**Руководство по соблюдению клиентами АО «РЕГИОН ЭсМ» правил информационной безопасности**

Настоящее Руководство по соблюдению клиентами АО «РЕГИОН ЭсМ» информационной безопасности при использовании информационных систем АО «РЕГИОН ЭсМ» (далее – Руководство и Общество соответственно) разработано Обществом в соответствии с требованиями Положения 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 (утв. Банком России 17.04.2019 № 684-П) и подлежит доведению до сведения клиентов Общества путем размещения на сайте Общества в сети Интернет.

**1. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц.**

* 1. Клиенты Общества несут риски возможных финансовых потерь вследствие следующих обстоятельств:
* получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации;
* утрата (потеря, хищение) носителей ключей электронной подписи, с использованием которых осуществляются финансовые операции;
* воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции (персональный компьютер, планшет, мобильный телефон и пр., далее – устройство);
* совершение в отношении клиента Общества иных противоправных действий.
	1. При осуществлении финансовых операций клиентам Общества следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами. Такие риски могут возникать, помимо прочего, вследствие следующих событий:
* кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа, посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
* установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Общества;
* использования злоумышленником утерянного или украденного телефона для получения СМС-кодов, которые могут применяться Обществом в качестве элемента простой электронной подписи либо дополнительного способа идентификации клиента, для подтверждения несанкционированных финансовых операций;
* кража или несанкционированный доступ к устройству, с которого клиент Общества пользуется услугами Общества для получения данных и/или несанкционированного доступа к услугам с этого устройства.
* получение злоумышленниками персональных данных клиента Общества, пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием. Описанный риск может реализоваться, помимо прочего, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит клиента сообщить ему указанные конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
* перехват почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Обществом. В случае получения доступа к почте клиента, отправка сообщений Обществу от его имени.
	1. Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несет Владелец учётных данных. Общество не несет ответственности в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

**2. Меры по предотвращению несанкционированного доступа к защищаемой информации.**

* 1. Клиентам Общества следует предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации таких клиентов. Для указанных целей клиентам Общества следует принять ,помимо прочего, следующие меры:
		1. Обеспечение надлежащей защиты устройства, с помощью которого клиенты пользуются услугами Общества и обмениваются информацией с Обществом:
* использование только лицензированного программного обеспечения, полученного из доверенных источников.
* запрет на установку программ из непроверенных источников.
* использование средств электронной безопасности и защиты, таких как антивирус с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и прочих;
* настройка прав доступа к устройству таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем;
* хранение и использование устройства спосоом, исключающим риски его кражи и/или утери.
* своевременное обновление операционной системы устройства;
* активация парольной или иной защиты для доступа к устройству;
* незамедлительное изменение учетных данных, используемых для доступа к услугам Общества, после удаления с устройства обнаруженного вредоносного программного обеспечения;.
* передача защищаемой информации клиентов только через безопасные беспроводные беспроводные сети. Работая в общедоступных беспроводных сетях клиентам не следует вводить учетные данные, используемые для доступа к услугам Общества.
	+ 1. Обеспечение конфиденциальности защищаемой информации:
* хранение в тайне аутентификационных/идентификационных данных и ключевой информации, полученных от Общества: паролей, СМС-кодов, кодовых слов, закрытых ключей, сертификатов. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Общества о их компрометации;
* соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, CVC/CVV кодах. В случае запроса у клиента указанной информации в связи с оказанием услуг Обществом, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру раскрытия информации через независимый канал связи, например, в контакт-центре Общества.
	+ 1. Проявление осторожности и предусмотрительности:
* клиенту Общества следует проявлять повышенную осторожность в следующих обстоятельствах:
	1. при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;
	2. при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;
	3. при получении файлов в архиве с паролем, так как в таком файле может быть вредоносный код.

Вредоносный код, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве.

* следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц;
* клиентам Общества не следует заходить в системы удаленного доступа с недоверенных устройств, которые клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
* при наличии в средствах массовой информации и на сайте Общества сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению;
* при обращении в контакт-центр Общества клиенту следует осуществлять звонок только по номеру телефона, указанному на сайте Общества в сети Интернет;
* при предоставлении клиентом доступа к устройству третьим лицам клиент несет риск загрузки такими лицами на устройство вредоносного кода. В случае утраты устройства злоумышленники могут воспользоваться им для доступа к системам Общества от лица клиента;
* при утрате телефона, используемого для получения СМС-кодов или доступа к системам Общества, клиенту необходимо совершить следующие действия:
1. проинформировать Общество по телефону контакт-центра и/или адресу электронной почты, указанным на сайте Общества в сети Интернет;
2. по возможности оперативно с учетом прочих рисков и особенностей использования телефона клиента заблокировать и перевыпустить сим-карту;
3. сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество;
* при подозрении на несанкционированный доступ и/или компрометацию устройства клиенту необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество, в отношении ключевой информации, если это уместно для оказываемого клиенту Обществом вида услуг – отозвать скомпрометированный закрытый ключ;
* клиенту рекомендуется использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;
* в случае выхода из строя сим карты, используемой для получения СМС-кодов, клиенту следует незамедлительно обратиться к своему сотовому оператору для уточнения причин неработоспособности сим-карты и восстановления связи.
* контактная информация, предоставленная клиентом Обществу, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости с представитель Общества мог оперативно связаться с клиентом.
	+ 1. При работе с ключами электронной подписи необходимо:
* использовать для хранения секретных ключей электронной подписи внешние носители;
* крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы;
* использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве.
	+ 1. При работе с защищаемой информацией на персональном компьютере 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 антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
* использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
* использовать сложные пароли;
* ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.
	+ 1. При работе с мобильным устройством необходимо:
* не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;
* использовать только официальные мобильные приложения, загруженные при помощи официального магазина приложений;
* не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в смс-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;
* установить на устройстве пароль для доступа к устройству.
	+ 1. При обмене информацией через сеть Интернет необходимо:
* 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 информацию на подозрительных сайтах и других неизвестных клиенту ресурсах;
* исключить посещение сайтов сомнительного содержания;
* не сохранять пароли в памяти интернет-браузера, если третьи лица имеют доступ к компьютеру;
* не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;
* открывать файлы только известных расширений;
	1. При подозрении в компрометации ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо обращаться в Общество по телефону контакт-центра и/или адресу электронной почты, указанным на сайте Общества в сети Интернет.