Рекомендации клиентам АО БАНК НБС
по защите информации от воздействия вредоносного кода

Настоящие Рекомендации даны клиентам АО БАНК НБС в целях защиты информации от воздействия программного кода, приводящего к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код) в целях противодействия осуществлению переводов денежных средств без согласия клиента, а так же о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления, и мерах по их снижению.

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.

Банк отмечает следующее. Несмотря на отсутствие симптомов, компьютер может быть заражен вредоносными программами, возможно встраивание вредоносного кода в сборку операционной системы, при этом антивирусное программное обеспечение может не сигнализировать о заражении при проверке компьютера.

Рекомендации АО БАНК НБС.

- **По парольной защите.**

Учетные записи операционной системы должны быть защищены паролями с учётом следующих параметров:
– длина пароля должна быть не менее 8 символов;
– в пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы;
– в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
– в качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;

– пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля;
– при смене пароля новый пароль не должен совпадать с ранее используемыми паролями;
– запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли;
– не храните логин и пароль в мобильном телефоне, смартфоне.

➢ **По способам защиты от вредоносных программ.**

Абсолютной защиты от вредоносных программ не существует, но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами.

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)[1];
– 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.

[1] Специализированные программы 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.

- **По эксплуатации внешнего ключевого носителя.**

– устройства, которые используются в качестве ключевого носителя для электронной подписи (далее – ЭП), должны быть сертифицированы[2];

– для повышения уровня безопасности хранения ключей ЭП используйте устройства строгой аутентификации и хранения данных, что позволяет существенно снизить вероятность хищения ключей ЭП злоумышленниками;

– для надежной защиты ключа ЭП на носителе рекомендуется установить надежный пароль;

– внешний ключевой носитель должен храниться у владельца ключа, которому он принадлежит;

– во время работы с внешним ключевым носителем доступ к ним посторонних лиц должен быть исключен;

– для хранения внешнего ключевого носителя должны применяться надежные металлические сейфы;

– уничтожение ключей ЭП может производиться путем физического уничтожения внешнего ключевого носителя, на котором они расположены, или путем стирания без повреждения внешнего ключевого носителя (для обеспечения возможности его многократного использования);

– в случае компрометации или подозрения на компрометацию ключа ЭП Клиент, владелец квалифицированного сертификата, прекращает обмен электронными документами с использованием скомпрометированного ключа и незамедлительно информирует Удостоверяющий центр о компрометации посредством любого вида связи с целью блокировки ключа ЭП.

- **В целях сокращения рисков событий**, связанных с нарушениями в сфере информационной безопасности, следует определить внутренними документами порядок работы с информацией и ее защитой, закрепить выполнение функций и ответственность за защиту информации на должностное лицо.

[2] Два типа ключевых носителей:

Защищенные носители – носители ключевой информации, предназначенные для хранения ключей ЭП. Они имеют специальную защищенную память, в которую записываются ключи и сертификаты ЭП. Такие носители сертифицируются по требованиям ФСТЭК России.

Аппаратные криптоключи – специальный вид носителей, которые могут быть использованы для хранения ключей ЭП (как и защищенные носители), а также имеют встроенные средства ЭП. Такие носители сертифицируются ФСТЭК России и ФСБ России, поэтому, обычно, имеют 2 сертификата.