УДК 004:51-7

МОДЕЛЬ ИНТЕГРИРОВАННОЙ СРЕДЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

[1]Петров М.Н., [2]Абенова Ж.С., [2]Набиев Н.К.

[1]Сибирский государственный аэрокосмический университет имени академика М.Ф. Решетнева, Красноярск;

[2]АО «Национальная компания «Қазақстан Ғарыш Сапары», Астана, e-mail: zhuza44@mail.ru

В настоящей статье с помощью математического аппарата описаны модель функционирования системы управления и модель пользователя интегрированной среды информационного взаимодействия (ИСИВ). ИСИВ позволит наиболее эффективно контролировать текущее состояние проекта с помощью веб-портала. Основная цель применения веб-портала – это обеспечение доступа к единой платформе для получения и обмена информации от различных источников, централизованное хранение данных, возможность поддержки использования архива проектов и накопления знаний независимо от географического положения и времени суток. Также следует отметить, что немаловажным фактором является обеспечение информационной безопасности веб-портала. Поэтому в данной работе посредством теории графов в виде множеств вершин и их дуг определены логическая взаимосвязь между пользователями и правами доступа в систему, также описаны множества уязвимостей системы и их последствия в случае успешной атаки извне. Обобщенный граф, описывающий множество средств защиты системы ИСИВ, позволит разработать рекомендации по повышению уровня безопасности функционирования системы ИСИВ.

Ключевые слова: модель, веб-приложение, веб-портал, теоретико-множественный подход, система управления, теория графов

MODEL OF AN INTEGRATED ENVIRONMENT OF INFORMATION COOPERATION

[1]Petrov M.N., [2]Abenova Zh.S., [2]Nabiev N.K.

[1]Reshetnev Siberian State Aerospace University, Krasnoyarsk;

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

In this paper there is a model of functioning of the control system and user model of an integrated environment of information cooperation (IEIC) described by a mathematical tool. IEIC will allow most effective way to control current status of the project by web-portal. The primary purpose of web-portal is to ensure access to a common platform for getting and exchanging information from multiple sources, centralized storage, the ability to support the use of archive projects and the accumulation of knowledge regardless of geographical location and time. Also, it should be noted that one of the important factors is providing an information security of web portal. Therefore in this work defined logical relationship between users and access rights in the system by the graph theory as a set of vertices and arcs, and vulnerabilities and their consequences in the event of a successful attack from the outside described by the set of system. Generalized graph that describes the set of remedies of IEIC system, allow developing recommendations to improve the level of security functioning of the IEIC system.

Keywords: model, web-application, web-portal, set-theoretical approach, control system, graph theory

В настоящее время потребность в получении качественной, объемной и своевременной информации, которой обмениваются потребители и производитель, является одним из важнейших конкурентных факторов предприятия. Поэтому создание интегрированной среды информационного взаимодействия (ИСИВ) поможет решить проблемы информационного характера, остро стоящие в высокотехнологических отраслях, например в космической. ИСИВ позволит наиболее эффективно контролировать текущее состояние проекта с помощью веб-портала, совершенствуя систему корпоративного управления [2]. Основная цель применения веб-портала – это обеспечение доступа к единой платформе для получения и обмена информации от различных источников, централизованное хранение данных, возможность поддержки использования архива проектов и накопления знаний независимо от географического положения и времени суток. Однако не следует забывать, что вопросы безопасности веб-приложений становятся все более актуальными и востребованными. Согласно статистике уязвимостей веб-приложений в 2015 году в 76% рассмотренных систем была выявлена возможность получения злоумышленником полного контроля над отдельными критически важными ресурсами [7]. Чтобы СУ ИСИВ функционировала и была неуязвима перед информационными атаками, необходимо описать СУ ИСИВ и взаимосвязь множеств незащищенности системы, множеств атак и их последствия, множеств прав пользователей веб-портала и т.д.

Для управления и контроля веб-порталом опишем с помощью математических методов систему управления ИСИВ (СУ ИСИВ) [5]. На рис. 1 представлена обобщенная модель СУ ИСИВ между внутренними и внешними пользователями, где:

– *OE* (outside environment) – вектор значений воздействия внешнего окружения;

– *X* – вектор значений связи от внешнего пользователя к СУ ИСИВ;

– *X** – вектор значений связи от СУ ИСИВ к внешнему пользователю;

– *Y* – вектор значений связи от внутреннего пользователя к СУ ИСИВ;

– *Y** – вектор значений связи от СУ ИСИВ к внутреннему пользователю;

– *Q* – вектор значений факторов, влияющих на функционирование СУ ИСИВ (например, атаки злоумышленников, сбои в канале связи и т.д.);

– *M* и *N* – векторы значений прямого взаимодействия между внешними и внутренними пользователями.

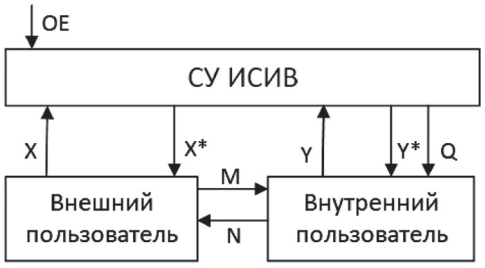

Рис. 1. Обобщенная модель СУ ИСИВ

Внешний пользователь – это субъект, заказывающий или использующий товары или услуги предприятия и имеющий возможность обмениваться информацией через веб-портал или напрямую с предприятием [1].

Внутренний пользователь – это субъект, выполняющий работы или оказывающий услуги, необходимые внешнему субъекту, при помощи находящейся в его распоряжении производственной системы. Также задает параметры функционирования СУ ИСИВ и обменивается информацией с клиентами, в том числе потенциальными [1].

СУ ИСИВ состоит из клиентской и административной части. Клиентская часть – это собственно веб-портал, который видит посетитель или зарегистрированный пользователь. Отображение информации, доступ к персональным данным в клиентской части происходит за счет шаблона и модулей, которые выводятся в специально заранее отведенных позициях шаблона.

Административная часть – это панель управления веб-порталом, которая выполняет следующие действия: добавление, редактирование и удаление контента, анализ действий посетителей, модерация сообщений, обеспечение безопасности веб-портала и т.д. В административную панель входят автономный блок управления (АБУ) и блок предварительной подготовки параметров (БППП) веб-портала [1].

БППП отвечает за функционирование веб-портала и состоит из различных расширений для формирования автономного блока управления веб-порталом.

В свою очередь, АБУ веб-порталом предназначен для поиска информации, регистрации, авторизации, экспорта и импорта информации с учетом прав доступа пользователей без участия БППП веб-портала.

Более детально структура СУ ИСИВ представлена на рис. 2, где:

– *H* – вектор значений связи от АБУ к веб-порталу;

– *H*″ – вектор обратной связи от веб-портала к АБУ;

– *P* – вектор связи от БППП к АБУ;

– *P** – вектор обратной связи от АБУ к БППП.

Пусть множество {*X*, *X**, *Q*, *Y*} описывает взаимодействие клиента с предприятием через СУ ИСИВ, а множество {*M*, *N*} описывает взаимодействие клиента с предприятием прямой связью. Следовательно, множество {*X*, *X**, *Q*, *Y*} заменяет или дополняет {*M*, *N*}.

Сотрудник компании с помощью вектора *Y* задает параметры функционирования веб-портала, которые проходят проверку на наличие ошибок в структуре документа (проверка синтаксических ошибок, вложенности тэгов и др. критерии) в БППП и преобразуются в вектор P для передачи полученных данных АБУ. Далее АБУ формирует вектор H для управления и контроля за веб-порталом. В случае обратной связи вектор *Y** используется для проверки входных данных от БППП, которые вызваны вектором P* (обнаружение уязвимостей и сбоев системы, веб-атаки и т.п.). Вектор *Q* обуславливает такие параметры, как количество посещаемости веб-портала, определение наиболее востребованных продукций/услуг, анализ сетевого трафика и поисковой оптимизации.

Также следует отметить, что с помощью вектора *Q* внутренние пользователи обмениваются информацией через веб-портал

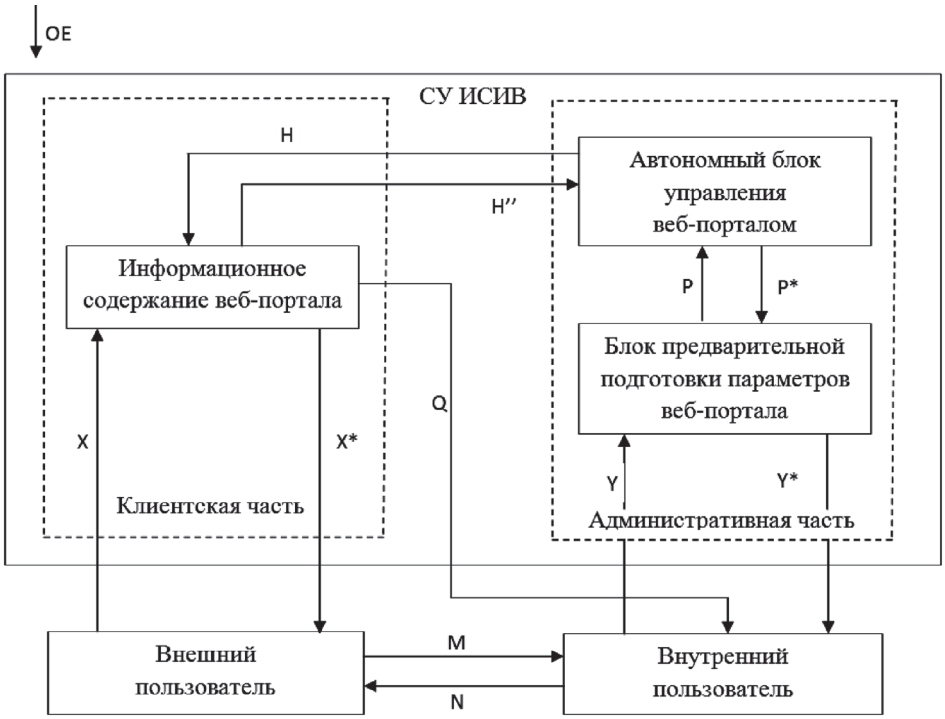

Рис. 2. Детальная структура СУ ИСИВ

с внешними пользователями. В данном случае, после того как компания получила информацию с помощью вектора Q (то есть $X \to Q$) от внешнего пользователя, сотрудник компании передает ответ напрямую через вектор M или через веб-портал ($Y \to P \to H \to X$*).

Используя теоретико-множественный подход, можно описать модель пользователя СУ ИСИВ [4, 5].

Пусть $IU = \{iu_1, iu_2, iu_3, \ldots, iu_n\}$ – множество внутренних пользователей (internal users) административной панели ИСИВ; $OU = \{ou_1, ou_2, ou_3, \ldots, ou_m\}$ – множество внешних пользователей (outside users) клиентской части ИСИВ.

Также необходимо отметить, что пользователь не прошедший аутентификацию также может просматривать информационный материал и обращаться через обратную связь к сотрудникам систему ИСИВ. Тогда множество пользователей ИСИВ будут описаны следующей системой:

где

– ID = {IDn, IDm} – множество идентификаторов доступа в систему, где IDn = {idn_1, $idn_{2,\ldots,}$ idn_n} – множество идентификаторов доступа в административную панель ИСИВ, IDm = {idm_1, $idm_{2,\ldots,}$ idm_m} – множество идентификаторов доступа в клиентскую часть ИСИВ;

– PD – персональные данные пользователей;

– INS = {INSn, INSm} – множество инструкций, определяющих ограничение доступа и роль пользователя ИСИВ, где INSn = {$insn_{1,}$ $insn_2$, …, $insn_n$} описывает инструкции для административной части СУ ИСИВ, INSm = {$insm_{1,}$ $insm_2$, …, $insm_m$} описывает инструкции для клиентской части ИСИВ;

– P – параметр, определяющий текущее состояние пользователя (например, блокирован пользователь или нет).

Система (*) показывает, что внутренние пользователи должны иметь уникальные персональные данные и идентификатор

$$USER = \begin{cases} iu_n = \{idn_n, PD, insn_n, P | idn_n \in ID, insn_n \in INSn, \\ \qquad P \in \{True, False\}, PD = \varnothing, idn_n = \varnothing\}; \\ \forall ou_m = \{idm_m, PD, insm_m, P | idm_m \in ID, insm_m \in INSm, \\ \qquad P \in \{True, False\}, \forall in_n \neq ou_m\}, \end{cases} \quad (*)$$

доступа в СУ ИСИВ. В целях безопасности системы у каждого пользователя будет свой уровень доступа и полномочия в СУ ИСИВ, которые описываются правилами INS. Внешний пользователь делится на зарегистрированного пользователя и посетителя клиентской части СУ ИСИВ. Поэтому для внешнего пользователя не обязательно иметь уникальные персональные данные и идентификатор доступа в СУ ИСИВ.

Согласно рис. 2, в целях безопасности и удобства работы СУ ИСИВ разделена на клиентскую и административную части. Управление клиентской частью происходит через административную панель, что обеспечивает дополнительную защиту для атаки извне. Тем не менее для проведения атаки внешним злоумышленником на веб-портал, достаточно определить уязвимость системы. Поэтому для защиты информационного ресурса ИСИВ опишем модель информационной атаки на систему из трех основных множеств: $K = \{k_1, k_2, k_3, ..., k_n | n \in N\}$ – множество незащищенностей системы, $A = \{a_1, a_2, a_3, ..., a_n | n \in N\}$ – 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. Тогда взаимное отношение трех множеств можно описать с помощью тернарного отношения $M = K \times A \times Z$, которое интерпретируется следующим образом: атака, реализуемая множеством способов A, направленная на веб-портал злоумышленником, использующим множество незащищенностей K, приводит к множеству отрицательных воздействий на систему из множества Z.

Для бесперебойного функционирования веб-портала опишем множество средств защиты $F = \{f_1, f_2, f_3, ..., f_n | n \in N\}$ для системы ИСИВ в виде обобщенного графа $G = \{L; E\}$, где $L = \{l_1, l_2, l_3, l_4, l_5\}$ – множество вершин графа, $E = \{e_1, e_2, e_3, e_4\}$, $E \subseteq L$ – множество дуг графа. Каждой дуге графа ставится в соответствие тернарное отношение $M = K \times A \times Z$. В каждую вершину графа G могут входить одновременно несколько дуг, которые приводят к одинаковым последствиям [3].

Введем следующие обозначения для описания графа G. К множеству F относятся организационные и технические средства защиты системы ИСИВ. Множество информационных ресурсов клиентской и административной частей веб-портала обозначим как множество $D = \{d_1, d_2, d_3, ..., d_n | n \in N\}$, множество аппаратного обеспечения – как множество $H = \{h_1, h_2, h_3, ..., h_n | n \in N\}$, множество программного обеспечения как $S = \{s_1, s_2, s_3, ..., s_n | n \in N\}$, множество пользователей ИСИВ как U, множество инструкций, определяющих ограничение доступа и роль пользователя ИСИВ, как множество INS.

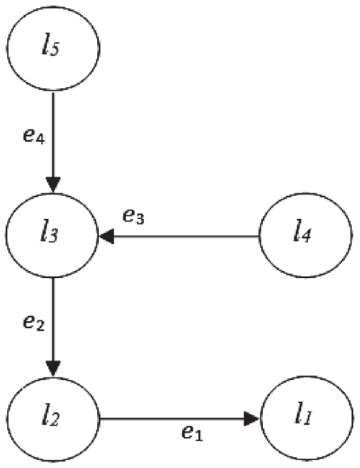

Рис. 3. Обобщенный граф G = {L; E}

Обобщенный граф G, изображенный на рис. 3, представляет собой модель взаимоотношений множеств *F, D, S, H, M, USER, INS* друг с другом. Первым делом формируется множество H в вершине l_1 для хранения и передачи информации множества D, к нему относятся веб-серверы, сетевое оборудование и т.д. Далее в вершине l_2 формируется множество S – множество прикладных программных приложений, предназначенных для выполнения определенных задач и рассчитанных на взаимодействие с пользователями системы ИСИВ. Дуга $e_1 = s_n \times h_n$ задает взаимосвязь между множествами S и H (где $s_n \in S$, $h_n \in H$), как прикладное программное приложение s_n, установленное на аппаратном обеспечении h_n. В вершине l_3 расположено множество D, куда входят служебные данные, файловые ресурсы, документы пользователей ИСИВ. Дуга e_2 с помощью тернарного отношения $d_n \times s_n \times h_n$ описывает взаимоотношения информационных ресурсов d_n, которые обрабатываются элементами s_n, установленных на h_n. Вершина l_4 определяет множество категорий пользователей веб-портала *USER*, а также множество INS, описывающее права доступа для категорий пользователей в клиентскую и административную части СУ ИСИВ. Дуга e_3 формирует взаимосвязь трех множеств *USER, D, INS*, как *USER×D×INS* и интерпретируется следующим образом: множество пользователей СУ ИСИВ *USER*

имеют доступ к множеству ресурсов веб-портала *D,* регламентирующие множеством правил INS, ограничивающие права доступа пользователей в целях безопасности. Вершина графа l_5 – множество методов защиты *F* обеспечивает защиту ресурсов *D* с учетом взаимодействия множеств *K*, *A*, *Z*. Тернарное отношение M определяет оценку ущерба, который может быть нанесен в случае успешной атаки на информационные ресурсы веб-портала. Дуга e_4 описывает множество методов защиты F информационного ресурса *D* с учетом множества M $(e_4 = f_n \times d_n \times \mathrm{M}, f_n \in F | \; n = \overline{1,N})$.

С помощью графовой модели $G = \{L; E\}$ можно оценить значения риска с учетом определения уровня ущерба в случае успешной атаки на систему ИСИВ посредством описания множеств незащищенностей системы, способов атак на систему и множеств отрицательных воздействий на систему [5].

Заключение

Показана модель СУ ИСИВ, которая имеет большое значение, заключающаяся в разработке приложений для структурирования контента и представления информации из различных источников в одном месте. С помощью данной модели будет реализован веб-портал для проектных организаций в сфере космической деятельности. Для эффективной защиты СУ ИСИВ описана с помощью теории графов логическая взаимосвязь между множествами уязвимостей, информационной атаки извне и их последствия на систему ИСИВ. Уравнение (*) и граф *G* помогут описать права доступа к ресурсам веб-портала для разных категорий пользователей, также позволить учесть взаимосвязь уязвимостей системы при нарушении функционирования СУ ИСИВ или атаки и их возможные последствия. В дальнейшем обобщенный граф $G = \{L; E\}$ позволит разработать рекомендации по повышению уровня безопасного функционирования для клиентской и административной частей системы веб-портала.

Список литературы

1. Воройский Ф.С. Информатика. Энциклопедический систематизированный словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. – М.: Физматлит, 2006. – 945 с.

2. Деятельность и направление компании АО «Национальная компания «Қазақстан Ғарыш Сапары». – Режим доступа: http://gharysh.kz/about/activity/ (дата обращения: 07.09.2016 г.).

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

4. Киреенко С.Г., Гриншпон И.Э. Элементы теории множеств: учебное пособие. – Томск, 2003. – 42 с.

5. Краснянский М.Н., Карпушкин С.В., Остроух А.В. Проектирование информационных систем управления документооборотом научно-образовательных учреждений: монография. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2015. – 216 с.

6. Меньков А.В., Острейковский В.А. Теоретические основы автоматизированного управления. – М.: Изд-во Оникс, 2005. – 640 с.

7. Статистика уязвимостей корпоративных информационных систем. – Positive Technologies, 2016. – Режим доступа: http://www.ptsecurity.ru/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf (дата обращения: 20.07.2016 г.).

References

1. Voroisky F.S. Informatika. Entsiklopedicheskiy sistematizirovannyy slovar-spravochnik: vvedeniye v sovremennyye informatsionnyye i telekommunikatsionnyye tekhnologii v terminakh i faktakh. M.: Fizmatlit, 2006. 945p.

2. Activities and direction of the Joint-Stock Company «National Company «Kazakhstan Gharysh Sapary». Rezhim dostupa: http://gharysh.kz/about/activity/ (data obrashcheniya: 07.09.2016 g.).

3. Domnin l.N. Elementy teorii grafov: uchebnoye posobiye. Penza: Izd-vo Penz.gos.un-ta, 2007. 144 p.

4. Kireyenko S.G., Grinshpon I.E. Elementy teorii mnozhestv (uchebnoye posobiye). Tomsk, 2003. 42 p.

5. Krasnyanskiy M.N., Karpushkin S.V., Ostroukh A.V. Proyektirovaniye informatsionnykh sistem upravleniya dokumentooborotom nauchno-obrazovatelnykh uchrezhdeniy: monografiya. Tambov: izd-vo FGBOU VPO «TGTU», 2015. 216 p.

6. Menkov A.V., Ostreykovskiy V.A. Teoreticheskiye osnovy avtomatizirovannogo upravleniya. M.: Izd-vo Oniks, 2005. 640 p.

7. Statistika uyazvimostey korporativnykh informatsionnykh sistem. Positive Technologies, 2016. Rezhim dostupa: http://www.ptsecurity.ru/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf (data obrashcheniya: 20.07.2016 g.).