Алматы қаласы город Алматы

**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»**

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

1. Программное обеспечение дистанционного оказания услуг банка, организации включает:
2. программное обеспечение серверов веб-приложений (далее – веб-приложение);
3. программное обеспечение для мобильных устройств (далее – мобильное приложение);
4. программное обеспечение серверов программных интерфейсов (далее – серверное ППО).
5. Разработка и (или) доработка программного обеспечения дистанционного оказания услуг осуществляется банком, организацией в соответствии с утвержденным исполнительным органом внутренним документом, регламентирующим порядок разработки и (или) доработки программного обеспечения, этапы разработки и их участников.
6. В случае, если разработка и (или) доработка программного обеспечения дистанционного оказания услуг банка, организации передана сторонней организации и (или) третьему лицу, банк, организация обеспечивают исполнение сторонней организацией и (или) третьим лицом требований настоящей главы и внутренних документов, отвечают за состояние безопасности программного обеспечения дистанционного оказания услуг.
7. 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.
8. 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:
9. статический анализ исходного кода;
10. анализ компонентов и (или) сторонних библиотек.
11. 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:
12. наличие механизмов, допускающих инъекции вредоносного кода;
13. использование уязвимых операторов и (или) функций языков программирования;
14. использование слабых и (или) уязвимых криптографических алгоритмов;
15. использование кода, вызывающего при определенных условиях отказ в обслуживании или существенное замедление работы приложения;
16. наличие механизмов обхода систем защиты приложения;
17. использование в коде секретов в открытом виде;
18. нарушение шаблонов и практик обеспечения безопасности приложения.
19. 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.
20. 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.
21. Банк, организация осуществляют ввод в эксплуатацию программного обеспечения дистанционного оказания услуг и (или) его новых версий после согласования с подразделением по информационной безопасности.
22. 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.
23. 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.
24. 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.
25. Изменение кода доступа (пароля) к мобильному приложению осуществляется посредством биометрической идентификации клиента с использованием биометрических данных, подтвержденных ЦОИД или полученных посредством устройств банка, организации.
26. Идентификация и аутентификация клиента в программном обеспечении дистанционного оказания услуг осуществляется с применением способов двухфакторной аутентификации (использованием двух из трех факторов: знания, владения, неотъемлемости). Делегирование функций идентификации и аутентификации клиента сторонним организациям и (или) третьим лицам не допускается.
27. Кроссдоменная аутентификация осуществляется только между доменами третьего уровня или выше, которые имеют общий родительский домен второго уровня, или между доменом второго уровня и его дочерними доменами.
28. Веб-приложение обеспечивает:
29. однозначность идентификации принадлежности веб-приложения банку, организации (доменное имя, логотипы, корпоративные цвета);
30. запрет на сохранение в памяти браузера авторизационных данных;
31. маскирование вводимых секретов;
32. информирование на странице авторизации клиента о мерах обеспечения кибергигиены, которым рекомендуется следовать при использовании веб-приложения;
33. обработку ошибок и исключений безопасным способом, не допуская отображение в интерфейсе клиента конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы.
34. Мобильное приложение не использует функционал встраиваемых веб-страниц (компонент WebView (ВебВью).
35. Мобильное приложение обеспечивает:
36. однозначность идентификации принадлежности мобильного приложения банку, организации (данные в официальном магазине приложений, логотипы, корпоративные цвета);
37. 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;
38. уведомление клиента о наличии обновлений мобильного приложения;
39. возможность принудительной установки обновлений мобильного приложения или блокировки функционала мобильного приложения до их установки в случаях необходимости устранения критичных уязвимостей;
40. хранение конфиденциальных данных в защищенном контейнере мобильного приложения или хранилище системных учетных данных;
41. обмен данными только с авторизованным серверным ППО банка, организации;
42. исключение кэширования конфиденциальных данных;
43. исключение из резервных копий мобильного приложения конфиденциальных данных;
44. информирование клиента о действенных методах обеспечения кибергигиены, которым рекомендуется следовать при использовании мобильного приложения;
45. информирование клиента о событиях авторизации под его учетной записью, изменения и (или) восстановления пароля, изменения зарегистрированного банком, организацией номера мобильного телефона;
46. 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.
47. Серверное ППО обеспечивает:
48. контроль скорости приема запросов со стороны мобильных и веб-приложений клиента;
49. обработку ошибок и исключений безопасным способом, не допуская в ответе раскрытия конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы;
50. идентификацию и аутентификацию мобильных приложений и связанных с ними устройств;
51. 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 с 1 января 2024 года.

**Должность ФИО**