«Мобильді бизнес клиент» (заңды тұлғалар үшін) жүйесінде қашықтықтан банктік қызмет көрсету талаптарына 3 Қосымша

Приложение 3
к Условиям дистанционного банковского обслуживания в системе «Мобильный ,бизнес клиент» (для юридических лиц)

«Мобильді бизнес клиент» жүйесінде жұмыс кезіндегі қауіпсіздікті қамтамасыз ету бойынша рәсім/Процедура по обеспечению безопасности при работе в системе «Мобильный бизнес клиент»

1. Заңды тұлғаларға арналған «Мобильді бизнес клиент» жүйесі (бұдан әрі - «Мобильдік банкинг» жүйесі») Клиент пен Банк арасындағы қауіпсіз қосылудың орнатылуын қамтамасыз ететін SSL (Secure Sockets Layer) хаттамасының көмегімен ақпаратты шифрлеу механизмдеріне негізделген қауіпсіздіктің кепілдік берілген деңгейімен жалпыға ортақ Интернет желісі арқылы Ақпараттық қызметтерді қашықтықтан алуға, сондай-ақ Аутентификацияларды ұялы телефонның нөміріне Пайдаланушыға ұсынылған Смс-кодпен растауға арналған.

2. Қауіпсіздіктің кепілдік берілген деңгейін қамтамасыз ету мақсатында «Мольдік банкинг» жүйесінің құрамына келесі қорғау құралдары кіреді:

1) байланыс тораптары легитимді емес трафиктен қорғау бойынша қызметтерді қолданумен Интернет желісінің провайдерімен ұсынылады;

2) Банктің желілік қауіпсіздігі, сондай-ақ желілік қолжетімділікті шектеу үшін пакеттік фильтрация функциялары бар бағдарламалық-аппараттық фаерволдар, сондай-ақ аутентификация, сәйкестендіру және трафик пен құрал-жабдық журналдарын талдау құралдары пайдаланылады;

3) құпия ақпаратты жаһанды Интернет желісінде жарияланған Web-серверде сақтаудың болмауы;

4) серверді ауыстыру жағдайын болдырмауға мүмкіндік беретін трафиктерді шифрлеу алгоритмдерін пайдалану арқылы Клиент пен «Мобильдік банкинг» жүйесінің сервері арасында деректермен қауіпсіз алмасуды жүзеге асыру, Клиент пен сервер тарапынан хабарламалармен алмасу хаттамаларын салыстыру есебінен қауіпсіздік жүйесіндегі кемшіліктерді алдын ала анықтау. Берілетін ақпараттың құпиялылығы «Мобильдік банкинг» жүйесіне кіру және операцияларды растауды жүзеге асыру үшін аутентификация, авторландыру процедураларын пайдаланумен, SSL (Secure Sockets Layer) хаттамасының көмегімен деректерді шифрлеуқамтамасыз етіледі;

5) берілетін ақпараттың тұтастығы әрбір SSL пакетті хеширлеумен қамтамасыз етіледі;

7) Клиентті "Мобильдік банкинг" жүйесінің Пайдаланушысы ретінде тіркеу үшін Клиентте логин, құпиясөз, осы Улиентке ресімделген ұялы байланыс абонентінің белсенді нөмірінің және Интернетке қол жеткізудің болуы талап етіледі;

8) "Мобильдік банкинг" жүйесіне бірінші рет кіруді жүзеге асырғанда, Банкте тіркелу кезінде алынған құпиясөзбен, Смс-код түрінде алынған бір рет қолданылатын құпиясөзбен құпиясөзді міндетті түрде ауыстыру жүргізіледі. Қауіпсіздік мақсатында құпиясөзге қойылатын талаптар келесідей регламенттелген:

- құпиясөздің ұзындығы 8 символдан кем емес;

1. Система «Мобильный бизнес клиент» для юридических лиц (далее - «система «Мобильный банкинг») предназначена для удаленного получения Информационных услуг через общедоступную сеть Интернет с гарантированным уровнем безопасности, основанного на механизмах шифрования информации с помощью протокола SSL (Secure Sockets Layer), который обеспечивает установление безопасного соединения между Клиентом и Банком, а также подтверждения Аутентификации Смс-кодом, предоставляемым Пользователю на номер мобильного телефона.

2. В целях обеспечения гарантированного уровня безопасности система «Мобильный банкинг» включает в себя следующие средства защиты:

1) каналы связи предоставляются провайдером сети Интернет с применением услуг по защите от нелегитимного трафика;

2) для сетевой безопасности Банка, а также разграничения сетевого доступа, применяются программно-аппаратные фаерволы с функциями пакетной фильтрации, а также средства аутентификации, идентификации и анализа трафика и журналов оборудования;

3) отсутствие хранения конфиденциальной информации на опубликованном в глобальной сети Интернет Web-сервере;

4) осуществление безопасного обмена данными между Клиентом и сервером системы «Мобильный банкинг» путем использования алгоритмов шифрования трафика, которые позволяют исключить ситуацию подмены сервера, раннее выявление недостатков в системе безопасности за счет сопоставления протоколов обмена сообщениями на стороне Клиента и сервера. Конфиденциальность передаваемой информации обеспечивается шифрацией данных посредством протокола SSL (Secure Sockets Layer), с использованием процедур аутентификации, авторизации для осуществлений входа в систему «Мобильный банкинг» и подтверждения операций;

5) целостность передаваемой информации обеспечивается хешированием каждого SSL пакета;

6)

7) для регистрации Клиента в качестве Пользователя системы «Мобильный банкинг» требуется наличие у Клиента логина, пароля, активного номера абонента сотовой связи, оформленного на данного Клиента и доступа в Интернет;

8) при осуществлении первого входа в систему «Мобильный банкинг», неперсонифицированным паролем, полученным при регистрации в Банке, одноразовым паролем, полученным в виде Смс-кода, происходит обязательная смена пароля. Требования к паролю в целях безопасности регламентированы следующим образом:

- длина пароля не менее 8 символов;

- құпиясөз күрделілігіне қойылатын талаптар (құпиясөзде сандар, әр түрлі регистрдің әріптері, арнайы символдар болуы тиіс);

9) Егер Мобильді телефон, Клиент/Пайдаланушы "Мобильді банкинг" жүйесіне кіргеннен кейін, 5 (бес) минуттан артық әрекетсіз болып қалса, "Мобильді банкинг" жүйесімен "Мобильді банкинг" жүйесінен автоматты түрде шығу және сессияны аяқтау жүзеге асырылады;

11) жіберілетін хабарламалардың мазмұны "Мобильдік банкинг" жүйесінде нақты әрекетті растауды бір мәнді көрсетеді және бірегей сәйкестендіргіші бар;

12) құпиясөзді дұрыс енгізбеуге үш әрекет жасағаннан кейін, Банк автоматты түрде Клиенттің "Мобильдік банкинг" жүйесіне кіруін бұғаттауды жүзеге асырады. "Мобильді банкинг" жүйесіне қолжетімділікті бұғаттаудан шығару үшін, Клиент Пайдаланушыларды қолдау тобына жүгінуі қажетрдің алаяқтық әрекеттерінен қорғайды.

3. «Мобильдік банкинг» жүйесіндегі жұмыс кезінде қауіпсіздіктің кепілдік берілген деңгейін қамтамасыз ету мақсатында Клиент/Пайдаланушысы келесілерді қоса алғанда, алайда бұлармен шектелмей өз бетінше қауіпсіздіктің тиісті деңгейін қамтамасыз етуі тиіс:

1) «Мобильдік банкинг» жүйесіне кіру кезінде тек, логинін, кілтсөзін, жылдам қатынау үшін код,Смс-код енгізу қажет. Банк өзге ақпаратты сұратпайды;

2) Үшінші тұлғаларға (оған қоса Банк қызметкерлеріне немесе Клиенттің/Пайдаланушының туысқандарына) логиннің, кілтсөздің, жылдам қатынауға арналған кодтың,Смс-кодтың жария етілуіне жол бермеуді қамтамасыз ету.

3) түрлі лицензиясыз, бөгде, күмән тудыратын, сондай-ақ зиянкес бағдарламалардың болуына тексерілмеген бағдарламалық қамсыздандыруды пайдалануды болдырмауды қамтамасыз етуге;

4) лицензиялы, уақытылы жаңартылатын вирусқа қарсы бағдарламалық қамсыздандыруды міндетті пайдалануды қамтамасыз етуге. Вирустардың әрекеті сәйкестендіру ақпаратын ұстап алу және оны алаяқтарға беруге бағытталуы тиіс;

5) онда анықталған кемшіліктерді жою мақсатында өндіруші компания ұсынатын, қазіргі заманға сай автоматты жаңартылумен, қазіргі заманға сәйкес операциондық жүйелерді пайдалануды қамтамасыз етуге. операциондық жүйесі мен браузерін тұрақты жаңартуды (патч) жүргізуге, бұл қауіпсіздік деңгейін айтарлықтай арттырады;

6) ұялы телефонға вирустардың болуына тексерілмеген бөлінетін ақпарат тасымалдағыштарды қоспауға;

7) кілтсөзде өз атын, туылған күнін пайдалануға болмайды, тек сандар немесе қарапайым сөздер. кілтсөзде бас әріптерді, сандар мен арнайы белгілерді пайдалануға тырысу қажет;

8) кілтсөзді міндетті ауыстыру арасындағы әрекет ету мерзімі 30 (отыз) күнтізбелік күнді құрайды;

9) Интернет-қосылуды орнататын бағдарламаларды, ұялы телефонда немесе өзге де электронды ақпарат тасымалдағыштарда мәтіндік файлдарда кілтсөз(дер)ді сақтамау қажет, себебі бұл кезде оны ұрлау және жариялау қаупі туындайды;

10) жұмыс аяқталғаннан кейін «Шығу» батырмасының көмегімен «Мобильдік банкинг» жүйесінің

- требования к сложности пароля (пароль должен содержать: цифры, буквы разного регистра, спец символы);

9) если мобильный телефон после входа Клиентом/Пользователем в систему «Мобильный банкинг» остается бездействующим более 5 (пяти) минут, системой «Мобильный банкинг» осуществляется автоматический выход из системы «Мобильный банкинг» и завершение сессии;

11) содержимое отправляемых сообщений однозначно указывает на подтверждение конкретного действия в системе «Мобильный банкинг» и имеет уникальный идентификатор;

12) после трех попыток неверного ввода пароля, Банк автоматически осуществляет блокирование доступа Клиента в систему «Мобильный банкинг». Для разблокирования доступа в систему «Мобильный банкинг», Клиенту необходимо обратиться в Группу поддержки пользователей;

3. В целях обеспечения гарантированного уровня безопасности при работе в системе «Мобильный банкинг», Клиенту/Пользователю (-ям) необходимо самостоятельно обеспечивать должный уровень безопасности, включая, но не ограничиваясь:

1) при входе в систему «Мобильный банкинг» вводить только логин, пароль, код для быстрого доступа, Смс-код. Никакой другой информации Банк не запрашивает;

2) обеспечивать недопущение разглашения логина, пароля, кода быстрого доступа, Смс-кода третьим лицам (включая работников Банка или родственников Клиента/Пользователя);

3) обеспечивать недопущение использования различного нелицензионного, стороннего, сомнительного, а также не проверенного программного обеспечения на наличие вредоносных программ;

4) обеспечивать обязательное использование лицензионного, своевременно обновляющегося антивирусного программного обеспечения. Действие вирусов может быть направлено на перехват идентификационной информации и передаче ее злоумышленникам;

5) обеспечивать использование современных операционных систем, с автоматическим своевременным обновлением, рекомендуемым компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления (патчи) операционной системы и браузера, что значительно повышает уровень безопасности;

6) не подключать к мобильному телефону не проверенные на наличие вирусов отчуждаемые носители информации;

7) не использовать в пароле свое имя, дату рождения, только цифры или простые слова. Необходимо стараться применять в сочетании заглавные буквы, цифры и специальные символы;

8) срок действия между обязательной смены пароля составляет 30 (тридцать) календарных дней;

9) никогда не сохранять пароль (-и) в программах, устанавливающих Интернет-соединение, в текстовых файлах на мобильном телефоне либо на других электронных носителях информации, так как при этом существует риск его кражи и компрометации;

10) после окончания работы необходимо закрывать окно системы «Мобильный банкинг» с помощью кнопки

терезесін жабу қажет және ұялы телефонды «Мобильдік банкинг» жүйесіндегі ағымдағы сессиясымен қараусыз қалдыруға болмайды;

11) ұялы телефонның жұмысында жаңылыстар немесе «Мобильді банкинг» жүйесімен жұмыс істеу кезінде немесе сеанс аяқталғаннан кейін оның бұзылып қалуы (операциондық жүйені жүктеуге байланысты қиындықтар, қатаң дискінің істен шығуы және т.б.) жағдайында дереу ұялы телефондыі сөндіріп, сондай-ақ Банкке жүгініп, Сіздің атыңыздан рұқсат етілмеген операциялардың жүргізілмегендігіне көз жеткізу қажет;

12) «Мобильді банкинг» жүйесінің қызмет етуінің дұрыстығына кез келген күмән туындаған кезде дереу Банкке жүгіну қажет;

13) «Мобильді банкинг» жүйесіне қосылу кезінде Сізді өзге сайтқа қайта бағыттау туралы браузердің ескертуі туындаған жағдайда операцияларды орындауды кейінге қалдырыңыз және Банктің Пайдаланушыларға қолдау көрсету тобына жүгініңіз.

4. Пайдаланушының қалауы бойынша «Мобильді банкинг» жүйесіндегі жұмыс кезінде ақпаратты қорғау және қауіпсіздігін қамтамасыз ету бойынша сәйкестендіру белгілері бойынша (ішкі IP фильтрациясы, сыртқы IP фильтрациясы, MAC мекен-жайлар бойынша фильтрация) қолжетімділік фильтрациясын ұйымдастыру, сондай-ақ уақытша талаптар бойынша қолжетімділікті баптау сияқты қосымша шараларды қолдануға болады.

5. Даулы жағдайларды талдауды жүзеге асыру үшін Банк Пайдаланушының барлық әрекеттерін мұрағаттауды жүргізуді қамтамасыз етеді. Клиент Пайдаланушыларының «Мобильді банкинг» жүйесіндегі барлық әрекеттері «Мобильді банкинг» жүйесімен қалыптастырылған электронды журналдарға жазылады.

6. Банктік құпияны құрайтын ақпаратқа рұқсат етілмеген қолжетімділікті және/немесе қолжетімділік талпыныстары, оны рұқсат етілмеген пайдалану, рұқсат етілмеген төлемді немесе ақшаны аударуды жүргізу және өзге де рұқсат етілмеген әрекеттер анықталған кезде, сондай-ақ Банк пен Клиенттің ақпараттық қауіпсіздігіне қауіп төндіретін жағдайларда Банк уәкілеттік берілген электронды байланыс арналары бойынша осындай ескертулерді жолдау арқылы анықталған күннен кейін келесі жұмыс күнінен кешіктірмей осы туралы Клиентке ескертеді және дереу олардың салдарларын жою және олардың болашақта пайда болуының алдын алу үшін барлық қажетті шараларды қабылдайды

7. Осы Процедуралардың 6 тармағында көрсетілген рұқсат етілмеген әрекеттер тундаған жағдайда Банк «Мобильді банкинг» жүйесінің көмегімен қызметтерді ұсынуды уақытша тоқтатуға құқылы.

8. Клиентке / Пайдаланушыға тыйым салынады: Мобильді банкингте техникалық шектеулерді айналып өтуге, бағдарламалық қамтамасыз етудің бастапқы кодын (бастапқы мәтінін) зерттеуге, көшіруге, бағдарламалық қамтамасыз етудің бастапқы кодын бөлшектеуге немесе қандай да бір басқа тәсілмен алуға, сынақ жүргізуге, Мобильді банкинг пентестерін жүргізуге, қандай да бір алдын ала алынбаған тәсілмен Мобильді банкингті пайдалануға, Мобильді банкинг сервисіне немесе Мобильді банкинг серверлеріне рұқсатсыз кіруге, Банктің ақпараттық қауіпсіздігіне қауіп төндіретін іс-

«Выход» и никогда не оставлять мобильный телефон с текущей сессией в системе «Мобильный банкинг» без присмотра;

11) в случае сбоев в работе мобильного телефона или его поломки во время работы с системой «Мобильный банкинг» или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.), следует немедленно выключить мобильный телефон, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции;

12) при возникновении любых сомнений в правильности функционирования системы «Мобильный банкинг» незамедлительно обратиться в Банк;

13) в случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении системы «Мобильный банкинг» отложите совершение операций и обратитесь в Группу поддержки пользователей Банка.

4. По желанию Пользователя возможно предусмотреть дополнительные меры по реализации защиты и безопасности информации при работе в системе «Мобильный банкинг», например, такие как: организация фильтрации доступов по идентификационным признакам (фильтрация внутренних IP, фильтрация внешних IP, фильтрация по MAC адресам), а также настройка доступа по временным критериям.

5. Для осуществления анализа спорных ситуаций, Банком обеспечивается ведения архива всех действий Пользователя. Все действия Пользователей Клиента в системе «Мобильный банкинг» записываются в электронные журналы, сформированные системой «Мобильный банкинг».

6. При обнаружении несанкционированного доступа и/или попыток такого доступа к информации, составляющей банковскую тайну, ее несанкционированного изменения, осуществления несанкционированного платежа или перевода денег и иных несанкционированных действий, а также ситуаций, представляющих угрозу информационной безопасности Банка и Клиента,Банк уведомляет об этом Клиента, не позднее следующего рабочего дня после их обнаружения путем направления таких уведомлений по уполномоченным электронным каналам связи и незамедлительно принимает все необходимые меры для устранения их последствий и предотвращения их появления в будущем.

7. В случае возникновения несанкционированных действий, указанных в пункте 6 настоящих Процедур, Банк вправе приостановить предоставление услуг посредством системы «Мобильный банкинг».

8. Клиенту/Пользователю запрещается: пытаться обойти технические ограничения в Мобильном банкинге, осуществлять любые действия, направленные на изучение, копирование исходного кода (исходного текста) программного обеспечения, разбирать или каким-либо другим способом пытаться извлечь исходный код программного обеспечения, проводить испытание, пентесты Мобильного банкинга, использовать Мобильный банкинг каким-либо не предназначеным способом, допускать несанкционированный

әрекеттерді жасауға бағытталған кез келген іс-әрекеттерді жүзеге асыруға.

доступ к сервису Мобильного банкинга или серверам Мобильного банкинга, совершать действия, представляющих угрозу информационной безопасности Банка.