Утверждены
Протоколом Совета директоров
АО «Товарная биржа «Modern Trading Solutions»
от 23 мая 2023 года

Антивирусная политика

Назначение

Настоящая политика определяет требования по защите информационно-телекоммуникационной инфраструктуры «**ВАШЕЙ КОМПАНИИ**» от угроз информационной безопасности, причина возникновения которых связанна с распространением вредоносного программного обеспечения. Данные требования минимизируют вероятность возникновения негативных последствий для ИТКИ «**ВАШЕЙ КОМПАНИИ**» вследствие отсутствия защиты информационно-телекоммуникационной инфраструктуры. Негативные последствия могут включать в себя раскрытие или утрату чувствительной и конфиденциальной информации, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы «**ВАШЕЙ КОМПАНИИ**»

1. Всегда используйте полученное из доверенного источника и принятое в качестве стандарта в «**ВАШЕЙ КОМПАНИИ**» антивирусное программное обеспечение. Используйте и поддерживайте антивирусное программное обеспечение в актуальном состоянии.

2. Никогда не открывайте вложения к сообщениям электронной почты, полученным из неизвестных, подозрительных или недоверенных источников. Такие вложения должны незамедлительно удаляться.

3. Сообщения электронной почты содержащей спам, цепочки сообщений и другую нежелательную почту должны удаляться без пересылки, в соответствии с принятой в «**ВАШЕЙ КОМПАНИИ**» Политикой допустимого использования ИС.

4. Не скачивайте информацию из неизвестных или подозрительных источников.

5. Избегайте предоставления общего доступа к логическим дискам с правами чтения/записи в случае если это не требуется в рамках выполнения основной деятельности.

6. Прежде чем использовать носители информации, полученные от неизвестных или подозрительных источников, сканируйте их на отсутствие вирусов.

7. Резервируйте важные данные и настройки системы регулярно. Резервные копии храните в безопасном месте.

8. В случае необходимости запуска приложения, конфликтующего с установленным антивирусным программным обеспечением, необходимо выполнить полную проверку рабочей станции на наличие вирусов, отключить антивирусное программное обеспечение и запустить необходимое приложение. Должно быть доподлинно известно, что запускаемое приложение не приведет к негативным последствиям. После выполнения задач связанных с использованием приложения, возобновите работу антивирусного программного обеспечения. При отключенном антивирусном программном обеспечении запрещается запускать любые приложения (электронная почта или открытие общего доступа к файловым ресурсам) в результате действия которых ваша рабочая станция может быть подвержена инфицированию вредоносным ПО.

9. Появление нового вредоносного программного обеспечения обнаруживаются ежедневно. Периодически проверяйте Антивирусную политику на предмет необходимости внесения в нее изменений.