



www.volsu.ru

# ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

---

---

DOI: <https://doi.org/10.15688/NBIT.jvolsu.2018.2.1>

УДК 332(075.8)

ББК 65.422

## ВОПРОСЫ БЕЗОПАСНОСТИ СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

**Александра Владимировна Власенко**

Кандидат технических наук, доцент,  
заведующий кафедрой компьютерных технологий и информационной безопасности,  
Кубанский государственный технологический университет  
vlaskenko@kubstu.ru, alex\_vlaskenko@list.ru  
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

**Ирина Анатольевна Корх**

Аспирант кафедры компьютерных технологий и информационной безопасности,  
Кубанский государственный технологический университет  
aia2004@inbox.ru  
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

**Аннотация.** Наиболее востребованным направлением в современной банковской системе является внедрение и развитие систем дистанционного обслуживания. Цель работы – проанализировать систему дистанционного банковского обслуживания, определить нормативно-методические документы, регламентирующие вопросы информационной безопасности и варианты выполнения требований регуляторов. Результатом исследования следует считать подтверждение или опровержение актуальности проблемы.

**Ключевые слова:** банк, дистанционное банковское обслуживание, информационная безопасность, криптографическая защита, система ДБО.

Банковская система Российской Федерации в своей деятельности опирается на федеральное законодательство, а также от-

раслевые и межотраслевые стандарты, разрабатываемые Международным сообществом и Центральным Банком Российской

Федерации. Под термином дистанционного банковского обслуживания (ДБО) понимаются технологии по оказанию кредитными организациями услуг по удаленной передаче распоряжений клиентов (без визита в офис банка) с использованием различных каналов связи [1, с. 187; 4].

Информационная безопасность в системах «банк – клиент» осуществляется несколькими видами защиты. Подтверждение подлинности клиента производится путем применения электронной подписи. Канал передачи данных и сами данные шифруются. Для осуществления вышеописанных функций системы «банк – клиент» при любой про-

граммной реализации клиент предварительно должен сгенерировать и зарегистрировать в банке криптографические ключи, а также получить электронные цифровые сертификаты.

Кроме защиты передаваемых данных, персональные данные, попавшие в систему дистанционного банковского обслуживания, также нуждаются в защите [2, с. 231; 3].

В Российской Федерации вопросами информационной безопасности вообще и банковской сферы в частности занимаются несколько ведомств. Разделение нормативно-правового регулирования вопросов ДБО представлено в таблице.

### Нормативно-правовые документы, регулирующие вопросы ДБО

Законодательный уровень	Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (в ред. от 03.07.2016)
	Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (в ред. от 08.07.2016)
	Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. от 29.07.2017)
	«Кодекс Российской Федерации об административных правонарушениях» от 30.11.2001 № 195-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 30.06.2003 № 86-ФЗ)
	Федеральный закон от 07.02.2017 № 13-ФЗ «О внесении изменений в КоАП»; Федеральный закон от 07.02.2017 № 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»; изменения ст. 13.11. «Нарушение законодательства Российской Федерации в области персональных данных» вступают в силу с 01.07.2017
	Указ Президента РФ № 351 от 17.03.2008 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
	Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
	Постановление Правительства РФ от 16.04.2012 № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем»
	Постановление Правительства РФ от 13.06.2012 № 584 г. Москва «Об утверждении Положения о защите информации в платежной системе»
Нормативный уровень	Положение Банка России «О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России», утв. Банком России 23.06.1998 № 36-П (в ред. от 13.12.2001)
	Положение Банка России «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», утв. Банком России 09.06.2012 № 382-П (с изменениями от 14.08.2014) (вместе с «Порядком проведения оценки соответствия и документирования ее результатов» зарегистрировано в Минюсте РФ 14.06.2012 № 24575)
	Руководящие документы ФСТЭК России
	Руководящие документы ФСБ России

Методический уровень	Письмо Банка России «О средствах защиты информации, применяемых при обработке персональных данных» от 17.11.2011 № 015-16-9/4713
	Письмо Банка России «Об исполнении Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в части идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)» от 30.08.2006 № 115-Т
	Письмо Банка России «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)» от 27.04.2007 № 60-Т (в ред. от 13.04.2016)
	Письмо Банка России «О Рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети Интернет (включая интернет-банкинг)» от 05.08.2003 № 60-Т (в ред. от 13.04.2016)
	Письмо Банка России «О рисках при дистанционном банковском обслуживании» от 07.12.2007 № 197-Т
	Письмо Банка России «О средствах защиты информации, применяемых при обработке персональных данных» от 17.11.2011 № 015-16-9/4713

В соответствии с требованиями регуляторов разработчики программного обеспечения и банки имеют два направления к реализации системы защиты дистанционного обслуживания. Первое – использование сертифицированного программного средства криптографической защиты информации отечественного производства, второе – использование зарубежного программного обеспечения, не требующего сертификации.

В настоящее время при столь разнообразном российском рынке продуктов существует тенденция к использованию зарубежной криптографии, что обусловлено отсутствием сертификации данных модулей и отсутствием технических регламентов работы с СДБО. Из письма Центрального Банка РФ: «...до выпуска документов, обеспечивающих выполнение требований законодательства, считаем возможным применение для обеспечения безопасности персональных данных при их обработке в информационных системах встроенных защитных мер, сертифицированных СЗИ, а также средств защиты, не включенных в Единый перечень товаров, к которым применяются запреты или ограничения на ввоз или вывоз государствами-участниками таможенного союза в рамках Евразийского экономического сообщества в торговле с третьими странами» [5].

Динамика развития банковской отрасли показывает, что системы ДБО актуальны и востребованы бизнес-сообществом. Использовать зарубежную криптографию удобно, но работа с ней не попадает под Российское законодательство по защите информации, следовательно, все требования банков носят рекомендательный характер и повышается риск компрометации ключей. Российская криптография описана, но требует обязательной сертификации и потому встраивание ее в системы дистанционного обслуживания достаточно дорого. Кроме того, необходимо приобретение дополнительных средств криптографической защиты для установки на каждое клиентское место [6]. Не все вопросы защиты информации в СДБО нормативно определены. Есть некоторая двойственность в понимании требований регуляторов по информационной безопасности банковских систем и систем обработки персональных данных в ДБО. Проблема актуальна и требует решения.

#### СПИСОК ЛИТЕРАТУРЫ

1. Валенцева, Н. И. Банковская система в современной экономике : учеб. пособие / Н. И. Валенцева [и др.]; под ред. О. И. Лаврушина. – М. : Юрайт, 2012. – 360 с.
2. Власенко, А. В. Защита конфиденциальной информации, передаваемой по открытым каналам

связи / А. В. Власенко, В. Г. Смирнов // Известия ЮФУ. Технические науки. – 2003. – № 4 (33). – С. 230–232.

3. Власенко, А. В. Защита персональных данных при авторизации пользователя в распределенных информационных системах, построенных на основе web-технологий / А. В. Власенко, П. И. Дзьобан, Р. В. Жук // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2017. – № 2 (201). – С. 120–128.

4. Жуков, Е. Ф. Банковское дело : учебник / Е. Ф. Жуков [и др.]; под ред. Е. Ф. Жукова, Н. Д. Эриашвили. – 4-е изд., перераб. и доп. – М. : ЮНИТИ-ДАНА, 2014. – 687 с.

5. Письмо ЦБР от 17 ноября 2011 г. № 015-16-9/4713 «О средствах защиты информации, применяемых при обработке персональных данных». – Доступ из информ.-правового портала «Гарант.ру».

6. Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» – Доступ из информ.-правового портала «Гарант.ру».

## REFERENCES

1. Valentseva N.I. *Bankovskaya sistema v sovremennoy ekonomike* [Banking System in Modern Economy]. Moscow, Yurayt Publ., 2012. 360 p.

2. Vlasenko A.V., Smirnov V.G. *Zashchita konfidentsialnoy informatsii, predavaemoy po*

otkrytym kanalom svyazi [Protection of Confidential Information Transmitted via Open Communication Channels]. *Izvestiya YuFU. Tekhnicheskie nauki*, 2003, no. 4 (33), pp. 230-232.

3. Vlasenko A.V., Dzoban P.I., Zhuk R.V. *Zashchita personalnykh dannykh pri avtorizatsii polzovatelya v raspredelennykh informatsionnykh sistemakh, postroennykh na osnove web-tekhnologiy* [Protection of Personal Data at User Authorization in Distributed Information Systems Based on Web-Technologies]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki*, 2017, no. 2 (201), pp. 120-128.

4. Zhukov E.F., Eriashvili N.D. *Bankovskoe delo* [Banking]. Moscow, YuNITI-DANA Publ., 2014. 687 p.

5. *Pismo TsBR ot ot 17 noyabrya 2011 g. № 015-16-9/4713 «O sredstvakh zashchity informatsii, primenyaemykh pri obrabotke personalnykh dannykh»* [Letter of the Central Bank of Russia of 17 November 2011 No. 015-16-9/4713 ‘On the Techniques of Information Protection Used in the Processing of Personal Data’]. Access from Reference and Information Portal ‘Garant’.

6. *Polozhenie Banka Rossii ot 9 iyunya 2012 g. № 382-P «O trebovaniyakh k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv i o poryadke osushchestvleniya Bankom Rossii kontrolya za soblyudeniem trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv»* [Provision of the Bank of Russia of 9 June 2012 No. 382-P ‘On Requirements to Information Protection at Money Transfers and Exercising Control over Their Implementation by the Bank of Russia’]. Access from Reference and Information Portal ‘Garant’.

## ISSUES OF SECURITY OF REMOTE BANKING SYSTEMS

**Aleksandra V. Vlasenko**

Candidate of Sciences (Engineering), Associate Professor,  
Head of Department of Computer Technologies and Information Security,  
Kuban State Technological University  
vlasenko@kubstu.ru, alex\_vlasenko@list.ru  
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

**Irina A. Korkh**

Postgraduate Student, Department of Computer Technologies and Information Security,  
Kuban State Technological University  
aia2004@inbox.ru  
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

**Abstract.** The banking system of the Russian Federation is based on Federal legislation, as well as industry and inter-industry standards developed by the International community and the Central Bank of the Russian Federation. The introduction and development of remote banking services is the most popular direction in the modern banking system. The term ‘remote banking service’ refers to the technology of providing services for the remote transmission of orders by credit institutions (without clients’ presence in bank office), using different communication channels.

Information security in bank-client systems is carried out by several types of protection. Client authentication is confirmed by the use of an electronic signature. The data channel and the data itself are encrypted. In order to implement the above-described functions of the bank-client system in any software, the client must first generate and register cryptographic keys with the bank and obtain electronic digital certificates.

In addition to the protection of the transferred data, personal data that have entered the system of remote banking services also need protection.

The research purpose is to analyze the system of remote banking services, to identify regulatory and methodological documents regulating information security issues, options for meeting the requirements of regulators. Confirmation or refutation of the issue’s urgency should be considered as research results.

**Key words:** bank, remote banking service, information security, cryptographic protection, system of remote banking service.