BNP PARIBAS

Ваш банк
в мире
перемен

Условия использования Системы Клиент-Банк, в частности, об ограничениях способов и мест использования и случаях повышенного риска использования Системы Клиент-Банк

Terms of the Client-Bank System use, in particular, on the restrictions of methods and places of use, cases of increased risk of using the Client-Bank System

Уважаемый Клиент,

Dear Client,

Обращаем Ваше внимание на необходимость строгого соблюдения мер информационной безопасности при работе с Системой Клиент-Банк (далее – «Система»). Необходимые меры и рекомендации для минимизации существующих рисков указаны в прилагаемой к настоящему уведомлению Памятке по соблюдению мер информационной безопасности при работе в Системе.

We would like to direct your attention to the requirement to strictly observe information security measures when using Client-Bank System (the "System"). Necessary measures and recommendations to minimize existing risks are mentioned in document attached hereto – Reminder on compliance with security measures while operating the Client-Bank System.

В настоящее время против клиентов российских банков продолжают действовать злоумышленники, которые внедряют на персональных компьютерах («ПК»), подключенных к сети Интернет, вредоносное программное обеспечение («ПО"), позволяющее осуществлять удаленный доступ и несанкционированную отправку фальшивых платежных документов, изменяя реквизиты документов в момент их подписания уполномоченными лицами. После этого мошенники стараются вывести ПК клиента из строя с целью сокрытия факта списания средств от клиента и обеспечения возможности обналичивания похищенных средств.

At the moment, intruders keep targeting clients of Russian banks by installing malicious software on personal computers connected to the Internet which allows them to remotely access and send false payment documents in unauthorised manner by changing document details when authorised persons sign such documents. Thereafter, fraudsters aim to disable client's PC in order to cover-up the fact of debiting client's funds and to make sure stolen funds can be cashed.

Внедрение указанного зловредного ПО на ПК клиентов производится с использованием вирусных программ, массово распространяемых в сети Интернет через взломанные сайты, социальные сети и другие сетевые сервисы, электронную почту, свободно распространяемое ПО и пр. Через сайты российских и международных социальных сетей и через рекламно-баннерные сети распространяется наибольшее количество вредоносных программ. При этом новые модификации вирусов, сигнатуры которых еще не включены в антивирусные базы, успешно преодолевают защиту антивирусного ПО.

Installation of malicious software to clients' PC's is made through viral code massively distributed over the Internet via compromised websites, social networks and other network services, email, freeware, etc. The most malicious software is distributed through websites of Russian and international social networks and through ad and banner networks. At the same time, virus modifications, signatures of which are not yet included into anti-virus databases, successfully overcome anti-virus software protection.

Банк проводит регулярные доработки Системы в части противодействия имеющимся угрозам и рекомендует всегда использовать актуальную версию Системы. Интернет-версия Системы обновляется автоматически.

The Bank arranges for regular updates of the System with respect to counteracting existing threats, and it recommends to always use the up-to-date System version. The web-version of the System is updated automatically.

Обращаем Ваше внимание на следующие случаи повышенного риска использования Системы в качестве электронного средства платежа:

Please note the following cases when the use of the System as electronic means of payment involves increased risks:

- Использование ПК, предназначенного для установки Системы и использования Системой, для доступа через сеть Интернет в вирусо-опасные ресурсы, такие как

- Use of a PC dedicated for installation and use of the System, for access to social networks and other network services through Internet and virus threatening resources, including email clients;

социальные сети, другие сетевые сервисы, включая почтовые клиенты;
- Наличие на ПК, предназначенном для установки и использования Системы, вредоносного ПО, программ удаленного доступа к ресурсам ПК либо свободно распространяемого ПО;
- Отсутствие на ПК, предназначенном для установки и использования Системы, антивирусных баз либо нерегулярное их обновление;
- Использование неактуальной версии Системы;
- Отсутствие резервного копирования информации;
- Доступ к Системе неуполномоченных лиц;
- Необеспечение мер, направленных на защиту криптографических ключей и парольной информации от копирования и завладения неуполномоченными лицами;
- Хранение криптографических ключей нескольких пользователей Системы, а также лиц, обладающих криптографическими ключами электронной подписи, на одном носителе информации;
- Непринятие мер, направленных на незамедлительную блокировку и смену криптографических ключей, а также смену паролей доступа в Систему в случаях их компрометации;
- Предоставление лицам излишних прав доступа к Системе, выходящих за рамки фактически исполняемых данными лицами функциональных обязанностей;
- Хищение носителей информации и/или объектов Системы или несанкционированное копирование данных;
- Отсутствие контроля физического доступа к объектам Системы;
- Нерегулярная проверка входящих электронных документов в Системе.

Для снижения рисков, в частности риска мошенничества, настоятельно рекомендуем Вам принять необходимые организационно-технические мероприятия по обеспечению и постоянному контролю состояния безопасности и условий эксплуатации клиентских рабочих мест Системы, а также соответствующему обучению и проверке знаний персонала, эксплуатирующего Систему. В случае внезапного выхода из строя компьютера с установленной Системой необходимо срочно запросить в Банке выписку по счету для проверки легитимности всех списаний.

- Cases when malicious software and programs for remote access to PC resources or freeware are installed on a PC dedicated for System installation and use;
- Lack of or irregular updates of anti-virus databases installed on the PC dedicated for installation and use of the System;
- Use of an outdated version of the System;
- Lack of information backups;
- Access to the System by unauthorised persons;
- Failure to ensure protective measures with respect to cryptographic keys and password information from copying and gaining possession by unauthorised persons;
- Not taking measures to immediately block and replace cryptographic keys, as well as to change access passwords to the System, if they are compromised;
- Storage of cryptographic keys of several users of System, as well as the persons having the cryptographic keys of the digital signature, on one information carrier;
- Providing to persons excessive System access rights, which are out of the scope of the actual functional responsibilities of such persons;
- Theft of information carriers and/or System objects, or unauthorised data copying;
- Lack of control over physical access to System objects;
- Irregular inspection of incoming electronic documents in the System;

In order to mitigate risks, and in particular fraud risks, we strongly recommend to take necessary administrative and technical measures with respect to ensuring and continuously controlling security status and operating conditions of client's work stations, as well as those related to respective training and skill testing of personnel operating the System. In case of an unexpected break-down of a computer with the System installed thereon, it is required to immediately request an account statement from the Bank to check whether or not all debiting transactions are legitimate.

Приложение к Условиям использования Системы Клиент-Банк, в частности, об ограничениях способов и мест использования и случаях повышенного риска использования Системы Клиент-Банк

Appendix to the Terms of the Client-Bank System use, in particular, on the restrictions of methods and places of use, cases of increased risk of using the Client-Bank System

Памятка

по соблюдению мер информационной безопасности при работе в Системе Клиент-Банк

Reminder

on compliance with security measures while operating the Client-Bank System

1. Меры информационной безопасности при эксплуатации Системы.

1.1. При эксплуатации Системы необходимо следовать эксплуатационной документации, предоставленной в рамках Договора и его приложений.

1.2. Рекомендуем Вам контролировать наличие актуальной версии эксплуатационной документации и выполнение её положений.

1.3. Для реализации возможности восстановления функционирования Системы, в случаях сбоев и (или) отказов в работе, рекомендуем Вам осуществлять резервное копирование информации.

1. Information Security Measures When Operating the System

1.1. When operating the System, it is required to follow operating manuals provided under this Agreement and appendices thereto.

1.2. We recommend you keep under control the availability of an up-to-date version of operating manuals and the compliance with the provisions thereof.

1.3. In order to enable System recovery after failures and (or) breakdowns, we recommend to perform information backups.

2. Меры информационной безопасности при осуществлении доступа к Системе:

Для защиты от несанкционированного доступа («НСД») и нерегламентированного доступа («НРД») рекомендуем Вам:

2.1. Осуществлять регистрацию лиц, обладающих правами: доступа к объектам Системы; по управлению криптографическими ключами; по воздействию на объекты информационной инфраструктуры Системы. А также контролировать и регистрировать действия лиц, которым назначены данные роли.

2.2. Осуществлять разграничение полномочий в Системе в соответствии с рекомендациями Банка; назначать своим сотрудникам минимально необходимые для выполнения их функциональных обязанностей прав доступа к Системе.

2.3. Контролировать физический доступ к объектам Системы; предотвращать физическое воздействие на средства вычислительной техники, входящие в состав Системы; принимать меры, направленные на предотвращение хищения носителей информации; контролировать отсутствие на объектах Системы посторонних средств (средств, предназначенных для несанкционированного получения информации).

2. Information Security Measures When Accessing the System:

In order to protect the System against unauthorized access or unrestricted access, we recommend to:

2.1. Register persons having access rights: to System objects; to manage cryptographic keys; to make an impact on information infrastructure objects of the System. As well as to control and register actions of persons who have been assigned with such roles.

2.2. To delineate responsibilities in the System in line with Bank's recommendations; to assign minimum essential System access rights to its employees required to perform their functional responsibilities.

2.3. To control physical access to System objects; to prevent physical impact on computing equipment that is part of the System; to take measures to prevent theft of information carriers; to control that there are no foreign matters on System objects (tools designed for unauthorized access to information).

3. Меры по защите от вредоносного ПО:

3.1 Перед установкой Системы, проведением настроек безопасности в процессе ее работы, необходимо проверить ПК на отсутствие вредоносного ПО, программ удаленного доступа к ресурсам ПК (TeamViewer, BeTwin,

3. Measures for Protection Against Malicious Software:

3.1 Prior to installing the System and setting up security in the course of its operation, it is required to examine the PC for presence of any malicious software, programs for remote access to PC resources (TeamViewer, BeTwin, RAdmin, etc.),

RAdmin и др.), программ работы с вирусо-опасными ресурсами и сервисами сети Интернет, включая почтовые клиенты. При проведении таких проверок рекомендуется осуществлять загрузку операционной Системы («ОС») с внешнего эталонного загрузочного диска.

3.2 На ПК, используемых в рамках Системы, должны быть установлены последние пакеты обновлений (Service Packs) и актуальные обновления безопасности ОС, базы антивирусного ПО, обновление которых должно проводиться регулярно, а лучше в автоматическом режиме.

3.3 У пользователей ПК в ОС не должно быть административных прав и прав «Power User» («Опытный пользователь»).

3.4 Для исключения ошибочных и преднамеренных действий пользователя, приводящих к снижению защищенности Системы и рискам финансовых потерь, необходимо средствами политик безопасности операционной Системы или специализированными средствами защиты ПК от НСД обеспечить для пользователя функционально-замкнутую среду, позволяющую ему запускать и работать только с разрешенными программами без доступа к файловой Системе и реестру ОС.

3.5 Необходимо исключить установку на ПК с Системой ПО, полученного из незаслуживающих доверия источников, а также нелицензионного и свободно-распространяемого ПО. Обновление версии Системы производится автоматически, встроенными средствами Системы.

3.6 Не привлекать для администрирования и обслуживания Системы ИТ-персонал на условиях предоставления ему удаленного доступа.

3.7 Осуществлять фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет.

4. Меры, направленные на защиту от копирования ключевой и парольной информации:

4.1 Криптографические ключи различных пользователей Системы, а также лиц, обладающих криптографическими ключами электронной подписи, необходимо хранить на различных внешних носителях информации. Следует избегать хранения на одном носителе информации криптографических ключей более чем одного пользователя Системы / лица, обладающего криптографическими ключами электронной подписи.

4.2 Криптографические ключи и информацию, необходимую для доступа в Систему (логины/пароли доступа к Системе), следует хранить в специальных местах хранения.

programs that involve communication with resources and services on the Internet that are insecure in terms of viruses, including email clients. When performing such examinations, it is recommended to restart the operation System from an external master boot disc.

3.2 PC's used with the System must have the latest Service Packs installed, as well as latest security OS updates, anti-virus software bases, that must be regularly updated, and preferably in an automatic mode.

3.3 PC users shall have no administration or power user rights within the operating System.

3.4 In order to exclude any faulty or wilful actions that result in decreasing System protection level and lead to financial loss risks, it is necessary to establish a functionally closed environment for the user which will allow it to run, and work with, authorised programs exclusively, without access to file System and registry of the operating System. Such environment shall be established by means of operating System security policies or specialised protective solutions for PC's against unauthorised access.

3.5 It is necessary to exclude cases when software obtained from untrustworthy sources, unlicensed software or freeware are installed to PC's with the System. System version shall be updated automatically, by means of built-in tools of the System.

3.6 No IT-staff shall be engaged for administering and maintaining the System subject to the condition to provide remote access rights.

3.7 To perform filtering of network packages upon information exchange between computer networks, where information infrastructure objects are located, and the Internet.

4. Measures to Protect Copying Key and Password Information:

4.1 Cryptographic keys of different users of System, as well as of the persons having the cryptographic keys of the electronic signature, must be stored on separate external information carriers. The storage on one information carrier of cryptographic keys of more than one user of the System / person having the cryptographic keys of the electronic signature must be avoided.

4.2 Cryptographic keys and information necessary to access the System (logins/access passwords) shall be stored in special storage locations.

4.3 It is prohibited to leave any media with cryptographic keys connected to PC after signing payment documents. Electronic signature secret

4.3 Нельзя оставлять носители с криптографическими ключами, подключенными к ПК, после подписания платежных документов. Носители секретных ключей электронных подписей нужно подключать к ПК только в момент подписания документов, после подписания носители сразу отключать и убирать в специальное место хранения (сейф, и т.п.).

4.4 Необходимо выполнять незамедлительную блокировку и смену криптографических ключей, а также смену паролей доступа в Систему в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.

4.5 Необходимо заменять криптографические ключи и пароли доступа в Систему во всех случаях увольнения или смены руководителей юридического лица, подписывавших распоряжения (доверенности) о предоставлении сотрудникам организации полномочий подписания электронной подписью электронных документов.

4.6 При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах не сообщать данную информацию.

4.7 Необходимо соблюдать требования Договора и приложений к нему.

5. Меры по контролю несанкционированных списаний:

5.1. Следует регулярно проверять входящие электронные документы в Системе. В случае отсутствия регулярных проверок Вы можете не прочитать уведомление о совершенных переводах денежных средств и не отследить несанкционированные операции в случае их совершения.

5.2. Необходимо проводить контроль сумм и получателей платежных документов в информационном окне Системы при выходе на связь с Банком, а также контролировать количество и сумму отправленных документов по полученным от Банка квитанциям.

5.3. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать Банк обо всех подозрительных или несанкционированных операциях в соответствии с Договором. При установке порядка регулярного контроля рекомендуем принимать в расчёт, что переводы денежных средств, в отношение которых наступила безотзывность перевода денежных средств, не могут быть приостановлены.

5.4. В случае неожиданного выхода из строя компьютера либо пропадания на нём программного обеспечения Системы, необходимо прекратить на ПК работу, отключив его от всех видов сетей, включая

key media must be connected to PC only at the time of signing the documents, and after the documents are signed, such media shall be immediately disconnected and placed into special storage location (safe deposits, etc.).

4.4 Cryptographic keys must be immediately blocked and replaced, as well as the System access passwords if they are compromised, and also upon their expiry according to the frequency as set forth in contracts and documentation.

4.5 Cryptographic keys and System access passwords shall be replaced in all cases when managers of the legal entity resign or are replaced, who sign instructions (powers of attorney) to grant authority to company's employees to sign electronic documents with an electronic signature.

4.6 If any persons on behalf of the Bank request provision or transmission of any confidential information (keys, passwords, etc.) by phone, email or text messages, in no event any such information shall be provided.

4.7 It is required to comply with the provisions of the Agreement and Appendices thereto.

5. Measures to Control Unauthorised Debiting Transactions:

5.1. It is necessary to regularly examine incoming electronic documents in the System. If no regular examinations are made, you might miss a notice of transfers made, and fail to identify unauthorised transactions if they take place.

5.2. Amounts and recipients of payment documents must be controlled using the information window of the System when connecting to the Bank, as well as the number and amount of documents sent shall be controlled as aligned with the reports received from the Bank.

5.3. It is required to regularly control account balance and to immediately inform the Bank of any suspicious or unauthorised transactions according to the Agreement. When setting up a regular control procedure, we recommend to consider that transfers with respect to which irrevocability of funds is applicable and has occurred, may not be suspended.

5.4. In case of an unexpected failure of a computer, or missing System software thereon, it is required to stop working on such PC by unplugging it from any kind of networks, including local computer network and modems, and to immediately contact the Bank to block the System, request an account statement directly from the Bank. If any unauthorised payment transactions are identified, it will be necessary to submit an application to the

локальную корпоративную сеть, и модемов, срочно связаться с Банком для блокировки Системы, запросить выписку по счету непосредственно в Банке. При обнаружении несанкционированных платежных операций написать заявление в Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. Работоспособность поврежденного ПК не восстанавливать до проведения технической экспертизы. Переустановку Системы проводить на новом ПК. После переустановки Системы произвести немедленную смену всех своих криптографических ключей.

5.5. Появление на экране ПК во время отсутствия соединения с Банком сообщений, провоцирующих на установление такого соединения, свидетельствует о наличии на ПК вредоносного ПО. В данной ситуации установление соединения с Банком может привести к отправке фальшивого документа. При появлении подобного сообщения необходимо провести контроль платежных документов, находящихся в статусе «Выгружен». Далее в любом случае действовать согласно п. 5.2 настоящей памятки. Помните, что реальные сообщения от Банка могут быть получены только в режиме установленного соединения.

Bank and to contact law enforcement authorities with a respective application. No damaged PC shall be recovered prior to performing a technical expert examination. The System shall be reinstalled on a new PC. After the System was reinstalled, all cryptographic keys shall be immediately replaced.

5.5. While there's no connection to the Bank, if any messages appear on the PC screen encouraging to install any such connection, it shall be the evidence that some malicious software was installed on the PC. In such case, establishing a connection with the Bank may result in sending a false document. In case of any such message, it is required to control all payment documents having the status of "Uploaded". And then, anyway to proceed acting according to Clause 5.2. hereof. Please remember, that actual messages from the Bank may be received only in the established connection mode.

6. Меры по поддержанию уровня информационной безопасности.

Для обеспечения высокого уровня информационной безопасности при эксплуатации Системы в Вашей организации должен быть назначен ответственный, который осуществляет:

6.1 Постоянный контроль соблюдения мер информационной безопасности, предусмотренных настоящей памяткой, документацией на Систему, и средства защиты.

6.2 Выявление, устранение и информирование руководства организации обо всех выявленных нарушениях.

6.3 Контроль устранения выявленных нарушений.

6.4 Документирование результатов проведенных работ и проверок.

6.5 Повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации; по порядку использования технических средств защиты информации.

6.6 Организацию и проведение мероприятий по усилению безопасности в соответствии с информационными сообщениями, которые направляются Банком непосредственно по Системе, прилагаются к выписке по счету, официальными письмами, а также публикуются на сайте Банка.

6. Measures to Maintain the Level of Information Security.

In order to maintain high level of information security when operating the System, there must be a responsible person appointed within your company who is responsibilities shall include:

6.1 Continuous control over compliance with information security measures set forth herein, System documentation and protection tools.

6.2 Identification and elimination of all identified violations and informing the company's management thereof.

6.3 Control over elimination of the identified violations.

6.4 Documenting results of works and inspections performed.

6.5 Raising awareness of the employees with respect to ensuring information protection in line with the procedure for application of operational measures to protect information, and in line with the procedure for use of technical tools for information protection.

6.6 Arranging and implementing measures to reinforce security in accordance with information notices sent by the Bank directly through the System, attached to account statements, official letters, and that are published on the Bank's website.