

УТВЕРЖДАЮ
Директор Микрокредитной компании
«Фонд микрофинансирования
предпринимательства Республики
Крым»

Аленина В.М.
(Приказ №13/1-19 от «31» мая 2019 года)

Рекомендации по защите информации от воздействия программных кодов,
приводящих к нарушению штатного функционирования средств вычислительной
техники, в целях противодействия незаконным финансовым операциям

Симферополь
2019

1. Общие положения

1. Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям (далее - Рекомендации) разработаны в соответствии с требованиями Положения Банка России от 17.04.2019 № 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».
2. Настоящие Рекомендации подготовлены в целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям, информирования клиентов Микрокредитной компании «Фонд микрофинансирования Республики Крым» (далее - Фонд) о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также 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, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.
3. Задачи защиты информации сводятся к минимизации ущерба и предотвращению злонамеренных действий. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Фонда, так и на стороне клиента.
4. Наиболее опасным является кража учетных данных – хищение личных данных клиента Фонда и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.
5. Риски получения несанкционированного доступа к информации, прежде всего, связаны с «фишингом», а также воздействием вредоносного кода.
6. «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.
7. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение,

нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

8. **Возможные риски** получения несанкционированного доступа к защищаемой информации:
 - доступ к защищаемой информации со стороны третьих лиц может повлечь за собой риски разглашения инсайдерской информации и информации конфиденциального характера, в том числе, сведений об операциях, активах, состоянии счетов, персональных данных и иной значимой информации;
 - получение доступа к защищаемой информации третьими лицами может повлечь за собой совершение финансовых операций с активами клиента лицами, не обладающими правом их осуществления, а также совершение ими иных юридически значимых действий, в частности, внесение изменений в регистрационные данные клиента, использование счетов и активов для совершения незаконных операций и др.;
 - использование лицами, не обладающими таким правом, доступа к защищаемой информации может повлечь за собой деструктивное воздействие на программное обеспечение Фонда, носители информации и их содержимое, что в свою очередь может привести к приостановке деятельности Фонда, невозможности использования клиентами услуг Фонда, потерям и убыткам, как для клиентов, так и для Фонда;
 - использование лицами, не обладающими таким правом, доступа к защищаемой информации может повлечь за собой блокирование работы компьютера либо иного устройства, используемого клиентом для совершения операций, получения услуг.

2. Рекомендации по защите информации от воздействия вредоносного кода

Вредоносная программа – это программа, наносящая вред компьютеру или иным устройствам, на которых она запускается. Вредоносные программы способны самостоятельно (то есть без ведома владельца устройства) создавать свои копии и распространять из различными способами, что может привести к полному разрушению информации, хранящейся на устройстве.

1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
4. Не используйте права администратора при отсутствии необходимости; в повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.
5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.
6. Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов

пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

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

8. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.

9. 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.

10. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

11. При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.

12. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.

13. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

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

1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных.

2. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Стока «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.

3. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия.

5. Страйтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно.

6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с <http://> вместо <https://>), не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа к защищаемой информации третьими лицами

1. Рекомендуется регулярно менять пароль для работы со своими учетными данными в системе. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

2 Используемые логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам.

3. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования.

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

5. В том случае, если Вы обнаружили, что Ваш пароль скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам.

6. Не пересылайте файлы с конфиденциальной информацией по электронной почте или через SMS-сообщения.

7. Рекомендуем исключить возможность физического доступа к компьютеру посторонних лиц.

8. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение.

9. Рекомендуем принять меры по контролю конфигурации компьютера, не допускать несанкционированных программно-аппаратных изменений конфигурации. Любые работы, связанные с изменением конфигурации (программной или аппаратной), должны производиться только квалифицированными сотрудниками компании, у которых есть соответствующий допуск к работе данного типа.

10. На компьютере необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Опера и т.д.) и иного прикладного программного обеспечения.

11. Рекомендуем применять на компьютере лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты.

12. Рекомендуется применять на компьютере специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.
13. На компьютере необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников.
14. Работа с гостевых рабочих мест увеличивает риск неправомерного использования аутентификационной информации. При выполнении операций с использованием чужих компьютеров или иных средств доступа не сохранять на них персональные данные и другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.
15. Носитель ключевой информации ЭП, содержащий ключ для аутентификации в домене, рекомендуется хранить только у его владельца. Не рекомендуется оставлять Носитель ключевой информации ЭП без присмотра, хранить в ящике рабочего стола и других, легкодоступных местах, передавать Носитель ключевой информации ЭП кому бы то ни было. Пользователь должен принять все меры для того, чтобы исключить возможность компрометации Носителя ключевой информации ЭП. Носитель ключевой информации ЭП, применяемый для заверения финансово-распорядительных электронных документов, не может быть доверяющим. При работе с носителем ключевой информации ЭП рекомендуется использовать только лицензированные средства криптографической защиты информации.
16. Рекомендуется установить, пароли на учётные записи пользователей операционной системы на компьютере. Работу на компьютере осуществлять только под учетной записью с ограниченными правами в операционной системе. Не допускать штатную работу под учетной записью с правами администратора в операционной системе компьютера.
17. В случае компрометации или подозрении на компрометацию устройства, с использованием которого клиентом совершались действия в целях осуществления финансовой операции, для предотвращения несанкционированного доступа, в том числе при утрате (потере, хищении) устройства, Клиенту необходимо незамедлительно обратиться в соответствующие организации для блокирования устройства с указанием причины.
18. При обслуживании компьютера сотрудниками технической поддержки организации клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий.
19. В случае передачи (списания) компьютера необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу организации клиента.