Рекомендации по защите информации от воздействия вредоносного кода

Используйте только лицензионное системное, прикладное и антивирусное программное обеспечение.

Не используйте права администратора при отсутствии необходимости; используйте устройство с учетной записью пользователя, не имеющего прав администратора.

Не используйте средства удаленного администрирования.

Своевременно обновляйте установленное системное, прикладное, антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, лечение (удаление) зараженных файлов должно производиться антивирусным средством в автоматическом режиме.

Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска устройства на предмет наличия вирусов и вредоносного программного кода.

Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.

Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

При работе в сети Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

При использовании сети Интернет не соглашайтесь на установку каких-либо сомнительных программ.

Желательно не использовать устройство, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые сайты, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

Рекомендуется воздержаться от использования устройства при подозрениях на наличие вирусов на нем (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности) для перевода денежных средств, до устранения угрозы.

При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.