Рекомендации Акционерного Общества «Управляющая Компания «СПУТНИК» (далее – Управляющая компания) по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям:

- использование на устройствах, используемых для финансовых операций, исключительно лицензионного программного обеспечения;
- использование специализированного программного обеспечения, обеспечивающего защиту устройств от вредоносных программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (антивирус, персональный межсетевой экран и т.п.);
- регулярное и своевременное обновление безопасности операционных систем устройств, используемых для финансовых операций и антивирусных баз данных, антивирусных программных комплексов;
- антивирусный контроль любой информации, получаемой и передаваемой с использованием устройства по телекоммуникационным каналам, а также информации на подключаемых к устройствам съемных носителях;
- предотвращение применения устройств, используемых для финансовых операций, для работы с сомнительными и развлекательными сайтами в сети Интернет;
- предотвращение подключения устройств, используемых для финансовых операций, к открытым публичным и непроверенным проводным и беспроводным сетям;
- запрет на установку программ из непроверенных источников на устройства, используемые для финансовых операций;
- запрет запуска/открытия файлов, загруженных с ненадежных сайтов в сети Интернет и/или полученных от неизвестных адресатов, или в случае сомнений в их подлинности;
- в случае обнаружения средствами антивирусной защиты вредоносного кода - необходимо немедленно приостановить работу с сервисами Управляющей компании, проконтролировать отсутствие несанкционированных действий, провести дополнительную проверку на предмет устранения выявленной проблемы, а при наличии любых подозрений в возможности незаконных финансовых операций – необходимо незамедлительно обратиться в Управляющую компанию для осуществления процедур по блокировке доступа к сервисам.

Информация о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

- риск получения несанкционированного доступа к защищаемой информации путем совершения мошеннических операций от имени финансовых организаций путем телефонных звонков, почтовых рассылок, размещения в сети Интернет ложных (поддельных) ресурсов и ссылок на них, с целью получения конфиденциальных сведений о клиентах – личных данных, логинов, паролей, номеров телефонов, адресов электронной почты, сведений о доступе к управлению банковскими счетами, счетами депо, лицевыми счетами в реестрах владельцев ценных бумаг, а также других сведений;
- риск появления на устройствах, с которых клиентом осуществляется работа с информационными сервисами, компьютерных вирусов и вредоносных программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения, либо на перехват информации, в том числе логинов, паролей и идентифицирующих сведений;

- риск незаконного завладения устройством клиента, в том числе при его утрате (потере, хищении), с использованием которого осуществлялось взаимодействие с Управляющей компанией;
- риск незаконного завладения ключом электронной подписи клиента, с использованием которой осуществлялось взаимодействие с Управляющей компанией, в том числе при его утрате (потере, хищении) либо при несанкционированном изготовлении копии (дубликата);
- операционные риски, в результате реализации которых к защищаемой информации с целью осуществления финансовых операций могут получить доступ лица, не обладающие правом их осуществления, ввиду нарушения работоспособности программно-технических средств Управляющей компании.

Информация 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:

- исключения возможности доступа к устройствам, используемых для финансовых операций третьим лицам;
- использование сложных паролей на всех устройствах, используемых для финансовых операций и компьютерных программах;
- запрет функции сохранения логина и пароля в памяти программного обеспечения - браузера, используемого для доступа к информационным системам Управляющей компании;
- в случае подозрений на возможную компрометацию (раскрытие) паролей - незамедлительная замена паролей.
- использование на устройствах, используемых для финансовых операций, исключительно лицензионного программного обеспечения;
- использование специализированного программного обеспечения, обеспечивающего защиту устройств от вредоносных программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (антивирус, персональный межсетевой экран и т.п.);
- регулярное и своевременное обновление безопасности операционных систем устройств и антивирусных баз данных, антивирусных программных комплексов;
- обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, а также ключей электронной подписи;
- запрет на установку программ из непроверенных источников на устройства, используемые для финансовых операций;
- запрет запуска/открытия файлов, загруженных с ненадежных сайтов в сети Интернет и/или полученных от неизвестных адресатов, или в случае сомнений в их подлинности;
- предотвращение применения устройств, для работы с сомнительными и развлекательными сайтами в сети Интернет;
- предотвращение подключения устройств к открытым публичным и непроверенным проводным и беспроводным сетям.