

Акционерное общество
«Национальный негосударственный пенсионный фонд»
(АО «Национальный НПФ»)

УТВЕРЖДЕН
Приказом АО «Национальный НПФ»
от «26» октября 2022 № 03-02-01/00635

Дата введения в действие
«26» октября 2022 г.

РУКОВОДСТВО
по соблюдению информационной безопасности клиентами
АО «Национальный НПФ»

Р-ННПФ-15-038-2022

Москва, 2022

Предисловие

1. Разработано начальником отдела информационной безопасности АО «Национальный НПФ».
2. Направлено на реализацию законодательно установленных требований в области информационной безопасности.
3. Периодичность проверки на актуальность – не реже одного раза в три года.
4. Вводится в действие впервые.

Содержание

| | |
|------------------------------------------------------------------------------------------------------------------|---|
| 1. Область применения..... | 4 |
| 2. Нормативные ссылки | 4 |
| 3. Сокращения..... | 4 |
| 4. Термины, определения..... | 4 |
| 5. Общие сведения | 5 |
| 6. Информация о возможных рисках получения несанкционированного доступа к защищаемой информации..... | 6 |
| 7. Рекомендации по защите информации от воздействия вредоносного кода (рекомендации по антивирусной защите)..... | 7 |
| 8. Рекомендации о мерах по предотвращению несанкционированного доступа к защищаемой информации..... | 8 |

1. Область применения

1.1. Настоящее Руководство определяет рекомендации в области защиты информации для клиентов АО «Национальный НПФ».

1.2. Требования настоящего Руководства обязательны для применения в АО «Национальный НПФ».

2. Нормативные ссылки

В настоящем Руководстве использованы нормативные ссылки на следующие документы:

2.1. Положение Центрального Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

3. Сокращения

В тексте настоящего Руководства применены следующие сокращения:

3.1. Фонд – АО «Национальный НПФ»;

3.2. НПФ – негосударственный пенсионный фонд.

4. Термины, определения

– **Технические средства** – устройства (включая, но не ограничиваясь, следующим перечнем: компьютер, ноутбук, планшет, мобильный телефон), с которых возможно осуществление доступа к официальным ресурсам Фонда.

– **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

– **Несанкционированный доступ** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

– **Защита информации от несанкционированного доступа** – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

– **Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

– **Несанкционированное воздействие на информацию** – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

– **Защита информации от несанкционированного воздействия** – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

5. Общие сведения

5.1. В соответствии с требованиями п.1.13 Положения Центрального Банка России 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» Фонд должен обеспечивать доведение до своих клиентов:

– рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям;

– информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

– информации о мерах 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, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

5.2. Рекомендации по защите информации позволяют снизить риски, в т.ч. минимизировать возможные негативные последствия их реализации, в случае следующих инцидентов защиты информации:

– несанкционированный доступ к информации;

– нанесение финансового ущерба клиентам финансовой организации;

– выполнение операций (транзакций), приводящих к финансовым последствиям финансовой организации и ее клиентов, осуществление переводов денежных средств по распоряжению лиц, не обладающих соответствующими полномочиями, или с использованием искаженной информации, содержащейся в соответствующих распоряжениях (электронных сообщениях).

5.3. Данные рекомендации предназначены для работы:

- с официальным сайтом Фонда в сети Интернет: nnpf.ru;
- с личным кабинетом клиента: lk.nnpf.ru/main/.

5.4. В случае любых подозрений о нарушениях или возможном инциденте информационной безопасности рекомендуется информировать Фонд:

- по контактными данным, указанным в Договоре;
- по номеру телефона: +7-(800)-555-99-91;
- по телефону офиса Фонда в вашем регионе;
- по электронной почте: nnpf@nnpf.ru.

6. Информация о возможных рисках получения несанкционированного доступа к защищаемой информации.

6.1. Согласно п.1.1 Положения Центрального Банка России 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» к защищаемой информации относится:

– информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками некредитных финансовых организаций и (или) клиентами некредитных финансовых организаций (далее - электронные сообщения);

– информация, необходимая некредитным финансовым организациям для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

информация об осуществленных некредитными финансовыми организациями и их клиентами финансовых операциях.

6.2. К рискам несанкционированного доступа относятся:

– несанкционированный доступ к устройствам (т.е. любому техническому средству, включая, но не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон, с помощью которого клиент осуществляет вход в автоматизированные системы для совершения финансовых операций или получения информации в отношении таких операций, влечет риск получения третьими лицами логина и пароля, используемых для входа в Системы, что может повлечь за собой получение несанкционированного доступа к защищаемой информации;

– несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии инвестиционного портфеля, другой значимой информации;

– несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента и иных действий, совершенных без воли клиента и направленных против его интересов.

6.3. Типовые случаи получения несанкционированного доступа к защищаемой информации:

– утеря или хищение технического средства, содержащего защищаемую информацию;

– несанкционированный просмотр информации, располагаемой на экране технического средства и бумажном носителе информации;

– утеря SIM-карты клиента;

– внедрение вредоносного кода на технические средства с целью получения удаленного доступа и/или хищения защищаемой информации;

– получение защищаемых данных, в т.ч. паспортных данных, номеров договоров и т.д. посредством обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Фонда или техническим специалистом, рассылает поддельные письма по электронной почте, по обычной почте;

– подмена официальных ресурсов Фонда (фишинг-атаки), посредством перехвата сетевого трафика при подключении к незащищенным и/или недоверенным WiFi-сетям, недоверенным структурированным кабельным сетям.

7. Рекомендации по защите информации от воздействия вредоносного кода (рекомендации по антивирусной защите)

7.1. Данные рекомендации приведены в отношении применения антивирусного программного обеспечения на устройствах, предназначенных для подключения к сети Интернет, официальному сайту Фонда и совершения операций в личном кабинете клиента Фонда.

7.2. Рекомендации при использовании антивирусного программного обеспечения на ноутбуках и персональных компьютерах:

– используйте на технических средствах лицензионное антивирусное программное обеспечение. К перечню рекомендуемых средств антивирусной защиты относятся продукты следующих компаний: АО «Лаборатория Касперского», ООО «Доктор Веб». Для Windows 10 допускается использование встроенного решения Microsoft «Защитник Windows»;

– регулярно обновляйте (не отключайте) антивирусные базы, компоненты средства антивирусной защиты;

– не отключайте компоненты защиты антивирусного программного обеспечения, включенные по умолчанию. Включите автоматическое лечение (удаление) зараженных файлов;

– выполняйте проверку загрузочных областей (быструю проверку) технического средства на вирусы и вредоносный код не реже 1 раза в неделю;

– выполняйте полную проверку технического средства на вирусы и вредоносный код не реже 1 раза в месяц;

- убедитесь, что антивирусное программное обеспечение запускается автоматически при загрузке операционной системы;

- не скачивайте приложения из недоверенных источников.

7.3. Рекомендации при использовании антивирусного программного обеспечения на мобильных устройствах и планшетах:

- не устанавливайте приложений с отрицательными отзывами, низкой репутацией в магазинах приложений или малым количеством скачиваний;

- не скачивайте приложения и не устанавливайте приложения из недоверенных и/или из неофициальных источников.

7.4. Рекомендации при подозрении заражения технического средства вредоносным кодом:

- необходимо прекратить использование технического средства в случае обнаружения вирусов и вредоносного кода, до момента полного лечения (удаления) обнаруженных вирусов и вредоносного кода;

- при подозрениях на наличие вирусов или вредоносного кода на техническом средстве (в частности, при появлении рекламы в процессе работы компьютера, ярлыков приложений), полностью воздержаться от использования технического средства до проведения полной антивирусной проверки и исправления ситуации;

- рекомендуется подвергать антивирусной проверке всю информацию, полученную посредством сети Интернет, на съемных носителях (USB-накопителях).

7.5. Рекомендации по предотвращению заражения вредоносным кодом при работе с электронной почтой:

- не открывайте письма и вложения к ним, полученные от неизвестных отправителей;

- не переходите по ссылкам, содержащимся в письмах, полученных от неизвестных отправителей.

8. Рекомендации о мерах по предотвращению несанкционированного доступа к защищаемой информации

8.1. Данные рекомендации приведены для предотвращения несанкционированного доступа к защищаемой информации и техническим средствам обработки защищаемой информации.

8.2. Рекомендации при работе с техническими средствами:

- применяйте технические средства с установленным официальным лицензионным программным обеспечением;

- не устанавливайте и не обновляйте программное обеспечение из недоверенных и/или неофициальных источников. При обновлении программного обеспечения рекомендуется воспользоваться встроенными в данное программное обеспечение средствами обновления;

- не соглашайтесь на установку программного обеспечения, предлагаемого при работе в сети Интернет, скаченного с неизвестных сайтов в сети Интернет, присланного по электронной почте;

- включите (не отключайте) автоматическое обновление операционной

системы и программного обеспечения;

- установите пароль или графический ключ на техническое средство;
- отключите показ содержимого SMS-сообщений на заблокированном экране мобильных технических средств;
- блокируйте техническое средство после использования, включите автоблокировку устройства при его неиспользовании;
- не используйте на технических средствах средства удаленного доступа и удаленного администрирования, к примеру: TeamViewer, Ammyy Admin, AnyDesk и другие;
- не сохраняйте защищаемую информацию и установленные пароли в текстовых файлах, в записках, иных приложениях на технических средствах, либо на иных электронных носителях;
- в случае утери мобильного телефона или SIM-карты, необходимо незамедлительно обратиться к оператору сотовой связи для осуществления блокировки SIM-карты;

8.3. Рекомендации при работе в сети Интернет:

- при посещении официального сайта Фонда убедитесь, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адрес сайта начинается с <https>, либо в начале адреса отображен в виде «замка»);
- не вводите защищаемую информацию на подозрительных сайтах и других неизвестных вам ресурсах;
- не используйте для подключения к сети Интернет публичные WiFi-сети (расположенные в кафе, ресторанах, торговых центрах, транспорте, иных общественных места).

8.4. Рекомендации при работе с электронной почтой:

- внимательно проверяйте электронный адрес, от которого пришло электронное письмо. Входящие письма должны заканчиваться на «@nnpf.ru».

Рекомендации при взаимодействии с третьими лицами:

- не передавайте применяемые технические средства третьим лицам, в т.ч. с целью выполнения обслуживания данных технических средств;
- не пользуйтесь чужими техническими устройствами для доступа к официальному сайту Фонда;
- не передавайте любые защищаемые данные или персональные данные третьим лицам, даже если они представляются сотрудниками Фонда. В случае возникновения сомнений перезвоните по контактному данным, указанным в договоре, или по номеру телефона: +7- (800)-555-99-91;
- не сообщайте никому содержимое SMS-сообщений, даже если они предоставляются сотрудниками Фонда.
- храните в недоступном для третьих лиц месте паспорт, договор, иные защищаемые данные.

8.5. Рекомендации при работе с ключами электронной подписи (если это применимо к договору клиента):

- необходимо использовать для хранения ключей электронной подписи внешние носители. Настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-

token, смарт-карта и т.п.;

– необходимо крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если ключевые носители не используются для работы;

– необходимо использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли в открытом виде на компьютере, мобильном устройстве или бумажном носителе.