УТВЕРЖДЕНЫ
Приказом
КСП Капитал УА ООО
от 19.10.2020
№П/2020/10/19/1

КСП КАПИТАЛ
УПРАВЛЕНИЕ
АКТИВАМИ

Рекомендации по информационной безопасности для клиентов Общества с ограниченной ответственностью «КСП Капитал Управление Активами» в целях противодействия незаконным финансовым операциям

Москва
2020

В соответствие 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» Общество с ограниченной ответственностью «КСП Капитал Управление Активами» (далее по тексту - Организация) доводит до сведения своих клиентов основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на обеспечение защиты информации, процессов, ресурсов, технического и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее используются термины, определение которых содержится в ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года N822-ст «Об утверждении национального стандарта») позволяют снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их корректной реализации.

В связи с тем, что требования информационной безопасности также могут быть отражены в договорах, регламентах, инструкциях и иных документах Организации, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

В целях снижения риска реализации инцидентов информационной безопасности – нежелательных или неожиданных событий защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов и (или) нарушить конфиденциальность, целостность и доступность информации вследствие:

- несанкционированного доступа к информации лицами, не обладающими соответствующими правами на выполнение любых операций, предусмотренных функционалом оператора (в том числе финансовых);
- потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;
- воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;
- совершения иных противоправных действий, связанных с информационной безопасностью,

рекомендуется соблюдать ряд мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в том числе автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов) и минимизации рисков:

1. При осуществлении критичных (финансовых) операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых и иных операций, влекущих негативные

последствия, лицами, не обладающими соответствующими правами. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими фактами:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода, и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;

b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от имени владельца устройства;

c. Использование злоумышленником утерянного или украденного мобильного устройства / планшета / ноутбука и т.п. для доступа к личной почте владельца устройства, получение кодов, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций;

d. Кража или несанкционированный доступ к устройству, с которого осуществляется использование услуг / сервисов Организации для получения данных и/или несанкционированный доступ к сервисам Организации с этого устройства;

e. Получение пароля и идентификатора доступа и/или кода из направленных на электронную почту сообщений и/или кодового слова или прочих конфиденциальных данных, в том числе паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием в случаях использования метода социальной инженерии (злоумышленник представляется сотрудником Организации, сотрудником информационной безопасности, техническим специалистом, и иным лицом, руководствуясь нерегламентированными и неправомерными действиями/функциями сотрудника, например, с просьбой сообщить конфиденциальные данные; направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, приводящее к негативным последствиям (в том числе финансовым)). Рекомендуется проверять правомочность сотрудника, который выступает от лица Организации и, при возможности, учитывать функциональные возможности данного лица, представившегося сотрудником Организации, а также проверять контакты сотрудника (например, телефон или почтовый адрес, с которого данный сотрудник производит взаимодействие с клиентом);

f. Перехвата электронных сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта используется для информационного обмена с Организацией, использование и отправка сообщений от имени пользователя.

2. Для снижения риска финансовых потерь необходимо:

a. Обеспечить защиту устройства, которое используется для взаимодействия с Организацией и пользования услугами/сервисами Организации. К указанным мерам защиты включая, но не ограничиваясь, могут быть отнесены:

- Использование только лицензионного программного обеспечения (далее – ПО), полученного из доверенных источников;
- Использование поддерживаемого производителем системного ПО;
- Запрет на установку программ из неизвестных источников;
- Контроль и учет установленного ПО, а также, наличие регламентированного перечня разрешенного ПО на выделенном автоматизированном рабочем месте/сервере;

- Наличие, настройка, аудит и корректное функционирование средств защиты: антивирусной защиты, межсетевого экранирования, системы обнаружения и предотвращения вторжений, системы защиты информации от несанкционированного доступа. При этом для корректного и достаточного построения системы защиты, как с организационной, так и с технической точки зрения, рекомендуется произвести моделирование угроз и нарушителей для дальнейшего определения необходимости в установке тех или иных средств защиты;
- Регулярное и своевременное обновление баз средств защиты (например, регулярное обновление сигнатур антивируса и системы обнаружения и предотвращения вторжений);
- Настройка и аудит прав доступа к устройству и помещению, в котором находится устройство, с целью предотвращения несанкционированного доступа и замены/кражи компонентов устройства;
- Соблюдение корректного хранения и использования устройства с целью избежания рисков кражи, несанкционированного доступа и/или утери;
- Использование проверенных версий операционных систем (например, совместимых со средствами защиты);
- Учет совместимости системного и прикладного ПО со средствами защиты;
- Использование паролей не менее 8 символов, содержащих спецсимволы, строчные и заглавные буквы, при необходимости, использование токенов, упраздняющих необходимость ручного ввода паролей, или смешанного типа идентификации и аутентификации. При смене пароля рекомендуется использовать пароль, отличающийся от предыдущего не менее чем на 3 символа.

b. Обеспечить конфиденциальность:

- Хранить в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Организации: пароли, коды, кодовые слова, ключи электронной подписи/шифрования;
- В случае компрометации немедленно принять меры для смены и/или блокировки;
- Соблюдать принцип разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, о CVC\CVV кодах, и иных данных. В случае если запрашивается указанная информация в привязке к сервисам Организации по возможности необходимо оценить ситуацию и уточнить полномочия и процедуру через независимый канал, например, через телефон/электронную почту Организации.

c. Проявлять осторожность и предусмотрительность:

- Рекомендуется проявлять осторожность при получении электронных писем со ссылками и вложениями, т.к. они могут привести к заражению устройства вредоносным кодом или направить на «фишинговую» страницу, замаскированную под сайт/личный кабинет Организации, при входе в который субъект оставляет идентификационные/аутентификационные данные для входа злоумышленника через официальный сайт/личный кабинет Организации. При занесении вредоносного кода на устройство и отсутствии эффективных антивирусных средств защиты, злоумышленник может получить доступ к любым данным и информационным системам на устройстве, а также продолжить заражение иных устройств через зараженное;

- Рекомендуется внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть направленно от злоумышленника, который маскируется под Организацию или иных доверенных лиц;
- Рекомендуется проявлять осторожность при просмотре/работе с Интернет-сайтами, так как вредоносный код может быть загружен с сайта;
- Рекомендуется пользоваться доверенным списком Интернет-ресурсов, исключая риск заражения через иные Интернет-ресурсы;
- Рекомендуется проявлять осторожность при обращении к файлам из неизвестных источников, в том числе к архивам с паролем, зашифрованным файлам/архивам;
- Рекомендуется избегать использование системы удаленного доступа с неизвестных устройств, которые не контролируются субъектом входа или администратором субъекта: на устройствах возможен вредоносный код, собирающий идентификационные и аутентификационные или иные данные, либо способный подменить операцию;
- Рекомендуется проявлять осведомленность с информацией в прессе, информационных ресурсах о последних/актуальных уязвимостях (например, «Банк данных угроз безопасности информации ФСТЭК России», расположенный по адресу: https://bdu.fstec.ru/);
- При взаимодействии с Организацией, рекомендуется осуществлять контакт только по номеру телефона/электронной почте, указанному(ой) в договоре или на официальном сайте Организации;
- Рекомендуется учитывать, что от лица Организации не производятся звонки или сообщения, в которых требуют передать, например, коды, пароли, номера карт, аутентификационные данные, кодовые слова;
- При компрометации аутентификационных данных или подозрении на несанкционированный доступ и/или компрометацию устройства рекомендуется сменить пароль, сообщить, при наличии, в отдел информационной безопасности, заблокировать доступ, обратившись в Организацию, в отношении ключевой информации – отозвать скомпрометированный ключ электронной подписи/шифрования, в соответствии с правилами, отраженными в договоре и документах, связанных с исполнением договора;
- Рекомендуется производить резервирование данных с целью скорейшего восстановления рабочего состояния устройства;
- Для осуществления финансовых операций рекомендуется использовать отдельное, защищенное устройство, доступ к которому есть только у пользователя.

d. При работе с ключами электронной подписи рекомендуется:

- Использовать для хранения ключей электронной подписи внешние носители, с выделенным хранением и контролем доступа, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например, e-token, смарт-карта и т.п.;
- С целью исключения ситуаций компрометации ключевых носителей не оставлять без присмотра ключевые носители и не передавать третьим лицам, извлекать носители из устройств, если ключевые носители не используются для работы;
- Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли в открытом виде на автоматизированном рабочем месте/мобильном устройстве.

e. При работе на автоматизированном рабочем месте необходимо:

- Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
- Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
- Использовать средства защиты информации, перечисленные выше в настоящих Рекомендациях (межсетевые экраны и средства защиты от несанкционированного доступа, антивирусы, средства контроля конфигурации устройств и пр.), регулярно обновляя базы средств защиты;
- Использовать сложные пароли, требования к которым приведены выше в настоящих Рекомендациях;
- Ограничить доступ к автоматизированному рабочему месту, мобильному устройству, в том числе в помещение, в котором находятся используемые устройства, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

f. При работе с мобильными устройствами рекомендуется:

- Не оставлять мобильное устройство без присмотра, исключить несанкционированное использование мобильного устройства и вход в используемые сервисы/ресурсы;
- Установить на мобильном устройстве пароль для доступа к устройству и сервису.

g. При обмене информацией через сеть Интернет рекомендуется:

- Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
- Не вводить персональную/аутентификационную информацию на подозрительных сайтах и других неизвестных ресурсах;
- Ограничить посещения сайтов сомнительного содержания, используя доверенный «пул» Интернет-ресурсов;
- Не сохранять пароли в памяти Интернет-браузера;
- Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
- Не открывать файлы полученные (скачанные) из неизвестных источников.

При подозрении компрометации идентификационных или аутентификационных данных, подозрении нарушений штатного функционирования средств вычислительной техники, которые способны повлечь совершения незаконных финансовых операций необходимо незамедлительно обращаться в Организацию.