ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СЕТИ

УДК 004.355, 004.454, 004.41

С.А. ЛАЗАРЕВ, П.П. СИЛАЕВ

МЕХАНИЗМ ПРИМЕНЕНИЯ ПОРТАТИВНЫХ ЦИФРОВЫХ УСТРОЙСТВ ДОСТУПА В СЕТИ КОРПОРАТИВНЫХ ПОРТАЛОВ

В данной статье рассмотрены основные технические аспекты и решения в рамках реализации механизма применения портативных цифровых устройств доступа в сети корпоративных порталов. В частности, рассмотрены программно-аппаратные особенности клиентской части данной системы доступа как наиболее сложной с точки зрения организации, а также сопутствующие программные средства и способы их интеграции, обеспечивающие взаимодействия между звеньями сложной цепочки компонентов системы.

Ключевые слова: *цифровой ключ доступа; цифровой носитель информации; электронный документ; распределенная сеть; управление доступом; информационный обмен; корпоративный портал.*

Актуальность данной задачи обусловлена необходимостью создания в рамках построения сети корпоративных порталов единого, универсального, защищенного и одновременно удобного механизма доступа к web-порталам. С этой целью необходимо исследовать механизм взаимодействия компонентов клиентской части системы контроля доступа на основе портативных цифровых устройств доступа (ПЦУД).

ОСОБЕННОСТИ ПОСТРОЕНИЯ ПОРТАТИВНОГО ЦИФРОВОГО УСТРОЙСТВА ДОСТУПА

В соответствии с предложенной методикой [1], в качестве основной функции ПЦУД выступает не только хранение идентификационных данных, но и непосредственное участие в процессе генерации шифрограммы. Исходя из этого, следует, что элементная база ПЦУД должна основываться на микропроцессорной системе, имеющей аппаратный вычислитель (как пример можно использовать 32-хразрядный микроконтроллер семейства AT91SAM7 фирмы Atmel [3]).

Важно отметить следующие особенности данного микроконтроллера, которые необходимы для решения всех аспектов поставленной задачи:

- относительно малые размеры, позволяющие сделать устройство портативным;
- высокое быстродействие (применительно к возложенным функциям);
- невысокая стоимость, позволяющая сделать продукт массовым;
- наличие порта устройства USB, позволяющего облегчить подключение к ПК;
- наличие встроенных битов блокировки и бита защиты, которые позволяют защитить прошивку микроконтроллера от несанкционированной перезаписи или хищения, что немаловажно в задачах криптографии.

При проектировании ПЦУД была разработана электрическая принципиальная схема, основа которой предложена разработчиком микроконтроллера [4].

ПРОТОКОЛ ВЗАИМОДЕЙСТВИЯ ПК И ПЦУД

Немаловажным аспектом является выбор протокола для информационного обмена между ПК и ПЦУД. Основные критерии для выбора протокола:

- возможность реализации протокола на базе выбранного микроконтроллера;
- высокая надежность взаимодействия устройства с ПК;

– невысокая скорость передачи данных по интерфейсу, поскольку предполагается передача блоков данных фиксированной длины;

– возможность создания коммуникации между ПК и ПЦУД с использованием известных методов и подходов.

Исходя из поставленных требований, в качестве протокола для взаимодействия ПК и ПЦУД можно рассмотреть протокол USB HID (Human Interface Device) [5].

На основе HID-технологии можно организовать взаимодействие с любым устройством, даже если оно не является в строгом смысле интерфейсным устройством человека и компьютера.

На стороне хоста обменом с устройством будет руководить стандартный HID-драйвер, включенный в поставку операционной системы.

Максимально возможная скорость передачи данных при такой организации обмена составляет 64 Кбит/сек. Такой показатель в сравнении с 12 Мбит/сек полной скорости USB-шины является большим минусом HID-технологии в вопросе выбора конкретной USB-реализации [5]. Однако для поставленной задачи указанной скорости вполне хватает. Беря во внимание размерности параметров алгоритмов шифрования, максимальное количество данных, передаваемых по USB-интерфейсу, равно 4 Кбайт в обоих направлениях, следовательно, для передачи данных потребуется менее 500 мс.

Спецификацию интерфейса определяет схема организации программных компонентов для обеспечения информационного обмена между ПК и ПЦУД. Основу данной схемы образуют две программы, выполняющие целевую функцию и взаимодействующие между собой через USB интерфейс: для ПК – прикладная программа, для ПЦУД – основная программа. Соединение и передачу данных обеспечивает драйвер USB HID, являющийся стандартным компонентом операционной системы.

ПОДХОДЫ К ОРГАНИЗАЦИИ ДОСТУПА К ЛОКАЛЬНЫМ РЕСУРСАМ ПК ИЗ БРАУЗЕРА

Исходя из поставленной задачи, информационное взаимодействие осуществляется по протоколу HTTP/HTTPS с целью обеспечения максимального удобства использования. Следовательно, все процессы аутентификации пользователя на web-портале должны быть инициированы браузером, выполняться в его рабочем пространстве и контролироваться им. Согласно предложенной методике, часть действий, необходимых для аутентификации, должны выполняться ресурсами ПЦУД. Возникает ситуация, при которой необходимо создать механизм двухстороннего взаимодействия с ПЦУД средствами интернет-технологий, которые позволяют выполнять сценарии на стороне клиента. Таким образом, схема организации программных компонентов (рис. 1) получает новую интерпретацию, где в роли прикладной программы выступает браузер или сценарий, работающий под его управлением – web-сценарий.

Данная схема весьма затруднительна с точки зрения её реализации, поскольку возникает противоречие. С одной стороны, взаимодействие с ПЦУД необходимо производить через драйвер ОС, относящийся к локальным ресурсам ПК и являющийся внешним окружением по отношению к браузеру. С другой стороны, браузер является средством доступа в глобальную сеть и имеет средства защиты от несанкционированного доступа к локальным ресурсам ПК и ограничения со стороны ОС, а также пресекает любые попытки обращения к ним.

Таким образом, возникает проблема, при которой необходимо получить доступ к локальным ресурсам средствами браузера, что не позволяет сделать его политика безопасности.

Решение данной проблемы может получить развитие в следующих направлениях:

– создание модуля для браузера (плагина);

– создание Java-апплета;

– создание прикладной программы для ОС, которая будет работать независимо и выступать в роли посредника между web-сценарием и модулем взаимодействия с ПЦУД.

При анализе данных подходов были выявлены достоинства и недостатки каждого из них в контексте проблемы, описанной выше. Полученные результаты зафиксированы в таблице 1.

Таблица 1 – Результаты сравнительного анализа предложенных web-технологий

Технология	Достоинства	Недостатки
Плагин для браузера	Полная интеграция с ОС на низком уровне, что упрощает механизм взаимодействия с ПЦУД	Необходимость в отдельной установке: для каждой версии браузера требуется свой плагин
Java-апплет	Полная совместимость со всеми браузерами	Получение доступа к локальным ресурсам возможно только после доверительного подписания апплета
Независимая прикладная программа-посредник	Полная интеграция с ОС на низком уровне, что упрощает механизм взаимодействия с ПЦУД	Требует дополнительной установки, что сильно осложняет общий механизм взаимодействия компонентов; необходимо наличие разных компиляций программы под различные ОС

Следует также отметить, что все рассмотренные технологии позволяют в той или иной степени получать доступ к локальным ресурсам ПК, тем самым решая описанную проблему. Однако применение Java-апплета позволяет обойти возникшую проблему и наиболее качественно решить поставленную задачу. Взаимодействие компонентов, решающих данную задачу, представлено на рисунке 1.

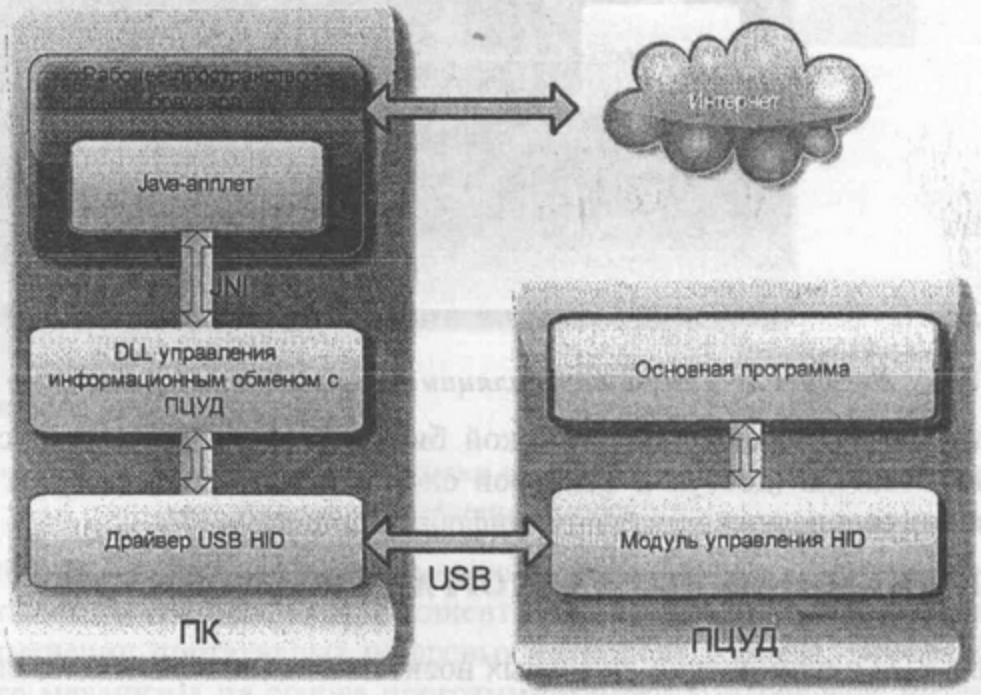

Рисунок 1 – Взаимодействие программных компонентов с использованием технологии JavaApplet

ВЗАИМОДЕЙСТВИЕ ПРОГРАММНЫХ КОМПОНЕНТОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ JAVA-APPLET

В стандартную комплектацию Java Runtime Environment (JRE) не входит какой-либо класс или метод, позволяющий осуществить доступ к USB-порту. Поэтому необходимо реализовать библиотеку, которая будет иметь методы взаимодействия с USB-устройством и осуществлять посреднические функции между Java-апплетом и драйвером USB.

Java-апплет будет осуществлять взаимодействие с библиотекой посредством механизма Java Native Interface (JNE) [6]. Это стандартный механизм для запуска кода, под управлением виртуальной машины Java (JVM), который написан на языках C/C++ или Ассемблера, скомпонованный в виде динамических библиотек и позволяющий не использовать статическое связывание. Это даёт возможность вызова функции C/C++ из программы на Java и наоборот.

Обязательным условием использования данного механизма является то, что native-библиотека должна располагаться на диске машины клиента в специальной директории. Следовательно, требуется инсталлировать библиотеку на пользовательскую машину, после чего Java-апплет сможет подключить ее. Для этого необходимо поместить Java-класс и библиотеку в jar-архив, который загрузится вместе с html-страницей. После этого Java-апплет развернёт DLL-библиотеку во временное хранилище машины пользователя и из него подгрузит DLL. Данную схему иллюстрирует рисунок 2.

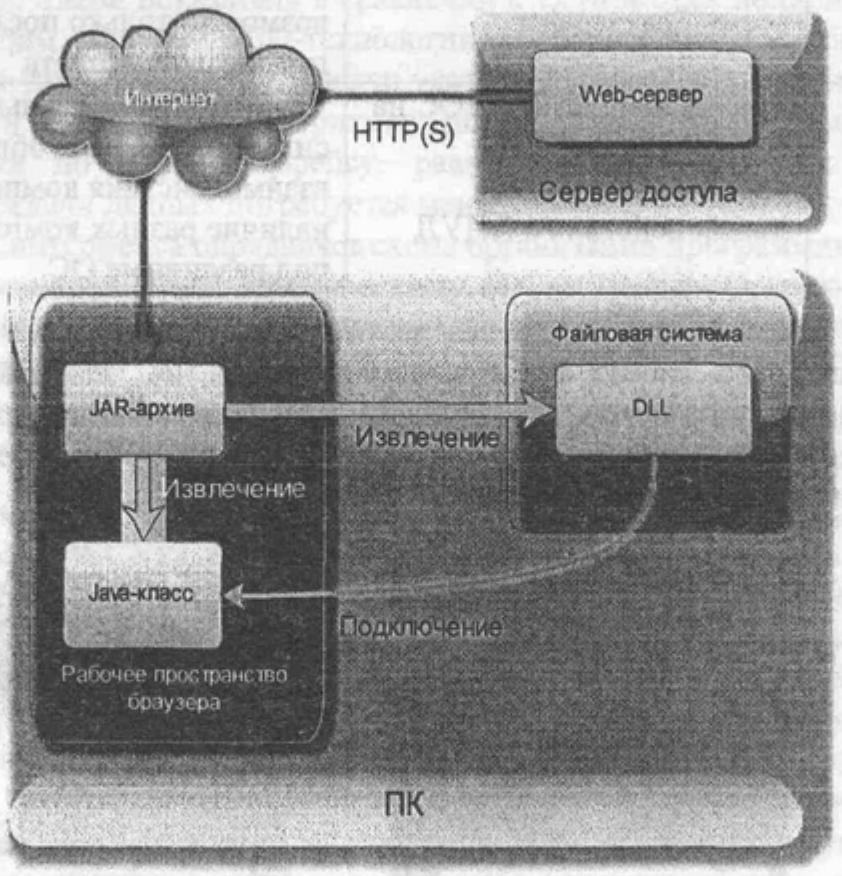

Рисунок 2 – Схема инсталляции библиотеки на клиентскую машину

В ходе развёртывания динамической библиотеки потребуется доступ к локальным ресурсам пользователя (доступ к файловой системе). Java-апплету будет разрешён доступ при условии его подписания электронно-цифровой подписью [7].

ИСПОЛЬЗОВАНИЕ ПЦУД ДЛЯ ОРГАНИЗАЦИИ ДОСТУПА К WEB-ПОРТАЛАМ

В статье [1] о применении цифровых носителей идентификационной информации для управления доступом в сети корпоративных порталов была рассмотрена схема информационного обмена в процессе аутентификации или подписания документа электронной подписью. Беря во внимание предложенные технические решения, упомянутая схема может быть трансформирована в схему, приведенную на рисунке 3.

При аутентификации пользователя в системе сервер отправляет случайную последовательность битов, которая формируется на основе запрашиваемых аутентификационных данных пользователя. Далее полученная последовательность битов передается в ПЦУД, реализуя предложенные выше методы и технологии. После этого ПЦУД шифрует полученную последовательность, используя алгоритмы шифрования, а также

секретный ключ, позволяющий однозначно идентифицировать в системе пользователя – владельца ключа. Сгенерированный шифр отправляется на сервер доступа, где проходит процедуру верификации. При получении положительного ответа по окончании проверки неизвестный признается подлинным пользователем системы, в результате чего создаётся открытая сессия для данного пользователя.

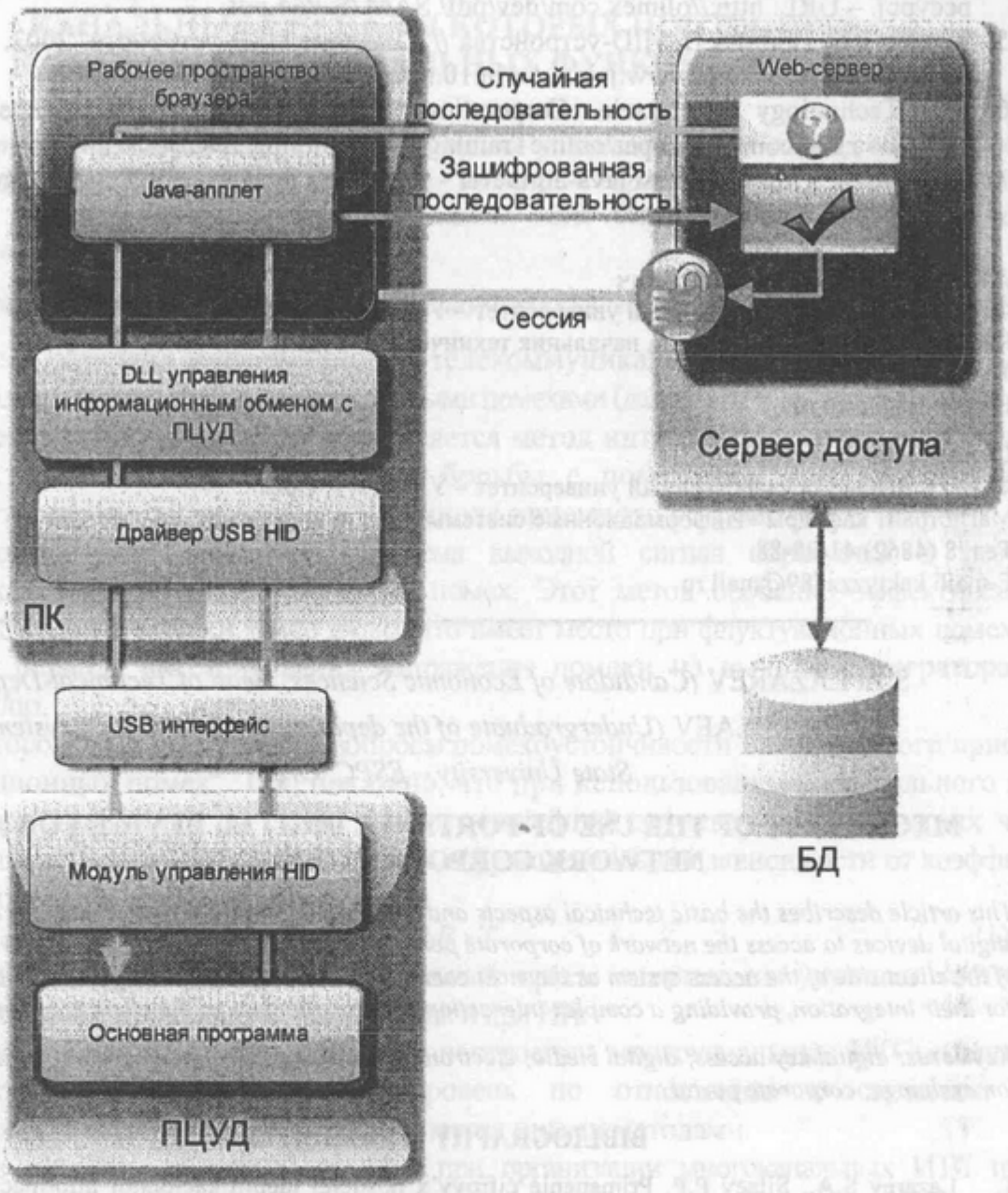

Рисунок 3 – Схема информационного обмена между пользователем и сервером доступа в процессе аутентификации

В заключении следует отметить, что в данной статье были рассмотрены особенности механизма взаимодействия компонентов клиентской части системы доступа, которая базируется на применении портативных цифровых устройств доступа. Предложен вариант реализации данного механизма на основе программируемого контроллера, интерфейса HID для USB и программной поддержки работы ПЦУД на основе Java-апплета.

СПИСОК ЛИТЕРАТУРЫ

1. Лазарев С.А., Силаев П.П. Применение цифровых носителей идентификационной информации для управления доступом в сети корпоративных порталов // Информационные системы и технологии. – Орел: Госуниверситет – УНПК, 2011. – № 3(65) май-июнь. – С. 108-114.
2. Константинов И.С., Лазарев С.А. Некоторые аспекты создания информационных ассоциаций в глобальных сетях на основе построения сети корпоративных порталов //

Информационные системы и технологии. – Орел: Госуниверситет–УНПК, 2011. – № 1(69) январь-февраль. – С. 103-106.
3. Описание микроконтроллеров семейства AT91SAM7 ARM-based // Atmel Corporation, 2011. – [Электронный ресурс]. – URL: http://www.atmel.com/dyn/resources/ prod_documents/doc6175.pdf.
4. Принципиальная электрическая схема AT91SAM7s64 // OLIMEX, 2009. – [Электронный ресурс]. – URL: http://olimex.com/dev/pdf/ SAM7S-P64.pdf.
5. Козлов Ю., Пронин В. HID-устройства // Создание USB-устройств, 2003. – [Электронный ресурс]. – URL: http://www.jais.ru/write10.html.
6. JNI Technology // Oracle Corporation, 2011. – [Электронный ресурс]. – URL: http://java.sun.com/developer/onlineTraining/Programming/JDCBook/jni.html.
7. Никитин А. Подписываем java-апплеты – получаем права. – 2009. – [Электронный ресурс]. – URL: http://svitter.ru/?p=43.

Лазарев Сергей Александрович
ФГБОУ ВПО «Государственный университет – УНПК», г. Орел
Кандидат экономических наук, начальник технического отдела
Тел.:8 (4862) 59-46-19
E-mail: lsa@ostu.ru

Силаев Павел Петрович
ФГБОУ ВПО «Государственный университет – УНПК», г. Орел
Магистрант кафедры «Информационные системы»
Тел.:8 (4862) 41-98-88
E-mail: kaktyzzz_89@mail.ru

S.A. LAZAREV *(Candidate of Economic Sciences, Head of Technical Department)*
P.P. SILAEV *(Undergraduate of the department «Information systems»)*
State University – ESPC, Orel

MECHANISM OF THE USE OF PORTABLE DIGITAL DEVICE FOR ACCESS TO NETWORK CORPORATE PORTALS

This article describes the basic technical aspects and solutions within the framework of the mechanism of portable digital devices to access the network of corporate portals In particular, we consider hardware and software features of the client side of the access system as the most complex in terms of organization, as well as related tools and methods for their integration, providing a complex interaction between the links of the chain components.

Keywords: *digital key access; digital media; electronic document; distributed network; access control; information exchange; corporate portal.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Lazarev S.A., Silaev P.P. Primenenie cifrovy'x nositelej identifikacionnoj informacii dlya upravleniya dostupom v seti korporativny'x portalov // Informacionny'e sistemy' i texnologii. – Oryol: Gosuniversitet – UNPK, 2011. – № 3(65) maj-iyun'. – S. 108-114.
2. Konstantinov I.S., Lazarev S.A. Nekotory'e aspekty' sozdaniya informacionny'x associacij v global'ny'x setyax na osnove postroeniya seti korporativny'x portalov // Informacionny'e sistemy' i texnologii. – Oryol: Gosuniversitet – UNPK, 2011. – № 1(69) yanvar'-fevral'. – S. 103-106.
3. Opisanie mikrokontrollyorov semejstva AT91SAM7 ARM-based // Atmel Corporation, 2011. – [E'lektronny'j resurs]. – URL: http://www.atmel.com/dyn/resources/prod_documents/doc6175.pdf.
4. Principial'naya e'lektricheskaya sxema AT91SAM7s64 // OLIMEX, 2009. – [E'lektronny'j resurs]. – URL: http://olimex.com/dev/pdf/ SAM7S-P64.pdf.
5. Kozlov Yu., Pronin V. HID-ustrojstva // Sozdanie USB-ustrojstv, 2003. – [E'lektronny'j resurs]. – URL: http://www.jais.ru/write10.html.
6. JNI Technology // Oracle Corporation, 2011. – [E'lektronny'j resurs]. – URL: http://java.sun.com/developer/onlineTraining/Programming/JDCBook/jni.html.
7. Nikitin A. Podpisy'vaem java-applety' – poluchaem prava. – 2009. – [E'lektronny'j resurs]. – URL: http://svitter ru/?p=43.