Утверждено приказом
генерального директора АО Актив
от 07 сентября 2020 г. № 64

_____ / Марков Я.Г. /
М.П.

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

Санкт-Петербург
2020 г.

Уважаемые клиенты!

В целях предупреждения последствий мошеннических действий третьих лиц, противодействия проведению незаконных финансовых операций в отношении ваших активов, учитываемых на счетах в АО Актив (далее - Общество), представляем настоящее уведомление о рисках несанкционированного доступа, а также перечень рекомендуемых мер по обеспечению защиты информации.

Для удобства взаимодействия с вами Общество предоставляет on-line сервисы дистанционного обслуживания (далее - Сервисы), при использовании которых необходимо помнить о возможных рисках несанкционированного доступа к обрабатываемой в них информации с целью осуществления незаконных финансовых операций лицами, не обладающими правом их осуществления. Источником таких рисков могут быть следующие неправомерные действия третьих лиц:

- применение вредоносных программ (компьютерных вирусов и т.п.) для нарушения штатного функционирования средств вычислительной техники либо перехвата информации, в том числе логинов/паролей (далее – вредоносный код);
- перехват (кража) защищаемой информации путем совершения мошеннических операций (звонков, почтовых рассылок, размещение в сети Интернет поддельных ресурсов и ссылок на них).

Во избежание инцидентов несанкционированного доступа, связанных с неправомерным использованием вашей компьютерной техники, используемой для работы с Сервисами, настоятельно советуем вам соблюдать приведенные далее рекомендации и принимать меры, изложенные в них. Они направлены на защиту информации от воздействия вредоносных кодов, предотвращение несанкционированного доступа к конфиденциальной информации, в том числе при утрате (потере, хищении) вашего устройства (мобильный телефон или съемный носитель криптоключа), с использованием которого вами совершаются действия в целях осуществления финансовой операций и своевременному обнаружению воздействия вредоносного кода.

Рекомендации
по безопасному использованию мобильных приложений

1. Устанавливайте приложение исключительно по ссылкам в авторизованных магазинах приложений (App Store или Google Play).

2. Своевременно устанавливайте обновления безопасности для операционной системы вашего мобильного устройства.

3. Используйте лицензионные, постоянно обновляемые средства антивирусной защиты.

4. Используйте средства блокировки входа на ваше мобильное устройство (Пароль, Пин-код, TouchID, FaceID и иные).

5. Никому не сообщайте пароль для доступа в приложение и одноразовый SMS-код подтверждения операций.

6. Не храните пароль для доступа в приложение на своем мобильном устройстве в открытом виде.

7. Если у вас есть подозрение, что ваши реквизиты доступа в приложение стали известны третьим лицам, заблокируйте устройства и незамедлительно обратитесь в клиентскую поддержку Общества.

8. Завершайте сеанс работы в приложении сразу после проведения всех необходимых операций при помощи кнопки «Выход».

9. В случае потери или хищения вашего мобильного устройства незамедлительно сообщите об этом в клиентскую поддержку Общества.

10. Не посещайте с использованием мобильного устройства, на котором установлена клиентская часть приложения, сайты сомнительного содержания.

11. Не устанавливайте на мобильное устройство, на котором используется клиентская часть приложения, программное обеспечение неизвестных разработчиков, распространяемое из сторонних источников (малоизвестных сервисов распространения приложений).

12. Не используйте приложение на мобильных устройствах, системная программная часть которых подверглась модификации, несанкционированной производителем (устройство подвергнуто процедурам «Jailbreak», получению «Root»-прав, разблокировке загрузчика, установке версий операционных систем от неофициальных разработчиков).

13. При отсутствии необходимости, не используйте приложение для совершения операций по счету или совершения иных юридически значимых действий при подключении телефона к публичным сетям WiFi.

Рекомендации
о мерах безопасного использования сервисов дистанционного обслуживания на персональном компьютере

При работе на персональном компьютере

1. Организуйте режим использования компьютера, с которого осуществляется использование Сервисов таким образом, чтобы исключить возможность его несанкционированного использования.

2. Используйте лицензионное программное обеспечение из проверенных и надежных источников. Регулярно выполняйте обновления операционной системы и прикладного программного обеспечения, особенно в части безопасности.

3. Крайне желательно использовать средство брандмауэр (firewall) для защиты операционной системы от сетевых атак.

4. На компьютере, используемом для работы с Сервисами, не должно быть учетных записей (пользователей) с пустыми паролями. Для повседневной работы не используйте учетную запись с правами Администратора.

5. Блокируйте компьютер при покидании рабочего места (сочетание клавиш «Windows» + «L» для операционной системы Windows).

6. Осуществляйте регулярный контроль состояния ваших счетов и сообщайте сотрудникам Общества обо всех подозрительных или несанкционированных операциях.

7. Регулярно выполняйте процедуру резервного копирования важной информации на случай ее повреждения или случайного уничтожения.

По обеспечению антивирусной защиты

1. Для защиты компьютера от вредоносного кода необходимо использовать лицензионное антивирусное программное обеспечение, функционирующее в автоматическом режиме.

2. Антивирусное программное обеспечение должно регулярно обновляться.

3. Не реже одного раза в неделю проводите полное антивирусное сканирование компьютера. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы.

4. Рекомендуется подвергать антивирусному контролю любую информацию, на съемных носителях (CD/DVD дисках, USB флеш-карты и т.п.). При технической возможности сканирование должно осуществляться в автоматическом режиме.

5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных,

пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо произвести внеплановую проверка на наличие вредоносного кода. После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей на новые.

6. Не отключайте антивирусное программное обеспечение, ни при каких обстоятельствах.

По использованию парольной защиты

1. Выбирайте свой пароль самостоятельно и никому его не сообщайте.

2. Не записывайте пароли, служащие для доступа к Сервисам на бумажных носителях или в файлах на жестком диске вашего компьютера. Постарайтесь запомнить свой пароль. Если Вы все-таки записали пароль на бумажном носителе, храните его в месте, недоступном для посторонних лиц.

3. Используйте для доступа к Сервисам сложные пароли, с наличием букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (!@#$%^&*(),.?).

4. Не используйте простые пароли, представляющие собой, осмысленные слова (password), дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (77777777, 111adZZZ).

5. Обязательно смените пароль в том случае, если он стал известен постороннему лицу.

При работе с электронной почтой

1. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «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.

2. 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.

3. Не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Такие письма подлежат немедленному удалению. Для того чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов. Особую опасность могут представлять файлы со следующими расширениями:

*.ade, *.adp, *.bat, *.cmd, *.com, *.cpl, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vbs, *.vbe, *.wsf, *.wsh, *.wsc.

При работе в сети Интернет

1. По возможности, не используйте для просмотра сайтов в сети Интернет компьютер, с которого осуществляется доступ к Сервисам.
2. Не посещайте сайты сомнительного содержания.
3. Не вводите аутентификационные данные на подозрительных сайтах и других неизвестных вам ресурсах.
4. Не используйте для работы в Сервисах компьютеры, расположенные в местах общего пользования (отелях, бизнес-центрах). Рекомендуется не использовать для работы с системой дистанционного обслуживания общедоступные каналы связи (например, Wi-Fi в кафе, отелях или аэропортах).
5. Не сохраняйте пароли в памяти Интернет-браузера, если третьи лица имеют доступ к компьютеру.

По использованию SMS - кода подтверждения операции

1. При подтверждении ваших операций одноразовым SMS-кодом (паролем), всегда обращайте внимание на условия, реквизиты и иные данные поручения (иного вашего распоряжения), которые вы подтверждаете, содержащиеся в полученном SMS - сообщении. Они должны соответствовать вашему волеизъявлению.
2. В случае утери мобильного телефона, на который Общество отправляет SMS - сообщения, незамедлительно обратитесь к оператору сотовой связи для блокировки вашей SIM - карты, а также в клиентскую поддержку Общества для выявления возможных несанкционированных операций.
3. Не устанавливайте на телефон, используемый для SMS подтверждения, приложения из сомнительных источников.

При работе с ключами электронной подписи

1. Рекомендуется хранить секретные ключи для доступа к Сервисам только на съемном носителе. Организуйте хранение съемного носителя в недоступном для посторонних лиц месте.
2. Используйте сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на устройстве.
3. Крайне внимательно относитесь к носителю ключей электронной подписи, не оставляйте его без присмотра и не передавайте третьим лицам.
4. Подключайте съемный носитель с секретным ключом доступа только в момент подключения к Сервисам.

5. Подключайте съемный носитель с ключом электронной подписи только в момент подписания Электронных документов. Не оставляйте съемный носитель с ключом подписи постоянно подключенным к компьютеру.

6. Закончив работу с Сервисами или прервав ее (даже на несколько минут), не забудьте извлечь съемный носитель и убрать его в доступное только Вам место.

7. Не копируйте содержимое съемного носителя с секретным ключом и не передавайте его никому даже на короткое время.

8. В случае, если съемный носитель с секретным ключом утерян, или у вас имеется подозрение, что ключ оказался у постороннего лица, даже на короткое время, незамедлительно заблокируйте ключ (путем уведомления службы поддержки Общества) и произведите генерацию нового ключа.

9. Если съемный носитель с секретным ключом испорчен, либо утерян по какой, либо другой причине, нужно сообщить об этом Службе поддержки Общества для приостановки его действия, а затем произвести генерацию нового ключа.

Только комплексное соблюдение описанных правил безопасности позволит вам не стать жертвой мошенников и иных злоумышленников и поможет обеспечить защиту ВАШИХ ДАННЫХ.

Пронумеровано, прошито
и скреплено печатью 9
(девять)
лист 26

Генеральный директор
АО Актив
Марков Я.Г.