ПРИЛОЖЕНИЕ/SCHEDULE

Уведомление о рекомендациях по снижению рисков осуществления перевода денежных средств без согласия клиента.

Уважаемый Клиент!

Обращаем Ваше внимание на необходимость строгого соблюдения перечисленных в настоящем документе мер при осуществлении перевода денежных средств. Необходимые меры и рекомендации для минимизации существующих рисков указаны в прилагаемых к настоящему уведомлению «РЕКОМЕНДАЦИЯХ по снижению рисков осуществления перевода денежных средств без согласия клиента».

В настоящее время против клиентов Российских банков, продолжают действовать злоумышленники, которые внедряют на устройства, подключенные 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 устройство клиента из строя с целью сокрытия факта списания средств от клиента и обеспечения возможности обналичивания похищенных средств.

Внедрение указанного зловредного ПО на устройства 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.

Обращаем Ваше внимание на следующие случаи повышенного риска при переводе денежных средств:

- Использование устройств, предназначенных для перевода денежных средств, для доступа через сеть Интернет в вирусо-опасные ресурсы, такие как социальные сети, другие сетевые сервисы, включая почтовые клиенты;
- Наличие на устройстве, предназначенном для перевода денежных средств, вредоносного ПО, программ удаленного доступа к ресурсам устройства либо свободно распространяемого ПО;
- Отсутствие на устройстве, предназначенном для перевода денежных средств, либо нерегулярное обновление антивирусных баз;
- Использование неактуальных версий систем, используемых для перевода денежных средств;
- Отсутствие резервного копирования

Notice on the recommendations for decrease of risk of money transfer without the consent of the client

Dear Client,

We would like to direct your attention to the requirement to strictly observe the measures listed hereunder during transfer of money. Necessary measures and recommendations to minimize existing risks are mentioned in document attached hereto - "Recommendations for decrease of risk of money transfer without the consent of the client ".

At the moment, intruders keep targeting clients of Russian banks by installing malicious software on devices 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 device in order to cover-up the fact of debiting client's funds and to make sure stolen funds can be cashed.

Installation of malicious software to clients' devices 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.

Please note the following cases of money transfers involves increased risks:

- Use for money transfer of a device, for access to social networks and other network services through Internet and virus threatening resources, including email clients;
- Cases when malicious software and programs for remote access to device resources or freeware are installed on a device dedicated for money transfers;
- Lack of or irregular updates of anti-virus databases installed on the device dedicated for money transfers;
- Use of an outdated version of the systems of money transfers;
- Lack of information backups;
- Access to the device dedicated for money transfers 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, if they are compromised;
- Storage of cryptographic keys of several users, as well as the persons having the cryptographic keys of the digital signature, on one information carrier;

информации;
• Доступ к устройству, используемому для перевода денежных средств, неуполномоченных лиц;
• Необеспечение мер, направленных на защиту криптографических ключей и парольной информации от копирования и завладения неуполномоченными лицами;
• Хранение ключей доступа/ электронной подписи нескольких пользователей, а также лиц, обладающих ключами электронной подписи, на одном носителе информации;
• Непринятие мер, направленных на незамедлительную блокировку и смену ключей доступа/ электронной подписи, а также смену паролей доступа в случаях их компрометации;
• Предоставление лицам излишних полномочий и/или прав доступа, выходящих за рамки фактически исполняемых данными лицами функциональных обязанностей;
• Хищение носителей информации и/или объектов, используемых при переводе денежных средств или несанкционированное копирование данных;
• Отсутствие контроля физического доступа к объектам, используемым при переводе денежных средств;
• Нерегулярная проверка входящих электронных документов.

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, а также соответствующему обучению и проверке знаний персонала. В случае внезапного выхода из строя устройства, используемого для перевода денежных средств, необходимо срочно запросить в банке выписку по счету для проверки легитимности всех списаний.

• Providing to persons excessive authorizations and/or access rights, which are out of the scope of the actual functional responsibilities of such persons;
• Theft of information carriers objects used during money transfers, or unauthorised data copying;
• Lack of control over physical access to objects used during money transfers;
• Irregular inspection of incoming electronic documents.

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. In case of an unexpected break-down of a device used for money transfers it is required to immediately request an account statement from the bank to check whether or not all debiting transactions are legitimate.

РЕКОМЕНДАЦИИ по снижению рисков осуществления перевода денежных средств без согласия клиента

1. Меры информационной безопасности при осуществлении перевода денежных средств.
1.1. При осуществлении перевода денежных средств необходимо следовать эксплуатационной документации на используемые электронные средства платежа, а также дистрибутивов, переданных в рамках установки/обновления электронных средств платежа.
1.2. Рекомендуем Вам контролировать наличие актуальной версии эксплуатационной документации и выполнение её положений.
1.3. Для реализации возможности восстановления функционирования объектов, используемых при осуществлении перевода денежных средств, в случаях сбоев и (или) отказов в работе, рекомендуем Вам осуществлять резервное копирование информации.

Recommendations for decrease of risk of money transfer without the consent of the client

1. Information Security Measures during money transfers
1.1. During money transfers, it is required to follow operating manuals theretofore the used electronic means of payment, as well as installation packages provided upon installation/update of the electronic means of payment.

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 recovery of objects used for the money transfers after failures and (or) breakdowns, we recommend to perform information backups.
1.4 We recommend segregate the roles for preparation and signing/sending the money transfers

1.4 Рекомендуем осуществлять разграничение ролей по формированию и подписанию/отправке переводов денежных средств, а также ролей по формированию и подтверждению возобновления исполнения переводов денежных средств в случаях приостановления операций списания Банком при их соответствии признакам осуществления перевода денежных средств без согласия Клиента.

2. Меры информационной безопасности при осуществлении доступа к объектам, используемым для осуществления перевода денежных средств:

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

2.1. Осуществлять регистрацию лиц, обладающих правами доступа к объектам используемым для осуществления перевода денежных средств; по управлению криптографическими ключами; по воздействию на объекты информационной инфраструктуры. А также контролировать и регистрировать действия лиц, которым назначены данные роли.

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

2.3. Контролировать физический доступ к объектам, используемым для осуществления перевода денежных средств; предотвращать физическое воздействие на средства вычислительной техники; принимать меры, направленные на предотвращение хищения носителей информации; контролировать отсутствие на устройствах, используемых для осуществления перевода денежных средств, посторонних средств (средств, предназначенных для несанкционированного получения информации).

3. Меры по защите от вредоносного ПО:

3.1. Перед началом осуществления перевода денежных средств, необходимо провести настройки безопасности устройства, проверить устройство на отсутствие вредоносного ПО, программ удаленного доступа (TeamViewer, BeTwin, RAdmin и др.), программ работы с вирусо-опасными ресурсами и сервисами сети Интернет, включая почтовые клиенты.

3.2. На устройствах, используемых для осуществления перевода денежных средств, должны быть установлены последние пакеты обновлений (Service Packs) и актуальные обновления безопасности Операционной Системы (ОС), базы антивирусного ПО, обновление которых должно проводиться регулярно, а лучше в автоматическом режиме.

3.3. У пользователей 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 и рискам финансовых потерь, необходимо средствами политик безопасности ОС или специализированными средствами защиты от НСД

as well as the roles for preparation and confirmation of renewal of execution of the Instruction in case of suspension of the operation if corresponding to characteristics of execution of the transfer of funds without Client's consent.

2. Information Security Measures When Accessing the objects used during the money transfers:

In order to protect against unauthorised access or unrestricted access, we recommend to:

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

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

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

3. Measures for Protection Against Malicious Software:

3.1. Prior to money transfers execution it is required to set up security in the course of its operation, to examine the device used for money transfers for presence of any malicious software, programs for remote access to PC resources (TeamViewer, BeTwin, RAdmin, etc.), programs that involve communication with resources and services on the Internet that are insecure in terms of viruses, including email clients.

3.2. Devices used for money transfers must have the latest Service Packs installed, as well as latest security Operating System (OS) updates, anti-virus software bases, that must be regularly updated, and preferably in an automatic mode.

3.3. Device users shall have no administration or power user rights within the OS.

3.4. In order to exclude any faulty or wilful actions that result in decreasing 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 OS. Such environment shall be established by means of OS security policies or specialised protective solutions for devices against unauthorised access.

3.5. It is necessary to exclude cases when software obtained from untrustworthy sources, unlicensed

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 устройство, используемое для осуществления перевода денежных средств ПО, полученного из незаслуживающих доверия источников, а также нелицензионного и свободно-распространяемого ПО.
3.6. Не привлекать для администрирования и обслуживания устройств 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. Ключи доступа/ электронной подписи различных пользователей, а также лиц, обладающих ключами доступа/ электронной подписи, необходимо хранить на различных внешних носителях информации. Следует избегать хранения на одном носителе информации ключей доступа более чем одного пользователя / лица, обладающего ключами электронной подписи.
4.2. Ключи доступа/ электронной подписи и информацию, необходимую для доступа (логины/пароли доступа), следует хранить в специальных местах хранения.
4.3. Нельзя оставлять носители с ключами доступа/ электронной подписи, подключенными к устройству, после подписания платежных документов. Носители секретных ключей ЭП нужно подключать к устройству 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 ключей доступа/электронной подписи, а также смену паролей доступа, в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.
4.5. Необходимо заменять ключи доступа/ электронной подписи и пароли доступа во всех случаях увольнения или смены руководителей юридического лица, подписывавших распоряжения (доверенности) о предоставлении сотрудникам организации полномочий подписания ЭП 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, а также Правил пользования СКЗИ (документ входит в состав дистрибутива электронной системы).

5. Меры по контролю несанкционированных списаний:

software or freeware are installed to devices used for money transfers.

3.6. No IT-staff shall be engaged for administering and maintaining the devices 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, 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 for access (logins/access passwords) shall be stored in special storage locations.

4.3. It is prohibited to leave any media with cryptographic keys connected to device after signing payment documents. Electronic signature secret key media must be connected to device 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 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 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, as well as Instructions to Use CISS (the document is part of electronic system installation package).
5. Measures to Control Unauthorised Debiting Transactions:
5.1. It is necessary to regularly examine incoming electronic documents in the electronic system. If no

5.1. Следует регулярно проверять входящие электронные документы в электронной 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 электронной 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 устройства, либо пропадания на нём программного обеспечения, необходимо прекратить на устройстве работу, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно связаться с Банком для блокировки, 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 устройства не восстанавливать до проведения технической экспертизы.

5.5. Появление на экране устройства во время отсутствия соединения с банком сообщений, провоцирующих на установление такого соединения, свидетельствует о наличии 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.

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.

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 electronic 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 device, or missing software thereon, it is required to stop working on such device by unplugging it from any kind of networks, including local computer network and modems, and to immediately contact the Bank to block the access, 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 Bank and to contact law enforcement authorities with a respective application. No damaged device shall be recovered prior to performing a technical expert examination.

5.5. While there's no connection to the bank, if any messages appear on the device screen encouraging to install any such connection, it shall be the evidence that some malicious software was installed on the device. 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. 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

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 электронной системе, прилагаются к выписке по счету, официальными письмами, а также публикуются на сайте Банка.

7. Меры по снижению рисков осуществления перевода денежных средств без согласия клиента при расчётах платежными поручениями

Для защиты от мошенничества при расчётах платежными поручениями необходимо:

7.1 Неукоснительно выполнять процедуры предоставления в банк платёжных и удостоверяющих документов, установленных Банком.

7.2 Учитывая многочисленные случаи использования мошенниками так называемой инсайдерской информации, установить ограниченный доступ сотрудников к работе с платежными поручениями и информации о ведущихся и планируемых расчётах.

7.3 Исключить возможность несанкционированного доступ а неуполномоченных лиц к печати организации.

7.4 Не допускать фактов подписи уполномоченными лицами незаполненных бланков платежных поручений впрок и передачи их третьим лицам.

7.5 Осуществлять разграничение ролей по формированию и подписанию платежных поручений.

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 electronic system, attached to account statements, official letters, and that are published on the Bank's website.

7. Measures to decrease the risk of money transfer without the consent of the client during the execution of payment orders. To protect against the fraud during the execution of payment orders it is required:

7.1 To strictly perform procedures of providing in bank of the payment and certifying documents established by Bank.

7.2 Considering numerous cases of use by swindlers of the so-called insider information, to establish limited access for employees to work with payment orders and information on the conducted and planned calculations.

7.3 To exclude a possibility of unauthorized access and unauthorized persons for stamp of the organization.

7.4 Not to allow the signature facts by the authorized persons of the blank payment order forms and the future transfers to third parties.

7.5 To perform differentiation of roles on forming and signing of payment orders.