

## Памятка для клиентов по защите информации

### 1. Рекомендации по защите информации от воздействия программных кодов, в целях противодействия незаконным финансовым операциям. Наиболее характерные внешние проявления вирусов и порядок действий в случае обнаружения вирусов.

- 1.1. Вирус представляет собой программу, которая разрушает информацию на магнитных носителях или нарушает работу ПЭВМ, а также обладает способностью к размножению, т.е. вирус может самостоятельно внедряться в другие программы, переносить себя на диски и дискеты, передаваться по локальной компьютерной сети.

Можно выделить несколько видов воздействия вирусов на ПЭВМ:

- вирусы разрушительного действия;
- вирусы, замедляющие работу ПЭВМ;
- вирусы рекламного характера;
- вирусы-шутки.

Самые опасные вирусы - это вирусы разрушительного действия. Наиболее характерные внешние проявления вирусов этого вида:

- нетипичная работа программ;
  - появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;
  - самопроизвольная перезагрузка операционной системы;
  - зависание компьютера;
  - появление неисправных участков (кластеров) на "винчестере";
  - неожиданные действия рабочих программ (не предусмотренные документацией на программы);
  - искажения данных в обрабатываемых файлах.
- 1.2. Вирусы, замедляющие работу ПЭВМ, проявляют себя тем, что работа процессора замедляется в 30-40 раз.
- 1.3. Вирусы рекламного характера и вирусы-шутки хотя и не портят информацию в ПЭВМ, однако замедляют работу или навязывают пользователю ненужные диалоги, что также замедляет весь процесс решения задачи.
- 1.4. Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.
- 1.5. При возникновении подозрения на наличие компьютерного вируса необходимо провести внеочередной антивирусный контроль.
- 1.6. В случае обнаружения при проведении антивирусной проверки зараженных вирусами файлов:
- приостановить работу;
  - провести лечение или уничтожение зараженных файлов;
  - обратиться к специалистам.

### 2. Рекомендации по снижению рисков получения несанкционированного доступа к конфиденциальной информации.

**ВНИМАНИЕ! Передача карты или ее реквизитов, Логина, ПИН кода, кода CVV2 или CVC2 указанный на оборотной стороне пластиковой карточки, предназначенных для доступа и подтверждения операций, другому лицу (в том числе работнику МФИ, Банка) означает, что Вы предоставляете возможность другим лицам проводить операции по счетам.**

При любых подозрениях на мошенничество, следует незамедлительно обратиться в Банк обслуживающий вашу пластиковую карту по номерам телефонов, указанным на оборотной стороне карты и на Официальном сайте Банка.