«АК БАРС МЕДИЦИНА»
(общество с ограниченной ответственностью)

«АК БАРС МЕДИЦИНА»
(җаваплылыгы чикләнгән җәмгыять)

Ак Барс
Медицина

**Приказ**

№ 20
Дата 27.06.2024

*Об утверждении*
*Рекомендаций по информационной безопасности*
*для клиентов ООО «АК БАРС МЕДИЦИНА»*

В целях определения требований к содержанию базового состава мер защиты информации, которые применяются Обществом для реализации требований к обеспечению защиты информации, установленных законодательством Российской Федерации в области информационной безопасности,

**ПРИКАЗЫВАЮ:**

1. Утвердить и ввести в действие «Рекомендации по информационной безопасности для клиентов ООО «АК БАРС МЕДИЦИНА» с даты подписания настоящего приказа (Приложение №1).
2. Заместителю исполнительного директора довести содержание настоящего приказа до всех работников Общества.
3. Контроль за исполнением настоящего приказа оставляю за собой.

**Исполнительный директор** **Д.Р. Зиганшин**

Закиров И.Р.
Рассылка: всем работникам

**Приложение №1**
**к Приказу №20 от 27.06 2024г.**

**Рекомендации по информационной безопасности для клиентов**
**ООО «АК БАРС МЕДИЦИНА»**

## 1. Термины и определения.

1.1. В целях настоящих Рекомендаций указанные ниже термины и сокращения используются в ООО «АК БАРС МЕДИЦИНА» (далее — Общество) в следующих значениях:

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

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

**Защищаемая информация:** 1) информация, содержащаяся в документах, составляемых при предоставлении медицинских услуг в электронном виде работниками Общества и (или) клиентами Общества; 2) информация, необходимая Обществу для авторизации своих клиентов в целях осуществления операций на рынке медицинских услуг; 3) информации об осуществленных Обществом и ее клиентами медицинских услуг и финансовых операциях; 4) ключевая информация средств криптографической защиты информации, используемая Обществом и ее клиентами при оказания медицинских услуг (в предусмотренных договорами на оказание медицинских услуг).

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

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

**Неуполномоченные лица** – лица, не обладающие правом на осуществления медицинских услуг.

**Несанкционированный доступ** – незаконное либо не разрешенное обладателем информации использование возможности получения информации и ее использования.

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

**Клиент (Пользователь, Пациент)** – обладатель защищаемой информации, используемой для проведения операций в рамках исполнения заключенных между Обществом и клиентом договоров на обслуживание на рынке медицинских услуг.

**Съемный носитель информации** – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (токен, CD, флэш-накопитель и т. д.).

**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 СМС-сообщение, который содержит ссылку на фишинговый сайт и мотивирует жертву войти на этот сайт.

**Шифрования диска** – технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать**.**

## 2. **Общие положения.**

2.1. Настоящие Рекомендации по обеспечению информационной безопасности, защите информации от воздействия вредоносного кода (программ) при работе в сети «Интернет» и при использовании системы дистанционного обслуживания в целях противодействия незаконным операциям на рынке медицинских услуг (далее – Рекомендации) разработаны Обществом в целях защиты информации от воздействия вредоносных кодов (программ), от несанкционированного доступа путём использования ложных (фальсифицированных) ресурсов сети «Интернет», по защите от различных видов мошенничества, в целях противодействия незаконным операциям на рынке медицинских услуг.

2.2. Целью Рекомендаций является доведение до клиентов Общества информации: 1) о возможных рисках получения несанкционированного доступа к защищаемой информации, в том числе с целью осуществления операций на рынке медицинских услуг, лицами, не обладающими правом их осуществления; 2) 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 операции на рынке медицинских услуг, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления операции на рынке медицинских услуг, и своевременному обнаружению воздействия вредоносного кода (программы).

2.3. 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 Общество, так и на стороне клиента.

2.4. 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.

2.5. 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.

2.6. Рекомендации доводятся до сведения клиентов Общества посредством уведомления клиентов в порядке, предусмотренном для уведомлений соответствующим договором об оказании медицинских услуг и (или) путем размещения Рекомендаций на сайте Общества.

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

## 3. **Рекомендации по безопасности при использовании устройств для доступа к дистанционному обслуживанию**.

3.1. Необходимо использовать лицензионное программное обеспечение на компьютере для работы с дистанционным обслуживанием (далее – ДО), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ДО, операционной системы, web-браузеров и иного прикладного программного обеспечения. На устройство не должно устанавливаться ПО, полученное из сомнительных источников (например, скачанное с файлообменников или торрентов).

3.2. На устройства клиента рекомендуется устанавливать только одну операционную систему, и только то ПО, которое необходимо для работы в Системе дистанционного обслуживания; на устройство не рекомендуется устанавливать ПО, содержащее средства разработки и отладки приложений, а также средства, позволяющие осуществлять несанкционированный доступ к системным ресурсам; пользователи не должны обладать правами локального администратора; настройку устройства клиента (управление привилегиями, квотами, установка прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети.

3.3. Необходимо использовать различные учетные записи при совместном использовании компьютера несколькими лицами (одно рабочее место Общество/семья).

3.4. При осуществлении доступа к Системе дистанционного обслуживания необходимо удостовериться в правильности указанного адреса в адресной строке браузера (исключить выход на сайты, внешне маскирующиеся под Систему дистанционного обслуживания, а также удостовериться в наличии значка защищенного соединения (замок).

3.5. Устройство должно быть защищено средствами сетевой защиты (файрвол/брандмауэр), разрешающими доступ в сеть «Интернет» только тем программам, которые необходимы для работы с системой и запрещающие любые иные обращения к устройству с других рабочих станций локальной сети и, в особенности, из внешних сетей через сеть «Интернет», в том числе его подключение к сетям общего доступа в местах свободного доступа в сеть «Интернет» (офисные центры, кафе и пр.).

3.6. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в систему, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение.

3.7. Включенное устройство не должно оставаться без контроля при наличии иных лиц в помещении, пока происходит сеанс связи с Обществом; время до автоматической блокировки экрана во время бездействия пользователя должно составлять не более 3 минут; разблокировка экрана должна происходить по паролю, желательно с сочетанием CTRL+ALT+DELETE перед входом в систему (безопасный вход в систему). Перед уходом с рабочего места на компьютере необходимо блокировать сеанс пользователя (например, в операционной системе Windows путем нажатия клавиш Win+L).

3.8. Необходимо строго ограничивать физический доступ к компьютеру, с которого ведется работа с системой ДО. Соблюдайте бдительность при работе специалистов, в случае их вызова. При обслуживании компьютера сотрудниками технической поддержки Общества клиента или сторонних организаций – обеспечивать контроль выполняемых ими действий.

3.9. 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 деятельности или имиджу организации клиента, в том числе следы работы в ДО.

3.10. При использовании мобильных устройств для доступа к дистанционному обслуживанию (ДО) должно выполняться следующие требования:

3.10.1. Установите на телефон антивирусное ПО и своевременно его обновляйте.

3.10.2. Использование современных лицензионных операционных систем (ОС) являющихся более защищенными, проведение регулярной установки обновлений ОС, системного и прикладного программного обеспечения, по мере их выпуска.

3.10.3. Не подключайте к услуге «Мобильное приложение» телефоны, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Общества.

3.10.4. Категорически не рекомендуется сохранять мобильный код и постоянный пароль на мобильное устройство, на которых запускается мобильное приложение, применяемое для совершения операций на рынке медицинских услуг.

3.10.5. Не оставляйте свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных услуг (приложений). Установите на телефоне/смартфон пароль.

3.10.6. При утрате мобильного телефона, на который Вы получаете сообщения с SMS-паролем, сразу же обратитесь к оператору сотовой связи и заблокируйте SIM-карту

3.10.7. При потере мобильного телефона с подключенным мобильным приложением следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты.

3.10.8. Не взламывайте мобильное устройство (например, через Jailbreaking или рутинг – процесс, который предоставляет получение прав пользователя root), так как это отключает защитные механизмы, заложенные производителем. В результате ваш телефон становится уязвимым к заражению вирусным ПО.

3.10.9. После окончания работы в Системе ДО обязательно корректно завершите работу (выйдите с использованием кнопки «Выход из приложения») и/или закройте приложение, браузер.

3.10.10. При смене номера телефона рекомендуется незамедлительно сообщить об этом в Общество.

## 4. Рекомендации по защите информации от воздействия вредоносной программы и несанкционированного доступа

4.1. 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.

4.2. 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.

4.3. 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.

4.4. Работать антивирусное ПО должно в автоматическом режиме; не реже одного раза в неделю должно проводиться полное антивирусное сканирование устройства; в случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы; антивирусное ПО не должно отключаться ни при каких обстоятельствах; рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов.

4.5. 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.

4.5.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам. Рекомендуется соблюдать осторожность при получении сообщений с файлами-вложениями. Следует уделять внимание расширениям файлов. Файлы, зараженные вредоносной программой, часто маскируются под обычные графические, аудио, видео файлы или файлы приложений MS Office и pdf, а также архивы, содержащие вышеперечисленные файлы. Режим отображения расширении файлов должен быть включен постоянно.

4.5.2. Не отвечайте на SMS-Сообщения, а также на сообщения, поступившие через различные мессенджеры, не нажимайте на ссылку, прикрепленный к данному сообщению.

4.5.3. 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.

4.6. Способами получения несанкционированного доступа к защищаемой информации (методы, техники социальной инженерии) являются:

4.6.1. Техника «Троянский конь» предполагает расчет злоумышленника на любопытство, страх и другие эмоции пользователей. В этих целях пользователю отправляется по электронной почте письмо, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу, компромат на сотрудника и т.п.; на самом деле в письме находится вредоносная программа.

4.6.2. Техника «Кви про Кво» (услуга за услугу) предполагает обращение злоумышленника по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и проинформировать о возникновении технических проблем на рабочем месте, и, соответственно, необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает пользователя к совершению действий, позволяющих атакующему выполнить определенные команды или установить необходимое ему ПО на компьютере пользователя.

4.6.3. Метод «Дорожное яблоко» представляет собой адаптацию «троянского коня» и состоит в подбрасывании пользователю съемного носителя информации, зараженного вредоносной программой; чтобы у пользователя возник интерес к данному съемному носителю информации, на него наносятся логотип компании или какая-нибудь надпись, например, «данные о продажах», «зарплата сотрудников» и т.п.; при запуске съемного носителя информации, зараженного вредоносной программой, вредоносная программа устанавливается на устройство клиента.

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

4.8. Во время процесса сеанса связи с Обществом должны быть отключены все неиспользуемые для связи с Обществом службы и процессы операционной системы Windows, в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, а именно: возможность терминального соединения с компьютерами, используемыми для работы по Системе дистанционного обслуживания, заблокирован порт 3389 (RDP Remote desktop); "Гостевой доступ" - заблокирована локальная учетная запись Guest; должна быть активирована подсистема регистрации событий информационной безопасности; на учетные записи пользователей операционной системы, должны быть установлены пароли, удовлетворяющие требованиям, установленным настоящим Рекомендациями; должно быть исключено подключение съемного носителя информации, не участвующих в работе Системы дистанционного обслуживания.

4.9. Не работайте в Системе ДО с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi), т.к. это может увеличивает риск кражи ваших персональных данных. Устройства, с которых

осуществляется доступ к Системе ДО, рекомендуется располагать в помещении, в котором исключен несанкционированный доступ.

4.10. 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, автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о клиенте.

4.11. Следует использовать разные пароли для различных web-сайтов, операционных систем, систем дистанционного обслуживания и систем, на которых Вы вводите конфиденциальные данные. Пароль от операционной системы, а также пароль для входа в Систему дистанционного обслуживания рекомендуется менять каждые 90 календарных дней.

4.12. 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.

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

4.14. Не рекомендуется сохранять пароль от доступа к Системе дистанционного обслуживания в браузере.

4.15. Рекомендации по обеспечению информационной безопасности, предъявляемые к ключевой информации клиента.

4.15.1. В случае использования Клиентом ключа электронной подписи при взаимодействии с Обществом в рамках заключения и (или) исполнения договоров об оказании медицинских услуг, ключевая информация (ключ электронной подписи) должна размещаться на сменном носителе информации (eToken PRO USB, Рутокен ЭЦП 2.0 и смарт-карта eToken ГОСТ). Размещение ключевой информации на жестком диске компьютера, на котором установлена Система дистанционного обслуживания, запрещено.

4.15.2. Съемный носитель информации с ключевой информацией должен быть установлен в считывающее устройство только во время работы в Системе дистанционного обслуживания. Размещение сменного носителя в считывающем устройстве вне сеансов работы в Системе дистанционного обслуживания должно быть исключено.

4.15.3. Съемный носитель информации с ключевой информацией должен использоваться только владельцем сертификата ключа проверки электронной подписи либо лицом, уполномоченным на использование такого сменного носителя.

4.15.4. Съемный носитель информации необходимо хранить в защищаемой комнате, в сейфе (металлическом ящике), исключающем доступ неуполномоченных лиц и повреждение материального носителя. Вся ответственность за конфиденциальность секретных ключей электронной подписи клиента лежит на клиенте, как на единственном владельце секретных ключей электронной подписи.

4.15.5. Не допускается снимать несанкционированные копии с носителей ключевой информации, передавать носители ключевой информации лицам, к ним не допущенным, записывать на носители ключевой информации постороннюю информацию.

4.16. Рекомендуется применять шифрование диска для защиты данных и для снижения рисков, связанных с несанкционированным доступом к данным. Шифруйте диски до записи конфиденциальных данных на них.

4.17. Действия клиента при получении сообщений из Общества о несанкционированных операциях, утрате мобильного устройства и (или) компрометации ключевой информации.

4.17.1. По всем случаям обнаружения подозрительных или несанкционированных операций, иных фактов, указанных в Рекомендаций, следует незамедлительно обратиться в

Общество по телефонам: 8 (843) 524-96-69, либо лично явиться в Общество с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.

4.18. Ни при каких обстоятельствах не рекомендуется отвечать на письма, якобы от имени Системы дистанционного обслуживания, Общества, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену https://akbarsmedicina.ru, пересылать секретный ключ, пароль доступа к системе или сеансовый ключ, установить какое-либо ПО на устройство и т.д.; о факте подобного обращения следует немедленно сообщить Обществу в рабочие часы Общества.

4.18.1. В случае поступления на мобильный номер телефона SMS-оповещения или электронного сообщения о совершенной операции, немедленно связаться с Обществом по указанным выше телефонам, иным каналам связи либо лично явиться в Общество, если операция не была Вами осуществлена.

4.18.2. При подозрении на компрометацию ключевой информации, в случаях кадровых перестановок у клиента – юридического лица в отношении лиц, имевших доступ к Системе дистанционного обслуживания, компьютеру и ключам, при подозрениях в несанкционированном доступе, при обнаружении вируса необходимо немедленно обратиться в Общество либо лично явиться в Общество с целью блокирования паролей и (или) скомпрометированных ключей электронно-цифровой подписи с последующей их заменой.

**Общество информирует Вас, что:**
**- не осуществляет рассылку электронных писем с просьбой прислать ключи электронно-цифровой подписи или пароль;**
**- не рассылает по электронной почте программы для установки на компьютеры клиентов, а также ссылки или указания на установку приложений через SMS/MMS/E-mail — сообщения.**

4.19. Рекомендуется регулярно выполнять резервное копирование важной информации, а также иметь системный загрузочный диск на случай подозрения на заражение компьютера.

4.20. Необходимо корректно завершать работу в ДО, используя для этого пункт меню «Выйти из системы».