**Рекомендации**

**клиентам Акционерного общества «Регистратор Интрако»**

**по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям.**

В соответствии с требованиями п.1.13 Положения Банка России от 20.04.2021 N 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» Акционерное общество «Регистратор Интрако» доводит до сведения основные рекомендации по защите информации от воздействия вредоносных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям:

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

- информацию 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.

**Возможные риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:**

**1.**Несанкционированный доступ к информации с использованием ложных ресурсов сети «Интернет» с целью получения конфиденциальных сведений (личных данных, логинов, паролей и др.) лицами, не обладающими правом осуществления финансовых операций;

**2**.Потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются финансовые операции;

**3.**Появление на устройствах, с которых осуществляется работа с информационным сервисом, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения либо на перехват информации, в том числе логинов и паролей;

**4.**Совершение иных противоправных действий, связанных с информационной безопасностью.

**Рекомендуемые меры 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:**

**1.**Использование в работе только лицензионного программного обеспечения, с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

**2.**Наличие средств защиты, таких как антивирус, с регулярно и своевременно обновляемыми базами, предпочтительно в автоматическом режиме. Рекомендуется установить по умолчанию максимальный уровень политики безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов;

**3.**Хранение в тайне аутентификационных и идентификационных данных и ключевой информации: пароли, СМС коды, кодовые слова, ключи электронной подписи, ключи шифрования, а в случае компрометации немедленное применение мер для смены и/или блокировки;

**4.**Предотвращение несанкционированного доступа, путем настройки прав доступа к устройству;

**5.**Запрет запуска файлов, загруженных с ненадежных интернет сайтов и полученных от неизвестных адресатов (в том числе, посредством электронной почты);

**6**.Антивирусный контроль любой информации, получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т.п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме;

**7**.Обеспечение сохранности устройств с целью минимизации рисков кражи и/или утери;

**8**.Своевременное обновление установленного программного обеспечения и операционной системы (установка критичных обновлений).