**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ**

**УНИВЕРСИТЕТ ИМЕНИ В.И. ЛЕНИНА»**

Кафедра информационных технологий

**ЛАБОРАТОРНАЯ РАБОТА № 1**

**по дисциплине «Информатика»**

**на тему**

**«Электронная цифровая подпись как элемент защиты информации»**

Выполнил: **Прохоров М.В.**

студент группы 1-41

Вариант № **96**

Проверил: доцент кафедры информационных

технологий **Егорова Н.Е.**

**Иваново 2022**

**СОДЕРЖАНИЕ**

1 Основные понятия 3

2 История возникновения 4

3 Алгоритмы 5

3.1 Использование хеш-функций 5

3.2 Симметричная схема 6

3.3 Асимметричная схема 7

3.4 Перечень алгоритмов ЭП 9

4 Использование ЭП 11

Список литературы, использованной при выполнении работы 13

**1 Основные понятия**

Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП), Цифровая подпись (ЦП) позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в криптовалютной системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов и не может быть подделана с помощью обычного копирования.

ЭЦП — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Широко применяемая в настоящее время технология электронной подписи основана на асимметричном шифровании с открытым ключом и опирается на следующие принципы:

Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. Механизм генерации ключей строго определён и является общеизвестным. При этом каждому открытому ключу соответствует определённый закрытый ключ. Если, например, Иван Иванов публикует свой открытый ключ, то можно быть уверенным, что соответствующий закрытый ключ есть только у него.

Имеются надёжные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.

Если электронный документ поддается расшифровке с помощью открытого ключа, то можно быть уверенным, что он был зашифрован с помощью уникального закрытого ключа. Если документ расшифрован с помощью открытого ключа Ивана Иванова, то это подтверждает его авторство: зашифровать данный документ мог только Иванов, т.к. он является единственным обладателем закрытого ключа.

Однако шифровать весь документ было бы неудобно, поэтому шифруется только его хеш — небольшой объём данных, жёстко привязанный к документу с помощью математических преобразований и идентифицирующий его. Шифрованный хеш и является электронной подписью.

**2 История возникновения**

В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись», хотя они всего лишь предполагали, что схемы ЭЦП могут существовать.

В 1977 году Рональд Ривест, Ади Шамир и Леонард Адлеман разработали криптографический алгоритм RSA, который без дополнительных модификаций можно использовать для создания примитивных цифровых подписей.

Вскоре после RSA были разработаны другие ЭЦП, такие, как алгоритмы цифровой подписи Рабина, Меркле и другие.

В 1984 году Шафи Гольдвассер, Сильвио Микали и Рональд Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны модели атак на алгоритмы ЭЦП, а также предложена схема GMR, отвечающая описанным требованиям (Криптосистема Гольдвассер — Микали).

**3 Алгоритмы**

Существует несколько схем построения цифровой подписи:

* На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
* На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

**3.1 Использование хеш-функций**

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хеш. Для вычисления хеша используются криптографические хеш-функции, что гарантирует выявление изменений документа при проверке подписи. Хеш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хеш-функция.

Использование хеш-функций даёт следующие преимущества:

* Вычислительная сложность. Обычно хеш цифрового документа делается во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хеша являются более быстрыми, чем алгоритмы ЭП. Поэтому формировать хеш документа и подписывать его получается намного быстрее, чем подписывать сам документ.
* Совместимость. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хеш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.
* Целостность. Без использования хеш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Использование хеш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭП, поэтому хеш-функция может использоваться любая или не использоваться вообще.

В большинстве ранних систем ЭП использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы для атак с использованием открытого ключа (см. ниже), так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст. Чтобы избежать этого, вместе с цифровой подписью используется хеш-функция, то есть, вычисление подписи осуществляется не относительно самого документа, а относительно его хеша. В этом случае в результате верификации можно получить только хеш исходного текста, следовательно, если используемая хеш-функция криптографически стойкая, то получить исходный текст будет вычислительно сложно, а значит атака такого типа становится невозможной.

**3.2 Симметричная схема**

Симметричные схемы ЭП менее распространены, чем асимметричные, так как после появления концепции цифровой подписи не удалось реализовать эффективные алгоритмы подписи, основанные на известных в то время симметричных шифрах. Первыми, кто обратил внимание на возможность симметричной схемы цифровой подписи, были основоположники самого понятия ЭП Диффи и Хеллман, которые опубликовали описание алгоритма подписи одного бита с помощью блочного шифра. Асимметричные схемы цифровой подписи опираются на вычислительно сложные задачи, сложность которых ещё не доказана, поэтому невозможно определить, будут ли эти схемы сломаны в ближайшее время, как это произошло со схемой, основанной на задаче об укладке ранца. Также для увеличения криптостойкости нужно увеличивать длину ключей, что приводит к необходимости переписывать программы, реализующие асимметричные схемы, и в некоторых случаях перепроектировать аппаратуру. Симметричные схемы основаны на хорошо изученных блочных шифрах.

В связи с этим симметричные схемы имеют следующие преимущества:

* Стойкость симметричных схем ЭП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.
* Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных ЭП есть и ряд недостатков:

Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.

Из-за рассмотренных недостатков симметричная схема ЭЦП Диффи-Хелмана не применяется, а используется её модификация, разработанная Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объёма вычислений. Для преодоления проблемы «одноразовости» ключей используется генерация отдельных ключей из главного ключа.

**3.3 Асимметричная схема**

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом (табл.1).

Но в отличие от асимметричных алгоритмов шифрования, в которых шифрование производится с помощью открытого ключа, а расшифровка — с помощью закрытого (расшифровать может только знающий секрет адресат), в асимметричных схемах цифровой подписи подписание производится с применением закрытого ключа, а проверка подписи — с применением открытого (расшифровать и проверить подпись может любой адресат).

Общепризнанная схема цифровой подписи охватывает три процесса (см. рис. 1):

* Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
* Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
* Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

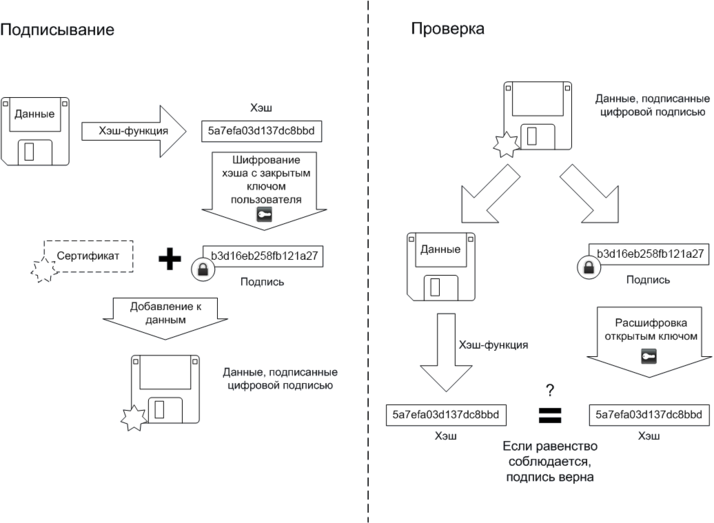
Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

* Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
* Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

Следует отличать электронную цифровую подпись от кода аутентичности сообщения (MAC).

*Таблица 1.* **Пример криптотекста с открытым ключом шифрования**

|  |  |  |
| --- | --- | --- |
| Криптотекст 1 | Криптотекст 2 | Криптотекст 3 |
| 1235267 | 5643452 | 1235267 |
| 3572651 | 3517289 | 3517289 |
| 4673956 | 4673956 | 4673956 |
| 3517289 | 3572651 | 3572651 |
| 7755628 | 7755628 | 7755628 |
| 5643452 | 1235267 | 5643452 |
| 8492746 | 8492746 | 8492746 |



**Рис. 1.** Схема, поясняющая алгоритмы подписи и проверки

**3.4 Перечень алгоритмов ЭП**

Асимметричные схемы (см. рис. 2):

* FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
* Схема Эль-Гамаля
* Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
* Российские стандарты электронной цифровой подписи (табл. 2): ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012 (основан на сложности вычисления дискретного логарифма в группе точек эллиптической кривой)

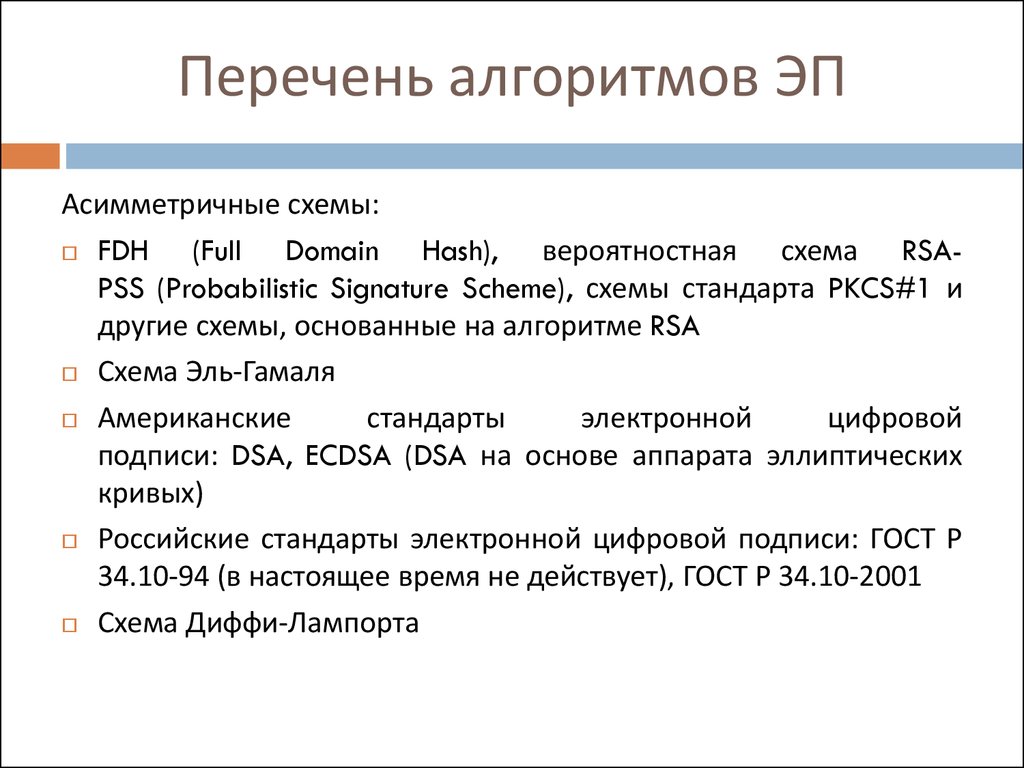
*Таблица 2.* **Российские стандарты электронной цифровой подписи**

|  |  |  |
| --- | --- | --- |
| Краткое наименование страны по [МК (ИСО 3166) 004-97](https://docs.cntd.ru/document/842501075) | Код страны  по [МК (ИСО 3166) 004-97](https://docs.cntd.ru/document/842501075) | Сокращенное наименование национального органа по стандартизации |
| Армения | AM | Минэкономики Республики Армения |
| Киргизия | KG | Кыргызстандарт |
| Россия | RU | Росстандарт |
| Таджикистан | TJ | Таджикстандарт |
| Туркмения | ТМ | Главгосслужба "Туркменстандартлары" |

* Евразийский союз: ГОСТ 34.310-2004[8] полностью идентичен российскому стандарту ГОСТ Р 34.10-2001
* Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
* Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 (в настоящее время не действует), СТБ 34.101.45-2013
* Схема Шнорра
* Pointcheval-Stern signature algorithm
* Вероятностная схема подписи Рабина
* Схема BLS (Boneh-Lynn-Shacham)
* Схема DLR (Donna-Lynn-Rivest)
* Схема GMR (Goldwasser-Micali-Rivest)

На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям:

* Групповая цифровая подпись
* Неоспоримая цифровая подпись
* «Слепая» цифровая подпись и справедливая «слепая» подпись
* Конфиденциальная цифровая подпись
* Цифровая подпись с доказуемостью подделки
* Доверенная цифровая подпись
* Разовая цифровая подпись



**Рис. 2.** Ассиметричные схемы

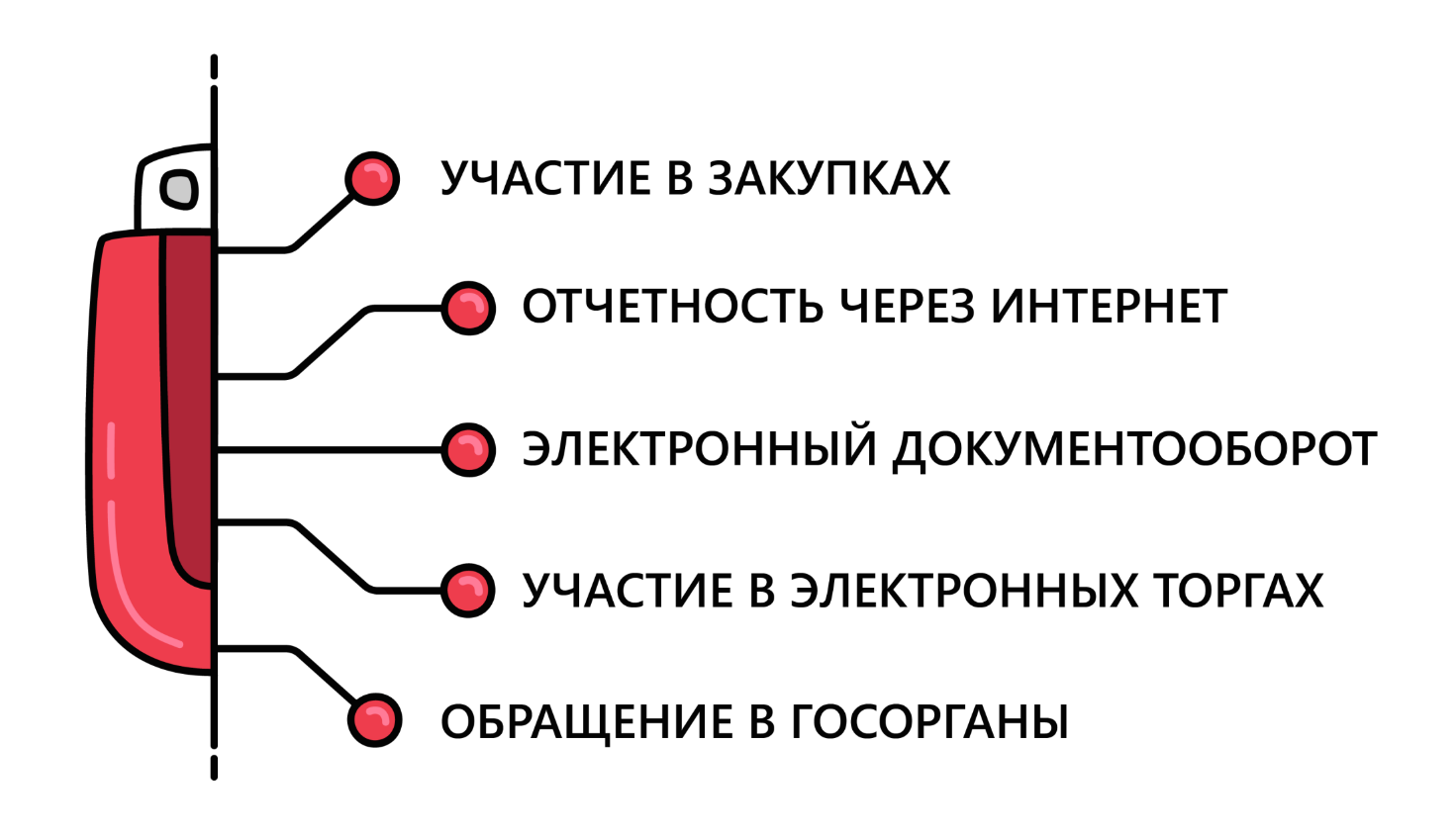
**4 Использование ЭП**

Использование ЭП предполагается для осуществления следующих важных направлений в электронной экономике (см. рис. 3):

* Полный контроль целостности передаваемого электронного платежного документа: в случае любого случайного или преднамеренного изменения документа цифровая подпись станет недействительной, потому как вычисляется она по специальному алгоритму на основании исходного состояния документа и соответствует лишь ему.
* Эффективная защита от изменений (подделки) документа. ЭП даёт гарантию, что при осуществлении контроля целостности будут выявлены всякого рода подделки. Как следствие, подделывание документов становится нецелесообразным в большинстве случаев.
* Фиксирование невозможности отказа от авторства данного документа. Этот аспект вытекает из того, что вновь создать правильную электронную подпись можно лишь в случае обладания так называемым закрытым ключом, который, в свою очередь, должен быть известен только владельцу этого самого ключа (автору документа). В этом случае владелец не сможет сформировать отказ от своей подписи, а значит — от документа.
* Формирование доказательств подтверждения авторства документа: исходя из того, что создать корректную электронную подпись можно, как указывалось выше, лишь зная закрытый ключ, а он по определению должен быть известен только владельцу-автору документа, то владелец ключей может однозначно доказать своё авторство подписи под документом. Более того, в документе могут быть подписаны только отдельные поля документа, такие как «автор», «внесённые изменения», «метка времени» и т. д. То есть, может быть доказательно подтверждено авторство не на весь документ.

Перечисленные выше свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

* Использование в банковских платежных системах;
* Электронная коммерция (торговля);
* Электронная регистрация сделок по объектам недвижимости;
* Таможенное декларирование товаров и услуг (таможенные декларации). Контролирующие функции исполнения государственного бюджета (если речь идет о стране) и исполнения сметных назначений и лимитов бюджетных обязательств (в данном случае если разговор идет об отрасли или о конкретном бюджетном учреждении). Управление государственными заказами;
* В электронных системах обращения граждан к органам власти, в том числе и по экономическим вопросам (в рамках таких проектов как «электронное правительство» и «электронный гражданин»);
* Формирование обязательной налоговой (фискальной), бюджетной, статистической и прочей отчетности перед государственными учреждениями и внебюджетными фондами;
* Организация юридически легитимного внутрикорпоративного, внутриотраслевого или национального электронного документооборота;
* Применение ЭЦП в различных расчетных и трейдинговых системах, а также Forex;
* Управление акционерным капиталом и долевым участием;
* ЭП является одним из ключевых компонентов сделок в криптовалютах.



**Рис. 3.** Использование ЭП

**СПИСОК ЛИТЕРАТУРЫ, ИСПОЛЬЗОВАННОЙ**

**ПРИ ВЫПОЛНЕНИИ РАБОТЫ**

1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — 173 с. — ISBN 978-5-89176-233-6
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — «Гелиос АРВ», 2002. — 480 с. — ISBN 5-85438-137-0
3. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004. — 432 с. — 3000 экз. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3
4. Б. А. Фороузан. Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций
5. Menezes A. J., Oorschot P. v., Vanstone S. A. Handbook of Applied Cryptography (англ.) — CRC Press, 1996. — 816 p. — (Discrete Mathematics and Its Applications) — ISBN 978-0-8493-8523-0
6. Мао В. Современная криптография: Теория и практика / пер. Д. А. Клюшина — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6