УТВЕРЖДАЮ
Генеральный директор
АО «Страховая компания «Астро-Волга»
_____ Остудин Я.В.
Приказ № 01-16/А-1 от 16 января 2025 г.

Рекомендации

по защите информации от воздействия программных кодов, приводящего 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 № 757-П, утвержденного Банком России 20.04.2021, АО «Страховая компания «Астро-Волга» 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, в том числе 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 ключевой 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:

1. Использование исключительно лицензионного программного обеспечения.

2. Использование специализированного программного обеспечения, обеспечивающего защиту устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, от вредоносного кода (антивирусных программных комплексов).

3. Регулярное обновление безопасности операционных систем и антивирусных баз данных, предпочтительно в автоматическом режиме.

4. 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.

5. Обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, а также ключей электронной подписи.

6. Ограничение возможности инсталляции в память устройств, с использованием которых совершаются действия в целях осуществления финансовых операций, программ и компонентов, полученных из ненадежных источников.

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

8. Осуществление регулярного контроля функционирования системы антивирусной защиты.

9. Не допускается отключение или несвоевременное обновление антивирусных средств.

10. Рекомендуется на постоянной основе регулярно, например, ежемесячно, проводить полную проверку на наличие вредоносного кода.

11. Не рекомендуется передавать устройства для использования третьим лицам, в том числе родственникам, так как на оставленном без

присмотра устройстве может быть совершён ряд действий, направленных на получение доступа к личному кабинету.

12. Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, а также SMS и MMS-сообщениях, сообщений мессенджеров, из недостоверных источников, в том числе ссылки на известные сайты.

13. Не рекомендуется загружать и устанавливать программное обеспечение, полученное из недостоверных источников: интернет-сайты, ссылки в SMS и MMS-сообщениях и открытках, сообщениях мессенджеров.

14. Не рекомендуется обходить установленные производителем защитные механизмы (например, через джейлбрейк (Jailbreak) или рутинг (Rooting)).

15. Не рекомендуется использовать публичные беспроводные сети (Wi-Fi), а также незащищенные беспроводные сети. Рекомендуется использовать подключение к сети Интернет через мобильного оператора (3G, 4G) или через доверенную защищенную беспроводную домашнюю сеть.

16. Необходимо хранить коды доступа, логины, пароли в тайне и предпринимать необходимые меры предосторожности для предотвращения их несанкционированного использования. Не рекомендуется записывать код доступа там, где доступ к нему могут получить посторонние лица.

17. Не сообщайте коды доступа, логины, пароли, SMS-коды, необходимые для проведения операций, ПИН-коды и контрольные коды, посторонним лицам, сотрудникам Компаний по телефону, электронной почте или иным способом. При наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Компании.

18. Не оставляйте свое устройство без присмотра. Рекомендуется установить пароль на доступ к устройствам и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к устройству в случае его утраты.

19. Банк России предупреждает граждан о мошеннических схемах:

http://www.cbr.ru/information_security/pmp/

https://cbr.ru/press/event/?id=12870