

Приложение к Приказу АО «ПроБанк» от 09.01.2019 (в редакции от 31.03.2020)

**Требования АО «ПроБанк» по обеспечению безопасности при работе**

**в системе PayPro, в том числе по организации и осуществлению клиентами защиты от вредоносного кода клиентских АРМ**

Уважаемый клиент, АО «ПроБанк» просит Вас ознакомиться с мерами предосторожности при работе в системе дистанционного банковского обслуживания PayPro.

1. Убедитесь, что в поле «адрес» или «узел» Вашего браузера адрес соответствует официальному адресу, по которому осуществляется доступ в систему [**https://bk.probank.pro/**](https://bk.probank.pro/)Признаком установки защищенного соединения является появление справа или cлева от адресной строки, либо справа вверху/внизу браузера изображение замка . Кликнув по изображению замка можно убедиться в подлинности сертификата.

1. Избегайте осуществления входа в систему **PayPro** в местах, где услуги Интернета являются общедоступными, например, Интернет-кафе.
2. Никому не говорите Ваш пароль и одноразовый пароль. Помните, что сотрудники Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (пароль или одноразовый пароль, полученный по SMS).
3. Для входа в систему **PayPro** необходимо указывать только логин (учетная запись) и пароль. Не вводите свой номер паспорта и другие данные при входе в систему **PayPro** или подтверждении операций. Если от Вас требуется ввод любой другой персональной информации (номер банковской карты или других личных данных), следует прекратить пользование услугой и связаться с Банком для блокировки учетной записи.
4. Проверяйте дату и время, а также IP-адрес Вашего последнего входа в систему **PayPro**. Эту информацию Вы можете увидеть на главной странице после входа в систему.
5. Если у вас есть подозрение, что Ваши учетная запись и пароль украдены/ скомпрометированы, как можно быстрее смените пароль в системе **PayPro** или заблокируйте доступ в систему через службу поддержки +7 (495) 347–47-47.
6. Для завершения работы с системой не выходите из **PayPro** закрытием браузера. В целях обеспечения сохранности Ваших данных необходимо осуществлять выход из системы нажатием ссылки «Выход» в верхней части рабочей области экрана.
7. Внимательно читайте SMS – уведомления и всегда проверяйте реквизиты операции в SMS-сообщении, содержащем одноразовый пароль. Если информация по операции не совпадает, не вводите одноразовый пароль и заблокируйте доступ в систему через службу поддержки +7 (495) 347–47-47.
8. Сгенерируйте в системе **PayPro** и используйте для совершения операций дополнительно к паролю, направляемому в SMS – уведомлении, суффикс безопасности.
9. Используйте для звонков в Банк только номера телефонов, указанные на официальной странице Банка в сети Интернет [**www.probank.pro**](http://www.probank.pro)
10. Используйте лицензионную операционную систему и своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемых компанией-разработчиком. Устанавливайте обновления только с официальных сайтов компаний-разработчиков.
11. Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Установите антивирус на ПО и своевременно обновляйте антивирусные базы данных.
12. Используйте дополнительные средства безопасности (например, программное обеспечение, позволяющее повысить уровень защиты Вашего устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам» - рассылок и др.).
13. Не подключаете устройству, с которого осуществляется доступ к системе **PayPro** и/или на которое Вы получаете SMS – уведомления с паролем непроверенные на наличие вирусов отчуждаемые носители.
14. Регулярно проверяйте устройство, с которого осуществляется доступ к системе **PayPro** и/или на которое Вы получаете SMS – уведомления с паролем, на наличие вирусов, как минимум раз в неделю.
15. Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на устройство, с которого осуществляется доступ к системе **PayPro** и/или на которое Вы получаете SMS – уведомления с паролем, вирусы и шпионские программы.
16. Не устанавливайте на устройство, с которого осуществляете доступ к системе PayPro и/или на которое Вы получаете SMS – уведомления с паролем, приложения, полученные от неизвестных Вам источников.
17. 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».
18. Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свое устройство, с которого осуществляется доступ к системе **PayPro** и/или на которое Вы получаете SMS – уведомления с паролем, на наличие вирусов или шпионского ПО.
19. При наличии возможности, не заходите в систему **PayPro** c того же устройства, на которое Банк направляет SMS – уведомления с паролем.
20. При утрате мобильного устройства, на который Банком направляются SMS - уведомления с паролем, незамедлительно обратитесь к своему оператору сотовой связи и заблокируйте SIM – карту.
21. Незамедлительно обратитесь в Банк для блокировки учетной записи в систему **PayPro** если Вы получили SMS – уведомление с паролем для подтверждения операции, которую Вы не совершали.