Рекомендации 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 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 № 684-П, утвержденного Банком России 17.04.2019, АО "ПРЦ" 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.

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

- риск получения несанкционированного доступа к информации с использованием ложных ресурсов сети Интернет с целью получения конфиденциальных сведений – личных данных, логинов, паролей и др. (фишинг);
- риск появления на устройствах, с которых осуществляется работа с информационным сервисом, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе логинов/паролей.

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:

- использование исключительно лицензионного программного обеспечения;
- использование специализированного программного обеспечения, обеспечивающего защиту устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, от вредоносного кода (антивирусных программных комплексов);
- регулярное обновление безопасности операционных систем и антивирусных баз данных, предпочтительно в автоматическом режиме;
- 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.), предпочтительно в автоматическом режиме;
- обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, а также ключей электронной подписи;
- ограничение возможности инсталляции в память устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, программ и компонентов, полученных из ненадежных источников;
- запрет запуска файлов, загруженных с ненадежных интернет сайтов и полученных от неизвестных адресатов (в том числе, посредством электронной почты);