Рекомендации

клиентам НКО-ЦК «СПБ Клиринг» (АО) о мерах по предотвращению несанкционированного доступа к защищаемой информации в соответствии с Положением Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

1. Общие положения

1.1. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищённости должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне НКО-ЦК «СПБ Клиринг» (АО), так и на стороне клиента, находящего на банковском обслуживании в НКО-ЦК «СПБ Клиринг» (АО) (при наличии клиента, находящегося на банковском обслуживании).

1.2. Наиболее опасным является кража учётных данных – хищение личных данных клиента НКО-ЦК «СПБ Клиринг» (АО) и их незаконное использование для выполнения несанкционированных операций от имени клиента, переводов денежных средств без добровольного согласия клиента. Оптимальный способ защиты от кражи учётных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.3. Риски получения несанкционированного доступа к информации, прежде всего, связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

1.4. «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространённых способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО), либо на перехват информации, в том числе аутентификационных данных.

1.6. Средства и методы защиты информации, применяемые в НКО-ЦК «СПБ Клиринг» (АО), позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

2.2. Пользуйтесь персональными компьютерами с установленным лицензионным ПО.

2.3. Своевременно обновляйте установленное системное и прикладное ПО (установка критичных обновлений).

2.4. Не используйте права администратора при отсутствии необходимости и в повседневной практике входите в систему с учётной записью пользователя, не имеющего прав администратора.

2.5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.

2.6. Не используйте на устройстве, предназначенного для доступа к системе дистанционного банковского обслуживания (далее - ДБО), средства удалённого администрирования.

2.7. Обязательно установите и своевременно обновляйте на компьютере антивирусное ПО. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) заражённых файлов производится антивирусным средством в автоматическом режиме.

2.8. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка носителя персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

2.9. Антивирусное ПО должно запускаться автоматически, с загрузкой операционной системы.

2.10. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съёмных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

2.11. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

2.12. При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.

2.13. Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе ДБО.

2.14. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.

2.15. Рекомендуем ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты. Старайтесь не использовать компьютер, с которого Вы осуществляете доступ к системе ДБО, переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.16. Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

2.17. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), следует полностью воздержаться от использования систем ДБО и проведения платежей до исправления ситуации.

2.18. НКО-ЦК «СПБ Клиринг» (АО) не несёт ответственности в случае возникновения финансовых потерь, понесённых Клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к системе ДБО.

3. Рекомендации по защите информации от несанкционированного доступа путём предотвращения использования ложных (фальсифицированных) ресурсов сети Интернет

3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний (например, сайты банков), которым Вы доверяете, имена которых могут использоваться для сбора конфиденциальной информации обманным путём.

3.2. Злоумышленниками возможно создание фальсифицированных WEB-сайтов – их доменные имена и стили оформления могут имитировать сайты НКО-ЦК «СПБ Клиринг» (АО) и содержать ложные банковские реквизиты и контактную информацию. Вступление в какие-либо деловые отношения с лицами, представляющими такие организации и использование подобных реквизитов, рискованно и может привести к уголовному преследованию. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению конфиденциальных данных. Помните, что сайты, визуально напоминающие сайт НКО-ЦК «СПБ Клиринг» (АО) или организации разработчика ДБО, создаются специально для незаконного получения информации. В случаях обнаружения фальсифицированного сайта, копирующего дизайн официального сайта или ДБО, пожалуйста, незамедлительно сообщите об этом в НКО-ЦК «СПБ Клиринг» (АО).

3.3. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой НКО-ЦК «СПБ Клиринг» (АО) в системе ДБО, и (или) использующих зарегистрированные товарные знаки и наименование НКО-ЦК «СПБ Клиринг» (АО), необходимо удостовериться, чтобы при подключении к системе ДБО защищённое SSL-соединение было установлено исключительно с официальным сайтом ДБО. Прежде чем ввести аутентификационные данные, Клиентам необходимо проверить по информации из SSL-сертификата подлинность сайта. Работу с ДБО рекомендуется осуществлять с использованием технических средств с индивидуальными дистанционно распознаваемыми идентификационными признаками (IP и MAC-адреса), предоставленными в НКО-ЦК «СПБ Клиринг» (АО)

3.4. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.5. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.6. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.7. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счёту угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.8. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьим лицам к системе дистанционного банковского обслуживания

4.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе ДБО (системе).

4.2. Перед вводом аутентификационных данных при входе в ДБО убедитесь, что соединение установлено именно со стартовой страницы ДБО и в адресной строке web-браузера.

4.3. При работе с ДБО для обеспечения конфиденциальности весь трафик между НКО-ЦК «СПБ Клиринг» (АО) и вашим компьютером шифруется с помощью защищённого протокола TLS (Transport Layer Security). Перед началом работы в ДБО необходимо удостовериться, что соединение установлено в защищённом режиме TLS. Расположение иконки зависит от версии web-браузера, но, как правило, «закрытый замок» располагается в конце правой части адресной строки, либо в правом нижнем углу экрана. При клике на данное изображение должны отображаться сведения о сертификате, важно также проверить наличие данных сведений, так как мошеннические сайты могут содержать имитацию иконки «закрытый замок».

4.4. Рекомендуется осуществлять смену пароля доступа к системе ДБО не реже одного раза в год. Длина Вашего пароля должна быть не менее 10 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.5. Используемые в ДБО аутентификационные данные, запрещается записывать и хранить в местах, доступных посторонним лицам.

4.6. Необходимо хранить аутентификационные данные в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать аутентификационные данные (логин и пароль) к ДБО там, где доступ к нему могут получить посторонние лица.

4.7. При использовании ключевых носителей и электронных подписей для доступа к ДБО генерацию рабочих ключей электронной подписи (далее – ЭП) на ключевом носителе осуществляется владельцем ключа ЭП самостоятельно.

4.8. Использование Ключевого носителя должно осуществляться исключительно владельцем ключа ЭП. Рекомендуется хранить ключевую информацию на отчуждаемом носителе и хранить его в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа.

4.9. Необходимо отключать, извлекать Ключевой носитель, если он не используются для работы в ДБО. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами.

4.10. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем банковском счёте и т. д.).

4.11. В том случае, если Вы обнаружили, что Ваши аутентификационные данные от ДБО скомпрометированы, рекомендуем Вам незамедлительно сменить их, сообщить в НКО-ЦК «СПБ Клиринг» (АО) о факте компрометации.

4.12. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в ДБО, необходимо как можно быстрее обратиться в НКО-ЦК «СПБ Клиринг» (АО) для получения инструкций по смене пароля.

4.13. Никому не разглашайте пароль от ДБО. НКО-ЦК «СПБ Клиринг» (АО) не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).

4.14. Не пересылайте файлы с конфиденциальной информацией для работы в НКО-ЦК «СПБ Клиринг» (АО) по электронной почте или через SMS-сообщения.

4.15. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе персонала, не имеющего отношения к работе с ДБО и посторонних лиц.

4.16. Незамедлительно обращайтесь в НКО-ЦК «СПБ Клиринг» (АО) в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

4.17. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в систему, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;

4.18. Принять меры по контролю конфигурации компьютера, с использованием которого осуществляется перевод денежных средств через ДБО, и её изменения. Не допускать несанкционированных программно-аппаратных изменений конфигурации.

4.19. На компьютере для работы с ДБО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ДБО, операционной системы, web-браузеров (Yandex Browser, Microsoft Edge, Mozilla FireFox, Google Chrome и т.д.) и иного прикладного программного обеспечения. Все это позволит устранить выявленные в системном и прикладном ПО уязвимости, которые могут быть использованы третьими лицами для получения несанкционированного доступа к компьютеру и системе ДБО.

4.20. Применять на компьютере для работы с ДБО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты. Только регулярные обновление антивирусных баз и проведение антивирусных проверок позволит Вам своевременно обнаружить и предотвратить появление вредоносных программ (особенно важно контролировать обновление, если нет постоянного подключения к Интернету).

4.21. Рекомендуется применять на компьютере для работы с ДБО специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств. Это позволит значительно снизить риск удалённого управления Вашим компьютером злоумышленниками из Интернет и локальной сети, а также может предотвратить кражу конфиденциальной информации. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Компьютера только к необходимым ресурсам, и серверам обновлений разработчиков используемого программного обеспечения, минимально необходимое количество соединений по конкретным портам доступа для осуществления обмена внутри офисной сети. Любые иные подключения рекомендуется запретить.

4.22. На компьютере для работы с ДБО необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения денежных средств. Помните, что почтовый документ, полученный от Вашего контрагента, известной компании или государственной службы, может быть результатом работы злоумышленников по имитации настоящего документа или мог быть отправлен в результате вирусного заражения компьютера отправителя сообщения, в том числе и Вашего контрагента.

4.23. В случае использования в компании собственного почтового сервера, необходимо убедиться, что используемое решение поддерживает функционал анализа содержимого почтовых сообщений не только на вирусы, но и обнаруживает в безопасной среде («песочница») аномальное поведение вложений и файлов, которые могут загружаться по ссылкам из сообщений. Решения класса «песочница» не обязательно покупать и устанавливать в организации – они могут быть уже встроены в сервисы электронной почты, предоставляемые крупными провайдерами, или могут быть арендованы в виде облачного решения.

4.24. При использовании внешних сервисов электронной почты используйте сервисы, предоставляющие двухфакторную аутентификацию (ввод одноразового пароля, сгенерированного специальным приложением). Это позволит защитить направляемую на Ваш почтовый ящик информацию от доступа третьих лиц.

4.25. При работе с электронной почтой при возможности

- заблокируйте получение в электронных письмах вложений с расширениями:*.bat; *.bin; *.chm; *.cmd; *.com; *.cpl; *.dll; *.exe; *.hta; *.htm; *.js; *.jse; *.lnk; *.msi; *.ocx; *.pif; *.reg; *.scr; *.swf; *.vbe; *.vbs; *.wsf; *.wsh; *.ps1; *.ade; *.adp; *.apk; *.appx; *.appxbundle; *.ade; *.dmg; *.ex; *.ex_; *.ins; *.isp; *.iso; *.jar; *.lib; *.mde; *.msc; *.msix; *.msixbundle; *.msp; *.mst; *.nsh; *.sct; *.shb; *.vb; *.vhd; *.vxd; *.wsc;

- проверяйте письма, в которых содержатся призывы к действиям («открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

- не переходите по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);

- не нажимайте на ссылки из электронных писем если они заменены на слова, не наводите на них мышкой и не просматривайте полный адрес сайтов;

- проверяйте ссылки, даже если письмо получено от знакомого пользователя;

- не открывайте вложения, если в них содержатся архивы с паролями;

- внимательно относитесь к электронным письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;

- в случае появления сомнений – удаляйте сообщение.

4.26. Не допускается работать с ДБО на компьютерах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования ключа ЭП и другой аутентификационной информации. Крайне нежелательно использовать для работы в системе ДБО публичные беспроводные сети (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользоваться «мобильным Интернетом» (LTE/GPRS/EDGE/HSPA/3G соединение). При использовании компьютеров и сетей доступа, не контролируемых Вами, существенно возрастает риск компрометации Ваших учётных данных, кражи денежных средств и конфиденциальных данных т.к. злоумышленники /другие пользователи могли установить/заразить вредоносным ПО данное оборудование. В случае, если вы по каким-либо причинам не смогли выполнить данную рекомендацию, постарайтесь в кротчайшие сроки подключится к системе ДБО с доверенного устройства из надёжной сети и измените пароль доступа на новый.

4.27. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере для работы с ДБО (для учетной записи с правами администратора – не менее 16 символов, для пользовательской учетной записи – не менее 10 символов). Работу с ДБО на компьютере осуществлять только под учётной записью с ограниченными правами в операционной системе. Не допускать штатную работу в ДБО под учётной записью с правами администратора в операционной системе компьютера.

4.28. В случае компрометации или подозрении на компрометацию закрытого ключа ЭП, для предотвращения несанкционированного доступа, в том числе при утрате (потере, хищении) Ключевого носителя, с использованием которого Клиент осуществляет доступ к ДБО, Клиенту необходимо незамедлительно обратиться в НКО-ЦК «СПБ Клиринг» (АО) для блокирования скомпрометированных ключей ЭП.

4.29. Регулярно проводить контроль сумм и получателей электронных документов в ДБО, а также контролировать количество и сумму отправленных электронных документов.

4.30. Регулярно контролировать состояние своих счетов и незамедлительно сообщать в НКО-ЦК «СПБ Клиринг» (АО) обо всех подозрительных или несанкционированных изменениях.

4.31. При подготовке платёжных документов на других компьютерах (документов, содержащих реквизиты для платежа) учитывайте, что подмена реквизитов может произойти на любом из компьютеров, где данная информация будет обрабатываться или передаваться.

4.32. При обслуживании компьютера сотрудниками технической поддержки организации Клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий.

4.33. Не передавать Ключевой носитель сотрудникам технической поддержки для проверки работы ДБО, проверки настроек взаимодействия с НКО-ЦК «СПБ Клиринг» (АО) и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить Ключевой носитель к компьютеру, убедиться, что пароль доступа к ключу вводится, не допуская ознакомления с ним посторонних лиц.

4.34. В случае передачи (списания) компьютера, на котором ранее была установлена ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу организации Клиента, в том числе следы работы в ДБО.

4.35. При увольнении ответственного сотрудника, имевшего доступ к ключевому носителю, уведомить НКО-ЦК «СПБ Клиринг» (АО) об его увольнении и обеспечить безопасность работы ДБО с использованием электронных документов и ЭП для нового ответственного сотрудника, назначенного клиентом для обеспечения работы с ДБО.

4.36. Если вам был передан USB-накопитель или вы получили по электронной почте заархивированные с паролем файлы или файлы офисных форматов doc, docx, xls, xlsx, ppt, pptx; файлы, содержащие макросы docm, xlsm, pptm, а также файлы Adobe Acrobat формата PDF, для открытия которых необходимо ввести пароль – помните, что такие файлы не могут быть проверены средствами обнаружения вредоносного ПО (антивирус или «песочница»), поэтому представляют высокий риск для заражения компьютера. Не используйте такие файлы на компьютере, с которого осуществляется доступ в систему ДБО. Если вам нужны такие файлы – работайте с ними на других компьютерах, предварительно убедившись, что файл получен из надёжного источника, и пароль был установлен именно его отправителем. Если файл в архиве, его необходимо извлечь из архива и проверить антивирусным ПО.

4.37. Очень часто злоумышленники для получения удалённого доступа в сеть компании используют различные тактики социальной инженерии. Одна из таких схем – попытка узнать у пользователей их учётные записи (логин) и пароль по телефону или с помощью различных сообщений в мессенджерах, поддельных страниц в сети Интернет. Злоумышленники используют современные средства коммуникации – электронную почту контрагента, к которой они смогли получить доступ, или почтовый ящик на бесплатном сервисе, оформленный и похожий на настоящий адрес контрагента, мессенджеры. Ещё одним вариантом проникновения в сеть компании является схема, когда возле офиса компании подбрасывается USB-носитель (флешка), на которой может быть нанесена маркировка/логотип компании или какой-либо другой логотип, который может заинтересовать сотрудников и побудить их попытаться открыть содержимое носителя на рабочем компьютере. В результате открытия такого носителя компьютер может оказаться под удалённым управлением злоумышленника.

4.38. Необходимо корректно завершать работу в ДБО, используя для этого пункт меню «Выйти из системы».

4.39. Контролируйте в системе ДБО реквизиты получателя при подписи и отправке в НКО-ЦК «СПБ Клиринг» (АО) ЭД, импортированных из внешних систем (например 1С и др.), чтобы не допустить случаи подмены реквизитов получателей вредоносным ПО в процессе импорта.

4.40. Проводите дополнительную проверку компании контрагента. Введя ИНН организации на поисковом сайте в Интернет можно, используя бесплатные сервисы, узнать об организации: дату регистрации, ФИО генерального директора / учредителя, вид деятельности, а также были ли изменения в её руководстве. Для кражи денежных средств злоумышленники обычно используют либо компании, которые были недавно зарегистрированы на подставных лиц, либо юридические лица, которые были приобретены у предыдущих владельцев вместе с расчётным счётом, ДБО и пластиковыми картами для быстрого снятия похищенных денежных средств. Во втором случае в информации о компании может отображаться дата внесения изменений в регистрационные данные компании.

5. Правила поведения в случае, если произошёл инцидент информационной безопасности

5.1. Если с помощью антивирусного ПО Вы обнаружили на компьютере, где используется система ДБО, или на любом другом компьютере, который используется для обработки платёжных документов, вирус, необходимо:

5.1.1. Отключить компьютер от телекоммуникационной сети (Интернет), вытащив из компьютера сетевой кабель или отключив WiFi соединение.

5.1.2. Осуществить с другого компьютера поиск в интернет по названию вируса, чтобы понять – может ли данный вирус использоваться как банковский троян, вирус для подмены реквизитов или для осуществления удалённого управления компьютером.

5.1.3. Если вирус соответствует указанным выше категориям, Вам необходимо с другого компьютера направить в НКО-ЦК «СПБ Клиринг» (АО) сообщение о вирусном заражении и возможном хищении денежных средств.

5.1.4. Не производите лечение файлов с помощью антивирусного ПО и не удаляйте какую-либо информацию с заражённого компьютера. В случае кражи денежных средств Вам могут потребоваться цифровые улики, оставленные злоумышленниками.

5.1.5. После обращения в НКО-ЦК «СПБ Клиринг» (АО) следуйте полученным инструкциям.