ПАМЯТКА ДЛЯ КЛИЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ООО МКК «Кредитофф»

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 ООО МКК «*Кредитофф*».

1.2. Настоящие памятка размещается в местах оказания услуг ООО МКК «*Кредитофф*», *в том числе на официальном сайте ООО МКК «Кредитофф».*

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1. **НФО** – ООО МКК «*Кредитофф*», являющееся некредитной финансовой организацией, осуществляющей финансовые операции в соответствии со ст. 76.1 Федерального закона от 10 июля 2002 г. N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

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

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 НФО, 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:

3.3.1. Информирование Клиентов НФО о возможных рисках получения Несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

3.3.2. Информирование Клиентов НФО 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;

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

3.3.4. Информирование Клиентов НФО о мерах по своевременному обнаружению воздействия Вредоносного кода;

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

3.4. Минимизация рисков получения Несанкционированного доступа к защищаемой информации достигается путем комплексного подхода: как со стороны НФО, так и со стороны Клиента.

3.2. НФО принимает меры по защите информации в соответствии со своими внутренними документами.

3.3. 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 относятся:

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. Утрата (потеря, хищение) Клиентом Устройства;

4.1.5. Отсутствие надлежащего программного обеспечения;

4.1.6. Отсутствие надлежащего антивирусного программного обеспечения;

4.1.7. 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

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, НФО 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 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. 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 разрешать доступ программам, скачиваемым из информационно-телекоммуникационной сети «Интернет», к излишней информации;
— не подключаться к публичным беспроводным сетям Wi-Fi, незащищенным беспроводным сетям.

5.1.4. Предотвратить Несанкционированный доступ к защищаемой информации при утрате (потере, хищении) Клиентом Устройства, в том числе:
— незамедлительно сообщить о факте утраты Устройства НФО;
— незамедлительно сообщить своему оператору сотовой связи о факте утраты Устройства и заблокировать SIM-карту;
— обратиться в правоохранительные органы.

5.2. В целях контроля конфигурации Устройства, с использованием которого Клиентом совершаются действия по осуществлению финансовой операции, НФО рекомендует:

5.2.1. Установить соответствующее программное обеспечение, в том числе:
— остановить свой выбор на лицензионном программном обеспечении;
— своевременно устанавливать доступные обновления операционной системы;
— загружать и устанавливать программное обеспечение только из проверенных источников.

5.3. В целях своевременного обнаружения воздействия Вредоносного кода НФО рекомендует:

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

5.3.2. Соблюдать рекомендации настоящей памятки по защите информации.