**Рекомендации ПАО «ИК РУСС-ИНВЕСТ» (далее – Компания)**

**по обеспечению информационной безопасности**

 **при работе с Личным кабинетом и ИТС QUIK**

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны, вирусы), обеспечивающие возможность похищения у пользователей финансовых интернет-систем файлов с ключами электронной подписи (далее – ключи ЭП) или с ключами СКЗИ и пароли, вводимые с клавиатуры. Трояны распространяются через E-mail, по каналам месенджеров, через принадлежащие преступникам сайты. Зафиксированы случаи заражения компьютеров и среди пользователей личных кабинетов финансовых компаний. При этом злоумышленники похищают логин и пароль, ключи ЭП или СКЗИ, что позволяет совершать операции от имени клиента.

**Внимание! Ответственность за безопасное хранение секретного ключа ЭП, секретного ключа СКЗИ и использование логина и пароля лежит на Вас.**

**Выполнение указанных ниже рекомендаций поможет обеспечить сохранность Ваших финансовых средств.**

**Рекомендации по обеспечению информационной безопасности при работе с Личным кабинетом и ИТС QUIK:**

1. Для системы Личный кабинет и ИТС QUIK использовать отдельный компьютер, не подключенный к неизвестным сетям и имеющий возможность подключения к сети Интернет, а именно, к сервису Личный кабинет и ИТС QUIK.
2. По возможности использовать аппаратно-программные средства защиты компьютера от несанкционированного доступа. Не использовать компьютер для работы в сети Интернет до установки средства антивирусной защиты и обновления сигнатур его вирусных баз.
3. Установить средство антивирусной защиты, обновить его вирусные базы, обязательно проверять средством антивирусной защиты E-mail сообщения и содержание жестких дисков на компьютере, который используется для системы Личный кабинет и/или ИТС QUIK, установить все рекомендуемые компанией-разработчиком обновления безопасности на операционную систему.
4. Использовать вход в систему Личный кабинет и ИТС QUIK только с официального сайта Компании или по предоставленному Компанией адресу.
5. Ни при каких обстоятельствах не вводить логин и пароль, предназначенные для входа в систему Личный кабинет и/или ИТС QUIK, на других сайтах.
6. Исключить хранение логина и пароля, секретного ключа ЭП, секретного ключа СКЗИ на жестком диске, в реестре компьютера, в сетевых каталогах и на прочих общественных ресурсах.
7. Генерацию пароля, генерацию ключей ЭП, генерацию ключей СКЗИ производить исключительно своими силами, без вмешательства третьих лиц.
8. Для хранения логина и пароля, секретного ключа ЭП, секретного ключа СКЗИ или их копий использовать место, исключающее возможность несанкционированного доступа к ним третьих лиц. Исключить передачу логина и пароля, секретного ключа ЭП, секретного ключа СКЗИ или их копий третьим лицам, а также передачу их по сети Интернет.

 В случае возникновения подозрения о компрометации пароля, секретного ключа ЭП или секретного ключа СКЗИ, Вам необходимо незамедлительно обратиться к ответственному специалисту Компании.

**К событиям, на основании которых Вы должны принять решение о компрометации относятся, включая, но не ограничиваясь, следующие события:**

- утрата носителя, на котором был записан логин и пароль и/или секретный ключ ЭП и/или секретный ключ СКЗИ (безвозвратная или с последующим обнаружением);

- возникновения подозрений на утечку информации или ее несанкционированное изменение в системе Личный кабинет и/или ИТС QUIK;

- доступ третьих лиц к носителю, на котором был записан логин и пароль и/или секретный ключ ЭП, и/или секретный ключ СКЗИ;

- вирусное заражение ПК, на котором производится работа с Личным кабинетом и/или с ИТС QUIK.

**Правильно составленный пароль для входа в систему Личный кабинет и ИТС QUIK и для доступа к секретным ключам ЭП и/или СКЗИ – одно из важнейших препятствий на пути злоумышленников. Смену и составление пароля производите с учетом следующих требований:**

- пароль должен содержать не менее семи символов;

- пароль должен включать буквы верхнего и нижнего регистра и два спецсимвола (@, #, $, %, <, ^, &, \*).

**К слабым относятся следующие пароли:**

- повторяющиеся;

- содержащие в том или ином виде ваш логин;

- личная информация, которая относительно легко может стать известной злоумышленнику, например, даты рождения, номера телефонов, клички домашних животных, имена детей и др.;

- слова, которые можно найти в словаре;

- комбинации расположенных рядом символов клавиатуры, например, qaz, qwerty, 123456 и др.;

- любое из указанного выше, дополненное цифрами, набранное в транслитерации, в обратном порядке или в верхнем регистре.