РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

при работе в информационной системе, в которой осуществляется выпуск цифровых финансовых активов

АО "Руб Икс" (далее – Оператор) принимает все необходимые и достаточные организационные и технические меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, защите персональных данных клиентов и (или) пользователей/заявителей интернет-ресурсов Оператора (далее – Клиенты) от неправомерного или случайного доступа, их уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий со стороны третьих лиц.

При использовании интернет-ресурсов Оператора Клиенты должны учитывать возможные риски несанкционированного доступа к информации, обрабатываемой на портале, и соблюдать рекомендации АО "Руб Икс" по минимизации этих рисков.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие рекомендации распространяются на всех Клиентов Оператора и рекомендуются для исполнения на средствах вычислительной техники (СВТ), с использованием которых Клиентами совершаются действия с ЦФА в информационной системе Оператора.

Реализация мер защиты информации, приведенных в настоящих рекомендациях, обеспечивает минимизацию рисков несанкционированного доступа к защищаемой информации.

Рекомендации разработаны с целью обеспечения безопасности информации, обрабатываемой АО "Руб Икс", в целях противодействия незаконным финансовым операциям (НФО), а также своевременного обнаружения и предотвращения воздействия вредоносного кода.

Все сотрудники, Клиенты и третьи лица, имеющие доступ к информационной системе Оператора, обязаны соблюдать данные рекомендации.

2. Возможные риски несанкционированного доступа

Основными рисками несанкционированного доступа к защищаемой информации являются:

- несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) Клиентом устройства;
- утечка или разглашение персональных данных;
- финансовый ущерб, включая несанкционированное осуществление финансовых операций.

Основными источниками рисков являются третьи лица, реализующие компьютерные атаки на СВТ Клиентов с целью получения выгоды или блокирования функционирования информационной системы Оператора. Основные способы реализации рисков:

- внедрение вредоносного кода;
- воздействие на Клиентов (социальная инженерия);
- физическое воздействие на СВТ или ключевые носители;
- использование уязвимостей программного обеспечения или конфигурации СВТ.

3. Рекомендации по защите информации от вредоносного кода

- Используйте только лицензионные антивирусные средства, полученные из доверенных источников.
- Обеспечьте автоматический запуск антивирусного ПО при загрузке ОС и его функционирование в резидентном режиме.
- Настройте антивирус на автоматический входной контроль:
  - съемных носителей;
  - файлов из внешних источников.
- Выполняйте регулярные проверки:
  - полная проверка — не реже 1 раза в неделю;
  - проверка важных областей — ежедневно;
  - проверка файлов из внешних источников — в реальном времени.
- Регулярно обновляйете антивирусное ПО и антивирусные базы.
- Проверяйте вложения в электронной почте перед открытием, особенно исполняемые файлы (*exe, .bat и др.). Не открывайте файлы с подозрительными расширениями без подтверждения отправителя.
- Не открывайте самораспаковывающиеся архивы и исполняемые файлы без проверки средствами антивируса.

4. Меры по предотвращению несанкционированного доступа

4.1. Противодействие социальной инженерии

- Никогда не сообщайте пароль или PIN-код от ключевого носителя или ИС ЦФА.
- Не открывайте письма и ссылки от неизвестных отправителей.
- Проверяйте адреса электронной почты и ссылки перед переходом на внешние ресурсы.
- Не включайте макросы в документах без подтверждения отправителя.
- Проверяйте адреса сайтов при их посещении. Внимательно проверяйте адрес сайта при его посещении, злоумышленники создают копии сайта для кражи ваших персональных данных и денежных средств (фишинговые сайты). Обращайте внимание на наличие безопасного соединения. В адресной строке браузера должен быть указан протокол https.
- Избегайте использования общедоступных Wi-Fi точек. Не используйте сомнительные или общедоступные точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля.

4.2. Физическая защита СВТ

- Исключите возможность бесконтрольного доступа посторонних к СВТ.
- Не оставляйте СВТ без присмотра после ввода пароля.
- При передаче СВТ в ремонт или пользование третьим лицам, удалите ключевую информацию.
- Защищайте устройства от физического воздействия. Не допускайте несанкционированного изменения аппаратной части СВТ.

4.3. Использование программного обеспечения

- Устанавливайте только лицензионное ПО и его обновления из доверенных источников.
- Не используйте отладочные или нестандартные версии ОС.
- Регулярно обновляйте ОС, браузеры и приложения.

4.4. Защита сетевого взаимодействия

- Отключайте неиспользуемые сервисы и порты.
- Используйте межсетевые экраны.
- Для безопасной передачи данных используйте протокол TLS.

4.5. Безопасная конфигурация СВТ

- Настройте BIOS/UEFI для исключения загрузки с неподдерживаемых носителей.
- Для доступа в BIOS и ОС используйте надежные пароли длиной не менее 10 символов с буквами, цифрами и спецсимволами.
- При возможности необходимо задать ограничение на количество неудачных попыток входа.
- Все учетные записи должны иметь минимально возможный уровень привилегий.

4.6. Защита ключей электронной подписи

- Используйте надежные пароли/ПИН-коды для доступа к ключевым носителям.
- Не храните пароли в открытом виде.
- При компрометации ключа немедленно уведомите Оператора по электронной почте support@rubx.ru.

5. Действия при подозрении на инцидент информационной безопасности

При обнаружении признаков компрометации учетных данных, ключей электронной подписи, устройства или попыток несанкционированного доступа Клиент обязан:

- немедленно прекратить работу в информационной системе Оператора;
- сменить пароли и ПИН-коды (при возможности);
- уведомить Оператора по электронной почте support@rubx.ru;
- при необходимости обратиться в правоохранительные органы.

6. Регулярное повышение осведомленности

Рекомендуется регулярно повышать уровень осведомленности в области информационной безопасности, чтобы быть в курсе новых угроз и методов защиты.

Данные рекомендации не должны рассматриваться как результат каких-либо консультационных или иных услуг, оказываемых Клиентам со стороны Оператора. Оператор ни прямо, ни косвенно не несет ответственность ни за действия или бездействия Клиентов, основанных на реализации настоящих рекомендаций, ни за последствия таких действий или бездействий.