УТВЕРЖДАЮ

Генеральный директор

ООО УК «АК БАРС КАПИТАЛ»

_____ /Гайзатуллин Р.Р./

Приказ №О01/09/01 от 09.01.2024г.

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КЛИЕНТОВ ООО УК «АК БАРС КАПИТАЛ»

г. Казань, 2024 г.

ОГЛАВЛЕНИЕ

1. Термины и определения

1.1 **Информация** – сведения (сообщения, данные) независимо от формы их представления.

1.2 **Информационная безопасность** – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

1.3 **Дистанционное обслуживание (ДО)** – общий термин для технологий предоставления услуг на основании распоряжений, передаваемых клиентом удаленным образом, чаще всего с использованием компьютерных и телефонных сетей.

1.4 **Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.5 **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. Распространенным способом фишинга является также и SMS-сообщение, который содержит ссылку на фишинговый сайт и мотивирует жертву войти на этот сайт.

1.6 **Вредоносная программа** – программы, специально разработанные с целью нанесения ущерба компьютерам и компьютерным системам.

2. Общие положения

2.1. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне ООО УК «АК БАРС КАПИТАЛ» (далее – Общество), так и на стороне клиента.

2.2. Наиболее опасным является кража учетных данных – хищение личных данных клиента Общества 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.

2.3. 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.

2.4. Средства и методы защиты информации, применяемые в Обществе, позволяют обеспечить необходимый уровень безопасности при условии выполнения клиентами рекомендаций, изложенных в настоящем документе.

3. Правила по защите информации от воздействия вредоносной программы и несанкционированного доступа при использовании устройств (персональные компьютеры, мобильные устройства) для доступа к дистанционному обслуживанию.

3.1. Необходимо строго ограничивать физический доступ к компьютеру, с которого ведется работа с системой дистанционного обслуживания (далее – ДО). Соблюдайте бдительность при работе специалистов, в случае их вызова.

3.2. При передаче компьютера третьим лицам, на котором ранее была установлена ДО, необходимо удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу организации Клиента, в том числе следы работы в ДО.

3.3. При использовании мобильных устройств для доступа к ДО должно выполняться следующие требования:

– установите на мобильное устройство антивирусное ПО и своевременно его обновляйте.

– не оставляйте свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование мобильных услуг (приложений). Установите на мобильные устройства пароль.

– при утрате мобильного устройства, на который Вы получаете сообщения с SMS-паролем либо мобильного устройства с подключенным мобильным приложением следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты.

3.4. При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер или на мобильное устройство специальных «шпионских» программ. Необходимо использовать лицензионное программное обеспечение на компьютере для работы с дистанционным обслуживанием.

3.5. Рекомендуется применять на компьютере для работы с ДО специализированные программные средства безопасности: средства защиты от несанкционированного доступа, обеспечить регулярное автоматическое обновление программного обеспечения этих средств.

3.6. Следует применять на компьютере для работы с ДО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения конфиденциальных данных.

3.7. Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использование ложных ресурсов сети Интернет, «интересной ссылки» в письме от якобы знакомой организации, в котором содержится ссылка), а также воздействием вредоносных программ.

3.7.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

3.7.2. Не отвечайте на SMS-Сообщения, не нажимайте на ссылку, прикрепленную к данному сообщению.

3.7.3. Общество не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.). Не направляйте файлы с конфиденциальной информацией для работы в системе по электронной почте или через SMS-сообщения.

3.8. Используйте только официальный сайт Общества для входа в ДО. Не входите в Систему ДО по ссылкам из поисковых сервисов. Убедитесь, что адресная строка начинается так: https://akbars-capital.ru.

3.9. Не работайте в ДО с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi), т.к. это может увеличить риск кражи ваших персональных данных. Устройства, с которых осуществляется доступ к ДО, рекомендуется располагать в помещении, в котором исключен несанкционированный доступ.

3.10. 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. Не используйте в качестве пароля один и тот же повторяющийся символ, либо комбинацию из нескольких рядом стоящих символов, имя, фамилию, день рождения и другие памятные даты, номер телефона и автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о клиенте.

3.11. Следует использовать разные пароли для различных web-сайтов и систем, на которых вы вводите конфиденциальные данные.

3.12. Не сохраняйте логин и пароль на бумажных носителях или в текстовых файлах в местах, доступных посторонним лицам. Необходимо хранить пароль в тайне и предпринимать меры предосторожности для предотвращения его использования посторонними лицами.

3.13. Не разглашайте свои пароли от различных web-сайтов и систем. Даже сотрудникам Общества. Помните, что пароли запрашивают только мошенники.

3.14. Необходимо корректно завершать работу в ДО, после окончания работы (выйдите с использованием кнопки «Выход из приложения» либо «Выйти из системы») и/или закройте приложение, браузер.