АКЦИОНЕРНОЕ ОБЩЕСТВО
«НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД ГАЗФОНД»
Симферопольский бульвар, д.13, г. Москва, Россия 117556 Телефон: +7(495)721-8383, 502-9002, 8(800)700-8383 Факс: +7(495)782-0850
E-mail: gazfond@gazfond.ru www.gazfond.ru

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 17.04.2019 №684-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».

АО «НПФ ГАЗФОНД» (далее – Фонд) предоставляет своим клиентам сервис «Кабинет клиента» (далее – Сервис) по адресу https://client.gazfond.ru/. Сервис предоставляется клиентам по открытым каналам связи информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), осуществляет передачу информации в электронной форме.

Для обеспечения информационной безопасности при использовании Сервиса должно уделяться внимание вопросам защиты информации как Фондом, так и клиентом.

При использовании Сервиса необходимо помнить о возможных рисках несанкционированного доступа к обрабатываемой в нем 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) персональных данных клиента 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 Сервисом, контролю конфигурации указанного устройства, и своевременному обнаружению воздействия вредоносного кода.

✓ В случае поступления обращения (телефонного звонка, электронного письма и т.п.) от имени специалиста Фонда с запросом предоставить пароль или код, относящийся к работе Сервиса, либо предоставить иные данные, ни в коем случае не сообщайте запрошенную информацию и незамедлительно свяжитесь с Фондом по телефону 8 (800) 700-83-83 (звонок по России бесплатный).

При возникновении технических сбоев или проблем с входом в Сервис работники Фонда не запрашивают персональные данные, пароли, коды или подтверждение номера телефона для начала работы с Сервисом.

✓ При обращении к Сервису убедитесь в том, что находитесь на официальной странице https://client.gazfond.ru/. Не рекомендуем переходить на данную страницу по ссылке с Интернет-ресурсов, за исключением официальных ресурсов Фонда.

✓ При входе в Сервис 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 работу с Сервисом на общедоступных устройствах (интернет-кафе, библиотеки) или через публичные точки доступа к сети «Интернет» (бесплатный Wi-Fi в кафе, метро, парках).

✓ После окончания использования Сервиса обязательно завершите сеанс работы кнопкой «Выйти».

✓ 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 электронный 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 или обратиться в Фонд для блокировки доступа к сервису.