такого рода: лучше биортогонального вейвлета 5-3 в среднем на 3 %, лучше биортогонального вейвлета 16-4 в среднем на 1,8 %.

Библиографические ссылки

1. *Гонсалес Р.*, *Вудс Р.* Цифровая обработка изображений. – М. : Техносфера, 2006. – 1072 с.

2. *Сэломон Д.* Сжатие данных изображений и звука. – М. : Техносфера, 2004. – 368 с.

3. *Самохвалов А. В.* Контурная информация при сжатии полутоновых изображений // Приволжский научный вестник. – 2013. – № 7(23). – С. 46–52.

4. *Уфимкин А. Я.*, *Самохвалов А. В.* Адаптивное цветотоновое преобразование при кодировании графической информации // Надежность и качество : тр. междунар. симпозиума. – Т. 1. – 2008. – С. 250–253.

5. *Самохвалов А. В.* Контурное кодирование полутонового изображения: выделение контурной информации на изображении // Приволжский научный вестник. – 2013. – № 7(23). – С. 53–61.

6. *Самохвалов А. В.* Компрессия контурного и кодирование маскированного изображений // Вестник ИжГТУ. – 2015. – № 1(65). – С. 105–108.

Получено 30.09.2015

УДК 621.36; 681.3.067

Е. Ф. Стукалина, кандидат технических наук, ИжГТУ имени М.Т. Калашникова
А. М. Сметанин, доктор технических наук, ИжГТУ имени М.Т. Калашникова
Л. М. Опоева, аспирант, ИжГТУ имени М.Т. Калашникова

ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ eToken В УЧЕБНОМ ПРОЦЕССЕ И НАУЧНОЙ РАБОТЕ

Внедрение новых стандартов обучения, таких как ФГОС ВПО нового поколения, поставило перед образовательными учреждениями большое количество разнообразных задач, связанных с формированием содержания образовательных программ и лабораторных практикумов. Поскольку внедрение компетентностного подхода в методические учебные материалы является существенным моментом новых образовательных стандартов, проанализировав рабочие программы учебных дисциплин по специальности 10.05.03 «Информационная безопасность автоматизированных систем», выделим следующие компетенции и рассмотрим возможные направления их формирования с учетом сложившихся технических решений на современном рынке средств защиты информации:

– способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

– способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

– способность организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30).

Формирование вышеперечисленных компетенций предусмотрено в учебных планах специальностей 090303, 10.05.03 при изучении таких дисциплин, как «Программно-аппаратные средства обеспечения информационной безопасности», «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем».

Для формирования вышеперечисленных компетенций в Ижевском государственном университете имени М. Т. Калашникова разработан и используется лабораторный практикум на базе электронных ключей eToken фирмы «Аладдин Р.Д.».

Процедура идентификации и аутентификации является первым рубежом обороны защищенной автоматизированной системы и изучается в рамках нескольких дисциплин специализации. На настоящий момент достаточно доступным средством аппаратной аутентификации пользователей в автоматизированных системах являются различные токены. Причем в зависимости от реализации и функционала такие ключи могут применяться для решения целого ряда задач в области информационной безопасности. Например, фирма «Аладдин Р.Д.» предлагает следующие решения на базе ключей eToken [1]:

– аутентификация и управление паролями;

– строгая аутентификация при обращении к защищенным сетевым ресурсам;

– строгая аутентификация при удаленном доступе к корпоративной сети (встраиваемая в систему VPN);

– строгая аутентификация при доступе к защищенным веб-ресурсам;

– защита начальной загрузки компьютера;

– шифрование данных;

– безопасность электронной почты;

– электронная цифровая подпись.

Ключи eToken можно использовать как для хорошо известной классической парольной аутентификации, так и легко интегрировать со многими решениями в области информационной безопасности. На этом основан лабораторный практикум «Комплексное обеспечение безопасности на основе USB-ключей» в ИжГТУ имени М. Т. Калашникова.

Практикум состоит из двух практических работ и трех лабораторных работ; на рисунке приведено содержание сборника.

В первой практической работе студенты знакомятся с приемами администрирования ключей eToken. Основная проблема заключается в том, что на этом этапе происходит инициализация устройства с обязательной сменой пароля администратора. Несколько неправильных попыток ввода пароля приводят к полной блокировке устройства, поэтому эта работа является в цикле лабораторного комплекса критически значимой, и все действия по смене пароля обязательно фиксируются в журнале учета устройств. Поскольку процедура инициализации eToken подразумевает форматирование памяти устройства, то в ходе этого процесса все созданные на eToken объекты с момента его выпуска удаляются, освобождается память, сбрасывается значение пароля. Инициализация будет целесообразной, например, в том случае, когда один из студентов завершает выполнение лабораторных работ с использованием данного ключа, чтобы этот ключ можно было подготовить для выполнения работ другим учащимся.

Содержание

Содержание сборника лабораторных работ «Комплексное обеспечение безопасности на основе USB-ключей»

Во второй практической работе рассматриваются приемы работы с ключами в режиме пользователя, в частности изучаются функции расширенного управления устройством, а именно переименование eToken, изменение пароля пользователя, удаление содержимого из памяти eToken, импорт сертификатов и др.

После получения навыков в администрировании ключей студенты выполняют лабораторные работы, смысл которых заключается во внедрении eToken в состав защищенных автоматизированных систем. Таким образом, у учащихся формируются компетенции, связанные с разработкой и эксплуатацией защищенных автоматизированных систем (ПК-18, ПК-19, ПК20).

В лабораторной работе № 1 с использованием утилиты eToken PKI Client учащиеся могут выполнять следующие процедуры с ключами защиты eToken:

– выбирать активный eToken;
– сменить пароль пользователя eToken;
– разблокировать eToken;
– удалить содержимое eToken;
– просмотреть данных об устройстве eToken;
– копировать информацию о eToken в буфер обмена;
– переименовать eToken;
– провести авторизацию eToken;
– импортировать сертификат в память eToken;
– выбирать дополнительный сертификат и сертификат, используемый по умолчанию;
– управлять считывателями;
– синхронизировать пароли.

В лабораторной работе № 2 на базе приложения TrueCrypt изучаются приемы хранения ключевой информации на электронном носителе eToken. TrueCrypt – это криптографическое программное обеспечение с открытым исходным кодом. Используется для шифрования информации «на лету» (разделов/дисков или устройств хранения данных, таких как USB флеш-память). При таком виде шифрования данные автоматически зашифровываются и расшифровываются перед их чтением или сохранением без какого-либо участия пользователя. Файловая система при этом шифруется в полном объеме (шифруются имена файлов, каталогов, содержание каждого файла, свободное место, метаданные и т. д.). Информация, находящаяся в зашифрованном разделе, не может быть прочитана (расшифрована) без введения правильного пароля/key-файла или ключей шифрования.

В лабораторной работе № 3 «Усиление парольной защиты с помощью ключей eToken» изучаются принципы усиления парольной защиты с помощью программно-аппаратных ключей eToken в среде программы eToken Network Logon. Программное обеспечение eToken Network Logon предназначено для решения проблемы «слабых» паролей при работе на компьютерах под управлением Microsoft Windows. С помощью данного ПО можно эффективно исполь-

зовать сложные пароли, либо цифровые сертификаты, для входа на рабочую станцию или в домен Windows.

eToken Network Logon обеспечивает:

– двухфакторную аутентификацию пользователей на рабочих станциях и в домене Windows с помощью USB-ключей или смарт-карт eToken;

– использование хранимых в защищенной памяти eToken регистрационных имен и паролей для локального входа на рабочие станции или для входа в домен;

– использование цифровых сертификатов стандарта X.509 и закрытых ключей для регистрации в домене Windows;

– безопасное генерирование, надежное хранение и удобное применение паролей, состоящих из набора случайных символов;

– блокирование компьютера при отсоединении eToken.

Возможности использования ключей eToken не ограничиваются рассмотренными выше и включенными в комплекс лабораторных работ. Для встраивания возможности работы с eToken в различные приложения компания-разработчик ключей eToken предлагает комплект разработчика Aladdin's eToken SDK, представляющий собой набор заголовочных файлов на языке C++, описывающих программный интерфейс ключей и смарт-карт eToken. В рамках дипломного проекта на кафедре «Системы и технологии информационной безопасности» ИжГТУ имени М. Т. Калашникова была разработана СУБД на платформе 1С: Предприятие 8.0, которая содержит дополнительный уровень двухфакторной аутентификации. При первой попытке обращения пользователя к определенной категории данных (конфиденциальной информации) система затребует у пользователя USB-ключ с занесенной в его защищенную область памяти ключевой информацией и потребует ввести PIN-код.

Для решения этой задачи необходимо было разработать модуль, реализующий двухфакторную аутентификацию пользователя. Общая идея этого модуля заключается в следующем. Каждый пользователь системы, имеющий доступ к конфиденциальной информации, должен иметь USB-ключ eToken, на котором должна храниться ключевая информация, записанная администратором безопасности. Ключевая информация, хранимая на eToken, представляет собой совокупность ключевой пары RSA и зашифрованной открытым ключом этой пары кодовую фразу. Открытая часть ключевой информации хранится подсистемой защиты в специальном справочнике пользователей системы. В этом же справочнике хранится служебная информация, необходимая для поиска ключевой информации на eToken.

Ввиду того, что встроенные в 1С: Предприятие 8.0 средства не поддерживают работу с ключами и смарт-картами eToken, но позволяют расширить возможности встроенного языка посредством подключаемых внешних модулей (внешних компонент), задача двухфакторной аутентификации в системе была разделена на 3 подзадачи:

– создание внешней компоненты для 1С: Предприятие, позволяющей работать с ключами и смарт-картами eToken;

– создание обработки в 1С: Предприятие для управления ключами eToken;

– определение списка особо защищаемых ресурсов и встраивание защиты в модули управления этими ресурсами.

Для реализации модуля работы с eToken были выполнены следующие этапы:

– реализован класс на языке C++, позволяющий работать с USB-ключом eToken и реализующий базовые методы работы с ключевой парой RSA и криптографические операции;

– создана внешняя компонента для 1С: Предприятие, использующая возможности созданного класса и реализующая функции:

а) генерации ключевой информации;

б) удаление ключевой информации;

в) модуля двухфакторной аутентификации пользователя;

– создана обработка для 1С: Предприятие, позволяющая управлять ключевой информацией и осуществлять двухфакторную аутентификацию пользователя в конфигурации;

– создан обработчик обращений к особо защищаемым объектам системы.

По результатам работы была опубликована научная статья «Проблемы аутентификации пользователей баз данных на основе ключей eToken» [2].

В итоге можно сказать, что использование ключей eToken эффективно как для формирования компетенций учащихся по специальностям 090903, 10.05.03 в ходе выполнения лабораторных практикумов, так и в научной и исследовательской работе студентов.

Библиографические ссылки

1. *Стукалина Е. Ф.*, *Подшивалов Д. В.* Проблемы аутентификации пользователей баз данных на основе ключей E-TOKEN // Современные информационные технологии в деятельности органов государственной власти «Информтех-2008» : материалы I Всерос. науч.-техн. конф. – Курск, 2008. – С. 167–168.

2. Там же.

Получено 01.10.2015