Утверждено
Приказом № 42 от «31» мая 2019 г.
Директор ООО «МКК «Экспресс-Займы»

_____
Т.А. Клюева

РЕКОМЕНДАЦИИ
по обеспечению защиты информации
клиентов ООО «МКК «Экспресс-Займы»

г. Славгород, 2019

1. Общие положения

1.1. Настоящие Рекомендации по обеспечению защиты информации клиентов ООО «МКК «Экспресс-Займы» (далее – Рекомендации) разработаны в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Положением Центрального Банка Российской Федерации от 17.04.2019 № 684-П «Об установлении обязательных для некредитных организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных операций», иными федеральными законами, иными нормативно-правовыми актами.

1.2.Рекомендации разработаны в целях:

- противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков, в том числе при оформлении заявки на выдачу микрозайма, оформлении необходимых документов для его получения (согласие на обработку персональных данных, заполнение анкеты заемщика, договора, запроса в бюро кредитных историй и др.);
- защиты информации, получаемой, подгатавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых ООО «МКК «Экспресс-Займы»;
- предотвращения несанкционированного доступа к информации и нарушения штатного функционирования средств вычислительной техники ООО «МКК «Экспресс-Займы», а также утечки персональных данных, лицами, не обладающими правом распоряжения данной информацией.

1.3. Настоящие Рекомендации носят рекомендательный характер для клиентов ООО «МКК «Экспресс-Займы» и призваны донести соблюдать необходимость выполнения мер по защите информации, указанной в разделе 2.

1.4. Понятия:

Организация – Общество с ограниченной ответственностью «Микрокредитная компания «Экспресс-Займы»;

Заемщик – физическое лицо, заключившее Договор потребительского микрозайма с Организацией и получившее от Организации денежные средства по договору потребительского микрозайма;

Микрозаем – заем, предоставляемый Организацией заемщику на условиях, предусмотренных договором займа, в сумме, не превышающей предельный размер обязательств заемщика перед займодавцем по основному долгу;

Договор микрозайма/Договор займа – оформленный в соответствии с нормами действующего законодательства договор, заключенный между Организацией и Заемщиком, в соответствии с которым Организация передает Заемщику денежные средства, а Заемщик обязуется их возвратить в соответствии с общими и индивидуальными условиями договора и настоящими Правилами. Договор является публичной офертой;

Вредоносное программное обеспечение – любое программное обеспечение, предназначенное для получения несанкционированного доступа к ресурсам мобильного устройства/компьютера или к хранимой на них информации, с целью незаконного использования ресурсов и причинения вреда, в том числе нанесения ущерба, владельцу такой информации.

2. Необходимые меры для обеспечения защиты информации

2.1. Перечень информации, подлежащей защите Организацией:

- информация, содержащаяся в документах, составляемых при осуществлении Организацией в электронном виде работниками Организации (электронные сообщения).
- информация, необходимая для авторизации клиентов Организации в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами;

- информация об осуществленных Организацией и ее клиентами финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемой Организацией при осуществлении финансовых операций.

2.2. Для соблюдения целей, указанных в п. 1.2. настоящих Рекомендаций, а также во избежание несанкционированного доступа к защищаемой информации лицам, не обладающими правом распоряжения данной информацией, утечки персональных данных, рекомендуется применять следующие меры защиты:

2.2.1. Не сообщать посторонним лицам персональные данные и информацию о банковских картах (счетах), логины и пароли доступов к ним, историю операций;

2.2.2. Не записывать логин и пароль, используемых для осуществления доступа к различным сетям, в том числе с помощью которых осуществляется доступ к совершению финансовых операций, в общедоступных местах;

2.2.3. Не использовать функцию запоминания логина и пароля в браузерах персонального компьютера, мобильных устройствах, в том числе в программах, предусматривающих платежную систему;

2.2.4. Не использовать одинаковые логин и пароль для доступа к различным системам;

2.2.5. При выборе пароля руководствоваться следующими правилами:
- длина пароля должна быть не менее 8 (Восемь) символов;
- в пароле обязательно должны присутствовать заглавные и прописные символы, цифры, а также специальные символы, например: #, %, $ и т.д.
- в качестве пароля не следует использовать имя, фамилию, дату рождения и другие памятные даты, номер телефона, автомобиля и другие данные, которые могут быть подобраны злоумышленниками путем анализа информации о пользователе;

2.2.6. Установить современное лицензионное антивирусное программное обеспечение, осуществляющее постоянный контроль за компьютером и мобильным устройством. Периодически запускать полную проверку компьютера, мобильного устройства. Регулярно обновлять антивирусные программы, программное обеспечение для работы в сети (интернет-браузер, почтовые программы и др.);

2.2.7. По возможности совершать операции, в том числе в платежных системах, только с собственного устройства в целях сохранения конфиденциальности персональных данных и иной защищаемой информации. При выполнении операций с использованием чужих компьютеров или иных средств доступа не сохранять на них персональные данные и другую информацию, при завершении работы убедиться, что вводные данные не сохранились;

2.2.8. Не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами;

2.2.9. Не переходить по ссылкам в письмах, полученных по электронной почте от сомнительных лиц, не открывать вложенные приложения, так как такие ресурсы могут содержать вредоносное программное обеспечение.

Особую опасность могут представлять файлы со следующими расширениями: *ade, *adp, *bas, *bat, *chm, *cmd, *com, *cpl, *crt, *eml, *exe, *hlp, *hta, *inf, *ins, *isp, *jse, *lnk, *mdb, *mde, *msc, *msi, *mst, *pcd, *pif, *reg, *scr, *sct, *shs, *url, *vbs, *vbe, *wsf, *wsh, *wsc.

2.2.10. В случае несанкционированных действий со средствами, находящимися на Ваших счетах, утраты (потери, хищения) устройства, с использованием которого осуществлялись финансовые операции, необходимо обратиться в правоохранительные органы и прекратить использование средств доступа в целях сохранения доказательственной базы;

2.3. В целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники необходимо:

2.3.1. обновлять антивирусные программы на постоянной основе;

2.3.2. осуществлять регулярный контроль работоспособности антивирусных программ;

2.3.3. создать условия, при которых невозможно несанкционированное отключение средств антивирусной защиты.