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

Общество с ограниченной ответственностью «Эрроу Эссет Менеджмент» рекомендует своим клиентам предпринимать следующие меры по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код), 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 (антивирусных программных комплексов);
- регулярное обновление безопасности операционных систем устройств 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 (магнитных, CD-дисках, DVD-дисках, USB-накопителях и т.п.);
- ограничение возможности инсталляции в память устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, программ и компонентов, полученных из ненадежных источников;
- предотвращение применения устройств, используемых для финансовых операций, для работы с сомнительными и развлекательными сайтами в сети Интернет (игровые сайты, сайты знакомств, сайты распространения программного обеспечения, мультимедийного контента, социальные и файлообменные сети и т.п.);
- предотвращение подключения устройств, используемых для финансовых операций, к открытым публичным и непроверенным проводным и беспроводным сетям (кафе, отели, парки, вокзалы и аэропорты);
- 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 финансовых организаций, 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 финансовые организации для осуществления процедур по блокировке доступа к сервисам или замены паролей.