Рекомендации
по обеспечению информационной безопасности
для клиентов НКО АО НРД

При эксплуатации информационных систем НКО АО НРД, используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств, финансовых операций (далее – информационные системы, операции), подключение к которым осуществляется с использованием сети Интернет, возникает риск реализации таких событий информационной безопасности, как:

- несанкционированный доступ к конфиденциальной информации[1] (в том числе ее компрометация, кража, разглашение);
- воздействия вредоносного кода;
- фишинговые атаки.

Последствия возникновения подобных событий могут привести к нарушению штатного функционирования устройств, с использованием которых осуществляется доступ к информационным системам, осуществлению операций лицами, не обладающими правом их осуществления, и, как следствие, возникновения финансовых потерь.

Указанные риски могут быть обусловлены такими ситуациями (включая, но не ограничиваясь), как:

- компрометация идентификационной информации, используемой для входа в информационную систему или, например, закрытого ключа электронной подписи, используемого для подписания распоряжений (поручений) для осуществления каких-либо операций.
- заражение устройства, с использованием которого осуществляется доступ в информационные системы, вредоносным кодом;
- кража устройства, с использованием которого осуществляется доступ в информационные системы, или несанкционированный доступ к данному устройству;
- получение фишинговых писем и рассылок, направляемых с целью получения доступа к идентификационным данным (и как следствие к защищаемой информации), или с целью заражения устройства вредоносным кодом.

Выполнение настоящих рекомендаций по обеспечению информационной безопасности позволит свести к минимуму риск несанкционированного доступа к конфиденциальной информации, мошенничества, и, как следствие, возникновения финансовых потерь. Вместе с тем не следует рассматривать настоящие рекомендации как исчерпывающий перечень мер защиты информации.

1. Физическая безопасность устройства

✓ Ограничьте доступ к устройству, с использованием которого осуществляется работа в информационных системах (далее – устройство). Лучше всего использовать отдельное защищенное устройство, доступ к которому предоставлен максимально ограниченному кругу лиц.

---

[1] к конфиденциальной информации относится (включая, но не ограничиваясь):
- персональные данные;
- информация, используемая для идентификации и аутентификации (логин и пароль);
- информация, содержащаяся в документах, составленных при осуществлении банковских и финансовых операций в электронном виде;
- информация, необходимая для авторизации при совершении действий в целях осуществления банковских и финансовых операций, а также удостоверения права распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информация об осуществленных банковских и финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемая при осуществлении банковских и финансовых операций.

- ✓ Размещайте устройство таким образом, чтобы минимизировать риск несанкционированного стороннего наблюдения/просмотра за его функционированием.
- ✓ В случае утраты устройства следует немедленно обратиться в техническую поддержку НКО АО НРД и заблокировать учетную запись, используемую для входа в информационные системы.

2. Безопасность программного обеспечения

- ✓ Средствами BIOS исключите возможность загрузки операционной системы с внешних устройств (CD/DVD дисков, USB flash-накопителей и т.п.). Установите пароль на вход в BIOS (администрирование) для исключения изменения настроек безопасности.
- ✓ Используйте только лицензионное системное и прикладное программное обеспечение и обеспечьте его своевременное обновление.
- ✓ Устанавливайте обновления, полученные только из официальных источников производителей программного обеспечения, в случае необходимости обеспечьте проведение тестирования обновлений на предмет выявления в них незадекларированных возможностей.
- ✓ Используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты устройства – персональные межсетевые экраны, средства контроля конфигурации устройств, программы защиты от «спам»-рассылок и т.п.
- ✓ Используйте учетную запись с минимальным уровнем привилегий, необходимых для работы в информационной системе. Исключите использование административной учетной записи при повседневной работе в информационной системе.
- ✓ Исключите использование систем удаленного управления устройством (например, TeamViewer, AnyDesk и т.п.).
- ✓ Завершение работы с устройством производите посредством выбора соответствующего пункта меню операционной системы.

3. Защита от вредоносного кода

- ✓ Используйте лицензионное антивирусное программное обеспечение. Обеспечьте регулярное обновление антивирусных баз.
- ✓ Регулярно выполняйте антивирусную проверку устройства. В случае обнаружения вредоносного программного обеспечения после его удаления незамедлительно смените пароль и ключ электронной подписи, используемые для доступа к информационной системе.
- ✓ В случае необходимости подключения съемного носителя информации к устройству обеспечьте проведение антивирусной проверки данного носителя на выделенном (отдельном) устройстве, имеющим актуальные антивирусные базы.

4. Безопасность идентификационных данных

- ✓ Не разглашайте идентификационные данные, которые используются для доступа к информационным системам. Логин и пароль, используемые для доступа к информационной системе, являются строго конфиденциальной информацией.
  Работники НКО АО НРД никогда не запрашивают пароли или иную строго конфиденциальную информацию. Если Вам предлагается ввести пароль для отмены какой-либо операции (или сообщить иную конфиденциальную информацию) следует прекратить сеанс использования информационной системы и связаться со специалистами технической поддержки НКО АО НРД.
- ✓ Используйте надежные пароли. При создании пароля обеспечьте выполнение следующих минимальных требований:

- длина пароля не менее 8-ми символов;
- пароль должен содержать строчные и прописные буквы, цифры и специальные символы;
- в качестве пароля не следует использовать свои фамилию, имя и отчество, фамилию, имя и отчество друзей и родственников, клички животных, памятные даты или пароли от других учетных записей, а также простые числовые или буквенные комбинации;
- смена пароля должна производится не реже одного раза в 90 дней.

✓ При входе в информационную систему исключите возможность несанкционированного просмотра вводимой идентификационной информации.
✓ При отсутствии активности в течение 15 минут сеанс работы с информационной системой должен быть принудительно завершен.
✓ Обеспечьте выход из информационной системы и блокировку рабочего экрана устройства при оставлении рабочего места (даже на несколько минут).
✓ При любых подозрениях на компрометацию ваших идентификационных данных, следует незамедлительно остановить работу в информационной системе и обратиться в техническую поддержку НКО АО НРД.

5. Безопасность носителя ключа электронной подписи

✓ Носитель ключа электронной подписи должен быть подключен к устройству только на период работы с информационной системой. После завершения работы с информационной системой носитель должен быть отключен от устройства и убран на хранение.
✓ Ограничьте доступ к носителю ключевой информации – только уполномоченные лица должны иметь право доступа.
✓ При использовании в качестве носителя ключа электронной подписи токенов со встроенными в них средствами криптографической защиты информации, обеспечьте выполнение требований по эксплуатации и обеспечению безопасности, установленные соответствующими техническими и руководящими документами на данное устройство.
✓ Выполняйте незамедлительную блокировку и смену ключей электронной подписи в случаях их компрометации (подозрении на компрометацию), а также по истечении срока действия с периодичностью, установленной договорами и соответствующей документацией.
✓ Обеспечьте смену ключей электронной подписи во всех случаях увольнения или смены лиц, наделенных правом подписывать распоряжения (доверенность) о предоставлении полномочий по подписи электронных документов либо подписи непосредственно распоряжений на совершение каких-либо операций в информационных системах.

6. Безопасность при работе в сети Интернет

✓ Исключите подключение устройства к открытым сетям общего доступа (например, сети Wi-Fi кафе, торгового центра, общественного транспорта и т.п.).
✓ Исключите посещение посторонних веб-сайтов при работе в информационных системах.
✓ Осуществляйте вход в информационные системы только с официального веб-сайта НКО АО НРД – убедитесь, что установлено защищенное SSL-соединение с официальным сайтом.
✓ Исключите подключение к информационным системам из каких-либо посторонних источников сети Интернет – мошенники могут создавать сайты-двойники (фишинговые сайты) для хищения идентификационной информации.

При обнаружении сайта-двойника передайте информацию о данном сайте специалистам технической поддержки НКО АО НРД.

- ✓ Проверяйте адресата, от которого получаете электронные письма. Не отвечайте на сообщения, полученные посредством SMS-сообщений или e-mail рассылок и требующие подтвердить или ввести ваши идентификационные данные на каких-либо сторонних ресурсах.
- ✓ Настройками сетевого оборудования, корпоративных и персональных сетевых экранов ограничивайте выход в сеть Интернет «белым списком» ресурсов. В «белый список» должны включаться исключительно доверенные сайты и хосты вашей организации, государственных органов и иных организаций, взаимодействие с которыми необходимо в производственном процессе, сервера обновлений системного и антивирусного программного обеспечения.
- ✓ Не открывайте подозрительные файлы, полученные по электронной почте – НКО АО НРД не рассылает какие-либо программные или исполняемые файлы по электронной почте и не требует установки обновлений информационных систем подобным образом.
- ✓ Регулярно контролируйте состояние своих счетов и выполнение операций по ним.
- ✓ Незамедлительно остановите работу и обратитесь в техническую поддержку НКО АО НРД при любых подозрениях на компрометацию ваших идентификационных данных, обнаружении выполнения подозрительных или несанкционированных операций, обнаружении успешных или не успешных попыток входа с неизвестных вам IP-адресов, а также в необычное для вас время суток.