РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПРЕАЦИЯМ

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.*

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.

Вирусы, замедляющие работу ПЭВМ, проявляют себя тем, что работа процессора замедляется в 30-40 раз.

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.

Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.

При возникновении подозрения на наличие компьютерного вируса необходимо провести внеочередной антивирусный контроль.

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.

В целях обеспечения защиты информации и носителей этой информации от использования ее злоумышленниками и предотвращения возможных негативных последствий вследствие реализации указанных рисков, рекомендуется:

- Не передавать данные 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).
- 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.
- Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции.
- Не использовать функцию запоминания логина и пароля в браузерах для используемых платежных систем.
- Не использовать одинаковые логин и пароль для доступа к различным системам.
- Регулярно производить смену паролей. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат.
- По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.
- Завершать сеанс работы с платежными системами, используя соответствующий пункт меню (например, «Выйти»).
- При выполнении операций в платежных системах с использованием чужих компьютеров или иных средств доступа не сохранять на них персональные данные и другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.
- Не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами. Не переходить по ссылкам в таких письмах, не открывать вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение). Не звонить по телефонам, указанным в подобных письмах, и не отвечать на них. Для связи использовать номера телефонов и электронные адреса, указанные на официальных сайтах владельцев финансовых сервисов.
- При регистрации на сторонних интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте.
- Не запускать на своем компьютере программы, полученные из незаслуживающих доверия источников.
- Использовать антивирусное программное обеспечение и межсетевые экраны.
- Регулярно производить обновление системных программных средств.