Рекомендации клиентам АО «НПФ Эволюция» по защите информации от вредоносных кодов в целях противодействия незаконным финансовым операциям

Возможные риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления

Использование средств вычислительной техники при совершении финансовых операций несет в себе риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций от имени клиента.

Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

Обмениваясь информацией по сети Интернет без использования дополнительных средств защиты информации, клиент принимает на себя риски ее раскрытия перед любыми третьими лицами.

АО «НПФ Эволюция» (далее Фонд) предпринимает все необходимые меры по минимизации рисков за счет использования современных механизмов обеспечения безопасности, выполнения требований законодательства, применения сертифицированных средств защиты, комплексов организационных мер, но при этом не имеет возможности гарантировать полное исключение рисков получения несанкционированного доступа или воздействия вредоносного кода на участках обработки и поступления информации, на устройствах вычислительной техники, находящихся вне его контроля.

Меры по предотвращению несанкционированного доступа к защищаемой информации

На сегодняшний день существует огромное количество разнообразных способов неправомерного доступа к информации, злоумышленники постоянно совершенствуют и дополняют методы социальной инженерии и манипулирования, используют новейшие средства и технологии.

Меры, позволяющие снизить риски несанкционированного доступа к защищаемой информации:

1. Выполнение правил, установленных эксплуатационной документацией на программное обеспечение, информационные ресурсы, средства защиты информации, включая средства электронной подписи.

2. Рекомендуется регулярно менять пароль для работы со своими учетными данными в информационных ресурсах Фонда. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

3. Воздерживайтесь от использования логинов и паролей, установленных ранее при работе с любыми иными ресурсами сети Интернет.

4. Рекомендуется не пересылать пароли по почте, смс, не хранить в открытом виде в компьютерных файлах и местах доступным третьим лицам.

5. При обнаружении компрометации пароля, рекомендуем незамедлительно сменить пароль на новый.

6. Рекомендуется исключить или затруднить доступ третьих лиц к использованию устройства, посредством которого осуществляются финансовые операции.

7. Рекомендуется исключить использование устройства, посредством которого осуществляются финансовые операции, для работы с сомнительными и развлекательными сайтами.

8. Для целей совершения финансовых операций рекомендуется ограничить набор программного обеспечения только минимально необходимым, использовать на устройстве только лицензионное, регулярно обновляемое программное обеспечение с актуальной технической поддержкой.

9. Рекомендуется не открывать вложения, полученные в электронных письмах от неизвестных отправителей.

10. Рекомендуется не осуществлять финансовые операции через открытые публичные и недоверенные сети WiFi.

Меры при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции:

1. Безотлагательно предпринять меры по блокировке доступа к информационным ресурсам Фонда, через которые с утраченного устройства осуществлялись финансовые операции, для чего позвонить по телефону или направить сообщение по электронной почте, указанные на официальной странице Фонда.

2. Провести процедуру замены паролей и другой аутентификационной информации в информационных ресурсах Фонда, через которые с утраченного устройства осуществлялись финансовые операции.

Меры по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции:

1. На устройстве, используемом для совершения финансовых операций, рекомендуется разрешать работу только с предварительной авторизацией пользователя устройства (pin-код, пароль и т.д.).

2. Не рекомендуется использовать при обычной работе административные права, позволяющие вносить изменения в конфигурацию устройства.

3. Периодически контролировать журналы событий антивирусного программного обеспечения, системные журналы, перечень установленных программ и запущенных процессов, перечень подключенных устройств.

4. При запросах дополнительных прав и разрешений любым программным обеспечением производить оценку действительной необходимости предоставления таких прав.

Меры по своевременному обнаружению воздействия вредоносного кода:

1. На компьютере и устройствах, используемых в целях совершения финансовых операций, рекомендуется устанавливать лицензионное антивирусное программного обеспечение, которое должно регулярно обновляться производителем.

2. «Лечение» и удаление зараженных файлов должно производиться антивирусным программным обеспечением в автоматическом режиме без участия пользователя.

3. Рекомендуется настроить антивирусное программное обеспечение на автоматическую полную проверку устройств на предмет наличия вредоносного программного кода не реже одного раза в неделю.

4. Рекомендуется подвергать антивирусной проверке любую информацию, получаемую из сети Интернет или на съемных носителях.

5. При возникновении подозрения на наличие компьютерного вируса, рекомендуется провести дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем.

6. В случае обнаружения антивирусным программным обеспечением вредоносного кода, рекомендуется проконтролировать отсутствие несанкционированных действий и, по возможности, произвести замену используемой в целях совершения финансовой операции аутентификационной информации.

7. В информационных ресурсах Фонда, посредством которых осуществляются финансовые операции, рекомендуется периодически проверять статистику сеансов работы, запрошенной информации, собственных запросов на совершение операций.