ПАМЯТКА ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ КЛИЕНТОВ АО «ФИНСДЕЛКА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая памятка разработана в соответствии с Положением Банка России от 20 апреля 2021 г. N 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» для клиентов АО «Финсделка».

1.2 Настоящая памятка предназначена для информирования клиентов о рисках несанкционированного доступа и мерах защиты информации при совершении финансовых операций с использованием финансовой платформы.

1.3 Настоящая памятка размещается на официальном сайте АО «Финсделка».

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1 Клиент – лицо, в отношении которого осуществляются меры по защите информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых АО «Финсделка».

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

2.3 Устройство – средство вычислительной техники, используемое клиентом и отделенное от автоматизированной системы АО «Финсделка», в которой содержится защищаемая информация и которое используется Клиентом с целью осуществления финансовых операций (мобильный телефон, персональный компьютер и т.д.)

2.4 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:

3.1.1 Информирование Клиентов АО «Финсделка» (далее – Клиент) о возможных рисках получения Несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления

3.1.2 Информирование Клиентов 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;

3.1.3 Информирование Клиентов о мерах по контролю конфигурации Устройства, с использованием которого Клиентом совершаются действия в целях осуществления финансовой операции;

3.1.4 Информирование Клиентов о мерах по своевременному обнаружению воздействия Вредоносного кода;

3.1.5 Информирование Клиентов о рекомендациях по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям.

3.2 Минимизация рисков получения Несанкционированного доступа к защищаемой информации достигается путем комплексного подхода: как со стороны АО «Финсделка», так и со стороны Клиента.

3.3 АО «Финсделка» принимает меры по защите информации в соответствии со своими внутренними документами.

3.4 Клиент принимает меры по защите информации в соответствии с настоящей памяткой.

4. ВОЗМОЖНЫЕ РИСКИ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

4.1 К общим причинам возникновения рисков получения Несанкционированного доступа к защищаемой информации относится:

4.1.1 Неограниченный доступ третьих лиц к Устройству;

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

4.1.3 Несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет»;

4.1.4 Перехват данных при использовании небезопасных сетей;

4.1.5 Утрата (потеря, хищение) Клиентом Устройства;

4.1.6 Отсутствие надлежащего программного обеспечения;

4.1.7 Отсутствие надлежащего антивирусного программного обеспечения и заражение устройства вредоносным кодом;

4.1.8 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 ПО ПРИМЕНЕНИЮ МЕР ПО ПРЕДОТВРАЩЕНИЮ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ВРЕДОНОСНОГО КОДА

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, АО «Финсделка» рекомендует:

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

— не оставлять Устройство без присмотра;

— не передавать Устройство третьим лицам;

— установить пароль, PIN-код или биометрическую защиту устройства.

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 из букв различного регистра, цифр и знаков препинания;

— 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;

— не использовать функцию запоминания логина и пароля при входе в информационный ресурс;

— не использовать в качестве пароля имена, памятные даты, номера телефонов и другую информацию, которая может быть получена третьими лицами.

5.1.3 Предотвратить несанкционированный доступ к защищаемой информации при утрате (потере, хищении) Клиентом Устройства, в том числе:

— незамедлительно сообщить своему оператору сотовой связи о факте утраты Устройства и заблокировать SIM-карту;

— заблокировать доступ к финансовой платформе;

— сменить пароли и коды доступа;
— обратиться в правоохранительные органы.

5.2 В целях предотвращения воздействия вредоносного кода рекомендуем:

5.2.1 Установить соответствующее антивирусное программное обеспечение, в том числе:
— установить антивирусную защиту;
— установить автоматическое обновление антивирусных баз;
— осуществлять регулярный контроль антивирусной защиты.

5.2.2 Своевременно обновлять операционную систему и приложения;

5.2.3 Регулярно проводить проверку устройства на наличие вредоносного кода.

5.2.4 Соблюдать режим конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет», в том числе:
— ограничивать доступ к Устройству ресурсам в информационно-телекоммуникационной системе «Интернет»;
— использовать только надежные рабочие порталы для информационного обмена в информационно-телекоммуникационной сети «Интернет»;
— проверять адрес электронной почты отправителя перед просмотром письма;
— внимательно анализировать ссылки;
— не открывать письма и вложения к ним, полученные по электронной почте, от неизвестных отправителей;
— не переходить по активным ссылкам, полученным по электронной почте, от неизвестных отправителей;
— не устанавливать программы из непроверенных источников;
— не разрешать доступ программам, скачиваемым из информационно-телекоммуникационной сети «Интернет», к излишней информации;
— не подключаться к публичным беспроводным сетям Wi-Fi, незащищенным беспроводным сетям.

5.3 Дополнительные рекомендации:
— регулярно проверяйте историю операций;
— подключите уведомления о транзакциях;
— не используйте чужие Устройства для входа в финансовую платформу.