**Памятка о мерах безопасности при работке с мобильным приложением и Интернет-Банком ЮГ-Инвестбанк (ПАО) для юридических лиц.**

Несмотря на то, что операционные системы **мобильных устройств** и приложения имеют различные инструменты для защиты персональных данных и денежных средств, ключевая роль в обеспечении безопасной работы принадлежит пользователю. Следуя приведенным ниже рекомендациям, вы максимально обезопасите себя от действий злоумышленников и вредоносного ПО:

• Установите и регулярно обновляйте специальное антивирусное ПО для мобильных устройств.

• Скачивайте и устанавливайте программное обеспечение из проверенных источников (рекомендованных производителями мобильных устройств).

• На устройствах, используемых для работы с приложением, не рекомендуется выполнять процедуры получения доступа к файловой системе устройства (Jailbreak, Rooting). Такие операции наносят существенный ущерб системе безопасности, предоставленной производителем устройства.

• Скачивайте и устанавливайте приложение "iBank для жизни" только из официальных магазинов приложений Google Play, App Store. Разработчик приложения должен быть указан как "БИФИТ".

• Не записывайте и не сохраняйте свой код доступа к приложению.

• Не сообщайте код доступа третьим лицам, в том числе сотрудникам банка.

• При получении любых сообщений или писем, связанных с работой приложения, обращайте внимание на отправителя. Подобные сообщения должны поступать только с официального сервисного номера или адреса электронной почты вашего банка.

• Не переходите по ссылкам и не открывайте вложения из писем от подозрительных или неизвестных отправителей.

• После завершения работы с документами и банковскими счетами каждый раз выполняйте выход из приложения.

• При подозрении, что ваш код доступа к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых вы не совершали, немедленно обратитесь в банк и заблокируйте свою учетную запись.

Система «iBank» обеспечивает гарантированный уровень безопасности, содержит механизмы шифрования информации и ЭП, поддерживает работу с аппаратными устройствами: MAC-токен BIFIT, Рутокен ЭЦП 2.0, MS\_KEY K - АНГАРА Исп.8.1.1.
В свою очередь пользователю системы следует на своем рабочем месте обеспечить должный уровень безопасности данных - паролей, ключей ЭП и т. п. информации, хищение которой может повлечь за собой материальный ущерб организации.
Ниже описаны основополагающие принципы безопасной работы пользователя с сервисами системы «iBank».

Дополнительные механизмы безопасности корпоративных клиентов• SMS-информирование о входе в систему, о поступлении в банк платежных документов, о движении средств по счетам клиентов.

• Расширенная многофакторная аутентификация при входе в систему с использованием одноразовых паролей.

• Механизм дополнительного подтверждения платежных поручений (дополнительно к ЭП). В качестве источников одноразовых паролей и кодов подтверждения используются: MAC-токены BIFIT, MAC-токены, SMS-сообщения, OTP-токены.

Меры безопасности при работе с ЭП

• Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать аппаратное устройство (MAC-токен BIFIT, Рутокен ЭЦП 2.0, S\_KEY K - АНГАРА Исп.8.1.1).

• В случае отсутствия аппаратного устройства, сохраните файл-хранилище ключей на съемном носителе (USB-накопитель). Не допускается сохранять его в местах, де к нему может получить доступ кто-либо, кроме вас. Съемный носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа.

• Пароль на доступ к ключу ЭП должен быть известен только вам как владельцу.

• Не допускайте постоянного и бесконтрольного подключения к компьютеру аппаратных устройств с ключами ЭП.

• Не передавайте аппаратное устройство с ключами ЭП никому.

• Не пользуйтесь Интернет-Банком в Интернет-кафе, а также там, где вы не уверены в безопасности компьютеров.

• При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно сообщите в Банк и заблокируйте ключ.

• При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) -обязательно сообщите в Банк и заблокируйте ключи ЭП.

Меры по защите компьютера, с которого выполняется работа в Интернет-Банке• Соблюдайте регламент ограниченного физического доступа к данному компьютеру. Должен быть утвержден список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в Интернет-Банке.

• Рекомендуется использовать отдельный компьютер исключительно для работы в Интернет-Банке.
Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.

• Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО полученное из непроверенных источников.

• Старайтесь использовать современные операционные системы (ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление OC, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.

• Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.

• Используйте и оперативно обновляйте специализированное ПО для защиты информации - антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.

• Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители.

• Регулярно проверяйте ваш компьютер на вирусы, как минимум раз в неделю.

Правила безопасной работы в интернете

• Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить ваш браузер на автоматическую блокировку таких окон.

• Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.

• Не читайте подозрительных электронных писем от незнакомых отправителей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл,
который имеет файловое расширение «exe».

• Максимально ограничьте использование Интернет-мессенджеров (Telegram, ICQ и пр.).

• Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.