«Утверждено»
Приказ Генерального директора
ООО «Управляющая компания
«Смарт капитал»
№ 2007232 от 20.07.2023

Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям для клиентов Общества с ограниченной ответственностью «Управляющая компания «Смарт капитал»

В соответствии с требованиями Положения Банка России от 20.04.2021 № 757-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 «Управляющая компания «Смарт капитал» (далее - Организация) доводит до сведения своих клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности - совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

В целях снижения риска реализации инцидентов информационной безопасности (ГОСТ Р 57580.1-2017) – 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 правом осуществления значимых (критичных) операций (в т.ч. 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 следующими фактами:

а. 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 в качестве дополнительной защиты для несанкционированных финансовых операций;

d. кража или несанкционированный доступ к устройству, с которого осуществляется использование услуг / сервисов для получения данных и/или несанкционированный доступ к сервисам 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, когда злоумышленник представляется сотрудником финансовой 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);

f. перехват 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. Перечень необходимых мер для снижения финансовых потерь.

a. Меры по обеспечению защиты устройства, которое используется для взаимодействия с Организацией и пользования услугами/сервисами Организации, к которым 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. Меры по обеспечению конфиденциальности, для чего следует:

✓ 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.

c. Проявление предосторожности и предусмотрительности:

✓ 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 Организации, где субъект может оставить свои идентификационные/аутентификационные данные. 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;

✓ при обращении к файлам из неизвестных источников, в том числе к архивам с паролем, зашифрованным файлам/архивам;

✓ при просмотре/работе с Интернет-сайтами, так как вредоносный код может быть загружен с сайта;

✓ внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть направленно от злоумышленника, который маскируется под Организацию или иных доверенных лиц;

✓ пользоваться доверенным списком Интернет-ресурсов, исключая риск заражения через иные Интернет-ресурсы;

✓ 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;

✓ производить резервирование данных недоступным для потенциального вредоносного кода способом с целью скорейшего восстановления рабочего состояния устройства;

✓ для осуществления финансовых операций использовать отдельное, защищенное устройство, доступ к которому есть только у пользователя;

✓ при оплате покупок в сети Интернет с помощью банковской карты использовать только варианты, где реализована технология 3D Secure (подтверждение операций с использованием одноразового кода);

✓ при взаимодействии с Организацией осуществлять контакт только по номеру телефона/электронной почте, указанному(ой) в договоре или на официальном сайте Организации www.smart-cap.ru;

✓ учитывать, что от лица Организации не производятся звонки или сообщения, в которых требуют передать, например, коды, пароли, номера карт, аутентификационные данные, кодовые слова.

d. При работе с ключами электронной подписи рекомендуется:

✓ использовать для хранения ключей электронной подписи внешние носители с выделенным хранением и контролем доступа;

✓ 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.