Рекомендации
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.

В соответствии с требованиями пункта 1.13 Положения Центрального Банка Российской Федерации 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 устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, Общество с Ограниченной ответственностью медицинская страховая организация «Панацея» (далее по тексту - Общество) доводит до физических лиц, получивших у Общества полисы Обязательного медицинского страхования, при реализации Федерального закона «Об обязательном медицинском страховании в Российской Федерации» от 29.11.2010 № 326-ФЗ (далее по тексту – застрахованные лица) рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным действиям.

Настоящие рекомендации по защите информации направлены на снижение вероятности возможных рисков, в том числе минимизировать негативные последствия при их реализации.

Под защищаемой информацией понимается:

• ключевая информация, используемая для доступа в личный кабинет;

• персональные данные застрахованных лиц, в том числе сведения о посещениях медицинских организаций, диагноз, составляющих врачебную тайну.

Методы и средства защиты информации, применяемые в Обществе, позволяют обеспечить необходимый уровень безопасности при осуществлении взаимодействия с застрахованными лицами и предотвратить утечку информации застрахованных лиц при условии выполнения застрахованных лицами рекомендаций, изложенных в данном документе.

Общие рекомендации для застрахованных лиц

На персональном устройстве, с которого осуществляется доступ в личный кабинет (далее по тексту устройство), застрахованного лица рекомендуется установить лицензионное антивирусное программного обеспечения.

Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка устройства на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

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.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное программное обеспечение, разработанное специально для почтовых клиентов.

При возникновении подозрения на наличие компьютерного вируса рекомендуется приостановить работу с системой до полного устранения неисправностей.

Старайтесь не использовать устройство, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т. п.), т.к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором застрахованному лицу под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым застрахованное лицо доверяет (например, Общества), и предназначены для сбора конфиденциальной информации обманным путем.

Перед просмотром электронного письма рекомендуется всегда проверять адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

Рекомендуется сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить застрахованное лицо действовать быстро и необдуманно.

Застрахованным лицам следует внимательно анализировать ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить клиента на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

Рекомендуется использовать надежные пароли. Длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых вводится конфиденциальные данные.

В случае возникновения подозрения в компрометации пароля для входа в личный кабинет, рекомендуется незамедлительно сменить пароль на новый.

Если ранее действующий пароль не срабатывает и не позволяет войти в личный кабинет, либо в случае утраты устройства необходимо как можно быстрее сменить пароль на новый, или обратиться в Общество.

Никому не разглашайте логин и пароль для доступа в личный кабинет.

Общество не рассылает электронных писем, SMS или других сообщений с просьбой уточнить парольную информацию застрахованных лиц.

Настоятельно рекомендуется не сохранять в web-браузере данные для входа в личный кабинет.

Не рекомендуется записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать третьим лицам.

Рекомендуем исключить возможность физического доступа к персональному устройству посторонних лиц.