Утверждаю:
ВРИО президента
АО «Банк Кредит Свисс (Москва)»
Тарыгин С.Г.

25 ноября 2019 г.

Approved:
JSC Bank Credit Suisse (Moscow)
Deputy President
Tarygin S.G.

25 November 2019

Рекомендации
клиентам АО «Банк Кредит Свисс (Москва)»
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники,
в целях противодействия незаконным финансовым операциям

В целях предупреждения последствий недобросовестных действий третьих лиц и противодействия незаконным финансовым операциям в отношении активов Клиентов, Акционерное общество «Банк Кредит Свисс (Москва)» (далее «Компания») предоставляет Клиентам, имеющим действующие договоры на банковское, брокерское, кастодиальное и другое обслуживание в Компании (далее –

Recommendations
to clients of JSC Bank Credit Suisse (Moscow), Ltd.
on information security and information protection measures from exposure to malicious codes that may result in business operations disruption and unauthorized financial transactions

To prevent unauthorized financial transactions with the Clients' assets, JSC Bank Credit Suisse (Moscow) (hereinafter – 'Company') provide to Clients

«Клиенты») настоящее уведомление о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и доводит до сведения Клиентов перечень рекомендуемых мер по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – «вредоносный код»), а также о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) Клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого Клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

(hereinafter – 'Clients') this notice of possible risks of obtaining unauthorized access to protected information for the purpose of financial transactions execution and recommends the Clients on measures for information protection from malicious codes impact, which lead to disruption of normal functioning of computer equipment (hereinafter - "malicious code"), as well as measures to prevent unauthorized access to protected information.

1. Возможные риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций

1. Possible risks of unauthorized access to protected information for the purpose of unauthorized financial transactions execution

лицами, не обладающими правом их осуществления

В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передеваемая и хранимая в автоматизированных системах в рамках обслуживания Клиента, содержащаяся в электронных документах, которыми Клиент обменивается с Компанией (электронные сообщения), информация, необходимая для авторизации клиента и удостоверения его прав на распоряжение активами (ключи, логины, пароли и т.п.), информация об осуществленных финансовых операциях, а также ключевая информация применяемых средств криптографической защиты (далее в совокупности – «защищаемая информация»), может быть подвергнута воздействию вредоносных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники.

Также результате неправомерных действий третьих лиц существует риск получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций по счетам Клиента лицами, не обладающими

As a result of illegal actions of third parties, information related to financial transactions received, prepared, processed, transferred and stored in IT systems can be impacted by malicious code.

Also as a result of illegal actions of third parties there is a risk of obtaining unauthorized access to protected information for the purpose of carrying out financial transactions on the Client 's accounts by persons who do not have the right to carry out them, which may lead to the following negative consequences:

правом их осуществления, что может повлечь за собой, в том числе, следующие негативные последствия:

- совершение злоумышленниками юридически значимых действий: операций с доступными активами, внесение изменений в регистрационные данные Клиента, подключение и отключений услуг, изменение лимитов и перечня торгуемых активов, использование счетов Клиента и находящихся на них активов для прикрытия каких-либо действий, носящих противоправный характер, иных действий, совершаемых против воли Клиента;

- деструктивное воздействие на носители информации и их содержимое, что, в свою очередь, может привести к воспрепятствыванию своевременного исполнения Клиентом или Компанией своих обязательств по договору или невозможности использования предоставляемых Компанией сервисов для реализации намерений Клиента;

- разглашение относящейся к Клиенту информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, оказываемых услугах, персональных данных, иной значимой информации.

Компания настоятельно рекомендует Клиентам соблюдать

- unauthorized transactions execution with assets, making changes to registration data of the Client, change of limits and list of traded assets, use of accounts of the Client and assets on them to cover any illegal actions;

- Disclosure of confidential information related to the Client: information on transactions, assets, status of accounts, services provided, personal data, other relevant information.

The Company strongly recommends that Clients comply with the following

нижеперечисленные рекомендации и принимать меры, изложенные в них.

recommendations and take the measures set forth therein.

2. Рекомендации по защите информации от воздействия вредоносного программного кода и его своевременному обнаружению

2.1. Вредоносный программа – это программа, наносящая вред компьютеру или иному устройству, на котором она запускается. Вредоносные программы способны самостоятельно, без ведома владельца устройства, создавать свои копии и распространять их различными способами, что может привести к полному или частичному разрушению информации, хранящейся на устройстве, а также хищению персональных данных Клиента.

2.2. На серверах, персональных компьютерах и иных устройствах Клиента, используемых для проведения финансовых операций, должно быть установлено специализированное программное обеспечение для поиска вредоносного кода. Рекомендуется установить максимальный уровень политики безопасности (не требующий ответов пользователя при обнаружении вредоносного кода) и не предоставлять права пользователям на изменение этого уровня безопасности.

2. Recommendations for protecting information from malicious code exposure and it's timely detection

2.1. Malware is a program that harms the computer or other device on which it runs. Malware can independently, without the knowledge of the device owner, create copies and distribute them in various ways, which can lead to complete or partial destruction of information stored on the device, as well as theft of personal data of the Client.

2.2. On servers, personal computers and other devices that Client uses for financial transactions execution anti-virus/malware protection software should be installed and updated.

Антивирусное ПО должно обновляться на регулярной основе.

2.3. Не реже одного раза в день в автоматическом режиме должна производиться полная проверка персонального компьютера либо другого устройства, с использованием которого Клиентом совершались действия в целях осуществления финансовой операции на предмет наличия вирусов и вредоносного программного кода. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по средствам телекоммуникационным каналам, а также информацию на съемных носителях, сканирование должно производиться в автоматическом режиме.

2.4. Рекомендуется не использовать компьютер, с которого Клиент осуществляет операции с денежными средствами и иными активами, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания, так как именно через эти ресурсы сети Интернет чаще всего распространяют вредоносные программы.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных

2.3. It's recommended to perform anti-virus/malware scanning daily on computers that are used for financial transactions.

2.4. Computer that Client uses for financial transactions execution are not to be used to communicate on social networks, visit entertainment sites and sites of doubtful content, as such resources are often used for malware distribution.

3. Recommendations to protect information from unauthorized access by using false (falsified) Internet resources

(фальсифицированных) ресурсов сети Интернет

3.1. Рекомендуется не вводить конфиденциальную информацию на поддельных или небезопасных web–сайтах, которые зачастую являются почти точной копией web–сайтов известных компаний, которым ранее Клиент доверял.

3.2. Рекомендуется не отвечать на подозрительные электронные письма с просьбой выслать пароль и другие конфиденциальные данные.

3.3. Рекомендуется перед просмотром электронного письма проверять адрес отправителя, так как строка «отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании.

3.4. Рекомендуется обращать внимание на обезличенные обращения в электронном письме и помнить, что многие мошеннические письма содержат призывы к безотлагательным действиям (например, что счету угрожает опасность, если немедленно не обновить важную информацию), пытаясь заставить действовать быстро и необдуманно.

3.5 Рекомендуется внимательно анализировать ссылки, так как они могут

3.1. It is recommended not to enter confidential information on websites, which are often almost an exact copy of websites of well-known companies that the Client previously trusted.

3.2. We recommend that you do not respond to suspicious emails asking you to send your password and other sensitive information.

3.3. It is recommended that you check the sender's address before viewing the e-mail, because the line "sender" may contain an e-mail address that is almost an exact copy of the address of this company.

3.4. It is recommended that you pay attention to email content and remember that many fraudulent emails call for urgent action (for example, that an account is in danger if important information is not immediately updated) in an attempt to force action quickly and ill-advised.

3.5 It is recommended to carefully analyze the links, as they may be an exact copy of the original ones, but be redirected to

быть точной копией подлинных, однако перенаправлять на мошеннический web-сайт; никогда не устанавливать и не сохранять без предварительной проверки антивирусной программы файлы, полученные из ненадежных источников, скаченные с неизвестных web-сайтов, присланные по электронной почте и полученные из иных источников. Подозрительные файлы должны быть немедленно удалены.

a fraudulent website; never install or save files obtained from untrusted sources, downloaded from unknown websites, sent by e-mail and received from other sources without first checking the antivirus program. Suspicious files must be deleted immediately.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется регулярно не реже 1 раза в 90 дней производить смену паролей для работы со своими учетными данными, использовать различные уникальные пароли для различных web-сайтов и систем, использовать пароли достаточной сложности.

4.2. В случае обнаружения компрометации пароля, рекомендуется незамедлительно сменить пароль на новый, либо обратиться с сотруднику Компании для получения инструкции по смене пароля.

4. Recommendations to prevent unauthorized access by third parties

4.1. Passwords should be regularly changed at least every 90 days and unique passwords with sufficient complexity should be used.

4.2. In case a password is compromised it must be changed immediately, or the Client should contact the Company's representative for instructions on how to change a password.

4.3 Рекомендуется исключить возможность физического доступа к компьютеру или иному устройству, с которого Клиент совершает действия в целях осуществления финансовых операций, посторонних лиц.

4.4. В случае получения уведомление либо обнаружения другим образом в системе операций, которых Клиент не совершал, необходимо незамедлительно обратиться к сотруднику Компании.

4.5. При утрате (потере, хищении) Клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовых операций, необходимо немедленно обратиться к сотруднику Компании для смены идентификационных данных клиента (ключи, логины, пароли и т.п) и блокировки доступа в систему с использованием старых идентификационных данных.

4.3 It is recommended to restrict physical access to a computer or other device, which the Client uses for the purpose of financial transactions execution.

4.4. In case the Client receives a system notice or otherwise detects in the system transactions which were not performed by the Client, it is necessary to contact Company's representative immediately.

4.5. In case of loss (incl. theft) of the computer equipment which is used by Client to perform actions for execution of financial transactions it is necessary to contact Company's representative immediately to change identification data of the Client (keys, logins, passwords, etc.) and to block the access to the system with use of old identification data.