ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (499) 300-30-00

От 15.08.2019 № 56-1-11/4184

на № 187 от 12.07.2019
№ 195 от 17.07.2019

О рассмотрении обращений

Личный кабинет

Президенту Саморегулируемой организации Национальная ассоциация негосударственных пенсионных фондов

К.С. Угрюмову

ИНН 5035019523

Уважаемый Константин Семенович!

Департамент информационной безопасности Банка России (далее– Департамент) рассмотрел обращения касательно требований к защите информации при осуществлении деятельности некредитных финансовых организаций и сообщает следующее.

В целях урегулирования вопросов применения Положения Банка России от 17 апреля 2019 года № 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» (далее – Положение № 684-П) предлагаем провести совместную встречу представителей Департамента и Национальной Ассоциации негосударственных пенсионных фондов (далее – рабочая встреча).

По существу представленных Вами вопросов предварительно направляем позицию Департамента.

I. По письму № 187 от 12.07.2019.

По вопросу 1.

Пунктом 1 Положения № 684-П определены виды защищаемой информации к которым в том числе относится информация, содержащаяся в «электронных сообщениях».

В отношении негосударственных пенсионных фондов (далее – НПФ), к такой информации относится следующая информация:

информация, используемая для авторизации и утверждения прав

№410 от 19.08.19.

клиента;

информация о пенсионных накоплениях клиента;

платежные поручения, проводимые в рамках финансовых операций;

другая информация, используемая в процессе выполнения НПФ финансовых операций.

По вопросу 2.

К финансовым операциям, осуществляемым в электронном виде, работниками и клиентами НПФ Департаментом предварительно отнесены следующие операции:

осуществление выплат клиентам НПФ в рамках обязательного пенсионного страхования и негосударственного пенсионного страхования;

передача средств НПФ управляющей компании НПФ;

передача средств клиентов в другие НПФ.

По вопросу 3, 4.

Согласно пункту 2 Положения № 684-П, некредитные финансовые организации должны обеспечивать доведение до своих клиентов рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям. Кроме того, некредитные финансовые организации должны обеспечивать доведение до своих клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также 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. При этом Положением № 684 - П способы доведения указанной информации до клиентов не устанавливаются. В этой связи некредитные финансовые организации самостоятельно определяют способы доведения информации до клиентов, как физических, так и юридических лиц. Вместе с тем в целях реализации пункта 2 Положения № 684-П целесообразно регистрировать факты ознакомления клиента с соответствующими рекомендациями.

По вопросу 5.

В настоящее время Департаментом осуществляется разработка методологии риск профиля некредитных финансовых организаций.

По вопросу 6.

Некредитная финансовая организация определяет применимый уровень защиты информации с учетом выполнения требований пунктов 5.2, 5.3 Положения № 684-П один раз в год, ежегодно не позднее первого рабочего дня календарного года определения уровня защиты информации (пункт 5.1. Положения № 684-П).

По вопросу 7.

Механизм применения и перечень настроек систем анализа защищенности определен в Рекомендациях в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».

По вопросу 8.

Согласно пункту 10 Положения № 684-П некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

Такими способами могут являться электронная подпись, аналоги собственноручной подписи, коды, пароли и другие средства. Между тем указанные способы должны обеспечивать целостность (неизменность) информации и подтвердить составление указанного электронного сообщения уполномоченным на это лицом.

Реализация указанных требований возлагается на некредитные финансовые организации, выбор способов подписания определяется самостоятельно на основе анализа рисков. При этом целесообразно применять дополнительные организационные и технологические меры обеспечения информационной безопасности

По вопросу 9.

Оценка определенного уровня защиты информации должна осуществляться сторонней организацией, имеющей лицензию на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (пункт 6.1 Положения № 683-П).

По вопросу 10.

Некредитная финансовая организация самостоятельно определяет оценку уровня рисков и методику их анализа.

По вопросу 12.

Некредитная финансовая организация самостоятельно определяет должностное лицо (отдельное структурное подразделение, в частности службу управления рисками НПФ или службу информационной безопасности НПФ), ответственное за управление рисками.

По вопросам 11,13,14.

Перечень типов инцидентов, а также порядок и сроки информирования Банка России о выявленных инцидентах защиты информации определены в Стандарте Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации».

II. По письму № 195 от 17.07.2019.

По вопросу 1.

В ответе на вопрос 2 к письму № 187 от 12.07.2019 представлен предварительный перечень операций НПФ, которые отнесены Департаментом к финансовым операциям.

В этой связи считаем целесообразным обсуждение на рабочей встрече вопроса о принадлежности операции по ведению пенсионных счетов НПФ к финансовым операциям.

По вопросу 2.

По мнению Департамента «личный кабинет» (веб-приложение, которое открывается в браузере и предоставляет клиентам-физическим лицам информацию о заключенных пенсионных договорах, текущем размере обязательств и их изменениях) целесообразно признать приложением, распространяемым некредитной финансовой организацией своим клиентам-физическим лицам для совершения действий в целях осуществления финансовых операций. В этой связи в отношении данного приложения следует проводить мероприятия, указанные в пункте 9 Положения № 684-П.

По вопросу 3

В соответствии с пунктом 9 Положения № 684-П сертификация или анализ уязвимостей проводится в отношении прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных

системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет».

В этой связи в случае, если вкладчики-юридические лица взаимодействуют с системой защищенного электронного документооборота НПФ посредством использования информационно-телекоммуникационной сети «Интернет», то на такую систему распространяются требования пункта 9 Положения № 684-П.

И.о. директора Департамента
информационной безопасности А.М. Сычев