$f : U \times E \times C \to 2^R$, описывающая права доступа учетной записи $u \in U$ к сущности $e \in E$ при инициализации сессии с контейнера $c \in C$. Тогда вектором доступа учетной записи u к сущности e будем называть набор пар $(c_1, f(u, e, c_1)), \ldots, (c_n, f(u, e, c_n))$.

5. В соответствии с этим определением к правилам преобразования состояний добавляется правило $create\_session\_remote(s, u, c, e)$, описывающее создание сессии удаленного доступа субъектом $s \in S$ с правами доступа учетной записи $u \in U$ к сущности $e \in E$ и назначение субъекту s в рамках этой сессии прав доступа учетной записи u в зависимости от ребра (u, e, v) в графе доступа и контейнера c, с которого порождена сессия субъектом s.

С использованим этих расширений языка ДП-моделей базовая СУД ДП-модель может быть разработана по стандартной схеме построения ДП-моделей в [1].

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011.

УДК 004.75

МОДЕЛЬ БЕЗОПАСНОСТИ КРОСС-ПЛАТФОРМЕННЫХ ВЕБ-СЕРВИСОВ ПОДДЕРЖКИ МУНИЦИПАЛЬНЫХ ЗАКУПОК

Д. Д. Кононов, С. В. Исаев

Целью работы является создание на основе RBAC [1] модели безопасности, учитывающей специфику веб-приложений. На базе этой модели разработаны программные средства для решения задач муниципального заказа администрации г. Красноярска, в том числе для проведения открытых электронных аукционов. Юридическая значимость действий пользователей обеспечивается использованием электронной цифровой подписи. Работа выполняется в рамках развития Автоматизированной системы проведения муниципальных заказов (АСП МЗ). Определяющими документами являются федеральные законы №1, 94 и 149.

В результате анализа предметной области была выбрана модель RBAC. В модель были внесены изменения, учитывающие особенности веб-приложений. К существующим понятиям «субъект» (subject), «роль» (role), «разрешение» (permission), «сессия» (session) были добавлены «токен» (token) и «запрос» (request).

Определение 1. *Токен* — набор атрибутов субъекта, позволяющих осуществить его аутентификацию в системе. Токеном является пара (имя, пароль) либо пара (сертификат ЭЦП, закрытый ключ ЭЦП).

Определение 2. *Запрос* — набор информации, пересылаемой клиентом серверу по протоколу HTTP. Запрос содержит набор заголовков, уникальный идентификатор ресурса, набор параметров имя/значение и тело запроса.

Запрос принадлежит сессии, в рамках одной сессии может выполняться несколько запросов. Понятия «запрос» и «разрешение» связаны отношением «многие-ко-многим». На множестве запросов вводится отношение включения.

Определение 3. Запрос A *включает* запрос B, если путь уникального идентификатора ресурса запроса A содержит путь уникального идентификатора ресурса запроса B с начальной позиции строки.

Например, запрос «/library/book» включает запрос «/library». Полученная модель отражает предметную область и позволяет эффективно разграничивать доступ в веб-системах.

В работе D. F. Ferraiolo et al. [2] рассматриваются вопросы применения модели RBAC для веб-приложений. В первом случае предлагается хранить идентифицирующую и служебную информацию (в том числе пароль), подписанную сервером, на стороне клиента в виде `cookies`. Данный метод не учитывает истечения срока действия и возможности компрометации сертификата сервера. Во втором случае используются атрибуты сертификата X.509 для хранения политик безопасности. Описанный подход имеет следующие недостатки. Во-первых, жестко указаны роли и разрешения, что не позволяет добавлять новые полномочия для субъекта без замены сертификата. Во-вторых, не учитывается ситуация, когда система работает с сертификатами разных удостоверяющих центров, имеющих собственные политики безопасности.

В настоящей работе предлагается комбинированный подход. Предварительная аутентификация производится с помощью имени пользователя и пароля, что дает субъекту доступ на чтение к закрытой части системы. Дальнейшие действия субъекта по добавлению, модификации и удалению информации подтверждаются электронной цифровой подписью, что обеспечивает юридическую значимость и аутентичность информации. На стороне клиента в `cookies` хранится только идентификатор сессии, который становится недействительным после ее завершения. Сертификат ЭЦП содержит только стандартные атрибуты X.509. Информация о политиках безопасности хранится на сервере системы и доступна для редактирования администратором. Данный подход позволяет использовать произвольный удостоверяющий центр для выдачи сертификатов пользователям и гибко настраивать права доступа.

Особое внимание уделялось возможности кросс-платформенного функционирования системы. В настоящий момент система может функционировать на платформах Windows, Linux, FreeBSD. В работе используется криптопровайдер КриптоПро CSP, который обеспечивает работу стандартов ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ 28147-89.

Реализованные веб-сервисы обеспечивают защиту публикуемых данных, простоту и удобство работы специалистов муниципального заказа, оперативность размещения информации на сайте, а также защиту от несанкционированного использования. Система успешно эксплуатируется более четырех лет. За период 2009–2010 гг. с использованием системы было проведено 354 электронных аукциона на общую сумму 238 660 934 руб., экономия бюджета составила 42 443 682 руб. Имеются свидетельства о регистрации программного обеспечения [3, 4].

ЛИТЕРАТУРА

1. *Sandhu R., Coyne E. J., Feinstein H. L., and Youman C. E.* Role-Based Access Control Models // IEEE Computer (IEEE Press). 1996. V. 29. No. 2. P. 38–47.
2. *Ferraiolo D. F., Kuhn D. R., and Chandramouli R.* Role-Based Access Control. Norwood, USA: Artech House, 2003.
3. *Ноженкова Л. Ф., Исаев С. В., Кононов Д. Д. и др.* Система проведения электронных интернет-аукционов // Свидетельство об официальной регистрации в Реестре программ для ЭВМ № 2009612095 от 24.04.2009. (Федеральная служба по интеллектуальной собственности, патентам и товарным знакам). 2009.
4. *Ноженкова Л. Ф., Исаев С. В., Кононов Д. Д., Исаева О. С.* Интернет-система поддержки муниципального заказа // Свидетельство об официальной регистрации в Реестре про-

грамм для ЭВМ № 2009612093 от 24.04.2009. (Федеральная служба по интеллектуальной собственности, патентам и товарным знакам). 2009.

УДК 004.056

РАЗРАБОТКА КОМПЛЕКСНОЙ ОБУЧАЕМОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ ФИШИНГОВЫХ АТАК[1]

А. В. Милошенко, Т. М. Соловьёв, Р. И. Черняк, М. В. Шумская

В настоящее время многие услуги стали доступны через Интернет. Финансовый сектор также не стал исключением. Появились различные платежные системы, интернет-кошельки и терминалы оплаты. Безопасность платежей внутри данных систем обеспечивается множеством высокотехнологичных решений, таких, как сертификаты безопасности, криптографические протоколы и др. Однако все эти решения оказываются неэффективными при применении злоумышленниками методов социальной инженерии, использующих слабости человеческого фактора.

Одним из наиболее распространенных видов такого рода атак сегодня является фишинг [1]. Фишинг (от англ. *phishing*, *password fishing* — выуживание паролей) — это вид сетевого мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей обманным путём. Популярной методикой фишинга является создание поддельных веб-сайтов, внешне неотличимых от подлинных. Ущерб от преступлений, связанных с фишингом, только за 2010 г. исчисляется миллиардами долларов США. При этом, согласно статистике, количество фишинговых атак с каждым годом увеличивается примерно в полтора раза.

Остановить бурное развитие такого рода преступлений можно посредством создания комплексных систем защиты от фишинговых атак. Поскольку арсенал фишеров растёт стремительными темпами, необходимо обеспечивать обучаемость таких систем. В настоящее время не существует подобного рода решений, о чем красноречиво повествует статистика, поэтому создание комплексной обучаемой высокоэффективной системы защиты от фишинговых атак является интересным и актуальным направлением. Создание такой системы предполагает предварительное изучение характерных признаков фишинговых ресурсов и разработку на их основе методов оценивания степени опасности информационного ресурса и определения потенциально опасных ресурсов. Этому, в основном, и посвящена данная работа. На основе полученных результатов предложена схема функционирования системы защиты от фишинговых атак.

Характерные признаки фишинговых ресурсов

Анализ существующих фишинговых ресурсов позволил составить перечень их характерных признаков.

1. *Сходство графического контента*

Основная задача злоумышленников при проведении фишинговой атаки — заставить пользователя поверить в аутентичность фишингового ресурса. Наиболее простым способом сделать это является заимствование графического оформления у атакуемого сайта.

Несмотря на большое количество исследований, задача определения степени сходства изображений в настоящее время не имеет универсального и эффективного решения. Объясняется это в первую очередь тем, что понятие похожести двух изображе-

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).