О внесении дополнения в постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах"

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 17 октября 2023 года № 75. Зарегистрировано в Министерстве юстиции Республики Казахстан 20 октября 2023 года № 33560

Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 16772) следующее дополнение:

в Требованиях к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, утвержденных указанным постановлением:

дополнить главой 10 следующего содержания:

"Глава 10. Требования к обеспечению безопасности программного обеспечения дистанционного оказания услуг банка, организации

144. Программное обеспечение дистанционного оказания услуг банка, организации включает:

1) программное обеспечение серверов веб-приложений (далее – веб-приложение);

2) программное обеспечение для мобильных устройств (далее – мобильное приложение);

3) программное обеспечение серверов программных интерфейсов (далее – серверное ППО).

145. Разработка и (или) доработка программного обеспечения дистанционного оказания услуг осуществляется банком, организацией в соответствии с внутренними

документами банка, организации, регламентирующими порядок разработки и (или) доработки программного обеспечения, этапы разработки и их участников.

146. В случае, если разработка и (или) доработка программного обеспечения дистанционного оказания услуг банка, организации передана сторонней организации и (или) третьему лицу, банк, организация обеспечивает исполнение сторонней организацией и (или) третьим лицом требований настоящей главы и внутренних документов, отвечает за состояние безопасности программного обеспечения дистанционного оказания услуг.

147. Хранение исходных кодов программного обеспечения дистанционного оказания услуг, разрабатываемых в банке, организации, осуществляется в специализированных системах управления репозиториями кода, размещаемых в периметре защиты банка, организации, с обеспечением резервного копирования.

148. Независимо от принятого в банке, организации подхода к разработке и (или) доработке программного обеспечения дистанционного оказания услуг, обязательным этапом является тестирование безопасности, в ходе которого осуществляются, как минимум, следующие мероприятия:

1) статический анализ исходного кода;

2) анализ компонентов и сторонних библиотек.

149. Статический анализ исходного кода программного обеспечения дистанционного оказания услуг банка, организации проводится с использованием сканера статического анализа исходных кодов, поддерживающего анализ всех используемых языков программирования в проверяемом программном обеспечении, в функции которого входит выявление следующих уязвимостей, но не ограничиваясь:

1) наличие механизмов, допускающих инъекции вредоносного кода;

2) использование уязвимых операторов и функций языков программирования;

3) использование слабых и уязвимых криптографических алгоритмов;

4) использование кода, вызывающего при определенных условиях отказ в обслуживании или существенное замедление работы приложения;

5) наличие механизмов обхода систем защиты приложения;

6) использование в коде секретов в открытом виде;

7) нарушение шаблонов и практик обеспечения безопасности приложения.

150. Анализ компонентов и (или) сторонних библиотек программного обеспечения дистанционного оказания услуг банка, организации проводится с целью выявления известных уязвимостей, присущих используемой версии компонента и (или) сторонней библиотеки, а также отслеживания зависимостей между компонентами и (или) сторонними библиотеками и их версиями.

151. Банк, организация обеспечивают реализацию корректирующих мер по устранению выявленных уязвимостей в порядке, определенном внутренним документом, утвержденным исполнительным органом. При этом критичные

уязвимости устраняются до ввода в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий.

152. Банк, организация осуществляют ввод в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий после согласования с подразделением по информационной безопасности.

153. Банк, организация обеспечивают хранение и доступ в оперативном режиме ко всем версиям исходных кодов программного обеспечения дистанционного оказания услуг и результатов тестирования безопасности, которые были введены в эксплуатацию в течение последних 3 (трех) лет.

154. Обмен данными между клиентской и серверной сторонами программного обеспечения дистанционного оказания услуг шифруется с использованием версии протокола шифрования Transport Layer Security (Транспорт Лэйер Секьюрити) не ниже 1.2.

155. При первичной регистрации клиента в мобильном приложении банк, организация осуществляют биометрическую идентификацию клиента посредством Центра обмена идентификационными данными (далее - ЦОИД) или с использованием биометрических данных, полученных посредством устройств банка, организации.

156. Изменение кода доступа (пароля) к мобильному приложению осуществляется с применением биометрической идентификации клиента с использованием биометрических данных, подтвержденных ЦОИД или полученных посредством устройств банка, организации.

157. Идентификация и аутентификация клиента в программном обеспечении дистанционного оказания услуг осуществляется с применением способов двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости) в соответствии с процедурами безопасности, установленными внутренними документами банка, организации.

158. Механизм кроссдоменной аутентификации программного обеспечения дистанционного оказания услуг согласовывается с подразделением по информационной безопасности.

159. Веб-приложение обеспечивает:

1) однозначность идентификации принадлежности веб-приложения банку, организации (доменное имя, логотипы, корпоративные цвета);

2) запрет на сохранение в памяти браузера авторизационных данных;

3) маскирование вводимых секретов;

4) информирование на странице авторизации клиента о мерах обеспечения кибергигиены, которым рекомендуется следовать при использовании веб-приложения;

5) обработку ошибок и исключений безопасным способом, не допуская отображение в интерфейсе клиента конфиденциальных данных, предоставляя минимально достаточную информацию об ошибке.

160. Мобильное приложение обеспечивает:

1) однозначность идентификации принадлежности мобильного приложения банку, организации (данные в официальном магазине приложений, логотипы, корпоративные цвета);

2) блокировку функционала по оказанию дистанционных услуг банка, организации в случае обнаружения признаков нарушения целостности и (или) обхода защитных механизмов операционной системы, обнаружения процессов удаленного управления;

3) уведомление клиента о наличии обновлений мобильного приложения;

4) возможность принудительной установки обновлений мобильного приложения или блокировки функционала мобильного приложения до их установки в случаях необходимости устранения критичных уязвимостей;

5) хранение конфиденциальных данных в защищенном контейнере мобильного приложения или хранилище системных учетных данных;

6) исключение кэширования конфиденциальных данных;

7) исключение из резервных копий мобильного приложения конфиденциальных данных в открытом виде;

8) информирование клиента о методах обеспечения кибергигиены, которым рекомендуется следовать при использовании мобильного приложения;

9) информирование клиента о событиях авторизации под его учетной записью, изменения и (или) восстановления пароля, изменения, зарегистрированного банком, организацией номера мобильного телефона;

10) в ходе осуществления операций с денежными средствами - передачу в серверное ППО банка, организации геолокационных данных мобильного устройства при наличии разрешения от клиента либо передачу информации об отсутствии такого разрешения.

161. Банк, организация обеспечивает на своей стороне:

1) обработку ошибок и исключений безопасным способом, не допуская в ответе раскрытия конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы;

2) идентификацию и аутентификацию мобильных приложений и связанных с ними устройств;

3) проверку данных на валидность для предотвращения атак с подделкой запросов и инъекций вредоносного кода.".

2. Департаменту информационной и кибербезопасности в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка.

4. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Председатель Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка *М. Абылкасымова*

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан