Общество с ограниченной ответственностью «СМП-Страхование»

УТВЕРЖДЕНА
приказом Генерального директора
ООО «СМП-Страхование» № 86
«13» 11 2020 г.

ПАМЯТКА
по защите информации, о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и о мерах по предотвращению несанкционированного доступа в ООО «СМП-Страхование»

Москва, 2020

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая памятка разработана в соответствии с Положением Банка России от 17 апреля 2019 г. N 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» для клиентов ООО «СМП-Страхование».

1.2. Настоящая памятка размещается в местах оказания услуг ООО «СМП-Страхование», в том числе на официальном сайте ООО «СМП-Страхование».

2. Основные понятия

2.1. **Общество** – ООО «СМП-Страхование».

2.2. **Клиент** – лицо, в отношении которого осуществляются меры по защите информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых Обществом.

2.3. **Вредоносный код** - программный код, приводящий к нарушению штатного функционирования средств вычислительной техники.

2.4. **Устройство** – средство вычислительной техники, используемое Клиентом и отделенное от автоматизированной системы Общества, в которой содержится защищаемая информация и которое используется Клиентом с целью осуществления финансовых операций (мобильный телефон, персональный компьютер и т.д.).

2.5. **Несанкционированный доступ** – доступ к информации или действия с информацией, нарушающие безопасность защищаемой информации, с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

3. Цели и порядок применения мер

3.1. Настоящая памятка разработана в следующих целях:

- информирования клиентов Общества о возможных рисках получения несанкционированного доступа третьими лицами к защищаемой информации;
- информирования клиентов Общества о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия по осуществлению финансовой операции;
- информирования клиентов Общества о мерах по контролю конфигурации устройства, с использованием которого клиентом совершаются действия по осуществлению финансовой операции;
- информирования клиентов Общества о мерах по своевременному обнаружению воздействия вредоносного кода;

– информирования клиентов Общества в целях противодействия незаконным финансовым операциям о рекомендациях по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники;

3.2. Минимизация рисков получения несанкционированного доступа к защищаемой информации достигается путем применения следующего комплексного подхода:

– Общество принимает меры по защите информации в соответствии со своими внутренними документами;

– клиенты принимают меры по защите информации в соответствии с настоящей памяткой.

4. Причины возникновения рисков получения несанкционированного доступа к защищаемой информации

4.1. К общим причинам возникновения рисков получения несанкционированного доступа к защищаемой информации относятся:

– неограниченный доступ третьих лиц к устройству;

– неограниченный доступ третьих лиц к информации о паролях и логинах, используемых для входа в информационные ресурсы;

– несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет»;

– утрата (потеря, хищение) Клиентом устройства;

– отсутствие надлежащего программного обеспечения;

– отсутствие надлежащего антивирусного программного обеспечения;

– несоблюдение Клиентом рекомендаций настоящей памятки по защите информации.

4.2. Перечень причин возникновения рисков получения несанкционированного доступа к защищаемой информации, определенный п. 4.1 настоящей памятки, не является исчерпывающим. Причины возникновения рисков получения несанкционированного доступа к защищаемой информации зависят от конкретной ситуации.

5. Рекомендации Клиентам по применению мер по предотвращению несанкционированного доступа

5.1. В целях предотвращения 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, Общество рекомендует:

5.1.1. Ограничить доступ третьих лиц к устройству, в том числе:

– не оставлять устройство без присмотра;

– не передавать устройство третьим лицам.

5.1.2. Ограничить доступ третьих лиц к информации о паролях и логинах, используемых для входа в информационные ресурсы, в том числе:

- использовать пароли, составленные не менее чем из 8 символов;
- использовать пароли, в которых одновременно содержатся буквы различного регистра, цифры и символы;
- использовать разные пароли и логины для входа в разные информационные ресурсы;
- хранить логины и пароли в тайне от третьих лиц;
- не записывать и не хранить логины и пароли для входа в информационные ресурсы на бумажном носителе, к которым возможен доступ третьих лиц;
- не использовать функцию запоминания логина и пароля при входе в информационный ресурс;
- не использовать в качестве пароля имена, памятные даты, номера телефонов и другую подобную информацию, которая может быть получена или угадана третьими лицами.

5.1.3. Соблюдать режим конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет», в том числе:

- ограничивать доступ ресурсам в информационно-телекоммуникационной сети «Интернет» к устройству Клиента;
- использовать только надежные порталы для информационного обмена в информационно-телекоммуникационной сети «Интернет»;
- проверять адрес электронной почты отправителя перед просмотром сообщения;
- внимательно проверять и анализировать ссылки на информационные ресурсы;
- не открывать сообщения и вложения к ним, полученные по электронной почте от неизвестных отправителей;
- не переходить по активным ссылкам, полученным по электронной почте от неизвестных отправителей;
- программам, скачиваемым из информационно-телекоммуникационной сети «Интернет», не разрешать доступ к излишней информации;
- при нахождении в общественных местах и местах скопления людей, располагать экран устройства таким образом, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами;
- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия вирусов;
- не отключать средства антивирусной защиты информации;

– не подключаться к публичным беспроводным сетям Wi-Fi, незащищенным беспроводным сетям.

5.1.4. В случае утраты (потере, хищении) клиентом устройства по возможности в кратчайший срок предотвратить несанкционированный доступ к защищаемой информации, в том числе:

– незамедлительно сообщить своему оператору сотовой связи о факте утраты устройства и заблокировать SIM-карту;

– незамедлительно сообщить о факте утраты устройства Обществу;

– незамедлительно сменить все логины, пароли, электронные ключи и прочие средства аутентификации, при помощи которых осуществлялся доступ с утраченного устройства;

– обратиться в правоохранительные органы.

5.2. В целях контроля конфигурации устройства, с использованием которого клиентом совершаются действия по осуществлению финансовой операции, Общество рекомендует:

5.2.1. Установить соответствующее программное обеспечение, в том числе:

– использовать только лицензионное программное обеспечение;

– своевременно устанавливать из официальных источников доступные обновления программного обеспечения и операционной системы;

– загружать и устанавливать программное обеспечение только из проверенных источников.

5.3. В целях своевременного обнаружения воздействия вредоносного кода Общество рекомендует:

5.3.1. Установить соответствующее антивирусное программное обеспечение, в том числе:

– установить известную (проверенную) антивирусную защиту;

– установить автоматическое обновление антивирусных баз;

– осуществлять регулярный контроль антивирусной защиты.

5.3.2. Соблюдать рекомендации настоящей памятки по защите информации.