Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.

В соответствии с Положением Банка России от 20 апреля 2021 г. № 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» АО СПВБ доводит до сведения своих клиентов и контрагентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники.

Возможные риски при получении несанкционированного доступа (далее – НСД) к защищаемой информации лицами, не допущенными и не обладающими правом на их осуществление:

- Риск получения НСД к информации с использованием фишинговых ссылок для получения конфиденциальной информации (логины, пароли, личные данные и т.д.);
- Риск заражения устройств, с которых осуществляется доступ и работа с информационными ресурсами, компьютерными вирусами и программами, направленными на нарушение работоспособности средства вычислительной техники (далее – СВТ) или полного выведения из строя СВТ, либо перехват конфиденциальных данных с или без нарушения работоспособности/выведения из строя СВТ.

Рекомендуемые меры по предотвращению НСД к защищаемой информации, в том числе при потере доступа к СВТ:

- Антивирусная защита и межсетевое экранирование СВТ, относящихся к контуру безопасности;
- Недопущение использования нелицензионного программного обеспечения;
- Запрет чтения/записи файлов, а также загрузки из ненадёжных или небезопасных источников сети Интернет и средствами электронного обмена сообщениями;
- Ограничение использования портов ввода/вывода информации, контроль входных и выходных устройств;
- Регулярное обновление средств антивирусной защиты информации, а также иных средств защиты информации;
- Регулярное обновление безопасности операционных систем;
- Обеспечение сохранности и недопущение компрометации усиленных квалифицированных электронных подписей, а также аутентификационных данных;
- Иные меры, предусмотренные действующим законодательством и нормативными актами РФ.