обязательно необходимо изменить стандартное имя администратора и его ID. Это обеспечит защиту критически важной учетной записи от подбора и взлома веб-ресурса роботами злоумышленника.

4. Так как прототип СУ ИСИВ еще не является финальной версией, необходимо обеспечить доступ в административную панель с определенных IP-адресов.

5. Ограничить количество ввода логина-пароля для пользователей в административную и клиентскую панели.

6. Отключить опции отладки системы и локализации, которая затруднит доступ в получении дополнительной информации о СУ ИСИВ.

7. Скрыть факт использования Open Source – инструментов и устранить их отличительные черты функционирования для затруднения поиска типовых уязвимостей в системе ИСИВ.

8. Обязательно выполнять резервное копирование, которое должно зависеть от обновления информационного содержимого веб-ресурса, вычислительных мощностей и дискового пространства. Резервное копирование желательно выполнять ночью, когда нагрузка на систему минимальна.

Результаты внедрения прототипа СУ ИСИВ в открытый доступ в период тестовой эксплуатации позволят разработать методику внедрения подобных систем в эксплуатацию, нацеленных на безопасное функционирование веб-ресурсов, разрабатываемых с помощью Open Source – инструментов.

Список литературы

1. NASA Open Source Development [Электронный ресурс]. – Режим доступа: https://www.nasa.gov/open/open-source-development.html (дата обращения: 15.11.2017).

2. Сервис для open source-пользователей научно-практических разработок от NASA. NASA Open Source Software Projects [Электронный ресурс]. – Режим доступа: https://code.nasa.gov (дата обращения: 15.11.2017).

3. Петров М.Н., Абенова Ж.С., Набиев Н.К. Исследование экспериментального прототипа системы интегрированной среды информационного взаимодействия // Вестник Сибирского гос. аэрокосмич.ун-та им. М.Ф. Решетнева. – 2017. – Т. 18, № 1. – С. 78–88.

4. Домнин Л.Н. Элементы теории графов: учеб. пособие / Л.Н. Домин. – Пенза: Изд-во Пенз.гос.ун-та, 2007. – 144 с.

5. Петров М.Н., Абенова Ж.С., Набиев Н.К. Прототипирование интегрированной среды информационного взаимодействия в космической отрасли // Решетневские чтения: материалы XX Юбилейной междун. науч-практ. конф. (Красноярск, 09–12 ноября 2016 г). – Красноярск, 2016. – Ч. 2. – С. 228–231.

6. Гольчевский Ю.В. Северин П.А. Безопасное Web-программирвоание: безопасность CMS: уч. пособие / Ю.В. Гольчевский, П.А. Северин. – Сыктывкар: Изд-во Сыктывкарского гос. ун-та, 2013. – 68 с.

7. Петров М.Н., Абенова Ж.С., Набиев Н.К. Модель интегрированной среды информационного взаимодействия // Фундаментальные исследования. – 2016. – № 10–2. – С. 322–326.

8. Open Web Application Security Project – открытый проект обеспечения безопасности веб-приложений, который классифицирует атаки и уязвимости веб-приложений [Электронный ресурс]. – Режим доступа: https://www.owasp.org/index.php/Main_Page (дата обращения: 04.10.2017).