Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра радиотехнических систем

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ РАДИОЭЛЕКТРОННЫХ ИДЕНТИФИКАТОРОВ

Методические указания
к лабораторной работе
по курсам «Теория кодирования и защита информации»,
«Теория кодирования и основы криптологии»
для студентов радиотехнических специальностей
всех форм обучения

Минск БГУИР 2011

УДК 004.056.5:336.71(076.5)
ББК 32.973.26-04я73+65.261я73
И88

С о с т а в и т е л и:
С. Б. Саломатин, Д. М. Бильдюк

Исследование системы защиты банковской информации на
И88 основе радиоэлектронных идентификаторов : метод. указания к лаб. работе по курсам «Теория кодирования и защита информации», «Теория кодирования и основы криптологии» для студ. радиотех. спец. всех форм обуч. / сост. С. Б. Саломатин, Д. М. Бильдюк. – Минск : БГУИР, 2011. – 28 с. : ил.
ISBN 978-985-488-294-9.

Издание содержит теоретические сведения об организации банковских систем на основе радиоэлектронных идентификаторов с использованием алгоритмов криптографического преобразования информации для организации протоколов аутентификации, обеспечения секретности и имитостойкости банковской информации. В лабораторной работе исследуются криптографические свойства алгоритмов электронной цифровой подписи, их влияние на свойства системы защиты банковской информации.

УДК 004.056.5:336.71(076.5)
ББК 32.973.26-04я73+65.261я73

ISBN 978-985-488-294-9

1 ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

1 Изучить применение криптографических методов защиты информации в системах на основе электронных пластиковых карт.

2 Изучить основные принципы функционирования банковских пластиковых карт.

3 Изучить принципы функционирования платежных систем на основе пластиковых карт.

4 Исследовать свойства алгоритмов электронной цифровой подписи.

5 Приобрести навыки построения криптографических протоколов и программ для организации систем защиты информации.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.1 Основные принципы построения банковской платежной системы

Электронной платежной системой называют совокупность методов и реализующих их субъектов, обеспечивающих в рамках системы использование банковских пластиковых карт в качестве платежного средства. Предприятия торговли и сервиса и отделения банков, принимающие карту в качестве платежного инструмента, образуют приемную сеть точек обслуживания карты.

С организационной точки зрения ядром платежной системы является ассоциация банков, объединенная договорными обязательствами, предприятия торговли и сервиса, а также специализированные организации, осуществляющие техническую поддержку обслуживания карт: процессинговые и коммуникационные центры, центры технического обслуживания и т. п.

Обобщенная схема функционирования электронной платежной системы представлена на рисунке 2.1, где к/с – корреспондентский счет.

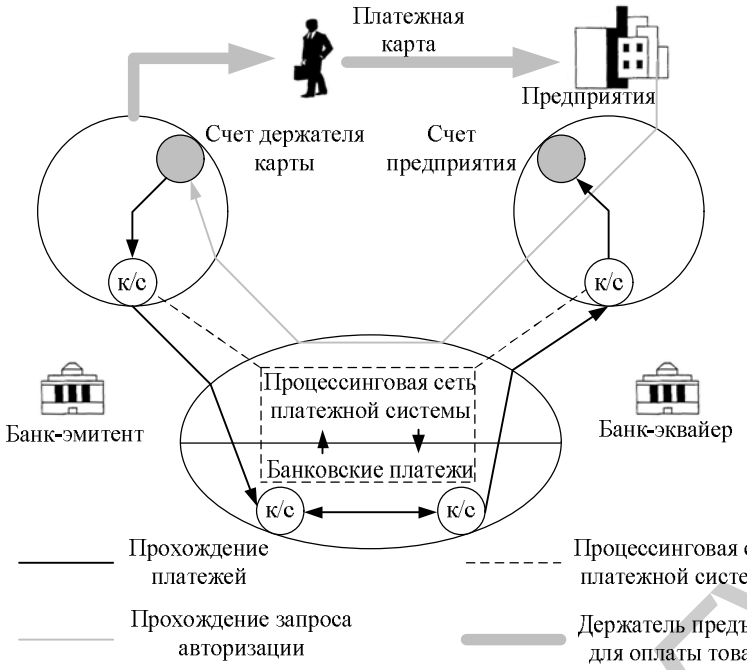

Рисунок 2.1 – Обобщенная схема функционирования электронной платежной системы

Банк, заключивший соглашение с платежной системой и получивший соответствующую лицензию, может выступать в двух качествах: как банк-эмитент и как банк-эквайер. Банк-эмитент выпускает пластиковые карты и гарантирует выполнение финансовых обязательств, связанных с использованием этих карт как платежных средств. Банк-эквайер обслуживает предприятия торговли и сервиса, принимающие к оплате карты как платежные средства, а также принимает эти платежные средства к обналичиванию в своих отделениях и через принадлежащие ему банкоматы.

Процессинговый центр представляет собой специализированную сервисную организацию, которая обеспечивает обработку поступающих от банков-эквайеров или непосредственно из точек обслуживания запросов на авторизацию и протоколов транзакций – фиксируемых данных о произведенных посредством карт платежах и выдачах наличными.

2.2 Радиоэлектронная идентификация

Идентификатор – некоторое устройство или признак, по которому определяется объект. Идентификаторами могут быть строка символов, карточка со штрих-кодом, различные бесконтактные радиотеги, proximity-карты, брелоки touch memory, магнитные карточки, смарт-карты, изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони и другие физические признаки.

Идентификация – процесс распознавания объекта или субъекта по его идентификатору. Идентификатор объекта предъявляется считывателю, который считывает и передает в систему его индивидуальный код для проведения процедуры распознавания.

Широкое распространение получили средства электронной идентификации – бесконтактные средства радиочастотной идентификации и смарт-карты. Объектом или субъектом идентификации могут быть человек, животное, транспортное средство, оборудование, контейнер с грузом, изделие в процессе производства, товар, ценные предметы.

Для достоверной идентификации субъекта – пользователя компьютерной системы или сети – необходимо провести не только процедуру собственно идентификации, но и выполнить проверку подлинности данного пользователя. Если пользователь имеет идентификатор, зарегистрированный в системе или сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным. Прежде чем получить доступ к ресурсам компьютерной системы или сети, пользователь проходит процесс первичного взаимодействия с компьютерной системой, который включает процедуры идентификации и аутентификации.

Для подтверждения своей подлинности пользователь может предъявлять системе разные сущности. В зависимости от предъявляемых пользователем сущностей процессы аутентификации могут быть разделены на следующие категории:

– на основе знания чего-либо (примерами могут служить пароль, персональный идентификационный код PIN, а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа «запрос–ответ»);

– на основе обладания чем-либо (обычно это магнитные карты, смарт-карты, сертификаты и устройства touch memory);

– на основе каких-либо неотъемлемых характеристик (эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя – голоса, радужной оболочки и сетчатки глаза, отпечатков пальцев, геометрии ладони и др.).

2.3 Структурная и функциональная организация радиоэлектронного идентификатора

В общем случае радиоэлектронный идентификатор представляет собой радиоэлектронное устройство, обладающее уникальным идентификатором, предъявляемым в системе идентификации по определенным правилам, часто способное доказать свою подлинность, а также содержащее механизмы контроля доступа к своим функциям.

Обобщенная структурная схема радиоэлектронного идентификатора представлена на рисунке 2.2.

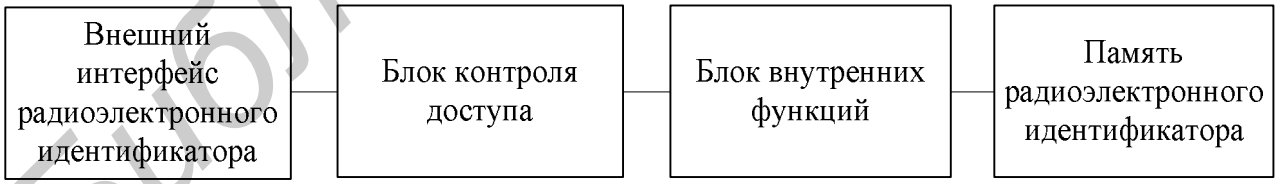

Рисунок 2.2 – Обобщенная структурная схема радиоэлектронного идентификатора

Интерфейс взаимодействия обеспечивает возможность обмена данными радиоэлектронного идентификатора с системой идентификации в соответствии с

7-уровневой моделью взаимодействия открытых систем (OSI/ISO). Наиболее распространенными являются следующие интерфейсы:

– USB (электронные брелоки, eTocken, некоторые смарт-карты и т. д.);

– ISO 7816 (базовый интерфейс для смарт-карт);

– радиочастотные интерфейсы стандартов ISO 14443, ISO 15693, ISO 18000, ISO 18092, ISO 10536 (устройства радиочастотной идентификации (RFID)).

Блок контроля доступа служит для разграничения доступа к внутренним функциям и ресурсам радиоэлектронного идентификатора. Часто основной функцией этого блока является поддержка процедуры верификации владельца идентификатора (обычно на базе пароля или PIN-кода).

Блок внутренних функций реализует следующие, необходимые для осуществления протоколов проверки подлинности владельца, идентификации и аутентификации идентификатора, обеспечения секретности и имитостойкости данных, а также для контроля ошибок функционирования самого индентификатора, процедуры:

– криптографическое преобразование информации;
– доступ к памяти;
– верификация;
– обеспечение атомарности функционирования идентификатора;
– генерация случайных последовательностей и т. д.

Память радиоэлектронного идентификатора чаще всего содержит уникальный идентификатор, данные и секретные параметры, используемые описанными выше функциями.

2.4 Осуществление банковских транзакций при помощи смарт-карт на основе электронной цифровой подписи

Электронная цифровая подпись (ЭЦП) данных используется в процедурах статической и динамической аутентификации карты. Необходимость применения асимметричных алгоритмов шифрования в этих процедурах вызвана тем, что

терминал не должен обладать секретами карты (симметричное шифрование всегда подразумевает знание участниками информационного обмена общего секрета).

Для того чтобы терминал мог проверить цифровую подпись некоторых данных карты, необходимо создание так называемой PKI-инфраструктуры (PKI – Public Key Infrastructure). В стандарте EMV PKI-инфраструктура в общем случае имеет трехуровневую древовидную структуру.

На первом уровне находится центр сертификации платежной системы. Центр сертификации генерирует пары закрытых и открытых ключей и рассылает открытые ключи центра сертификации обслуживающим банкам для загрузки в терминалы платежной системы.

На втором уровне дерева PKI-инфраструктуры находятся центры сертификации банков-эмитентов, являющихся участниками платежной системы. Эти центры также генерируют пары открытых и закрытых ключей и получают в центре сертификации платежной системы сертификаты своих открытых ключей. Сертификат открытого ключа представляет собой реквизиты открытого ключа, включая сам открытый ключ, его срок действия, идентификатор держателя и т. п., подписанные одним из закрытых ключей центра сертификации платежной системы.

На третьем уровне PKI-инфраструктуры располагаются открытые и закрытые ключи карт эмитента. Закрытые ключи, как им и положено, хранятся в защищенной области памяти МПК и недоступны внешним для карты программам. Открытые ключи сначала сертифицируются в центре сертификации банка-эмитента. Это означает, что открытые ключи вместе с их реквизитами подписываются одним из закрытых ключей эмитента карты. Далее сертификат открытого ключа карты располагается в памяти МПК и доступен терминалу при чтении им данных карты.

Цифровая подпись каких-либо данных на ключе карты проверяется терминалом следующим образом. Сначала терминал читает с карты сертификаты открытых ключей эмитента и карты, а также подписанные картой данные. Далее с помощью открытого ключа системы терминал проверяет правильность сертификата (правиль-

ность подписи и формата) ключа эмитента. Тем самым терминал устанавливает для себя факт того, что в схеме используется ключ, выданный платежной системой ее участнику. После доказательства правильности сертификата открытого ключа эмитента терминал с помощью этого ключа проверяет правильность сертификата открытого ключа карты, устанавливая таким образом, что в схеме используется карта, выданная участником платежной системы, и этот участник платежной системы (эмитент) был уполномочен последней на выпуск этой карты. Если подпись верна, считается, что карта успешно прошла процедуру статической аутентификации.

Статическая аутентификация карты в действительности аутентификацией карты не является, а является лишь средством обеспечения целостности некоторых критичных для приложения карты данных.

Динамическая аутентификация карты обеспечивает не только проверку целостности критичных данных карты, но и подтверждение подлинности карты. Трехуровневая структура PKI изображена на рисунке 2.3.

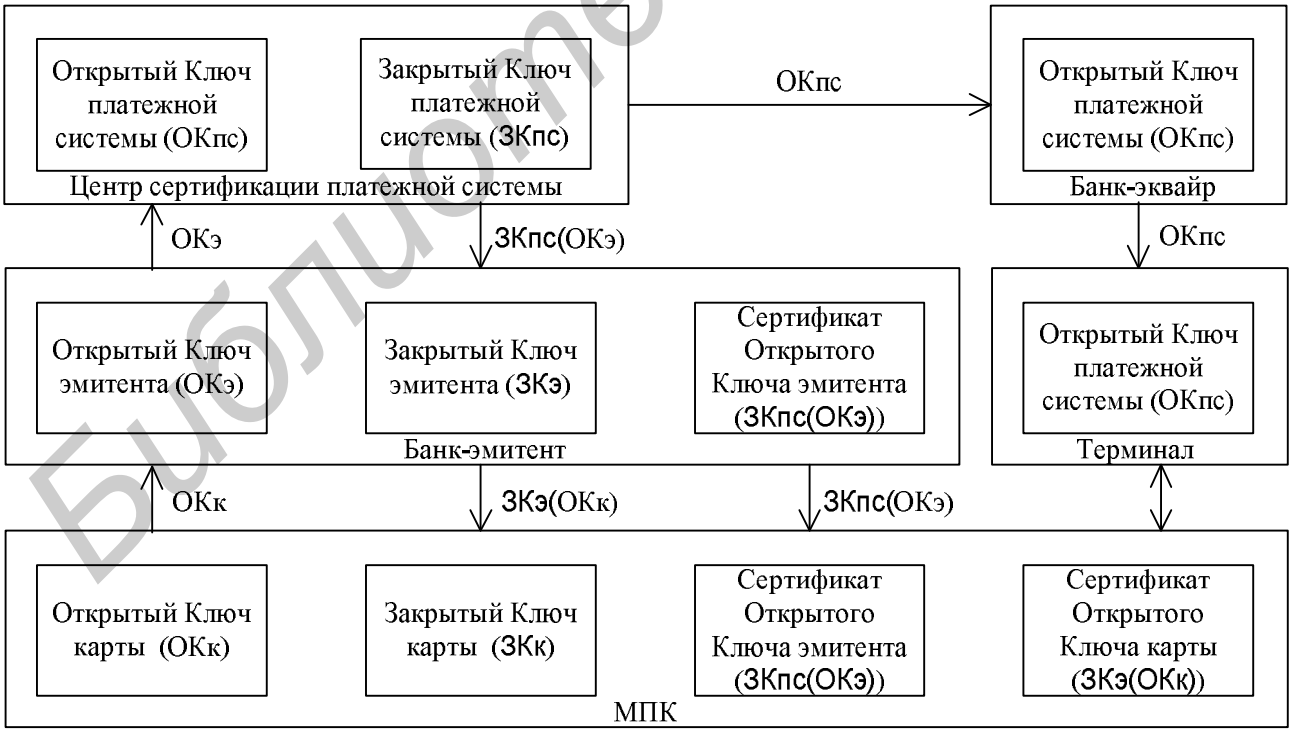

Рисунок 2.3 – Трехуровневая система PKI

Как видно из рисунка, в методах динамической аутентификации используется пара открытый/закрытый ключ самой карты.

Суть методов состоит в том, что терминал генерирует случайное число, передаваемое карте вместе с некоторыми другими данными для подписи. Карта возвращает терминалу подписанные данные и в случае, если терминал устанавливает, что подпись полученных от карты данных, а также сертификаты ключа эмитента и ключа карты оказываются правильными, он делает вывод о том, что карта подлинная. Действительно, поскольку карта заранее не знала предложенного ей терминалом случайного числа, факт правильности подписи означает, что подпись была сделана картой. Это в свою очередь означает, что карта является носителем секрета – закрытого ключа (с помощью которого была создана подпись), соответствующего открытому ключу.

Отметим, что структура сертификата открытого ключа карты такова, что при проверке этого сертификата автоматически выполняется статическая аутентификация карты, то есть проверяется целостность критичных данных карты.

2.5 Стойкость системы защиты банковской информации на основе платежных микропроцессорных карт

2.5.1 Основные виды угроз и методы защиты

Угрозы информационной безопасности банковских систем на основе МПК принято делить на две группы: угрозы с точки зрения эмиссии карт и угрозы с точки зрения обслуживания карт.

Угрозы с точки зрения эмиссии карт. К основным угрозам этой группы относятся: украденные/потерянные карты, неполученные карты, подделанные карты, CNP-мошенничество, кража персональных данных держателя карты.

Угрозы с точки зрения обслуживания карт. Основные виды мошенничества этой группы: повторный ввод операции, изменение содержимого слипов, перехват

счета торгового предприятия, использование отчетности торгового предприятия, мошенничества в банкоматах, угрозы физической безопасности карт.

Для борьбы с перечисленными выше угрозами используют комплексный подход, включающий следующие элементы защиты:

– утвержденную политику эмиссии карт, описывающую эмитируемые банком карточные продукты, их потребителей, процедуры обработки заявлений клиентов, доставки и выдачи карт, средства и системы защиты банка от злоумышленных действий, распределение ответственности между подразделениями банка, поведение персонала и руководства банка в случае обнаружения атак и т. п.;

– установку необходимых проверок в системах авторизации транзакций банка;

– поддержку стоп-листов скомпрометированных карт;

– систему мониторинга транзакций, позволяющих определить подозрительные транзакции;

– предоставление платежной системе отчетности о случаях мошенничества по картам банка;

– работу с клиентами банка.

Более подробно элементы защиты включают:

– блокировку карты в системе эмитента с выдачей кода ответа о необходимости захвата карты (этот метод является эффективным для дебетовых карт, операции по которым проходят в режиме реального времени);

– помещение карты в стоп-листы (для карт, по которым возможны операции в режиме оффлайн);

– визуальную защиту карт;

– использование средств, позволяющих определить изменение «рисунка» операций по картам клиентов;

– более интенсивное использование онлайновых авторизаций;

– выпуск карт в заблокированном состоянии в статусе «новая карта» с определенными процедурами разблокировки карт;

– выдачу карт через ближайшие к клиенту отделения банка;

– использование специализированных курьерских служб;

– обучение персонала торговых предприятий и держателей карт;

– определение точек компрометации реквизитов карт;

– взаимную аутентификацию участников транзакции;

– невозможность отказа от транзакции для всех участников транзакции;

– поддержку на сервере предприятия средств защиты сетевого доступа;

– шифрование конфиденциальных данных;

– использование антивирусных программ;

– своевременное применение «заплат безопасности» в используемом программном обеспечении;

– использование процедур разграничения доступа;

– повышение уровня физической безопасности карты.

2.5.2 Атаки на систему и физическая безопасность

Понятие физической безопасности включает в себя противодействие внешнему вмешательству и способность засвидетельствовать такое вмешательство. Одним из элементов физической безопасности смарт-карты является компоновка микросхемы и ее соединений в модуле микросхемы, заключенном в эпоксидный заполнитель. Эта компоновка обеспечивает как защищенность от некоторых видов внешнего вмешательства, так и способность такое вмешательство засвидетельствовать. Через эпоксидный состав нельзя проникнуть, не разрушив его, и чтобы сделать это, нужно завладеть картой. При проникновении в модуль остаются следы, свидетельствующие о факте вмешательства.

Все атаки на микропроцессорную карту могут быть условно разделены на атаки программные и физические.

Программные атаки в свою очередь делятся на две категории: атаки, нацеленные на вскрытие применяемых картой криптографических алгоритмов, и

атаки, использующие слабые места реализации программ, поддерживаемых картой.

Физические атаки также делятся на две категории: атаки проникающие и непроникающие.

Проникающие атаки требуют проникновения в тело микросхемы с целью ее обследования и последующего воспроизведения компоновки отдельных модулей чипа (модулей памяти, процессора и сопроцессоров, шин данных и адресов). Проникающие атаки требуют использования лабораторного оборудования, отнимают много времени на свою реализацию и по указанным причинам являются дорогостоящими.

Непроникающие атаки можно разделить на атаки:

– основанные на анализе времени, необходимого для выполнения криптографической операции;

– основанные на анализе потребления картой энергии;

– основанные на использовании ошибок (реакции чипа на изменение внешних условий его использования: колебаний подаваемого на него напряжения и тактовой частоты, изменения температуры отдельных компонентов чипа, облучения чипа светом или пучком ионов, воздействия на чип электромагнитного поля).

Для борьбы с описанными видами атак поставщики микросхем разработали большое количество контрмер. К наиболее универсальным контрмерам относятся:

– датчики и фильтры контроля условий работы микросхемы (к таким датчикам и фильтрам относятся световые и температурные датчики, а также фильтры, сглаживающие броски напряжения и изменения тактовой частоты);

– шифрование данных всех видов памяти (ROM, EEPROM, RAM) для предотвращения возможности анализа содержимого памяти;

– шифрование данных, передаваемых в шинах адресов и данных;

– использование модуля управления памятью для разделения приложений от операционной системы, шифрования данных, хранящихся в памяти EEPROM и RAM, и управления доступом к различным приложениям карты;

– средства борьбы с атаками, основанными на измерении по излучению микросхемы потребляемой ею энергии: камуфляжное излучение или, наоборот, уменьшение излучения за счет специальных фильтров; переменная логика выполнения одной и той же программы;

– использование специального дизайна процессора;

– использование специальных криптографических сопроцессоров;

– использование специального аппаратного генератора случайных чисел, применяемого для генерации ключей;

– использование активных средств защиты от проникающих атак.

2.5.3 Атаки на алгоритмы ЭЦП

Одним из методов защиты информации в банковских системах является использование инфраструктуры открытых ключей на базе микропроцессорных карт (пункт 2.4). Основой данной инфраструктуры является использование протоколов идентификации и аутентификации при помощи цифровых сертификатов, формируемых с использованием ассиметричных алгоритмов криптографического преобразования информации. Указанные алгоритмы используются для реализации протоколов статической и динамической аутентификаций карты в режиме оффлайн. Основным фундаментом организации протоколов аутентификации в системе являются алгоритмы проверки и выработки электронной цифровой подписи (ЭЦП). Поэтому криптографические свойства используемых в системе алгоритмов ЭЦП оказывают непосредственное влияние на уровень безопасности оффлайновых транзакций.

В банковской системе стандарта EMV приняты два основных алгоритма проверки и выработки ЭЦП: на базе алгоритма RSA и на базе операций над группами точек эллиптических кривых. Основой криптостойкости указанных алгоритмов ЭЦП является сложность решения задач факторизации больших чисел (модуля n в RSA) и дискретного логарифмирования (разложение произведения kP в группе точек эллиптической кривой).

Криптоанализ RSA

Элементарные атаки. Известны несколько видов атак, связанных с неправильным использованием алгоритма RSA: неправильная генерация простых чисел p и q, использование общего модуля n, атака на подпись RSA в схеме с нотариусом, малые значения секретной и открытой экспонент и т. д. Снизить эффективность указанных атак можно путем соблюдения нескольких правил:

– p и q не должны быть слишком близки друг к другу, иначе можно будет их найти, используя метод факторизации Ферма;

– для каждого пользователя должен использоваться свой модуль $n = pq$;

– при подписи добавлять в сообщение некоторое случайное число;

– использовать достаточно большие экспоненты открытого и закрытого ключей e и d. Если n имеет размер 1024 бита, необходимо, чтобы число d было не менее 256 бит длиной. С целью повышения скорости криптопреобразований рекомендовано использовать $e = 2^{16} + 1 = 65537$.

Атаки, связанные с факторизацией модуля n. Факторизация – разложение данного натурального числа на простые множители. Существование и единственность (с точностью до порядка следования множителей) такого разложения следуют из основной теоремы арифметики. В отличие от задачи распознавания простоты числа факторизация предположительно является сложной задачей.

В зависимости от сложности алгоритмы факторизации можно разбить на две группы. Первая группа – экспоненциальные алгоритмы, сложность которых экспоненциально зависит от длины входящих параметров (то есть от длины самого числа в бинарном представлении). Вторая группа – субэкспоненциальные алгоритмы, для обозначения сложности которых принята L-нотация:

$$L_N(\alpha, c) = O(\exp((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha})),$$

где N – число, подлежащее факторизации, $0 < \alpha < 1$ и c – некоторые константы.

Существование алгоритма факторизации с полиномиальной сложностью на классическом компьютере является одной из важных открытых проблем современной теории чисел. В то же время факторизация с полиномиальной сложностью возможна на квантовом компьютере с помощью алгоритма Шора.

Экспоненциальные алгоритмы:

– перебор возможных делителей – наиболее тривиальный алгоритм факторизации с вычислительной сложностью $O\left(N^{1/2}\right)$;

– ρ-алгоритм Полларда с вычислительной сложностью $O\left(N^{1/4}\right)$;

– $\rho-1$-алгоритм Полларда;

– $\rho+1$-алгоритм Уильямса;

– метод квадратичных форм Шенкса с вычислительной сложностью $O\left(N^{1/4}\right)$;

– метод Лемана.

Субэкспоненциальные алгоритмы:

– алгоритм Диксона с вычислительной сложностью $L_N\left(1/2,\ 2\sqrt{2}\right)$;

– метод непрерывных дробей с вычислительной сложностью $L_N\left(1/2,\ \sqrt{2}\right)$;

– метод квадратичного решета с вычислительной сложностью $L_N\left(1/2,\ 1\right)$;

– метод эллиптических кривых с вычислительной сложностью $L_N\left(1/2,\ \sqrt{2}\right)$, где ρ – наименьшее простое, которое делит N;

– решето числового поля: общий метод решета числового поля со сложностью $L_N\left(1/3,\ (64/9)^{1/3}\right)$ и специальный метод решета числового поля со сложностью $L_N\left(1/3,\ (32/9)^{1/3}\right)$.

Перебор делителей. Алгоритм факторизации или тестирования простоты числа путем полного перебора всех возможных потенциальных делителей.

Обычно перебор делителей заключается в переборе всех целых (как вариант: простых) чисел от двух до квадратного корня из факторизуемого числа n и в вычислении остатка от деления n на каждое из этих чисел. Если остаток от деления

на некоторое число m равен нулю, то m является делителем n. В этом случае либо n объявляется составным, и алгоритм заканчивает работу (если тестируется простота n), либо n сокращается на m и процедура повторяется (если осуществляется факторизация n). По достижении квадратного корня из n и невозможности сократить n ни на одно из меньших чисел n объявляется простым.

ρ-алгоритм Полларда. ρ-алгоритм Джона Полларда служит для факторизации целых чисел. Он основан на том, что вычисляется некий многочлен степени не выше второй от начального числа $X - f(X)$.

Алгоритм разложения на множители числа N:

Шаг 1 Выбирается многочлен $f(x)$ с целочисленными коэффициентами, степени не выше двух. Обычно берется многочлен вида $y = \left(x^2 + c\right) \bmod N$.

Шаг 2 Случайно выбирается $x_0 = y_0$; $x_0 = y_0$ меньше N.

Шаг 3 Вычисляются значения $x_i = f\left(x_{i-1}\right) \bmod N$, $y_i = f\left(f\left(y_{i-1}\right)\right) \bmod N$.

Шаг 4 Находится $d = \left(\left|x_i - y_i\right|,\ N\right)$.

Шаг 5 Если $d = 1$, происходит переход на «Шаг 3», если $d = N$, происходит остановка – факторизацию провести не удалось. Если $1 < d < N$, то найдено разложение числа N.

Факторизация Ленстры с помощью эллиптических кривых. На практике часто используется для выявления (отбрасывания) небольших простых делителей числа. Если полученное после работы алгоритма число все еще является составным, то остальные сомножители – большие числа. При увеличении количества кривых шансы найти простой сомножитель возрастают, но зависимость количество цифр числа – количество эллиптических кривых экспоненциальна.

Дано составное целое нечетное число N. Нужно найти его нетривиальный делитель d, $1 < d < N$.

Случайным образом выбирается эллиптическая кривая $E: y^2 = x^3 + ax + b$, где a и $b \in Z$, и некоторая точка $P = (x, y)$ на ней. Если попытка разложения

окажется неудачной, следует взять другие E и P и повторить алгоритм сначала.

Шаг 1 Выбирается целое число k, делящееся на степени малых простых чисел (не больших некоторого B), не превосходящих C, то есть $k = \prod_{l \le B} l^{\alpha_i}$, где $\alpha_i = \lfloor \log_l C \rfloor$.

Шаг 2 Вычисляется произведение $k \cdot P$ в группе точек эллиптической кривой.

Вычисления проводятся до тех пор, пока при попытке найти число, обратное к $2y$, не появляется число, не взаимно простое с N. Это произойдет при таком $k = k_1$, что $k_1 \cdot P = O$, то есть порядок P в группе E по модулю N является делителем k_1.

Шаг 3 При применении алгоритма Евклида вместо обращения знаменателя получаем нетривиальный НОД этого знаменателя и числа N. Он и будет собственным делителем числа N.

Вычисление дискретного логарифма в группе точек эллиптической кривой

Пусть $G = \langle G, \cdot \rangle$ – конечная мультипликативная группа, a и α – элементы группы G, n есть порядок элемента α. Натуральное число x называется дискретным логарифмом элемента a при основании α, если $\alpha^x = a$, где $0 \le x \le n$.

Проблема дискретного логарифмирования заключается в том, что необходимо найти дискретный логарифм x данного элемента $a = \alpha^x$ при основании α.

В аддитивной интерпретации рассматривается аддитивная группа G с элементами A и P при известном порядке N элемента P. Натуральное число k, $0 \le k \le N$ называется дискретным логарифмом элемента A при основании P, если $k \cdot P = A$.

Все известные алгоритмы для решения этих проблем (при соответственно выбранных группе G и элементе б (или P)) для мультипликативной группы конечного поля или группы точек эллиптической кривой субэкспоненциальны, т. е. число выполняемых ими операций оценивается как $2^{\log^C n}$, где $C > 0$ – некоторая

константа, а n – порядок группы. Для некоторых групп даже порядка $2^{200} – 2^{300}$ сложность дискретного логарифмирования слишком велика для современной (и ожидаемой в ближайшем будущем) вычислительной техники, и на этом факте основана значительная часть криптографии с открытым ключом. Приведем два алгоритма дискретного логарифмирования, в качестве группы возьмем аддитивную группу – группу точек эллиптической кривой.

Алгоритм «большой шаг – малый шаг»

Пусть $G = \langle G, + \rangle$ – конечная группа точек эллиптической кривой, A и P – элементы этой группы, N – порядок элемента P, $k \cdot P = A$.

Тогда число k можно найти, выполнив не более чем $2(\sqrt{N} + \log_2 N) - 1$ операций сложения в группе G.

Доказательство. Полагаем $r = \lfloor \sqrt{N} \rfloor + 1$. Рассмотрим ряды

$$0 \cdot P = O,\ 1 \cdot P,\ 2 \cdot P, \ldots,\ (r-1) \cdot P;$$

$$A,\quad A + (1 \cdot (-r)) \cdot P,\ A + (2 \cdot (-r)) \cdot P, \ldots,\ A + ((r-1) \cdot (-r)) \cdot P.$$

Если уравнение $k \cdot P = A$ разрешимо относительно k, то (учитывая, что для любого целого x можно указать целые числа s и t такие, что $x \equiv (sr + t) \bmod n$, где n, r – натуральные числа, $r^2 \geq n$, $0 \leq s < r$, $0 \leq t < r$) представим k в виде $k \equiv (sr + t) \bmod N$.

Так как N есть порядок элемента P, то $k \cdot P = (sr + t) \cdot P = A$ в том и только том случае, когда $t \cdot P = A + (-sr) \cdot P$, то есть когда найдется элемент второго ряда, совпадающий с некоторым элементом первого ряда.

При вычислении элементов первого ряда потребуется выполнить не более $r - 2$ сложений в группе G. Для вычисления $(-r) \cdot P = (N - r) \cdot P$ (учитывая, что для вычисления кратного $n \cdot m$, где m – элемент некоторого кольца, а n – натуральное число, достаточно выполнить не более $2\lfloor \log_2 n \rfloor$ операций сложения) потребуется

выполнить не более $2\log_2 N$ умножений. Не более чем $r-1$ сложений потребуется для вычисления всех членов второго ряда.

Таким образом, общее число операций умножения для решения уравнения $k \cdot P = A$ не превосходит $2r - 3 + 2\log_2 N \le 2(\sqrt{N} + 2\log_2 N) - 1$.

Алгоритм для групп составных порядков

Пусть $G = \langle G, + \rangle$ – конечная группа (можно считать, что это группа точек эллиптической кривой), A и P – элементы этой группы, N – порядок элемента P, $k \cdot P = A$. И пусть, кроме того, число N – составное:

$$N = r_1 \cdot r_2,\ 1 < r_1 < N,\ 1 < r_2 < N.$$

Тогда дискретный логарифм элемента A по основанию P можно вычислить, выполнив не более чем $2\left(\sqrt{r_1} + \sqrt{r_2}\right) + 6\log_2 r_1 r_2 + \log_2 r_1 - 1$ операций сложения в группе G.

Доказательство. Заметим, что любое целое число x, $0 \le x < n$ однозначно представляется в виде

$$k = r_2 \cdot l_1 + m_1;\ l_1, m_1 \in Z,\ 0 \le l_1 < r_1,\ 0 \le m_1 < r_2.$$

Равенство $k \cdot P = A$ можно записать в виде $(r_2 \cdot l_1 + m_1) \cdot P = A$.

Умножим обе части этого равенства на число r_1 и с учетом того, что $N = r_1 \cdot r_2$ и $N \cdot P = O$, получим $(r_1 \cdot m_1) \cdot P = r_1 \cdot A$.

Обозначив $P_1 = r_1 \cdot P$, $A_1 = r_1 - 1 \cdot A$, получим более удобное представление $m_1 \cdot P_1 = A_1$.

Легко проверить, что порядок точки P_1 равен r_2. Значение m_1 как дискретный логарифм A_1 по основанию P_1 можно вычислить, выполнив не более чем $2(\sqrt{r_1} + \log_2 r_1) - 1$ операций сложения в группе G.

Прибавляя $(-m_1) \cdot P$ к обеим частям равенства $(r_2 \cdot l_1 + m_1) \cdot P = A$, получим $l_1 \cdot P_2 = A_2$, где $P_2 = r_2 \cdot P$, $A_2 = A + (-m_1) \cdot P$.

Аналогично предыдущему, l_1 можно вычислить при помощи не более чем за $2(\sqrt{r_1}+\log_2 r_1)-1$ операций сложения в группе G. Далее P_1, A_1, P_2, A_2 вычисляются соответственно не более чем за $2\log_2 r_1$, $2\log_2 r_1$, $2\log_2 r_2$, $1+2\log_2 t$ операций сложения в группе G.

3 МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

3.1 Аппаратно-программная модель банковской системы

Модель системы состоит из трех компонентов:

– программной модели системы (приложение с исполняемым файлом EMVSystem);

– вспомогательных библиотек для работы с RSA и криптоалгоритмами на базе эллиптических кривых, исполняемых в программной среде Maple – EMVRSATool.mpl и EMVECCTool.mpl соответственно;

– аппаратной части – карт-ридера и смарт-карты с апплетом банковского приложения стандарта EMV.

Структура модели представлена на рисунке 3.1.

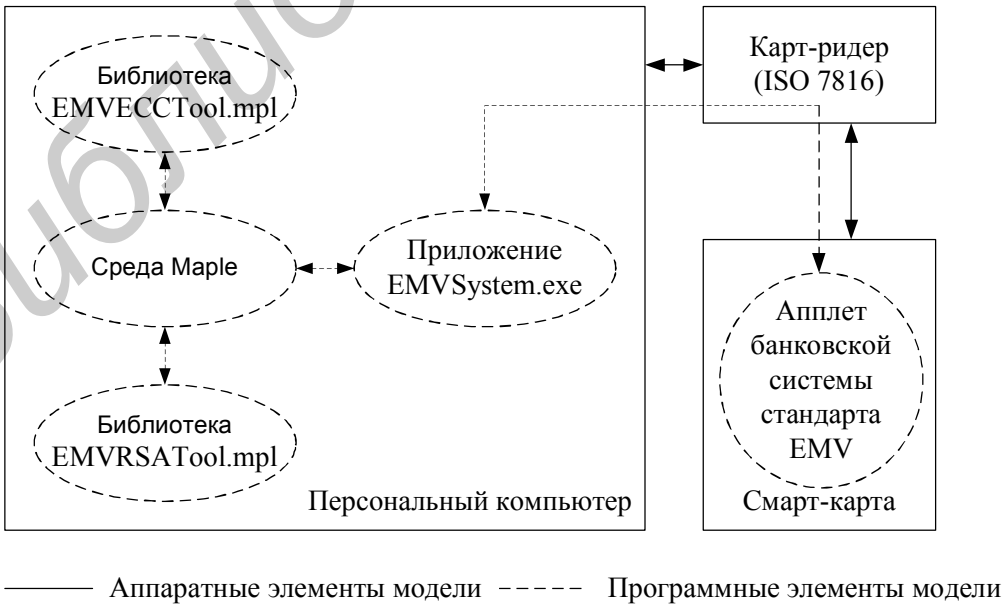

Рисунок 3.1 – Структура аппаратно-программной модели банковской системы

Приложение EMVSystem.exe является центральным элементом модели, функциональное назначение которого – взаимодействие (через карт-ридер) с апплетом смарт-карты, выполнение криптографических преобразований информации в соответствии с требованиями платежной системы EMV.

Апплет банковской системы стандарта EMV представляет собой программное обеспечение, функционирующее под управлением операционной системы смарт-карты и реализующее соответствующие протоколы аутентификации, обеспечения секретности и имитостойкости информации.

Библиотеки EMVRSATool.mpl и EMVECCTool.mpl при их использовании в программной среде Maple реализуют основные операции формирования и подготовки параметров криптоалгоритмов RSA и ECC, которые в свою очередь используются при моделировании работы системы в приложении EMVSystem.exe.

3.2 Формирование основных параметров криптоалгоритмов RSA и ECC в среде Maple

Формирование выполняется с помощью собственных процедур Maple, а также при помощи функций, реализованных в библиотеках EMVRSATool.mpl и EMVECCTool.mpl.

В библиотеке EMVRSATool.mpl реализовано исполнение следующих функций:

– генерация двух простых чисел p и q заданной размерности;

– формирование модуля, экспонент открытого и закрытого ключей;

– оценка вычислительной сложности факторизации модуля $N = p \cdot q$;

– факторизация модуля N с заданным временем ожидания методами, рассмотренными в пункте 2.5.3;

– формирование сигнатуры сообщения;

– преобразование информации в соответствии с алгоритмом RSA.

В библиотеке EMVECCTool.mpl реализовано исполнение следующих функций:

– формирование эллиптической кривой в соответствии с заданными параметрами: тип, поле, базис, порядок;

– выбор точки эллиптической кривой;

– формирование параметров алгоритма электронной цифровой подписи ECDSA;

– выработка электронной цифровой подписи;

– проверка электронной цифровой подписи;

– дискретное логарифмирование $A = k \cdot P$ в группе точек заданной эллиптической кривой, с заданным временем ожидания методами, рассмотренными в пункте 2.5.3.

Подробное описание и примеры использования выше описанных функций приведены в соответствующих файлах, прилагаемых к библиотекам.

3.3 Моделирование функционирования банковской системы

Моделирование осуществляется при помощи приложения EMVSystem.exe. Данное приложение состоит из шести основных модулей: «Центр сертификации», «Банк-эмитент», «Банк-эквайер», «Платежная карта», «Платежный терминал», «Настройки».

Каждый модуль приложения выполняет функции элементов системы в соответствии со своим названием. Модуль «Настройки» используется для выбора режима работы системы.

Каждый модуль представлен в виде таблицы (набора таблиц) и кнопок управления. Значения полей в таблицах формируются в программной среде Maple с использованием библиотек EMVRSATool.mpl и EMVECCTool.mpl, которые заносятся в соответствующие ячейки при помощи двойного щелчка левой клавишей мышки.

Графический интерфейс приложения представлен на рисунке 3.2.

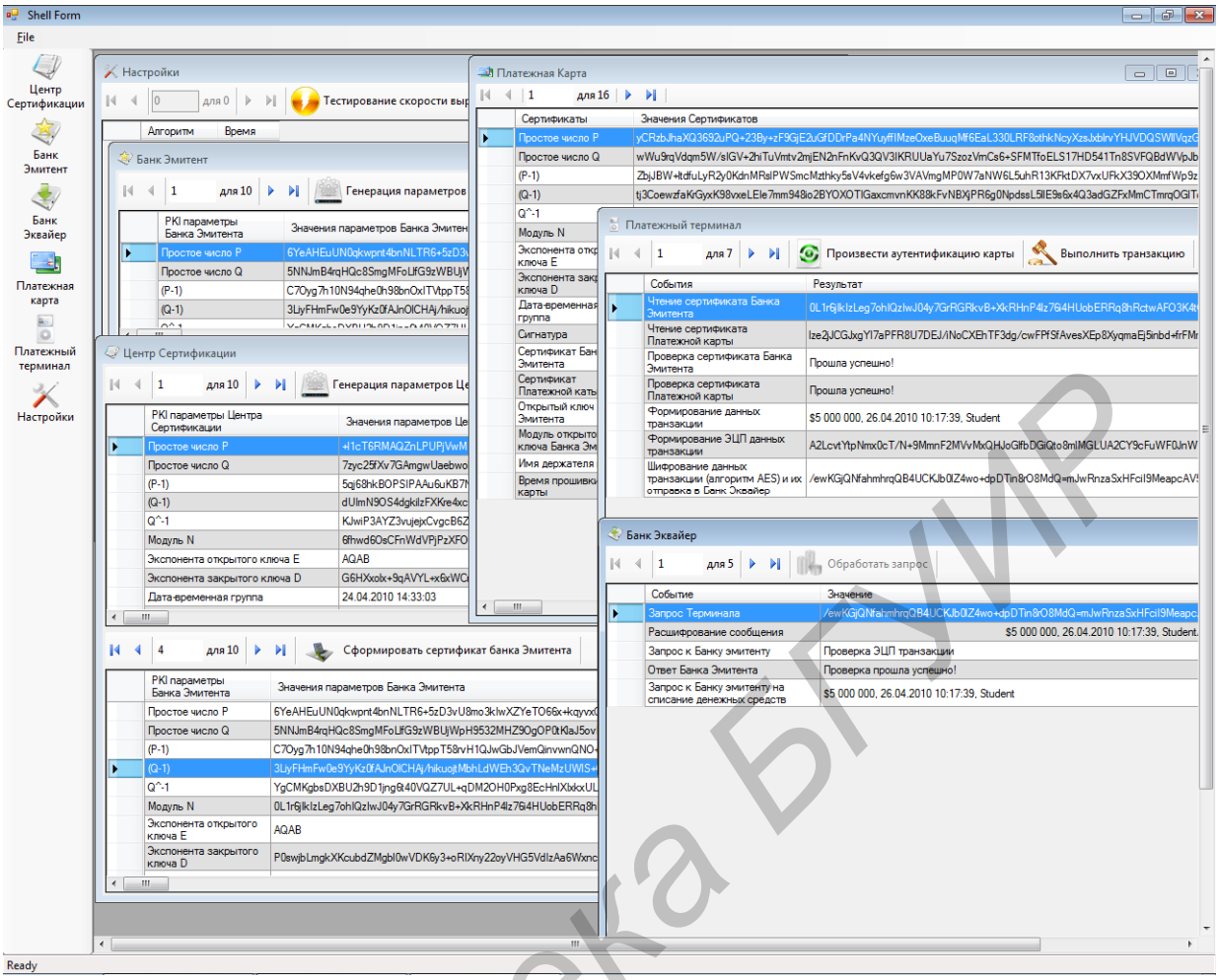

Рисунок 3.2 – Графический интерфейс приложения EMVSystem.exe

4 ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

4.1 Предварительное задание

На основе заданных трех пар простых чисел p и q сформируйте пары открытых и закрытых ключей для центра сертификации (алгоритм RSA), банка-эмитента и платежной карты соответственно. Сформируйте сертификаты открытых ключей системы и проведите алгоритм аутентификации платежной карты.

Исходные данные необходимо получить у преподавателя.

4.2 Ход выполнения работы

Формирование инфраструктуры открытых ключей

1 Используя функции библиотеки EMVRSATool.mpl, сформируйте сертификаты открытых ключей системы на базе алгоритма RSA.

2 С разрешения преподавателя подключите карт-ридер к ПК, вставьте в него карту и запустите приложение EMVSystem.exe.

3 Занесите сформированные сертификаты и ключи в соответствующие поля элементов системы.

4 Персонализируйте карту.

Моделирование транзакции

1 Откройте элемент «Платежный терминал».

2 Проведите динамическую аутентификацию карты.

3 Отправьте запрос в «Банк-эквайер» на списание средств со счета.

4 Проверьте валидность запроса.

Моделирование атаки и исследование криптостойкости алгоритмов ЭЦП

1 Откройте элемент «Платежный терминал», получите значение открытого ключа карты.

2 Используя функции библиотеки EMVRSATool.mpl, оцените сложность факторизации модуля.

3 Повторите пункт *Формирование инфраструктуры открытых ключей* с параметрами, заданными преподавателем.

4 Факторизуйте модуль различными методами.

5 Повторите пп. 1–3, используя функции библиотеки EMVECCTool.mpl для алгоритмов ЭЦП на базе эллиптических кривых.

6 Проведите процедуры дискретного логарифмирования различными методами.

7 Проанализируйте полученные результаты.

4.3 Расчетная часть

1 Исходные данные: число $N = p \cdot q$, где p и q – простые числа. Найдите эти числа методами, описанными в пункте 2.5.3. Значение N получите у преподавателя.

2 Исходные данные: несуперсингулярная кривая $Y^2 + XY = X^3 + X^2 + 1$ над полем $GF(2^5) = GF(2)(\alpha)$, где α – корень неприводимого многочлена $Z^5 + Z^2 + 1$, и базовая точка $P = (00101, 10110)$ этой кривой. Пусть $A = k \cdot P$. Вычислите константу k методами, описанными в пункте 2.5.3. Координаты точки A получите у преподавателя.

5 СОДЕРЖАНИЕ ОТЧЕТА

1 Формулировка цели работы.

2 Схемы ключевого пространства системы и протокола динамической аутентификации радиоэлектронного идентификатора.

3 Результаты моделирования.

4 Оценка результатов исследования, полученных в ходе моделирования.

5 Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

1 Дайте определение процессам идентификации и аутентификации, определите, в чем их различие.

2 Приведите обобщенную структурную схему радиоэлектронного идентификатора, поясните назначение ее структурных элементов.

3 Поясните основные принципы построения банковской платежной системы.

4 Поясните основные принципы организации инфраструктуры открытых ключей.

5 Приведите схему распределения ключевого пространства PKI.

6 Поясните процесс статической и динамической аутентификаций платежной карты, определите, в чем их различие.

7 Перечислите основные угрозы банковской платежной системы на базе платежных карт, поясните основные методы защиты от них.

8 Перечислите основные виды атак на физическую безопасность микропроцессорной карты.

9 Дайте оценку сложности факторизации чисел вида $N = p \cdot q$, где p и q – простые числа.

10 Дайте оценку сложности задачи дискретного логарифмирования в группе точек эллиптической кривой.

ЛИТЕРАТУРА

1 Дшхунян, В. Л. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В. Л. Дшхунян, В. Ф. Шаньгин. – М. : ООО «Издательство АСТ»: Издательство «НТ Пресс», 2004. – 695 с.

2 Марченко, А. В. Пластиковые деньги – Visa, MasterCard и другие / А. В. Маченко, С. В. Бочкарев. – М. : ЗАО «Олимп – Бизнес», 2006. – 240 с.

3 Полянская, О. Ю. Основы технологии PKI / О. Ю. Полянская, В. С. Горбатов. – М. : Горячая линия – Телеком, 2004. – 248 с.

4 Платежная система в Республике Беларусь // Банкаўскі веснік : спец. выпуск – №31/180. – 2001. – 53 с.

5 EMV 4.1. Спецификации микропроцессорных карт для платежных систем.

6 ISO 9797. Методы криптографической защиты данных.

7 ISO 9798. Информационная технология. Методы обеспечения безопасности. Аутентификация объектов.

8 ISO 9992. Сообщения между картой и терминалом.

9 ISO 10202. Карты финансовых транзакций.

Св. план 2010, поз. 71

Учебное издание

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ РАДИОЭЛЕКТРОННЫХ ИДЕНТИФИКАТОРОВ

Методические указания
к лабораторной работе по курсам
«Теория кодирования и защита информации»,
«Теория кодирования и основы криптологии»
для студентов радиотехнических специальностей
всех форм обучения

С о с т а в и т е л и:
Саломатин Сергей Борисович
Бильдюк Денис Михайлович

Редактор Т. П. Андрейченко
Корректор А. В. Тюхай
Компьютерная верстка А. В. Тюхай

Подписано в печать	Формат 60Ч84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л.
Уч.-изд. л. 1,5.	Тираж 150 экз.	Заказ 529.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6