Клиентам ООО «ЦУР»
Рекомендации о возможных рисках утраты или получения несанкционированного доступа к защищаемой информации и о мерах по предотвращению несанкционированного доступа к защищаемой информации

Общество с ограниченной ответственностью «Центр учета и регистрации» (далее – Регистратор, ООО «ЦУР») 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, утвержденных Банком России 20.04.2021 № 757-П доводит до Вашего сведения Рекомендации по обеспечению защиты информации (далее –Рекомендации).

Целью Рекомендаций является доведение до Клиентов Регистратора информации:

- по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям;

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

- о 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.

Рекомендации доводятся до сведения Клиентов Регистратора путем размещения Рекомендаций на сайте ООО «ЦУР».

Основные риски получения несанкционированного доступа к устройствам Клиента:

- риск совершения финансовых операций с активами Клиентов, в том числе путем формирования и отправки от имени клиента распоряжения на проведение финансовой операции, а также риск перехвата сообщений, отправляемых Регистратором на адрес электронной почты и/или абонентский номер Клиента, содержащих защищаемую информацию;

- риск совершения иных юридически значимых действий, в том числе включение и отключение услуг (включая платные услуги), внесение изменений в регистрационные данные Клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершение иных действий против воли Клиента;

- риск повреждения программного обеспечения Клиента, а также риск искажения, изменения, уничтожения или модификации информации об активах Клиента или данных самого Клиента;

- риск распространения, уничтожения, блокирования, модификации, передачи конфиденциальной информации.

Просим обратить Ваше внимание на наши рекомендации по защите информации от воздействия Вредоносного кода и меры по обеспечению защиты от несанкционированного доступа неуполномоченных лиц к устройствам Клиента:

1. Рекомендации по обеспечению безопасности устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, и иных носителей информации:

1.1. Не оставляйте без присмотра свой персональный компьютер, не передавайте его третьим лицам. Он должен располагаться в помещении, исключающем несанкционированный доступ к устройству. В случае передачи Вашего устройства другому пользователю, им может быть установлен на него Вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Регистратора, которые вы использовали.

1.2. Блокируйте экран устройства при покидании рабочего места, чтобы посторонние лица не смогли воспользоваться Вашей учетной записью.

1.3. Настройте устройство так, чтобы при его включении или разблокировке требовалось ввести пароль. Рекомендуем настроить автоматическую блокировку Вашего устройства при бездействии пользователя.

1.3.1. Никому не сообщайте Ваш личный пароль.

1.3.2. При выборе пароля целесообразно использовать следующие требования:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- в качестве пароля не используйте имя, фамилию, день рождения и другие памятные даты, номер телефона и другие данные, которые могут быть подобраны третьими лицами путем анализа собранной о пользователе информации.

1.3.3. Пароль от операционной системы, а также пароль для входа в электронные сервисы рекомендуется менять каждые 45 календарных дней. Не рекомендуется

ставить один и тот же пароль на операционную систему и электронные сервисы Регистратора.

1.3.4. Не рекомендуется записывать пароли на бумажные носители или в текстовые файлы на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам.

1.3.5. Не рекомендуется сохранять пароли для доступа к электронным сервисам Регистратора в web-браузере.

1.3.6. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

1.3.7. Пароль в обязательном порядке подлежит изменению в том случае, если он стал известен постороннему лицу или у Клиента есть на это подозрения.

1.4. Не пользуйтесь электронными сервисами Регистратора в местах с публичным доступом в сеть «Интернет» из-за отсутствия должной системы безопасности в указанных заведениях.

1.5. Примите меры по предотвращению несанкционированного доступа к защищаемой информации, а именно:

1.5.1. Защита рабочих станций:

- необходимо организовать охрану помещения и надежный пропускной режим;
- компьютер, с защищаемой информацией, должен находиться в помещении, доступ в которое возможен только определенному кругу лиц;
- при входе в операционную систему требуется применение паролей достаточной сложности.

1.5.2. Используйте при работе источники бесперебойного питания.

1.5.3. Обеспечьте наличие систем пожаротушения, направленных на предупреждение возникновения чрезвычайных ситуаций (пожаров).

1.5.4. Определите внутренний порядок получения доступа к ресурсам сети, в соответствии с функциональными обязанностями каждого работника (полномочия пользователя должны быть минимально необходимыми для выполнения им своих прямых обязанностей).

1.5.5. Не допускайте передачи важной информации в открытом виде за пределы контролируемых помещений. При передаче данных по каналам связи применяйте криптографические методы защиты информации.

1.5.6. Осуществляйте резервное копирование:

- создавайте архивы резервных копий, которые будут надежно защищены от уничтожения в случае стихийных бедствий, неумышленных или умышленных действий;

- используйте для хранения резервных копий несгораемые сейфы, банковские ячейки или специально оборудованные помещения.

1.6. Ваше мобильное устройство не должно оставляться без присмотра, чтобы исключить несанкционированный вход в электронные сервисы Регистратора.

2. Рекомендации при работе с программным обеспечением:

2.1. Используйте только лицензионное программное обеспечение, полученное из доверенных источников.

2.2. Регулярно устанавливайте обновления для операционной системы, браузеров и прикладного программного обеспечения. В случае обнаружения уязвимостей необходимые обновления требуется выполнить незамедлительно.

2.3. Не устанавливайте программы из сомнительных и недоверенных источников.

3. Рекомендации по антивирусной защите:

3.1. До первого подключения компьютера к Интернету и до подключения компьютера к локальной сети, установите на рабочую станцию средства защиты – антивирус, регулярно проводите его обновления.

3.2. Проводите проверку всей системы не реже одного раза в месяц. Выполните необходимые настройки на проведение проверок и удаление зараженных файлов.

4. Рекомендации по работе в системе электронного документооборота Регистратора:

4.1. Обмен Электронными документами осуществляется в соответствии с Правилами электронного документооборота Регистратора, Договором об ЭДО, а также иными договорами и соглашениями Регистратора и Клиента.

4.2. Не оставляйте активные сессии работы ЭДО, осуществляя выход из своей учетной записи в системе ЭДО после совершения необходимых операций.

5. Рекомендации по безопасной работе с ключевыми носителями электронной подписи:

5.1. Используйте для хранения ключей электронной подписи внешние носители при работе в системе электронного документооборота ООО «ЦУР». Рекомендуем Вам использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, рутокен и другие. Храните ключевые носители в запираемых сейфах, доступ к которым ограничен и возможен только уполномоченным сотрудникам. В системе электронного документооборота ООО «ЦУР» Клиентами используются усиленные квалифицированные электронные подписи, которые изготавливаются аккредитованными Удостоверяющими центрами.

5.2. При использовании ключевого носителя следует поменять на нем стандартный пароль, либо установить в случае его отсутствия.

5.3. Ключи электронной подписи (рабочие и резервные), срок действия которых истек, должны уничтожаться в соответствии с требованиями, указанными в Правилах электронного документооборота Регистратора и требованиями внутренних нормативных документов Клиента.

5.4. В случае принятия решения о компрометации ключей (утраты доверия к тому, что используемые закрытые ключи недоступны посторонним лицам) необходимо об этом незамедлительно уведомить Удостоверяющий центр и Регистратора. Порядок уведомления Регистратора осуществляется в соответствии с требованиями Правил электронного документооборота Регистратора.

6. Рекомендации по работе с почтовыми сообщениями:

6.1. Не открывайте подозрительные письма от неизвестных адресов, тем более в которых Вас вынуждают проводить необходимые срочные действия. При получении подобных писем, не переходите по со ссылками в них, не открывайте вложения (документы, скрипты, pdf-файлы), они могут привести к заражению Вашего устройства Вредоносным кодом.

Рекомендуем Вам воспользоваться в случае необходимости сервисами проверки на вредоносное содержимое (как подозрительных файлов, так и ссылок):

- https://www.virustotal.com/gui/home/url
- https://opentip.kaspersky.com

6.2. Не устанавливайте программное обеспечение, которое рекомендуется к установке в таких письмах.

6.3. Внимательно проверяйте адресата, от которого пришло электронное письмо, оно может быть от злоумышленника, который маскируется под Регистратор или иных доверенных лиц.

7. Рекомендации по безопасной работе в сети Интернет:

7.1. При использовании систем удостоверьтесь в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с протокола https, либо используется значок в виде замка). В случае наличия предупреждений вашего браузера о наличии небезопасного соединения, не вводите логин и пароль, немедленно закройте этот сайт.

7.2. Блокируйте подозрительные подключения при наличии на устройстве программ фильтрации сетевого трафика (брандмауэра), рекомендуем держать его включённым.

7.3. Не используйте и не открывайте сомнительные Интернет - ресурсы на Вашем устройстве.

8. Обращаем Ваше внимание, что связь с Регистратором поддерживается только по официальному номеру телефона, указанному на официальном сайте Регистратора или в договоре с ним. От Регистратора никогда не поступают звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер счета, кодовое слово и т.д.