НАЦИОНАЛЬНАЯ КАСТОДИАЛЬНАЯ КОМПАНИЯ

Утверждены приказом
Генерального директора АО «НКК»
от 26.09.2019 № П01-26/09-19

РЕКОМЕНДАЦИИ

по соблюдению информационной безопасности клиентами АО «НКК» в целях противодействия незаконным финансовым операциям

Москва · 2019

Оглавление

1. Общие положения документа

1.1 В целях противодействия незаконным финансовым операциям, и в соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» АО «Национальная кастодиальная компания» (далее – АО «НКК»), уведомляет организации, являющиеся клиентами АО «НКК» (далее – Организации), о необходимости соблюдения рекомендаций по информационной безопасности при осуществлении существенных для Организации, в том числе финансовых операций (далее – Критичные операции).

1.2 Применение совокупности мер, направленных на непосредственное обеспечение защиты информации, стандартизированных ГОСТ Р 57580.1-2017[1], позволяет снизить в значительной степени риски, связанные с нарушением информационной безопасности, и минимизировать возможные негативные последствия в случае их реализации, но не гарантирует абсолютной невозможности нарушения информационной безопасности.

2. Основные положения документа

2.1 Нарушения в области защиты информации, влияющие на бизнес-процессы Организации, а также на целостность и конфиденциальность информации, могут быть обусловлены следующими факторами:

- воздействие вредоносного кода на устройства, применяемые для информатизации бизнес-процессов, с использованием которых совершаются Критичные операции;
- несанкционированный доступ к информации лицами, не обладающими на это правом и осуществления ими Критичных операций;
- хищение или утеря носителей ключей электронной подписи, с использованием которых осуществляются Критичные операции;
- совершение в отношении организации иных противоправных действий, связанных с нарушением информационной безопасности.

[1] ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» // http://protect.gost.ru/document1.aspx?control=31&id=218176

2.2 Во избежание реализации сценариев, перечисленных в п. 2.1, настоятельно рекомендуется осуществление мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации, в том числе автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов Организации, описанных в ГОСТ Р 57580.1-2017.

2.3 При осуществлении Критичных операций необходимо принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления. Такие риски могут быть обусловлены (включая, но не ограничиваясь) следующими причинами:

- кража пароля и идентификатора доступа или иных конфиденциальных данных, например, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода; и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- внедрение в устройство вредоносного кода, который позволит злоумышленникам осуществить Критичные операции от имени Организации;
- кража или несанкционированный доступ к устройству, с использованием которого Организация пользуется услугами/сервисами АО «НКК» для получения данных и/или несанкционированного доступа к сервисам АО «НКК» с этого устройства;
- использование злоумышленниками утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться АО «НКК» в качестве дополнительной защиты от несанкционированных финансовых операций, в целях преодоления данной защиты;
- получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, номеров счетов, паспортных данных и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется по телефону сотрудником АО «НКК» и просит сообщить ему эти данные; или направляет фальсифицированные сообщения от имени АО «НКК» по электронной почте либо письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства, используемого для осуществления Критичных операций, либо для информационного обмена с АО «НКК»;

- перехват электронных сообщений и получение несанкционированного доступа к отчетам, выпискам и прочей финансовой информации в случае, если электронная почта Организации используется для информационного обмена с АО «НКК»;
- получение несанкционированного доступа к электронной почте Организации в целях, отправки фальсифицированных сообщений от имени Организации в АО «НКК».

3. Принципы конфиденциальности

3.1 Полученные от АО «НКК» данные, предназначенные для аутентификации Организации, следует хранить в тайне с принятием необходимых мер, направленных на предотвращение их разглашения. В случае компрометации указанных данных следует незамедлительно обратиться в АО «НКК», для их смены или блокировки.

3.2 Если имеет место запрос от имени АО «НКК» у Организации данных о счетах, паспортных данных, номеров кредитных/дебетовых карт, кодовых слов, паролей, используемых для взаимодействия с АО «НКК», следует проявлять должную бдительность, и перед раскрытием конфиденциальной информации об Организации и персональных данных ее сотрудников, убедиться, что запрос исходит именно от АО «НКК», например, перезвонив самостоятельно по телефонному номеру, указанному на официальном сайте АО «НКК» в сети Интернет.

4. Правила безопасной работы в сети Интернете

4.1 Не следует нажимать на всплывающие окна, которые содержат рекламу. Желательно настроить браузер, используемый Организацией, на автоматическую блокировку таких окон.

4.2 Не следует посещать непроверенные и небезопасные сайты. Это может привести к непреднамеренной загрузке на компьютер вирусов и шпионских программ.

4.3 Не следует читать подозрительных электронных писем от незнакомых физических или юридических лиц, так как они могут содержать вирусы. Следует внимательно читать темы сообщений.

4.4. Если нет уверенности в том, что электронное письмо пришло из надежного источника, не следует открывать его.

4.4 Не следует доверять дружественному тону электронных сообщений или уведомлениям о срочности содержащейся в них просьбы.

4.5 Не следует переходить по содержащимся в подозрительном электронном письме ссылкам, а также открывать вложенные файлы, особенно если в письме сообщается, что проблема требует безотлагательного решения, для чего требуется срочно открыть приложенный файл, имеющий имеет файловое расширение «exe».

4.6 Следует максимально ограничить использование Интернет-пейджеров (ICQ, Skype и пр.), а также мессенджеров (Wiber, WhatsApp и пр.).

4.7 Следует внимательно относиться к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений следует просканировать компьютер на наличие вирусов или шпионского ПО.

5. Меры безопасности при работе с электронной подписью

5.1 Для защиты ключей ЭП клиента от хищения с использованием вредоносных программ рекомендуется использовать сертифицированные USB-токены («iBank 2 Key», «Рутокен ЭЦП», «MS_KEY K», «JaCarta ГОСТ»).

5.2 В случае отсутствия USB-токена, файл-хранилище ключей рекомендуется сохранить на съемном носителе (USB-накопитель). Не допускается сохранять его в местах, где к нему может получить доступ кто-либо, кроме уполномоченных лиц. Съемный носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа.

5.3 Пароль на доступ к ключу ЭП должен быть известен только владельцу. Пароль должен быть сложным (более 8 знаков). Не следует хранить пароли в открытом доступе (компьютер, мобильное устройство).

5.4 Не следует допускать постоянного и бесконтрольного подключения к компьютеру USB-токена с ключами ЭП.

5.5 Не следует никому передавать USB-токен с ключами ЭП.

5.6 Не следует использовать USB-токен в Интернет-кафе и прочих общественно-доступных местах, а также там, где нет уверенности в безопасности компьютеров.

5.7 При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) следует обязательно сообщить о данном инциденте информационной безопасности в организацию, в отношении ресурсов которой осуществляется доступ и при необходимости заблокировать ключи ЭП.

6. Меры по защите компьютера

6.1 Следует использовать в работе только лицензионное программное обеспечение (далее - ПО). Не следует загружать и устанавливать ПО, полученное из непроверенных источников.

6.2 Следует использовать современные операционные системы (далее - ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Следует своевременно устанавливать исправления и обновления для ОС. Рекомендуется включить автоматическое обновление ОС, которое будет автоматически устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.

6.3 Следует использовать системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.

6.4 Следует использовать и оперативно обновлять специализированное ПО для защиты информации: антивирусное ПО (следует регулярно проверять компьютер на вирусы, как минимум раз в неделю); персональные межсетевые экраны; средства защиты от несанкционированного доступа и пр.

6.5 Не рекомендуется подключать к компьютеру съемные носители, не проверенные на наличие вирусов.

6.6 Рекомендуется использовать сложные пароли, для входа в компьютер.