Защита электронной информации от злоумышленников и… незрячих пользователей!

Protection of Electronic Information from Intruders and… Blind Users!

Захист електронної інформації від злодіїв і … незрячих користувачів!

Елфимова Г. С.
Российская государственная библиотека для слепых, Москва, Россия

Galina S. Elfimova
Russian State Library for the Blind, Moscow, Russia

Єлфимова Г. С.
Російська державна бібліотека для сліпих, Москва, Росія

Представлены методы защиты электронных ресурсов: криптография, паролевый доступ и включение в графическую оболочку. Рассмотрено их влияние на доступность информации незрячим пользователям. Приведены примеры решения проблемы из отечественной и зарубежной практики.

The following methods of electronic resources protection are described: Cryptography, password access and graphic wrapping. Their influence on the accessibility to blind users is discussed. The solutions realized in the national and foreign practice are presented.

Представлені методи захисту електронних ресурсів: криптографія, доступ за паролем і включення до графічної оболонки. Розглянуто їх вплив на доступність інформації для сліпих користувачів. Наведені приклади рішення проблеми з вітчизняної та зарубіжної практики.

Современная концепция создания компьютерных систем, в том числе и библиотечных, предполагает комплексное использование различных программных средств. Например, типовая система автоматизированного документооборота состоит из операционной среды, программных средств управления базами данных, телекоммуникационных программ, текстовых редакторов, ***антивирусных мониторов, средств криптографической защиты данных, а также средств аутентификации и идентификации пользователей.*** Главным условием функционирования такой компьютерной системы является обеспечение защиты от вмешательства в процесс обработки тех программ, присутствие которых в компьютерной системе не желательно (компьютерные вирусы, программные закладки и др.).

В наше далекое от альтруизма время первой и основной целью взлома компьютерной системы является получение прибыли. Казалось бы, на первый взгляд, понятия «библиотечный сайт» и «прибыль» друг с другом совершенно не связаны. Но если задуматься, то есть и в структуре сайтов библиотек такие элементы, которые могут быть использованы в коммерческой деятельности — электронные библиотеки и каталоги, а также особые базы данных такие, как например, библиотеки периодических изданий. Ярким примером которых является веб-портал Anderslezen. nl, созданный Федерацией библиотек для слепых Нидерландов. Основные средства защиты этого портала от несанкционированного вторжения — паролевый доступ, кодировка файлов (криптографическая защита) и, соответственно, специальные программы дешифровки и воспроизведения, распространяемые по подписке зарегистрированным пользователям.

Как видно из этого примера, проблемами защиты информации одинаково интересуются как зрячие, так и слепые люди, а также организации, вовлеченные в библиотечно-информационное обслуживание инвалидов по зрению. Формат представления электронных ресурсов уравнивает возможности зрячих и слепых пользователей, последним только нужно специализированное оборудование и то, чтобы разработчики программного обеспечения, в том числе выполняющего защитные функции, помнили о том, что работу свою они должны выполнять с учетом возможностей программ адаптивного доступа.

Первым по времени возникновения и, возможно, наиболее надежным на современном этапе считается криптографический метод защиты компьютерной информации. В простейшем варианте он состоит в преобразовании с помощью специального кода и алгоритма шифрования открытого текста в шифротекст, смысл которого непонятен для посторонних. Процесс обратного преобразования — расшифровывание.

Различные криптографические алгоритмы имеют различную степень надежности, так называемую стойкость алгоритма шифрования или стойкость шифра. Стойкость зависит от того, насколько легко криптоаналитик может взломать шифр. Если при этом стоимость затрат превышает ценность полученной в результате информации, то владельцу этого шифра, возможно, и беспокоиться не о чем. Предполагается, что внимание «криптоаналитика» привлечет скорее информация, исходящая от банков, военных организаций или секрет-

ных НИИ, чем, например, электронная переписка частных лиц или базы данных библиотек, предоставляющих этим лицам информационные услуги.

В настоящее время аспекты компьютерной криптографии широко и подробно освещаются на страницах книг и периодических изданий. Овладеть ими может любой. Во всем этом есть только одно «но», на котором мы закончим рассмотрение этого метода защиты информации без анализа доступности его незрячим пользователям — указом № 334 от 3 апреля 1995 года Президент России запретил «деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, […] предоставлением услуг в области шифрования информации» без государственных лицензий.

Возможно, в более поздних исследованиях мы вернемся к этому вопросу, а сейчас рассмотрим несколько наиболее широко применяемых в Сети методов, не подпадающих под столь строгий контроль правительственных ведомств.

Основным средством защиты компьютерных сетей от несанкционированного проникновения является ***система парольной защиты***. В этом случае перед началом сеанса работы пользователь обязан зарегистрироваться в системе, сообщив ей свое имя и пароль. Имя требуется для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации. Информация, введенная пользователем в диалоговом режиме, сравнивается с той, что имеется в распоряжении системы. Если проверка дает положительный результат, то пользователю становятся доступными все ресурсы системы, связанные с его именем.

Часто на сайтах, защищенных парольным доступом, используется ***функция блокировки***: количество подряд идущих повторных вводов конкретного пользовательского имени и соответствующего ему пароля ограничивается двумя-тремя и в случае, если это число превышено, вход в систему с использованием данного имени блокируется в течение фиксированного периода времени или до вмешательства системного администратора. Система, аналогичная введению PIN в мобильных телефонах.

При этом, если вероятность введения неправильного пароля самим легальным пользователем достаточна велика (заедание клавиш, не переключение регистра RU/EN, опечатка и многие другие причины), то в случае, когда речь идет о незрячем пользователе, вероятность эта становится еще выше. В свете этого, а также того, что вряд ли кому-либо из профессиональных компьютерных взломщиков придет в голову подбирать пароль «методом тыка» из сотен или тысяч вариантов, функция блокировки в первую очередь «защищает» систему от самого пользователя. При этом даже эксперты по защите электронной информации признают, что «скорость такого подбора пароля будет чрезвычайно низкой, и гораздо более эффективным является другой метод взлома парольной защиты операционной системы, при котором атаке подвергается системный файл, содержащий информацию о ее легальных пользователях и паролях».

Помимо рассмотренного выше есть еще, по крайней мере, один вариант блокировки системы, который используется, например, на компьютерах публичного доступа в библиотеках Голландии: отключение системы, если правильный пароль не введен за отведенный для этого период времени (очень короткий, кстати говоря — до 30 секунд). Возможно, это оправдано с точки зрения защиты информации о предыдущем пользователе, но в случае, если за компьютер садится инвалид по зрению и работает с программой чтения с экрана, этого времени не хватает на то, чтобы ознакомиться со структурой страницы, прочитать представленную на ней информацию и со своей стороны ввести необходимые данные. Так может быть не стоит перестраховываться и вводить функции блокировки? Или, по крайней мере, снять их на библиотечных компьютерах?

Еще один элемент, часто встречающийся на сайтах, защищенных парольным доступом, — ***защита от автоматических регистраций***. В рамках этой статьи мы не будем обсуждать степень необходимости и эффективности использования этого метода на веб-сайтах. Рассмотрим только несколько примеров применения его в электронных почтовых ящиках.

Приведенная выше иллюстрация говорит сама за себя. На сайт почтовой службы выходит незрячий пользователь, он хочет зарегистрироваться, и ему предлагается: «введите шестизначное число, которое **вы видите** на картинке». Здесь необходимо оговориться, что программа чтения с экрана, в частности, наиболее распространенный в России Jaws, не распознает текст, включенный в графическую оболочку. Но далее, после окна ввода, следует ссылка **«Если вы не видите число»**. Предполагается, что, перейдя по этой ссылке в какой-то другой раздел, незрячий пользователь получит решение проблемы восприятия графического объекта. Вместо этого всплывает текст: «Ввод числа необходим для защиты от автоматических регистраций. ***Если Вы не видите картинку с числом, проверьте, включен ли в Вашем браузере показ картинок***. После включения показа картинок Вы можете вернуться к регистрации. ***Если Вы сомневаетесь в том, что за число изображено на картинке, попробуйте ввести самое похожее***. Если угадать не получится, Вы сможете повторить попытку с другой комбинацией цифр». Выглядит, как насмешка над незрячим человеком!

Все большее число сайтов переходит на ***новый метод защиты данных — представление текста в виде графического объекта***. Предполагается, что работающий с текстом пользователь при наличии соответствующих программных средств может скопировать текст и с помощью редактора перевести в требуемый формат. В основе этого метода верификации лежит представление о том, что пользователь способен вручную выполнить задачу, не выполнимую для компьютерной программы — выделить текст из графического объекта.

Но, как мы уже говорили, проблема заключается в том, что программы экранного доступа, используемые незрячими, не дают им возможности считывать текст, заключенный в графическую оболочку. Таким образом, слепым людям оказывается частично или полностью недоступной информация, представленная данным способом.

Несколько примеров из практики. Страница американской компании PayPal, предоставляет своим пользователям возможность осуществления денежных переводов через Интернет. В справочном разделе сайта указывается, что на странице использована схема графической верификации и предлагается скопировать требуемый текст в программу-редактор. Там же оговаривается, что в случае не способности пользователя к визуальному восприятию текста, ему предоставляется возможность перейти на «ссылку доступности». После использования этой функции текст воспроизводится в виде аудио файла неудовлетворительного качества и без возможности повтора. Тем не менее, это уже существенный прогресс по сравнению с примером почтовой службы.

Корпорация America Online (AOL) выбрала метод защиты данных, во многом похожий на систему защиты PayPal. При этом специалисты America Online попытались решить проблему обеспечения незрячим пользователям доступа к информации, включенной в графическую оболочку. В скобках необходимо заметить, что в ноябре 1999 года Национальная федерация слепых США (NFB) предъявила компании America On-line иск с требованием сделать компьютерную продукцию компании доступной незрячим пользователям. К этому времени услугами AOL пользовалось уже более 19 млн. человек во всем мире. Ее система представления информации быстро завоевала статус стандарта для компьютерной промышленности, но этот стандарт совершенно не подходил для слепых. В течение нескольких лет между AOL и NFB велись переговоры, и решение о прекращении судебного разбирательства было принято только после того, как America On-line обязалась привести все свои разработки в соответствие с рекомендациями NFB. С этого времени федерация слепых получает от компании регулярные отчеты о проводимой работе. Не удивительно, что и новая система защиты данных AOL была вынесена на обсуждение.

Метод, использованный на сайте PayPal, по техническим причинам применить было невозможно. Специалисты из компьютерного центра Национальной федерации слепых США предложили метод скрытого представления текста, не воспроизводимого на экране, но читаемого программой экранного доступа.

Служба WhoIs Network Solutions позволяет пользователям получать информацию об Интернет-доменах, таких как nfb.org, npr.org, microsoft.com и любых других, зарегистрированных в Network Solutions. Предполагается, что эта услуга должна быть бесплатно доступна всем. Но инвалиды по зрению пользоваться этой услугой не могут.

Каждый раз, запрашивая домен, включенный в службу WhoIs, пользователь сталкивается с необходимостью выделять текст из графической оболочки. Учитывая охват этой сетевой службы, речь идет уже не о трудностях однократного обращения к ресурсу, а о лишении незрячих доступа к обширным значимым по содержанию базам данных. И в отличие от America Online служба Network Solutions никогда не выносила этот вопрос на обсуждение.

На самом деле проблема заключается не в нежелании службы WhoIs обсуждать вопросы доступности Интернет-ресурсов незрячим, а в том, что система графической защиты успешно прошла этап проверки и ее начинает использовать все большее число сайтов. Таким образом, если не будет найдено альтернативное решение, большая часть Интернет окажется недоступной инвалидам по зрению.

Западные и отечественные эксперты единодушно утверждают, что на данном этапе они нет готового технического решения проблемы, но уже накоплен достаточно большой опыт и знания о том, как слепой человек работает с компьютером и на основе этого, возможно, со временем удастся решить рассмотренные в статье проблемы.