«Интернет-банкинг» («VTB Online banking») жүйесінде
Дистанциялық банктік қызмет көрсетудің шартына
10 Қосымша

Приложение 10
к Условиям дистанционного банковского обслуживания
в системе «Интернет-банкинг» («VTB Online banking»)

«Интернет-банкинг» («VTB Online banking») жүйесінде жұмыс кезіндегі қауіпсіздікті қамтамасыз ету бойынша рәсім/Процедура по обеспечению безопасности при работе в системе «Интернет-банкинг» («VTB Online banking»)

1. «Интернет-банкинг» («VTB Online banking») жүйесі (бұдан әрі - «Интернет-банкинг» жүйесі») банктік шот(тар)ты қашықтан басқаруға және 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 өзге де электронды банктік қызметтерге, сондай-ақ барлық операцияларды Электронды-сандық қолтаңбамен және арнайы e-Token PRO 72k Java электронды тасымалдағыштарда сақталатын қауіпсіздік кілтсөзімен растауға арналған.

2. Қауіпсіздіктің кепілдік берілген деңгейін қамтамасыз ету мақсатында «Интернет-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 «Интернет-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 «Интернет-банкинг» жүйесіне кіру және операцияларды растауды жүзеге асыру үшін аутентификация, авторландыру процедураларын пайдаланумен, SSL (Secure Sockets Layer) хаттамасының көмегімен деректерді шифрлеу, сондай-ақ екіфакторлы аутентификация және e-Token PRO 72k Java Электронды-сандық қолтаңбада қауіпсіз сақтаудың аппараттық-бағдарламалық кешенімен қамтамасыз етіледі;

5) e-Token PRO 72k Java қондырғысы қатаң аутентификацияға, құпия деректерді қауіпсіз сақтауға, криптографиялық есептеулерді және ассиметриялық кілттермен, сандық сертификаттармен, шифрлеу кілттерімен және Электронды-сандық қолтаңбамен жұмысты орындауға арналған қорғалған тасымалдағыш болып табылады.

E-Token PRO 72k Java сертификацияланған және 1073-2007 ҚР СТ стандарты бойынша қауіпсіздіктің 3 (үшінші) деңгейіне сәйкес келеді. Бұл TumarCSP криптоаплеті мен «KISC Certificate RK-02» РМК ҚБЕО сертификатын пайдалану кезінде 1073-2007 ҚР СТ бойынша жүйені қорғаудың 3 (үшінші) деңгейіне көшуге мүмкіндік береді (*қауіпсіздіктің үшінші деңгейіндегі СКЗИ бір кілт(тер)ті пайдалану көлеміндегі өзгеруінен келтірілетін зиян 1 000 000 (бір миллион) минимальді есептік көрсеткіштен аспайтын ақпаратты қорғауға арналған*). Қондырғы Электронды-

1. Система «Интернет-банкинг» («VTB Online banking») (далее - «система «Интернет-банкинг») предназначена для удаленного управления банковским (-ими) счетом (-ами) и получения иных электронных банковских 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 всех операций Электронно-цифровой подписью и паролем безопасно хранящихся на специальных электронных носителях e-Token PRO 72k Java.

2. В целях обеспечения гарантированного уровня безопасности система «Интернет-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 «Интернет-банкинга» 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 «Интернет-банкинг» и подтверждения операций, а также аппаратно-программным комплексом двухфакторной аутентификации и безопасного хранения Электронно-цифровой подписи e-Token PRO 72k Java;

5) устройство e-Token PRO 72k Java предоставляет собой защищенный носитель, предназначенный для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами, цифровыми сертификатами, ключами шифрования и Электронно-цифровой подписи. E-Token PRO 72k Java сертифицирован и соответствует 3 (третьему) уровню безопасности по стандарту СТ РК 1073-2007, что совместно с использованием криптоаплета TumarCSP и сертификата РГП КЦМР «KISC Certificate RK-02» и позволяет превзойти 3 (третий) уровень защиты системы по СТ РК 1073-2007 *(СКЗИ третьего уровня безопасности предназначены для защиты информации, ущерб от изменения которой в объеме использования одного и того же ключа (одних и тех же ключей), не превышает 1 000 000 (один миллион) минимальных расчетных показателей.)*

сандық қолтаңба механизмін жабық кілт қауіпсіз сақталып, ешқашан қондырғыдан кетпеуін қамтамасыз ететіндей жүзеге асыруға мүмкіндік береді;
6) кілттік контейнеріне кілтсөзді Банк Клиенті өз бетінше ЭСҚ Қорғалған тасымалдағышын - eToken PRO 72K (Java) бірінші рет қосқан кезде стандарттыдан өзгертуі тиіс. Кілтсөзді ауыстыру туралы ұсыныс Tumar CSP криптопровайдерімен автоматты түрде генерацияланатын болады. «Интернет-банкинг» жүйесінде жұмысты орындау стандартты кілтсөзді ауыстырусыз мүмкін болмайды;
7) берілетін ақпараттың тұтастығы әрбір SSL пакетті хеширлеумен қамтамасыз етіледі;
8) ақпараттың дұрыстығы Электронды-сандық қолтаңбаны пайдаланумен қамтамасыз етіледі;
9) Клиентті «Интернет-банкинг» жүйесінің Пайдаланушысы ретінде тіркеу үшін Клиентте Банкте ашылған ағымдағы шоты, логині, кілтсөзі және уәкілетті Куәландырушы орталықта, жекелей айтқанда Қазақстандық банкаралық есеп айырысу орталығында (ҚБЕО) тіркелген Электронды-сандық қолтаңбаның Тіркелген куәлігімен «Интернет-банкинг» жүйесіне кіруге арналған e-Token PRO 72k Java қондырғысы болуы тиіс;
10) «Интернет-банкинг» жүйесіне Банкте тіркелу кезінде қорғалған Пин-конвертте алынған жеке тұлғаландырылмаған кілтсөз арқылы бірінші рет кіруді жүзеге асырған жағдайда кілтсөз міндетті түрде ауыстырылады. Қауіпсіздік мақсатында кілтсөзге қойылатын талаптар келесідей жүйеленген:

- Клиент/Пайдаланушы «Интернет-банкинг» жүйесіне кіргеннен кейін компьютер 10 (он) минуттан артық әрекетсіз күйінде тұрып қалса, «Интернет-банкинг» жүйесі автоматты түрде «Интернет-банкинг» жүйесінен шығуды және сессияны аяқтауды жүзеге асырады;
- Клиенттің «Интернет-банкинг» жүйесі арқылы электронды банктік қызметтерді алуға сұранысының шынайылығын тексеру Банкпен Электронды-сандық қолтаңба арқылы автоматты түрде жүзеге асырылады. Бұл кезде Клиенттің «Интернет-банкинг» жүйесіндегі әрбір әрекеті Электронды-сандық қолтаңбаның қорғалған тасымалдағышында - e-Token PRO 72K (Java) сақталатын Электронды-сандық қолтаңба арқылы растауды талап етеді. Бұл кезде Клиентке Электронды-сандық қолтаңбаның кілт контейнеріне қолжетімділік үшін кілтсөзді қолмен теруге тура келеді. Осы арқылы операциялардың валидтілігі расталады. Бұл Клиентті алаяқтар мен киберқылмыскерлердің алаяқтық әрекеттерінен сақтайды.

3. «Интернет-банкинг» жүйесіндегі жұмыс кезінде қауіпсіздіктің кепілдік берілген деңгейін қамтамасыз ету мақсатында «Интернет-банкинг» жүйесінің Клиенті/Пайдаланушысы келесілерді қоса алғанда, алайда бұлармен шектелмей өз жұмыс орнында қауіпсіздіктің тиісті деңгейін қамтамасыз етуі тиіс:
1) «Интернет-банкинг» жүйесіне кіру кезінде тек Пайдаланушының атауын, логинін және кілтсөзін енгізу қажет. Банк өзге ақпаратты сұратпайды;
2) «Интернет-банкинг» жүйесінде жұмыс істеу үшін шектелген жеке қолжетімділікті дербес компьютерді пайдалануға, бұл компьютердегі өзге әрекеттер орындалмауы тиіс, мысалы, өзге бағдарламалармен, электронды поштамен жұмыс, Интернетте сайттарға кіру;

3) Кілттер кешенін қауіпсіз сақтауды тасымалдағышта (USB Flash - eToken PRO 72k Java) жүзеге асыру. Оны пайдалануды

Устройство позволяет осуществлять механизм Электронно-цифровой подписи так, чтобы закрытый ключ безопасно хранился и никогда не покидал устройства;
6) пароль на ключевой контейнер Клиент Банка должен изменить со стандартного при первом подключении Защищенного носителя ЭЦП - eToken PRO 72K (Java) самостоятельно. Предложение о смене пароля будет сгенерировано криптопровайдером Tumar CSP автоматически. Выполнение операций в системе «Интернет-банкинг» без смены стандартного пароля невозможно;
7) целостность передаваемой информации обеспечивается хешированием каждого SSL пакета;
8) подлинность информации обеспечивается применением Электронно-цифровой подписи;
9) для регистрации Клиента в качестве Пользователя системы «Интернет-банкинг» требуется наличие у Клиента открытого текущего счета в Банке, логина, пароля и устройства e-Token PRO 72k Java для входа в систему «Интернет-банкинг» с Регистрационным свидетельством Электронно-цифровой подписи, зарегистрированным в уполномоченном Удостоверяющем центре, а именно в Казахстанском центре межбанковских расчетов (КЦМР);
10) при осуществлении первого входа в систему «Интернет-банкинг», неперсонифицированным паролем, полученным при регистрации в Банке, в защищенном Пин-конверте, происходит обязательная смена пароля. Требования к паролю в целях безопасности регламентированы следующим образом:

- если компьютер после входа Клиентом/Пользователем в систему «Интернет-банкинг» остается бездействующим более 10 (десяти) минут, системой «Интернет-банкинг» осуществляется автоматический выход из системы «Интернет-банкинг» и завершение сессии;
- проверка подлинности запроса Клиента о получении электронной банковской услуги через систему «Интернет-банкинг» осуществляется Банком автоматически посредством запроса Электронно-цифровой подписи. При этом каждое действие Клиента в системе «Интернет-банкинг», требует подтверждения, посредством Электронно-цифровой подписи, хранящейся на защищенном носителе Электронно-цифровой подписи – e-Token PRO 72K (Java), при этом Клиенту, потребуется вручную вводить пароль для доступа к ключевому контейнеру Электронно-цифровой подписи, тем самым подтверждая валидность операций, что защищает Клиента от мошеннических действий злоумышленников и киберпреступников.

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

1) при входе в систему «Интернет-банкинг» вводить только имя Пользователя, логин и пароль. Никакой другой информации Банк не запрашивает;
2) использовать отдельный компьютер с ограниченным физическим доступом, исключительно для работы в системе «Интернет-банкинг», другие действия на этом компьютере осуществляться не должны, а именно, такие как работа с другими программами, электронной почтой, посещения сайтов в Интернете;
3) осуществлять безопасное хранение Комплекта ключей только на съемном носителе (USB Flash - eToken PRO 72k

екінші тұлғаларға (Банктің және Клиенттің қызметкерлерін немесе олардың туыстарын қоса алғанда) беруді болдырмау шартымен жүзеге асыру қажет. USB eToken жұмыс орнында орнатуға тек «Интернет-банкинг» жүйесімен жұмыс істеу уақытына ғана жұмыс орнында беріледі;

4) «Интернет-банкинг» жүйесінде жұмыс кезінде бірнеше кілтті пайдалану жағдайында (бірінші және екінші қолтаңба) бұл кілттерді бір USB eToken-ге тасымалдамауға, сондай-ақ компьютерге түрлі USB eToken (кілт тасымалдағыштар) бір уақытта қоспауға;
5) «Интернет-банкинг» жүйесінде жұмыс істеуге арналған жеке логинді және арнайы қалыптастырылған кілтсөздердің кез келгенін екінші тұлғаларға (Банктің және Клиенттердің қызметкерлерін немесе олардың туыстарын қоса алғанда) жариялауды болдырмауды қамтамасыз етуге;
6) түрлі лицензиясыз, бөгде, күмән тудыратын, сондай-ақ зиянкес бағдарламалардың болуына тексерілмеген бағдарламалық қамсыздандыруды пайдалануды болдырмауды қамтамасыз етуге;
7) лицензиялы, уақытылы жаңартылатын вирусқа қарсы бағдарламалық қамсыздандыруды міндетті пайдалануды қамтамасыз етуге. Вирустардың әрекеті Пайдаланушының сәйкестендіру ақпаратын ұстап алу және оны алаяқтарға беруге бағытталуы тиіс;
8) онда анықталған кемшіліктерді жою мақсатында өндіруші компания ұсынатын, қазіргі заманға сай автоматты жаңартылумен, өз компьютерінің қазіргі заманға сәйкес операциондық жүйелерді пайдалануды қамтамасыз етуге. Өз компьютеріңіздің операциондық жүйесі мен браузерін тұрақты жаңартуды (патч) жүргізуге, бұл қауіпсіздік деңгейін айтарлықтай арттырады;
9) компьютерге вирустардың болуына тексерілмеген бөлінетін ақпарат тасымалдағыштарды қоспауға;
10) қосымша қауіпсіздікті қамтамасыз ету мақсатында Пайдаланушы кілтсөзді енгізу кезінде енгізілетін белгілерді ұстап алу мүмкіндігін жою үшін «Виртуальді клавиатураны» пайдалана алады;
11) кілтсөзде өз атын, туылған күнін пайдалануға болмайды, тек сандар немесе қарапайым сөздер, кілтсөздің ұзындығы 8 (сегіз) белгіден кем болмауы тиіс. кілтсөзде бас әріптерді, сандар мен арнайы белгілерді пайдалануға тырысу қажет;
12) кілтсөзді міндетті ауыстыру арасындағы әрекет ету мерзімі 30 (отыз) күнтізбелік күнді құрайды;
13) Интернет-қосылуды орнататын бағдарламаларды, компьютерде немесе өзге де электронды ақпарат тасымалдағыштарда мәтіндік файлдарда кілтсөз(дер)ді сақтамау қажет, себебі бұл кезде оны ұрлау және жариялау қаупі туындайды;
14) жұмыс аяқталғаннан кейін «Шығу» батырмасының көмегімен «Интернет-банкинг» жүйесінің терезесін жабу қажет және компьютерді «Интернет-банкинг» жүйесіндегі ағымдағы сессиясымен қараусыз қалдыруға болмайды;
15) ЭСҚ кілттерін ауыстыруды олардың әрекет ету мерзімі аяқталғанға дейін жүргізу қажет. Сонымен қатар ЭСҚ кілттерін ауыстыруды «Интернет-банкинг» жүйесіне қолжетімділік болған тұлғалар, сондай-ақ ЭСҚ кілттерін алуға сенімхатқа қол қою құқығы бар жетекшілер жұмыстан босатылған және/немесе ауысқан және оларға күмән туындаған барлық жағдайларда жүргізу қажет;
16) компьютердің жұмысында жаңылыстар немесе «Интернет-банкинг» жүйесімен жұмыс істеу кезінде немесе сеанс аяқталғаннан кейін оның бұзылып қалуы (операциондық жүйені жүктеуге байланысты қиындықтар,

Java), использование которого осуществлять при условии недопущения передачи вторым лицам (включая работников Банка и работников Клиента или их родственников). Установка USB eToken на рабочее место допускается только непосредственно на время работы с системой «Интернет-банкинг»;
4) в случае использования нескольких ключей при работе в системе «Интернет-банкинг» (первой и второй подписи) не переносить эти ключи на один USB eToken, а также не подключать одновременно различные USB eToken **(**ключевые носители) к компьютеру;
5) обеспечивать недопущение разглашения личного логина и любого из паролей, сформированных для работы в системе «Интернет-банкинг» вторым лицам (включая работников Банка и работников Клиента или их родственников);

6) обеспечивать недопущение использования различного нелицензионного, стороннего, сомнительного, а также не проверенного программного обеспечения на наличие вредоносных программ;
7) обеспечивать обязательное использование лицензионного, своевременно обновляющегося антивирусного программного обеспечения. Действие вирусов может быть направлено на перехват идентификационной информации Пользователя и передаче ее злоумышленникам;
8) обеспечивать использование современных операционных систем своего компьютера, с автоматическим своевременным обновлением, рекомендуемым компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления (патчи) операционной системы и браузера Вашего компьютера, что значительно повышает уровень безопасности;
9) не подключать к компьютеру не проверенные на наличие вирусов отчуждаемые носители информации;
10) в целях обеспечения дополнительной безопасности Пользователь при вводе пароля может использовать «Виртуальную клавиатуру», исключая тем самым возможность перехвата вводимых символов;
11) не использовать в пароле свое имя, дату рождения, только цифры или простые слова, длина пароля должна быть не менее 8 (восьми) символов. Необходимо стараться применять в сочетании заглавные буквы, цифры и специальные символы;
12) срок действия между обязательной смены пароля составляет 30 (тридцать) календарных дней;
13) никогда не сохранять пароль (-и) в программах, устанавливающих Интернет-соединение, в текстовых файлах на компьютере либо на других электронных носителях информации, так как при этом существует риск его кражи и компрометации;
14) после окончания работы необходимо закрывать окно системы «Интернет-банкинг» с помощью кнопки «Выход» и никогда не оставлять компьютер с текущей сессией в системе «Интернет-банкинг» без присмотра;
15) производить замену ключей ЭЦП до истечения срока их действия. Кроме того, необходимо проводить замену ключей ЭЦП во всех случаях увольнения и\или смены лиц, имеющих доступ к системе «Интернет-банкинг», а также руководителей с правом подписи доверенностей на получение ключей ЭЦП, и в случае подозрения на их компрометацию;

16) в случае сбоев в работе компьютера или его поломки во время работы с системой «Интернет-банкинг» или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.), следует немедленно извлечь

қатаң дискінің істен шығуы және т.б.) жағдайында дереу кілттерді шығарып, компьютерді сөндіріп, сондай-ақ Банкке жүгініп, Сіздің атыңыздан рұқсат етілмеген операциялардың жүргізілмегендігіне көз жеткізу қажет;
17) «Интернет-банкинг» жүйесінің қызмет етуінің дұрыстығына кез келген күмән туындаған кезде дереу Банкке жүгіну қажет;
18) «Интернет-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. Кілтсөзді 3 (үш) рет қате енгізгеннен кейін Банк Пайдаланушының кілтсөзін 30 (отыз) минут мерзіміне шектеуді жүзеге асырады. Егер аталған жағдай жарты сағат ішінде тағы қайталанатын болса, «Интернет-банкинг» жүйесі автоматты түрде Қауіпсіздік басқармасының қызметкерлеріне пошталық хабарлама қалыптастырады. Олар шаралар қабылдайды және қажет болған жағдайда Пайдаланушыны «Интернет-банкинг» жүйесінде шектейді. Егер Пайдаланушы қандай да бір себептермен өз кілтсөзін есіне түсіре алмаса, ол Пин-конверттегі жеке тұлғаландырылмаған кілтсөзді алу үшін Банктің бөлімшесіне хабарласып, «Интернет-банкинг» жүйесіне кілтсөзді ауыстырумен кіруді жүзеге асыруы тиіс.
5. Пайдаланушының қалауы бойынша «Интернет-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.
6. Даулы жағдайларды талдауды жүзеге асыру үшін Банк Клиенттің Пайдаланушысы және Банк жолдаған/қабылдаған барлық Электронды құжаттарды мұрағаттауды қамтамасыз етеді. Клиент Пайдаланушыларының «Интернет-банкинг» жүйесіндегі барлық әрекеттері Интернет-банкинг» жүйесімен қалыптастырылған электронды журналдарға жазылады.
7. 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 Банкпен электронды банктік қызметтерді ұсыну кезінде туындайтын 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
8. Осы Процедуралардың 7 тармағында көрсетілген рұқсат етілмеген әрекеттер тундаған жағдайда Банк «Интернет-банкинг» жүйесінің көмегімен электронды банктік қызметтерді ұсынуды уақытша тоқтатуға құқылы.

ключи и выключить компьютер, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции;

17) при возникновении любых сомнений в правильности функционирования системы «Интернет-банкинг» незамедлительно обратиться в Банк;
18) в случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении системы «Интернет-банкинг» отложите совершение операций и обратитесь в Группу поддержки пользователей Банка.

4. После 3 (трех) попыток неверного ввода пароля, Банк автоматически осуществляет блокирование пароля Пользователя сроком на 30 (тридцать) минут. Если данное событие происходит повторно в течение полутора часов система «Интернет-банкинг» автоматически формирует почтовое сообщение сотрудникам Управления безопасности, которые принимают меры и при необходимости блокируют Пользователя в системе «Интернет-банкинг». Если Пользователь по каким-либо причинам не может вспомнить свой пароль, то ему необходимо обратиться в подразделение Банка для получения неперсонифицированного пароля в Пин-конверте и осуществить вход в систему «Интернет-банкинг» с последующей сменой пароля.
5. По желанию Пользователя возможно предусмотреть дополнительные меры по реализации защиты и безопасности информации при работе в системе «Интернет-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.

6. Для осуществления анализа спорных ситуаций, Банком обеспечивается ведения архива всех отосланных/принятых Пользователем Клиента и Банком Электронных документов. Все действия Пользователей Клиента в системе «Интернет-банкинг» записываются в электронные журналы, сформированные системой «Интернет-банкинг».
7. 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, возникающих при предоставлении Банком электронных банковских услуг, 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.
8. В случае возникновения несанкционированных действий, указанных в пункте 7 настоящих Процедур, Банк вправе приостановить предоставление электронных банковских услуг посредством системы «Интернет-банкинга».