

Утверждено Приказом Генерального директора  
АО ИК «ЦЕРИХ Кэпитал Менеджмент»

№20 О/Д от 20.02.2020

А.С. Тузов /



**Рекомендации для клиентов АО ИК «ЦЕРИХ Кэпитал Менеджмент» по обеспечению информационной безопасности, защите информации от воздействия вредоносного кода при работе в сети «Интернет» и использовании системы дистанционного обслуживания в целях противодействия незаконным финансовым операциям**

### **Общие положения**

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 ИК «ЦЕРИХ Кэпитал Менеджмент» (далее по тексту - Компания) доводит до сведения своих Клиентов основные рекомендации по защите информации от воздействия вредоносных программ в целях противодействия незаконным финансовым операциям.

Настоящие Рекомендации подготовлены в целях защиты информации от воздействия программных кодов, возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а так же мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

### **Определение терминов и сокращений**

В целях настоящих Рекомендаций указанные ниже термины и сокращения используются в следующих значениях:

**вредоносная программа (вредоносный код)** - любое программное обеспечение (программный код), приводящее к нарушению штатного функционирования средства вычислительной техники; предназначенное для получения несанкционированного доступа к вычислительным ресурсам устройства Клиента или к информации, хранимой на устройстве Клиента с целью несанкционированного использования ресурсов устройства Клиента или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу устройства Клиента путем внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование Клиентов – пользователей Систем дистанционного обслуживания, и приводит к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче защищаемой и иной информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи;

**защищаемая информация:** 1) информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Компании и (или) Клиентами Компании; 2) информация, необходимая Компании для авторизации своих Клиентов в целях осуществления финансовых операций и удостоверения права Клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом; 3) информации об осуществленных

Компанией и ее Клиентами финансовых операциях; 4) ключевая информация средств криптографической защиты информации, используемая Компанией и ее Клиентами при осуществлении финансовых операций (в предусмотренных договорами на оказание услуг на рынке ценных бумаг случаях).

**неуполномоченные лица** – лица, не обладающие правом осуществления торговых и финансовых операций от имени Клиента;

**несанкционированный доступ** - незаконное либо не разрешенное обладателем информации использование возможности получения информации и ее использования.

**ПО** – программное обеспечение;

**пользователь (Клиент)** - обладатель защищаемой информации, используемой для проведения торговых и финансовых операций в рамках исполнения заключенных между Компанией и Клиентом договоров на обслуживание на рынке ценных бумаг;

**сайт Компании** – официальный сайт Компании в сети «Интернет», размещенный по адресу <https://www.zerich.com>;

**съемный носитель информации** – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (флэш-накопитель, CD и т.д.);

**Система дистанционного обслуживания** – системы дистанционного обслуживания Клиентов Компании (Личный кабинет Simple, ИТС QUIK и т.д.);

**сеть «Интернет»** – всемирная система объединённых компьютерных сетей для хранения, обработки и передачи информации (информационно-телекоммуникационная сеть «Интернет»);

**устройство Клиента** – устройство, с использованием которого Клиентом совершаются действия в целях осуществления финансовой операции. К таким устройствам относятся персональные компьютеры, различного рода портативные компьютеры (ноутбуки, нетбуки, смартбуки), а также мобильные телефоны, смартфоны и т.д. (далее – **мобильное устройство**).

Иные термины, специально не определенные настоящими Рекомендациями, используются в значениях, установленных законами и иными нормативными правовыми актами Российской Федерации.

**Для снижения риска финансовых потерь Компания рекомендует Клиентам:**

**1. Обеспечьте конфиденциальность информации -**

1.1. Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Компании или сформированные самостоятельно в системе дистанционного обслуживания Компании: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и/или блокировки;

1.2. Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Компании по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Компании;

**2. Соблюдайте осторожность и предусмотрительность:**

2.1. Будьте осторожны при получении электронных писем со ссылками и вложениями, так как они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;

2.2. Внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Компанию или иных уполномоченных лиц;

2.3. Будьте осторожны при работе с Интернет-сайтами, так как вредоносный код может быть загружен с сайта;

2.4. Будьте осторожны с файлами из новых или «недоверенных» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);

2.5. Не заходите в системы удаленного доступа с незнакомых (чужих) устройств, которые Вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

2.6. При наличии в рамках Вашей услуги сервиса контакт- центра - осуществляйте звонок только по номеру телефона, указанному в договоре или на сайте Компании. Имейте в виду, что от лица Компании не могут поступать звонки или сообщения, в которых от вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д. Кодовое слово может быть запрошено только, если вы сами позвонили в контакт – центр Компании;

2.7. Если Вы передаете Ваш телефон и/или устройство другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для несанкционированного доступа к системам дистанционного обслуживания Компании. В связи с этим при утере, краже телефона (SIM-карты), используемого для получения СМС-кодов или доступа к системам дистанционного обслуживания, необходимо незамедлительно проинформировать Компанию через контактный центр. Также целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить SIM-карту, а также сменить пароль в системе дистанционного обслуживания;

2.8. При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Компанию, в отношении ключевой информации, если это уместно для вашей услуги – отзвать скомпрометированный ключ электронной подписи/шифрования, в соответствии с правилами, отраженными в договоре, приложениях к договору и иных документах, связанных с исполнением договора;

2.9. Использовать для торговых и финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас;

2.10. Контролируйте свой телефон, используемый для получения SMS-кодов. В случае выхода из строя SIM карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

### **3. При работе на компьютере необходимо:**

3.1. Использовать лицензионное программное обеспечение (операционные системы, офисные программы и т.д.);

3.2. Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные программы и т.д.);

3.3. Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы, регулярно запускать проверку компьютера на наличие вредоносного ПО;

3.4. Использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;

3.5. Использовать надежные пароли, содержащие не менее 8 различных символов (сочетание букв/цифр, большого/малого регистра);

3.6. Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

#### **4. При работе с мобильным приложением необходимо:**

4.1. Сохранять конфиденциальность паролей (как постоянных, так и одноразовых), кодов, предназначенных для входа в мобильное приложение, в том числе на раскрывать данную информацию третьим лицам, включая сотрудников Компании;

4.2. Никогда не сохранять код, предназначенный для входа в мобильное приложение, а также постоянный пароль на Ваше мобильное устройство, на котором запускается мобильное приложение, применяемое для совершения торговых и финансовых операций;

4.3. Не оставлять без присмотра мобильное устройство, на котором запускается мобильное приложение, применяемое для совершения торговых и финансовых операций,

4.4. Использовать для совершения торговых и финансовых операций те мобильные приложения, права на которые передаются Вам непосредственно Компанией;

4.5. Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте;

4.6. Установить парольную защиту на мобильное устройство, на котором запускается мобильное приложение;

4.7. Своевременно устанавливать доступные официальные обновления операционной системы и приложений на мобильное устройство;

4.8. При смене номера мобильного телефона, указанного в Ваших регистрационных данных в Компании, - незамедлительно сообщить об этом в Компанию.

#### **5. При работе с ключами электронной подписи необходимо:**

5.1. Использовать для хранения ключей электронной подписи внешние носители;

5.2. Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы;

5.3. Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли открытом виде на компьютере/мобильном устройстве.

5.4. незамедлительно обращаться в Компанию при возникновении подозрения в компрометации ключей электронной подписи/шифрования, в несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов.