НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД
ГАЗПРОМБАНК-ФОНД
АКЦИОНЕРНОЕ ОБЩЕСТВО

# РЕКОМЕНДАЦИИ

**по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям**

Рекомендации разработаны в соответствии с требованиями Положения 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».

Для обеспечения информационной безопасности при осуществлении электронного взаимодействия между Акционерным обществом «Негосударственный пенсионный фонд Газпромбанк-фонд» (далее – Фондом) и его клиентами по открытым каналам связи информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет) должно уделяться внимание вопросам защиты информации как Фондом, так и клиентом.

Необходимо помнить о возможных рисках несанкционированного доступа к передаваемой информации. Источником таких рисков могут быть следующие неправомерные действия третьих лиц:

- применение вредоносных программных кодов (компьютерных вирусов и т.п.) для нарушения штатного функционирования средств вычислительной техники (далее – вредоносный код);
- перехват (кража) защищаемой информации путем совершения мошеннических операций (телефонных звонков, почтовых рассылок, размещение в сети Интернет поддельных ресурсов и ссылок на них).

Приведенные далее рекомендации направлены на предотвращение несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого он взаимодействует с Фондом, контролю конфигурации указанного устройства, и своевременному обнаружению воздействия вредоносного кода.

✓ В случае поступления обращения (звонка, электронного письма и т.п.) от имени специалиста Фонда с запросом предоставить пароль, либо иные данные, относящиеся к электронному взаимодействию с Фондом, ни в коем случае не сообщайте запрошенную информацию.

При возникновении технических сбоев при осуществлении электронного взаимодействия работники Фонда не запрашивают персональные данные, пароли или подтверждение номера телефона для проведения восстановительных работ.

✓ Официальный сайт Фонда доступен в сети Интернет по адресу https://www.gpbf.ru/. При входе на официальный сайт Фонда проверьте, что

установлено защищенное SSL-соединение (в начале адресной строки браузера должны быть символы https://, слева или справа адресной строки, в зависимости от браузера, должен присутствовать знак закрытого замка; при этом адрес и замок не должны быть выделены красным цветом).

✓ По возможности, исключите электронное взаимодействие с Фондом на общедоступных устройствах (интернет-кафе, библиотеки) или через публичные точки доступа к сети Интернет (бесплатный Wi-Fi в кафе, метро, парках).

✓ Устанавливайте только лицензионное программное обеспечение (операционные системы, приложения), полученное из проверенных и надежных источников, своевременно устанавливайте все обновления программного обеспечения, повышающие безопасность.

✓ Для защиты от воздействия вредоносного кода используйте актуальную версию лицензионного антивирусного программного обеспечения на персональном компьютере или мобильном устройстве с включенными функциями автоматического запуска, регулярного полного сканирования системы и обновления вирусных баз.

✓ При работе с электронной почтой всегда проверяйте адрес отправителя, не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

✓ Не используйте права администратора на компьютере без необходимости. Для повседневного использования входите в систему с правами обычного пользователя.

✓ Старайтесь исключить возможность бесконтрольного доступа третьих лиц (гостей, коллег, знакомых) к вашему компьютеру или мобильному устройству.

✓ Никому не сообщайте пароли и секретные коды, не храните их на легкодоступных носителях (бумажных, электронных), а также воздержитесь от использования функции сохранения паролей в браузере.

✓ При подозрении в том, что кто-либо завладел вашим паролем, необходимо незамедлительно предпринять действия по смене пароля.