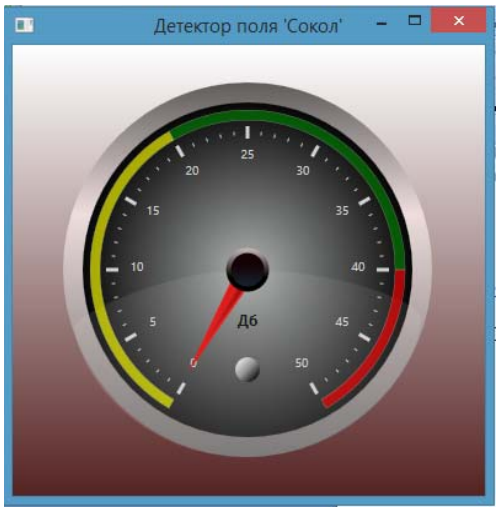

Рис. 4. Главное окно программы

Чтобы добиться положительных результатов, необходимо регулярно проводить проверку помещений на наличие радиопередающих закладных устройств, особенно тех, где проводятся совещания и важные переговоры.

Работа выполнена при поддержке Фонда содействия развитию малых форм предприятий в научно-технической сфере в рамках программы УМНИК.

Литература

1. Торокин, А. А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. — М.: Гелиос АРВ, 2005. — 960 с.

2. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации.- М.: МО РФ, 1998. - 224 с.

Н.И. Биркун, Ж.Ж. Тураров, А.О. Зозуля

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ УЯЗВИМОСТИ СИСТЕМЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ТЕХНОЛОГИИ CAPTCHA

(Академия ФСО России)

На сегодняшний день CAPTCHA является стандартным методом защиты различных сайтов от "спама", вредоносных программ или автоматической регистрации. Существует большое количество различных реализаций CAPTCHA. Наиболее распространенные – это системы предлагающие пользователю определить последовательность искаженных символов (букв и цифр) и ввести их в указанное поле.

С точки зрения применения в компьютерных системах CAPTCHA-методы можно отнести как к процедуре авторизации, так и к процедуре аутентификации. Это связано с тем, что в большинстве случаев, технология CAPTCHA применяется как сопутствующая процедуре аутентификации с по-

мощью парольной защиты. Современные методы повышения защищенности CAPTCHA предлагаются в основном специалистами в области технологий "компьютерного зрения", распознавания образов или анализа документов. Однако, также применяются подходы, основывающиеся на опыте проектирования и создания систем информационной безопасности.

В основе методики оценки уязвимости обозначенной системы, лежит анализ алгоритма генерации и процесса модификации исходного CAPTCHA-образа с применением множества фильтров обработки графических изображений с целью сведения к минимуму или полного устранения факторов искажений, внесенных генератором CAPTCHA-образов. В результате применения этого множества фильтров, исходный CAPTCHA-образ преобразуется в множество тестовых CAPTCHA-образов $\{CAPTCHA^{m}_{тст}\}$, каждый m-й элемент которого является экземпляром, обеспечивающим корректное распознавание одного или более символа последовательности $S_{CAPTCHA}$. Далее каждый элемент множества $\{CAPTCHA^{m}_{тст}\}$ передается на вход системы распознавания, реализующей алгоритм OCR. Результатом обработки каждого элемента множества $\{CAPTCHA^{m}_{тст}\}$ является последовательность символов содержащая от 0 до $S_{CAPTCHA}$ корректно распознанных символов аутентификационной последовательности. Таким образом, сформированное множество $\{CAPTCHA^{m}_{тст}\}$ преобразуется во множество тестовых последовательностей $S_{CAPTCHA}$ $\{S^{тст}_{CAPTCHA}\}$ в общем случае содержащее все корректно распознанные символы аутентификационной последовательности $S_{CAPTCHA}$.

В задачу исследования не входила разработка алгоритма выбора корректно распознанных символов из множества $\{S^{тст}_{CAPTCHA}\}$. Предполагается, что формирование экземпляра последовательности $S'_{CAPTCHA}$ выполняется вручную, поскольку основной целью разрабатываемой методики оценки уязвимости является подтверждение (или опровержение) факта, что для рассматриваемого CAPTCHA-образа имеется возможность получения всех корректно распознанных символов аутентификационной последовательности $S_{CAPTCHA}$.

Разработанную методику оценки уязвимости систем аутентификации на основе технологии CAPTCHA можно представить графически. Из рисунка 1 видно, что разработанная методика состоит из следующих взаимосвязанных этапов:

Этап 1. Обесцвечивание CAPTCHA-образа.

Этот этап является первоначальным обязательным этапом модификации CAPTCHA-образа. Его необходимость обусловлена тем, что существующие OCR-алгоритмы оптимизированы для работы с черно-белыми образами и отсутствие цветового зашумления является важным фактором их успешной работы. Для обесцвечивания CAPTCHA-образа бал выбран инструмент Desaturate.

Характеристики обесцвечивания могут варьироваться, в силу чего на выходе этапа 1 получится подмножество $\{CAPTCHA_1\}$, и все дальнейшие этапы применяются к каждому элементу этого подмножества.

Этап 2. Выделение границ объектов в CAPTCHA-образе.

Зашумление объектами является эффективным способом искажения CAPTCHA-объекта. Однако ряд фильтров позволяют определить границы всех объектов, расположенных на образе и соответственно отделить их от фона. Для эффективного определения границ CAPTCHA-символов использовались следующие фильтры: Sharpen, Sharpen Edges, Poster Edges, Accented Edges.

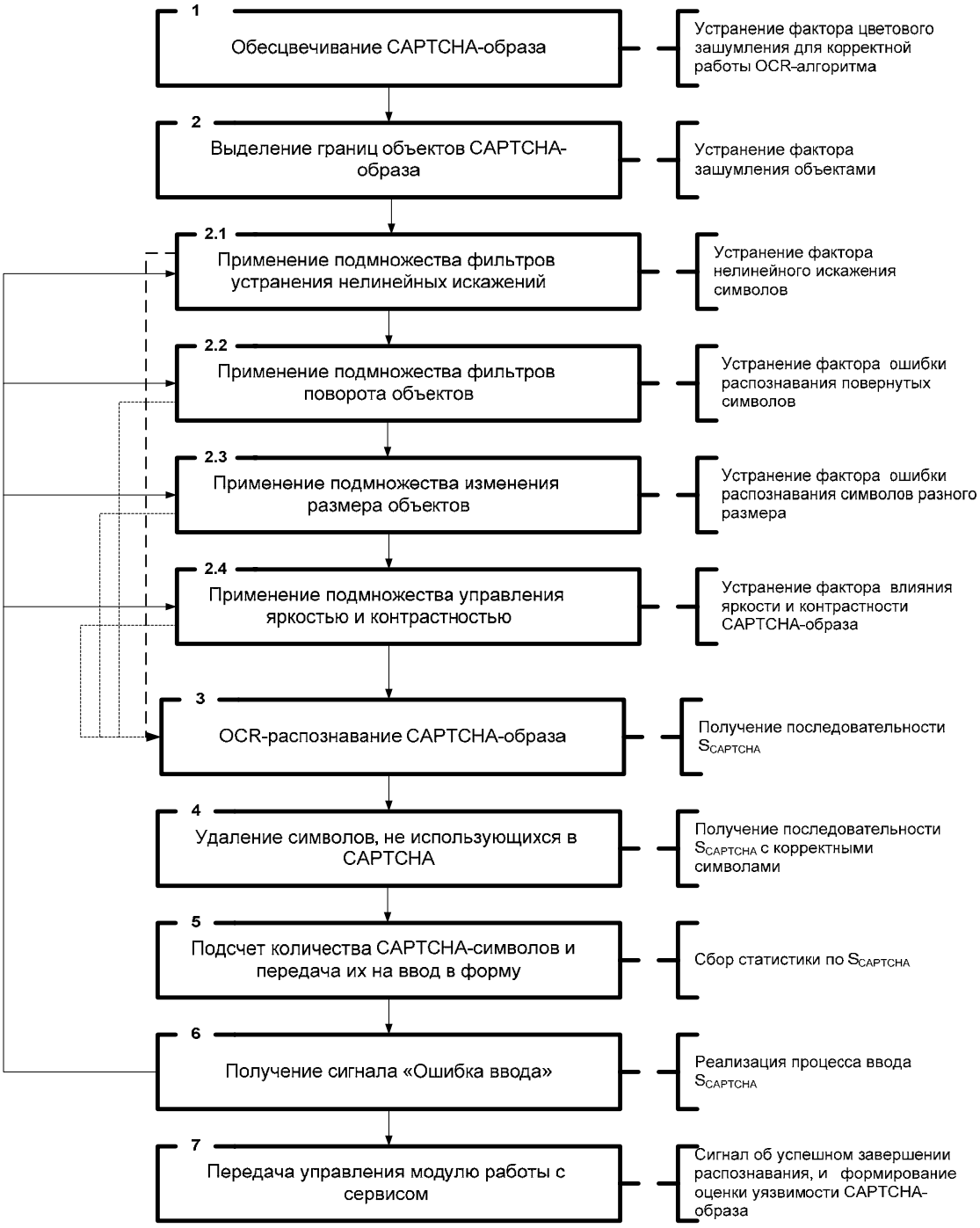

Рис. 1. Графическое представление методики оценки уязвимости системы аутентификации на основе технологии CAPTCHA

Результатом выполнения этапа два является подмножество образов $\{CAPTCHA_2\}$, каждый элемент которого потенциально может содержать, как совокупность символов и объектов зашумления, так и только совокупность символов, или только совокупность объектов зашумления.

Полученное подмножество $\{CAPTCHA_2\}$ является базовым для выполнение последовательности этапов 2.1-2.4, каждый из которых применяет к элементам подмножества $\{CAPTCHA_2\}$ фильтры, устраняющие факторы искажения символов.

Так на этапе 2.1 с использованием фильтров Liguify, Lens Correction производится попытка устранения фактора нелинейного искажения символов, а именно:

На этапе 2.2 с использованием фильтров поворота образа и объектов внутри него производится попытка размещения символов строго вертикально.

На этапе 2.3 производится изменение размера объектов с целью получения оптимального для алгоритма OCR размера символов.

На этапе 2.4, используя инструменты Brightness/ Contrast и Invert производится варьирование яркостью и контрастностью пары «объект-фон», для получения наиболее оптимальных для алгоритма OCR характеристик.

После реализации каждого из этапов 2.1-2.4 полученные подмножества $\{CAPTCHA_{2.1}\}$-$\{CAPTCHA_{2.4}\}$ передаются алгоритму OCR (этап 3).

После распознавания каждого из элементов подмножеств $\{CAPTCHA_{2.1}\}$-$\{CAPTCHA_{2.4}\}$, специально разработанный алгоритм подсчитывает каждом элементе распознанных последовательностей $\{S^{2.1}{}_{CAPTCHA}\}$-$\{S^{2.4}{}_{CAPTCHA}\}$ количество CAPTCHA-символов, которыми могут быть только буквы английского и русского алфавитов или цифры (этап 5). При этом символы, не являющиеся CAPTCHA-символами, удаляются (этап 4).

На этапе 5 ведется статистика успешно распознанных символов, которая в дальнейшем применяется при формировании конечной оценки уязвимости.

Далее полученные элементы подмножеств $\{S^{2.1}{}_{CAPTCHA}\}$-$\{S^{2.4}{}_{CAPTCHA}\}$ поочередно вводятся в форму системы аутентификации.

В зависимости от результата обработки формы (успешная обработка или формирование сообщения об ошибке ввода (этап 6)) этапы 2.1-2.4 либо повторяются с варьированием значений используемых в них фильтров, либо производится переход к формированию оценки уязвимости системы аутентификации (этап 7).

Разработанная методика может служить основой для разработки и проектирования программного прототипа, позволяющего оценивать уязвимость системы аутентификации на основе технологии CAPTCHA.

Литература

1. Козачок, В.И. Основы информационной безопасности [Текст] : учебное пособие / В.И. Козачок, А.И. Козачок, Н.И. Биркун и др.; под общ. ред. В.И. Козачка – Орел: Академия ФСО России, 2009. – 302 с.

2. Вендеров, А.М. Проектирование программного обеспечения экономических информационных систем [Текст] : учебник / А.М. Вендеров – М.: Финансы и статистика, 2000. – 262 с.

3. В поисках идеальной CAPTCHA [Электронный ресурс] : статья / www.captcha.ru.

А.М. Геращенко

ОСУЩЕСТВЛЕНИЕ ПОДГОТОВКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ АНГЛОЯЗЫЧНЫХ ОНЛАЙН-КУРСОВ

(Кубанский государственный технологический университет)

В связи со значительной и растущей ролью информационных технологий, особую значимость приобретает укрепление информационной безопасности. По этой причине существует необходимость как постоянного совершенствования подготовки профессионалов в данном направлении, так и повышения осведомленности в этой связи «среднестатистического обывателя», чья деятельность требует использования компьютерных и сетевых технологий. В силу быстрого и непрерывного технического развития рассматриваемой области, связанные с нею знания, умения и навыки нуждаются в постоянном совершенствовании и обновлении. При этом обеспечение информационной безопасности относится к числу тех сфер деятельности, где учеба на собственных ошибках, несмотря на свою значительную роль, представляется гораздо менее предпочтительной, нежели заблаговременная информированность о возможных угрозах. Соответственно, лица, задействованные в обеспечении информационной безопасности, нуждаются в своевременной подготовке к предупреждению и решению возможных проблем в этой связи.

При этом, для расширения профессионального кругозора, целесообразно обращаться как к отечественным достижениям, так и к опыту зарубежных стран – прежде всего тех, которые внесли наиболее весомый вклад в развитие информационных технологий. Дополнительную актуальность такой целесообразности способны придать также проблемы межгосударственных отношений, в результате которых осведомленность о положении вещей в сфере информационной безопасности соответствующих государств может принять характер знания сильных и слабых сторон вероятных противников.

Среди зарубежных стран, имеющих ценный опыт деятельности в плане разработки компьютерных систем и обеспечения информационной безопасности, важнейшее место занимают Великобритания и США. С целью знакомства с таким опытом, для специалиста в данной сфере было бы полезным прохождение соответствующих курсов в указанных странах. Этому способствует наличие значительного числа различных курсов по информационной безопасности (кибербезопасности), предлагаемых британскими и американскими учебными заведениями. Поскольку среднестатистический учащийся или работающий россиянин по различным причинам не может позволить себе полноценное очное