Информирование клиентов страхового брокера
об обеспечении защиты информации от воздействия вредоносных программных кодов,
о возможных рисках получения несанкционированного доступа к защищаемой информации
и мерах по его предотвращению

1. Основные понятия

1.1. Защита информации заключается в предотвращении воздействий со стороны злоумышленников и минимизации ущерба. Для обеспечения надлежащей степени защищенности необходимо уделять достаточное внимание вопросам информационной безопасности.

1.2. Важным средством защиты информации являются антивирусные программы. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах и мобильных устройствах компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее - ПО), либо на перехват информации, в том числе паролей.

1.3. Программный код, приводящий к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код) – это компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.
Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами.

1.4. Атака вредоносного кода – это его воздействие на автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование, осуществляемое локально или через информационно-телекоммуникационные сети, в том числе через ИТС «Интернет» (далее - сеть Интернет).

1.5. Фи́шинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (прежде всего, логинам и паролям). Это достигается путём проведения массовых рассылок электронных писем от имени известных компаний / популярных брендов, а также личных сообщений, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на веб-сайт, внешне не отличимый от настоящего, либо на сайт с редиректом (автоматической переадресацией пользователей с одного URL-адреса на другой). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному веб-сайту, что позволяет мошенникам получить доступ к его учетным записям (аккаунтам) и банковским счетам.

2. Рекомендации по защите информации от воздействия вредоносных кодов

2.1. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
2.2. Своевременно обновляйте установленное ПО и операционную систему.
2.3. Периодически удаляйте ПО, которое больше не нужно.
2.4. Установите антивирусное ПО, осуществляющее постоянный контроль за компьютером или мобильным устройством. Периодически запускайте полную проверку компьютера. Регулярно обновляйте антивирусные программы самостоятельно либо разрешайте автоматическое обновление при запросе программы.
2.5. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.).
2.6. При отсутствии необходимости, не используйте в повседневной практике права Администратора, - входите в систему с учетной записью пользователя, не имеющего прав администрирования.
2.7. Не используйте на устройстве, предназначенном для доступа к системам дистанционного финансового (банковского) обслуживания, средства удаленного администрирования.
2.8. Воздерживайтесь от применения программ онлайн-общения на компьютере, использующемся для работы в системе дистанционного финансового (банковского) обслуживания.
2.9. Старайтесь не использовать компьютер, с которого осуществляются переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти сетевые ресурсы чаще всего распространяются компьютерные вирусы.
2.10. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер «шпионских» программ.
2.11. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты.
Работая с электронной почтой, не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
При работе в сети Интернет не соглашайтесь на предлагаемую установку каких-либо сомнительных программ.
2.12. При возникновении подозрений о наличии вирусов на персональном компьютере (в частности, при неожиданных его «зависаниях», перезагрузках, сетевой активности), рекомендуем полностью воздержаться от использования систем дистанционного финансового (банковского) обслуживания и осуществления каких-либо платежей до исправления ситуации.
2.13. Как правило, финансовые организации не несут ответственность за финансовые потери, понесенные их клиентами в связи с нарушением и/или ненадлежащим исполнением требований по защите своих компьютерных устройств от вредоносных кодов.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фишинговых) ресурсов сети Интернет

3.1. Мошеннический (поддельный, ложный, фишинговый) сайт – это небезопасный сайт в сети Интернет, где пользователю под каким-либо предлогом предлагается ввести конфиденциальную информацию.
Как правило, такие сайты имитируют доменные имена и стили оформления сайтов известных компаний / брендов, содержат ложные банковские реквизиты и контактную информацию, и

предназначены для сбора конфиденциальной информации обманным путем, обычно, с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.
3.2. Вступление в какие-либо деловые отношения с лицами, ложно представляющими финансовую организацию, и использование предлагаемых ими ресурсов и реквизитов – рискованно, и может привести к нежелательным последствиям в виде финансового ущерба.
3.3. При подключении к системам дистанционного финансового (банковского) обслуживания необходимо удостовериться, что защищённое SSL-соединение было установлено именно с официальным сайтом финансовой организации.
3.4. Перед просмотром электронных писем всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании – поставщика финансовых услуг.
3.5. Внимательно читайте текст полученных электронных писем.
Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок.
Если в тексте встречаются слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.
Остерегайтесь также писем с безличными обращениями, - такими как, например, «Уважаемый пользователь» или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия. В электронных письмах настоящих финансовых организаций, как правило, к получателю обращаются по имени и фамилии либо по названию организации.
3.6. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить получателя действовать торопливо и необдуманно (например, пытаясь убедить получателя, что его банковскому счету угрожает опасность, если он немедленно не обновит критически важные данные). Старайтесь сохранять спокойствие, действуйте не торопясь и обдуманно.
3.7. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако, они могут перенаправлять на мошеннический веб-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности, не переходите по этой ссылке.
3.8. В случае обнаружения поддельного сайта финансовой организации, пожалуйста, незамедлительно сообщите об этом в финансовую организацию.

4. Дополнительные рекомендации по безопасности при использовании персональных компьютеров для доступа к дистанционному финансовому (банковскому) обслуживанию

4.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе дистанционного финансового (банковского) обслуживания (далее - ДФ(Б)О).
4.2. Рекомендуем исключить возможность физического доступа к компьютеру лиц, не имеющих отношения к работе с ДФ(Б)О.
4.3. Рекомендуется применять на компьютере для работы с ДФ(Б)О специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п.
4.4. На компьютере для работы с ДФ(Б)О необходимо исключить посещение веб-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т.п. (Использование нелицензионного ПО повышает риск получения несанкционированного доступа злоумышленников с целью хищения денежных средств).
4.5. Не рекомендуется работать с ДБФ(О) на компьютерах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых

рабочих мест увеличивает риск неправомерного использования аутентификационной информации.
4.6. В случае передачи (списания) компьютера, на котором ранее была установлена ДФ(Б)О, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально причинить финансовый ущерб;
4.7. Необходимо корректно завершать работу с ДФ(Б)О, используя для этого соответствующие пункты меню системы.
4.8. Рекомендуется регулярно менять пароль для работы со своими учетными данными в системе ДФ(Б)О; хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования.
Финансовые организации не рассылают электронных писем, SMS или других сообщений с просьбой уточнить конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).
4.9. Рекомендуется использовать разные уникальные пароли для различных веб-сайтов и систем, где вводятся конфиденциальные данные.
4.10. При обнаружении, что какой-либо пароль скомпрометирован, рекомендуем незамедлительно сменить этот пароль на новый.
4.11. При использовании Ключевого носителя его использование должно осуществляться исключительно владельцем ключа электронной подписи. Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе или диске), исключив возможность несанкционированного доступа к нему.
Необходимо отключать, извлекать Ключевой носитель, если он в данный момент не используются для работы в ДФ(Б)О. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам электронной подписи третьими лицами.
4.12. Не пересылайте файлы с конфиденциальной информацией по электронной почте или через SMS-сообщения.
4.13. Незамедлительно обращайтесь в финансовую организацию, если получено уведомление системы об операции, которая не производилась.

5. Дополнительные рекомендации по безопасности при использовании мобильных устройств для доступа к дистанционному финансовому (банковскому) обслуживанию

5.1. Рекомендуется не совмещать устройства доступа к мобильным финансовым услугам (например, к услуге «Мобильный банк») и устройства получения SMS-сообщений с подтверждающим одноразовым паролем (мобильный телефон / смартфон или планшет).
5.2. При утрате (потере) мобильного устройства, на которое приходят сообщения с SMS-паролем, рекомендуется сразу же заблокировать SIM-карту, обратившись к оператору сотовой связи.
5.3. При утрате (потере) мобильного устройства с подключенным мобильным приложением рекомендуется сразу же обратиться к оператору сотовой связи для блокировки SIM-карты и в финансовую организацию для блокировки мобильной финансовой услуги.
5.4. При внезапном прекращении работы SIM-карты рекомендуется сразу же обратиться к оператору сотовой связи за уточнением причин (возможно, это – результат мошеннических действий третьих лиц).
5.5. При смене номера телефона, на который подключена мобильная финансовая услуга, необходимо отключить услугу от старого номера телефона и подключить услугу на новый номер.
(Операторы сотовой связи могут передавать номер телефона другому абоненту, если он (номер) будет неактивным длительное время).

5.6. Во избежание несанкционированного использования мобильных финансовых услуг, рекомендуется устанавливать на них пароли доступа и не оставлять их (мобильные устройства) без присмотра.
5.7. Рекомендуется не подключать по просьбе третьих лиц их (чужие) мобильные устройства к мобильной финансовой услуге (даже если эти лица представляются сотрудниками финансовой организации).
5.8. При установке на мобильные устройства дополнительных программ рекомендуется обращать внимание на полномочия, которые необходимы конкретной устанавливаемой программе. Если устанавливаемая программа требует излишние полномочия – это повод для настороженности.
5.9. Рекомендуется не «взламывать» мобильные устройства, так как это отключает защитные механизмы, заложенные производителями, и мобильное устройство становится уязвимым к заражению вирусным ПО.