Приложение к Приказу № 19 от 30.01.2020 г.

Рекомендации

для клиентов АО БАНК НБС по защите от вредоносного кода, приводящего к нарушению штатного функционирования СВТ в целях противодействия осуществлению переводов денежных средств без согласия клиента.

Вредоносный код - любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам компьютера или к информации, хранимой компьютере, с целью несанкционированного использования ресурсов компьютера или причинения вреда (нанесения ущерба) владельцу информации, и владельцу компьютера, или владельцу компьютерной сети, путём копирования, искажения, удаления или подмены информации.

Признаки заражения:

- автоматическое открытие окон с незнакомым содержимым при запуске компьютера;
- блокировка доступа к официальным сайтам антивирусных компаний, или же к сайтам, оказывающим услуги по «лечению» компьютеров от вредоносных программ;
- появление новых неизвестных процессов в выводе диспетчера задач (например, окне «Процессы» диспетчера задач Windows);
- появление в ветках реестра, отвечающих за автозапуск, новых записей;
- запрет на изменение настроек компьютера в учётной записи администратора;
- невозможность запустить исполняемый файл (выдаётся сообщение об ошибке);
- появление всплывающих окон или системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса и названия;
- перезапуск компьютера во время старта какой-либо программы;
- случайное и/или беспорядочное отключение компьютера;
- случайное аварийное завершение программ;
- снижение производительности при достаточном объёме памяти, вплоть до «зависаний» вкупе с аномальным перегреванием системного блока;
- случайное появление «Синего экрана смерти» при запуске компьютера;
- появление неизвестных файлов и каталогов в файловой системе ОС, которые обычно выдают ошибку удаления;
- шифрование или повреждение пользовательских файлов;
- неизвестные изменения в содержимом системных файлов при открытии их в текстовом редакторе;
- быстрая утечка памяти на жёстком диске.

Однако, следует учитывать, что несмотря на отсутствие симптомов, компьютер может быть заражен вредоносными программами, возможно встраивание вредоносного кода в сборку операционной системы, при этом антивирусное ПО может не сигнализировать о заражении при проверке компьютера.

Способы защиты от вредоносных программ

Абсолютной защиты от вредоносных программ не существует, но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами. Ниже перечислены основные и наиболее эффективные меры для повышения безопасности:

- обязательно использовать антивирусные программы (антивирус, средство антивирусной защиты, средство обнаружения вредоносных программ, средство защиты от вредоносного кода) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом
- обязательно использовать постоянное автоматическое обновление антивирусных программ
- использовать операционные системы, не дающие изменять важные файлы без ведома пользователя;
- своевременно устанавливать обновления для используемого программного обеспечения;
    - если существует режим автоматического обновления, включить его;
    - использовать лицензионное программное обеспечение;
- постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит некоторым вредоносным программам инсталлироваться на персональном компьютере и изменить системные настройки.
- ограничить физический доступ к компьютеру посторонних лиц;
- использовать внешние носители информации только от проверенных источников на рабочем компьютере;
- не открывать компьютерные файлы, полученные от ненадёжных источников, на рабочем компьютере;
- использовать межсетевой экран (аппаратный или программный), контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь;
- использовать второй компьютер (не для работы) для запуска программ из малонадежных источников, на котором нет ценной информации, представляющей интерес для третьих лиц и злоумышленников;
- делать резервное копирование важной информации на внешние носители и отключать их от компьютера.
- хранить важную информацию, которая может представлять интерес для третьих лиц и злоумышленников, в зашифрованных архивах;
- стараться блокировать возможность несанкционированного изменения системных файлов.
- отключать потенциально опасную функциональность системы (например, autorun-носителей, сокрытие файлов, их расширений и пр.).
- не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- не открывать письма полученные из неизвестных источников.