|  |  |  |
| --- | --- | --- |
|  |  | **Утверждены****Приказом Генерального директора****ООО «АВИ Кэпитал»** |

**от 04.09.2024 № 04092024/АК-01**

**Дата вступления в действие: 04.09.2024**

**РЕКОМЕНДАЦИИ**

**по соблюдению информационной безопасности клиентами**

**ООО «АВИ Кэпитал» в целях противодействия незаконным**

**финансовым операциям**

В соответствие с требованиями Положения Банка России от 17.04.2019 № 684-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» ООО «АВИ Кэпитал» (далее – Организация) уведомляет своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации, а также доводит до клиентов основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код).

В частности, несанкционированный доступ со стороны третьих лиц к устройствам или ключевой информации, с помощью которых осуществляется вход в автоматизированные системы, установка на устройство вредоносного кода или перехват электронных сообщений могут повлечь совершение третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, разглашение конфиденциальной информации и совершение иных действий без воли клиента Организации.

Для снижения рисков реализации инцидентов информационной безопасности необходимо выполнять ряд рекомендаций. Инциденты информационной безопасности (здесь и далее термины из ГОСТ Р 57580.1-2017) – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов организации и (или) нарушить конфиденциальности, целостности и доступности информации вследствие:

* несанкционированного доступа к информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);
* потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;
* воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;
* совершения иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется применять совокупность мер по защите информации, направленных на повышение уровня информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты) при использовании объектов информатизации.

Рекомендации по соблюдению информационной безопасности не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

Для снижения возможных рисков финансовых потерь вследствие воздействия вредоносных кодов, несанкционированного доступа к защищаемой информации, рекомендуется:

1. Обеспечить безопасность устройства:
	* Ограничить доступ к устройству посторонних лиц.
	* Использовать только лицензионное программное обеспечение и операционные системы, осуществлять их регулярное обновление. Имейте в виду, что обновления снижают риски заражения вредоносным кодом.
	* Блокировать устройство после использования.
	* Использовать и регулярно обновлять антивирусное программное обеспечение.
	* Исключить использование средств удаленного администрирования на устройствах.
	* Хранение, использование устройства с целью избежать рисков кражи и/или утери.
	* Не работать в Системах с устройства, использующего подключение к общедоступной wi-fi сети.
2. Безопасность паролей:
	* Необходимо использовать сложные пароли, длиной не менее 8 символов, включающие заглавные и прописные буквы, цифры и специальные символы.
	* Не передавать третьим лицам пароли, коды доступа к устройству, а также пароли доступа в системы.
	* Регулярно проводить смену паролей.
	* Не хранить пароли совместно с устройством.
3. Соблюдать следующие рекомендации при работе через сеть Интернет:
	* Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам.
	* Не вводить персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах.
	* Не открывать файлы, полученные из неизвестных источников, они могут привести к заражению вашего устройства вредоносным кодом.

В случае утери/хищении устройства или компрометации ключевой информации, а также подозрения на совершение третьими лицами мошеннических действий незамедлительно информировать Организацию.