№8 өтініш-оферта
ҚБҚ Пайдаланушыларын қосуға /өзгертуге /алып тастауға өтініш
/Заявление на подключение /изменение /отключение Пользователей ДБО
(қажеттісін таңдап, толтыру)
/(необходимое выбрать и заполнить)

г._____ қ.

Клиенттің толық атауы /Полное наименование Клиента
_____
орналасқан мекенжайы: /расположенного по адресу _____ филиалда (негізгі) қызмет көрсетіледі./обслуживающийся в Филиале(основной)
Электрондық мекенжайы /Электронный адрес_____телефон___**+7 (__ __ __)__ __ __ __ __ __ __**

☐ **Жаңа ҚБҚ пайдаланушысын қосу/Подключить нового пользователя ДБО**

ТАӘ /ФИО	**Жеке басын куәландыратын құжаттың нөмірі /Номер документа удостоверяющмй личность**	**Электрондық мекенжайы /Электронный адрес**	**Ұялы телефон нөмірі /Номер мобильного телефона**	**Қол қою құқығы /Право подписи**	**Тіркеу куәлігінің сериялық нөмірі (ЭЦҚ қолдану кезінде) /Серийный номер регистрационного свидетельства (при использовании ЭЦП)**	**ОТР құрылғысының сериялық нөмірі (қолдану кезінде) /Серийный номер ОТР устройства (при использовании)**
			7(_ _ _)_ _ _ _ _ _ _			
			7(_ _ _)_ _ _ _ _ _ _			
			7(_ _ _)_ _ _ _ _ _ _			
			7(_ _ _)_ _ _ _ _ _ _			
			7(_ _ _)_ _ _ _ _ _ _			

ҚБҚ пайдаланушыны «Кеңейтілген құқықтар» қызметіне қосу (қажет болған жағдайда)/Дополнительно подключить пользователя ДБО к услуге «Расширенные права» (при необходимости)

ТАӘ /ФИО	Қол қою құқығы /Право подписи	Шот/барлық шоттар /Счет/Все счета	Құжаттың ең көп сомасы (соманы көрсету)/Максимальная сумма документа (указать сумму)

☐ **Бұрын қосылған пайдаланушыға өзгерістер енгізу (қажеттісін толтыру)/Внести изменения к ранее подключенному пользователю (нужное заполнить)**

ТАӘ /ФИО	Электрондық мекенжайы /Электронный адрес	Ұялы телефон нөмірі /Номер мобильного телефона	Қол қою құқығы /Право подписи	Тіркеу куәлігінің сериялық нөмірі /Серийный номер регистрационного свидетельства	OTP құрылғысының сериялық нөмірі /Серийный номер OTP устройства
		7(_ _ _)_ _ _ _ _ _ _			
		7(_ _ _)_ _ _ _ _ _ _			

ҚБҚ-дағы Клиенттің Жұмыс орнының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі талаптар мен ұсыныстар

1. Жалпы ережелер

1.1. «ҚБҚ WEB – интерфейсінің ақпараттық қауіпсіздігі кешендік (ұйымдық, әкімшілік, техникалық және бағдарламалық) шаралармен және құралдармен қамтамасыз етілуі тиіс.

1.2. Ақпарат қауіпсіздігін қамтамасыз ету мақсатында:

- Клиенттің басшылығы әрбір пайдаланушыға нақты функциялар мен өкілеттіктерді бекітіп берумен ҚБҚ-дағы жұмысқа жіберілетін пайдаланушылар мен әкімшілердің тізімін бекітуі тиіс;
- Клиенттің басшылығы ҚБҚ қауіпсіздігін қамтамасыз етуге жауапты қызметкер тағайындауы тиіс
- ҚБҚ пайдаланушылар ҚБҚ құжаттамасы мен осы әдістемелік нұсқаулықтарға сәйкес пайдалану ережелерімен таныстырылуы тиіс
- ҚБҚ-ға кіру деректері мен басты ақпарат тасымалдаушылары санкцияланбаған қол жеткізуден (СҚЖ)

1.3. Жабық ЭСҚ кілттерін сақтауға арналған USB-токен қорғалған тасымалдаушысын пайдалану құпия кілттерді көшірмелеуден қорғайды, бірақ баяндалған талаптарды орындаудан босатпайды .

1.4. Өз компьютерінде қауіпсіз ортаны қамтамасыз ету үшін Клиент:

- Электронды хаттарды сүзгілеу үшін .exe .cmd .bat .dll ықтимал қауіпті қосымшаларды оқшаулайтын БЖ орнатуы тиіс;
- Туындайтын қателіктерді, пайдаланушылардың кіруін және бағдарламалардың іске қосылуын тіркейтін жүйелік оқиғалар аудитін іс қосуы, дамыл-дамыл журналды тексеріп, қателіктерді елеп отыруы тиіс;
- Компьютердің вируспен зақымданғаны жөнінде күдік туындаған жағдайда жұмыс станцияларын тексеруі тиіс

2. ҚБҚ-ны санкцияланбаған қол жеткізуден (СҚЖ) қорғау жөніндегі талаптар

2.1. ҚБҚ-ға кіру деректері мен басты ақпарат тасымалдаушыларын келесі мүмкіндіктерді болдырмау мақсатында санкцияланбаған қол жеткізуден қорғауй:

- ҚБҚ құралдары орнатылған компьютерлерде компьютерлік вирустар мен ҚБҚ БЖ бүлдіруге, жұмыс қабілеттілігін бұзуға немесе түрлендіруге немесе ақпаратты қолға түсіруге бағытталған бағдарламалардың пайда болуы;
- ҚБҚ техникалық және бағдарламалық құралдарына, сондай-ақ олардың құрамына санкцияланбаған өзгерістердің енгізілуі ;
- Электрондық құжатқа (ЭҚ) санкцияланбаған өзгерістердің енгізілуі;

2.2. ҚБҚ-ны жеке бөлінген дербес компьютерде пайдалану ұсынылады. Бұл компьютер міндетті түрде желілік шабуылдардан қорғаныспен және вирусқа қарсы қорғаныспен қамтамасыз етілуі тиіс.

2.3. ҚБҚ-ны санкцияланбаған қол жеткізуден қорғау мақсатында компьютерлерге санкцияланбаған қол жеткізуден қорғаудың бағдарламалық-аппараттық кешенін орнату ұсынылады.

2.4. СҚЖ-дан қорғаныс кешенінің көмегімен ҚБҚ тұтастығын бақылауды қамтамасыз ететін және пайдаланушылардың жұмысын оларға берілетін мүмкіндіктер мен өкілеттіктер аясында ғана мүмкін жасайтын функционалды тұйық ортаны қалыптастыру ұсынылады. Жүйелік және тиелетін файлдар, сондай-ақ ақпаратты криптографиялық қорғау құралдарының (АКҚҚ) жұмысымен байланысты файлдар қорғалуы тиіс

2.5. ҚБҚ-мен жұмыс үшін пайдаланылатын дербес компьютерде БЖ әзірлеу құралдары мен ретке келтіргіштер орнатылмауы тиіс.

2.6. ҚБҚ-мен жұмыс үшін пайдаланылатын дербес компьютерлердің жүйелік блоктарын санкцияланбаған ашуға кедергі келтіретін шаралар қабылдау қажет.

2.7. СҚЖ-дан қорғаудың бағдарламалық-аппараттық құралдары әкімшісінің құқықтары ҚБҚ қауіпсіздігін қамтамасыз ету үшін жауапты қызметкерге беріледі. Бұл қызметкер әрбір ЭҚ қабылдау/тапсыруға, ЭҚ құрастыруға және басты ақпарат тасымалдаушыларын//ОТР құрылғыларын пайдалануға қатысатын ҚБҚ пайдаланушысы үшін қол жеткізу құқықтарын қалыптастырады.

2.8. Компьютерлерді СҚЖ-дан қорғау үшін сондай-ақ операциялық жүйенің штаттық мүмкіндіктері пайдаланылуы тиіс.

3. Басты ақпарат тасымалдаушыларын сақтауды және пайдалануды ұйымдастыру жөніндегі талаптар

3.1. Клиент жабық криптографиялық кілттерді өздігінен түрлендіруі тиіс.

3.2. Басты ақпарат тасымалдаушылары/ОТР құрылғылары тек олар тиесілі тұлғаларда ғана сақталуы тиіс.

3.3. Құпия кілттері бар басты ақпарат тасымалдаушыларын сақтау және пайдалану тәртібі оларға санкцияланбаған қол жеткізу мүмкіндігін болдырмауы тиіс.

3.4. Басты ақпарат тасымалдаушыларына/ОТР құрылғыларына қолжетімділігі бар тұлғалардың тізімі бекітіп берілген функциялары мен өкілеттіктеріне сәйкес Клиент басшылығының бұйрығымен немесе өкімімен анықталады.

3.5. Басты ақпарат тасымалдаушыларымен/ОТР құрылғыларымен жұмыс жасау кезінде бөтен тұлғалардың оларға қол жеткізуін болдырмау қажет.

3.6. Басты ақпарат тасымалдаушыларын/ОТР құрылғыларын сақтау үшін сенімді металл сейфтері орнатылуы тиіс.

3.7. Жұмыс күні аяқталғанда, сондай-ақ Банкпен байланыс жасау сеанстарынан тыс уақытта басты ақпарат тасымалдаушылары/ОТР құрылғылары сейфте сақталуы тиіс.

3.8. Басты ақпарат тасымалдаушыларын/ОТР құрылғыларын басқа құжаттармен олардан бөлек және бөтен тұлғалардың оларға жасырын қол жеткізу мүмкіндігін болдырмайтындай орамада бір сейфте сақтауға рұқсат беріледі.

3.9. Келесі аталғандарға рұқсат берілмейді:

- басты ақпарат тасымалдаушыларын/ОТР құрылғыларын олармен жұмыс жасауға жіберілмеген тұлғаларға беруге:
- құпия кілттерді дисплейге немесе принтерден шығаруға;
- басты ақпарат тасымалдаушысын ҚБҚ-ның жұмыс істеуі қарастырылмаған режимдерде компьютердің санауыш құрылғысына, сондай-ақ басқа компьютерлердің санауы құрылғыларына салуға;
- басты ақпарат тасымалдаушысын жұмыс орнында қараусыз қалдыруға;
- басты ақпарат тасымалдаушысына бөтен файлдарды жазуға рұқсат берілмейді.

4. ҚБҚ-ны санкцияланбаған қол жеткізуден қорғау жөніндегі практикалық ұсыныстар

4.1. ҚБҚ-ға желілік қолжетімділікті (оның ішінде желіге қашықтан кіруді) жергілікті желінің басқа жұмыс станцияларынан және әсіресе сыртқы желілерден толығымен оқшаулау ұсынылады.

4.2. ҚБҚ пайдаланушыларын Интернет желісін пайдаланудан шектеу ұсынылады. Міндетті тәртіппен вирусқа қарсы бағдарламалық жасақтаманы орнату және ұдайы жаңартып отыру қажет.

4.3. Осы есептік жазбалар бойынша компьютерде бағдарламалық жасақтаманы орнату мүмкіндігін шектеу мақсатында жүйемен жұмыс жасайтын ҚБҚ пайдаланушыларына әкімші құқығы берілмеуі тиіс. Компьютердің файлдық ресурстарына, әсіресе жазбаға қол жеткізу минималды қажетті құқықтармен шектелуі тиіс. Пайдаланушылар тек қана оларға рұқсат етілген қосымшаларды ғана іске қосуы тиіс.

4.4. ҚБҚ пайдаланушылары міндетті түрде негізгі қауіпсіздік талаптарын сақтау мәселелері бойынша, әсіресе вирусқа қарсы бағдарламаларды пайдалану мәселелері бойынша нұсқаулықтар алуы тиіс.

4.5. Жергілікті (немесе домендік) саясаттармен компьютерде операциялық жүйеге кіру мүмкіндігі бар пайдаланушылардың тізімін шектеу ұсынылады.

4.6. Сыртқы электрондық поштаны (Интернет желісінен) қабылдауды шектеу немесе толығымен бас тарту ұсынылады. Алынатын пошта міндетті тәртіппен вирусқа қарсы құралдармен тексерілуі тиіс.

4.7. Компьютерде тек бір ғана НҚ орнатылуы тиіс.

4.8. Компьютердің BIOS құралдарымен қатты дискте орнатылғаннан өзгеше операциялық жүйені тиеу мүмкіндігін болдырмау, яғни дискеталардан, CD/DVD жетектерден және т.б. тиеуді өшіріп тастау қажет.

4.9. BIOS баптауларын өзгертуге қол жеткізу парольмен қорғалуы тиіс.

4.10. Операциялық жүйенің пайдаланушыларына парольдер тағайындалуы тиіс. Пароль ұзындығы кемінде алты символдан құралуы тиіс. Парольдің қолданылу мерзімі шектелуі тиіс/Пользователям операционной системы должны быть назначены пароли.

4.11. Санкцияланбаған ашуды болдырмау үшін компьютердің жүйелік блогына сүргі салу ұсынылады.

4.12. Компьютерге қолжетімділікті шектеу, пайдаланылатын БЖ тұтастығын тексеру үшін компьютерге СҚЖ-дан қорғаудың бағдарламалық-аппараттық кешенін («Аккорд», «Соболь» және т.с.с.) күйге келтіру ұсынылады.

4.13. Кілттерді тек жеке алмалы ақпарат тасымалдаушыларында сақтау және оларды басқа мақсаттар үшін пайдаланбау ұсынылады. Тасымалдаушыны тек ҚБҚ-мен жұмыс кезінде қол қою операцияларын орындау немесе Банкпен алмасу сәттерінде ғана дискжетекке салып, операция аяқталғанда тасымалдаушыны шығарып алу қажет. Басты ақпаратты бар тасымалдаушыларды басқа компьютерлерге қоспаңыз

4.14. Компьютерге сыртқы құрылғыларды, оның ішінде өндірістік қажеттілікпен қарастырылмаған ақпарат тасымалдаушыларын қосуға болмайды.

5. АКҚҚ есепке алу жөніндегі жалпы талаптар

5.1. АКҚҚ және басты тасымалдаушыларды//оларға ОТР құрылғыларды даналап есепке алу журналын жүргізу қажет.

5.2. Құпия кілттерді жою олар орналасқан кілттік тасымалдаушыны түбегейлі жою арқылы немесе кілттік тасымалдаушыны бүлдірмей өшіру арқылы жүргізіледі.

5.3. Кілттерді жоспарлы ауыстырғаннан кейін немесе кілттер сенімсіздендірілгеннен кейін АКҚҚ пайдаланушылар істен шығарылған ЭСҚ мен құпия шифрлеу кілттерін олар істен шығарылған сәттен кейін 10 (он) жұмыс күнінен кешіктірмей барлық магнитті тасымалдаушылардан жояды. Кілттердің жойылуы туралы Есепке алу журналында тиісті жазба жасалады.

Требования и рекомендации по обеспечению информационной безопасности Рабочего места Клиента в ДБО

1. Общие положения

1.1. «Информационная безопасность WEB – интерфейса ДБО должна обеспечиваться комплексными (организационными, административными, техническими и программными) мерами и средствами.

1.2. С целью обеспечения безопасности информации:

- руководством Клиента должен быть утвержден список пользователей и администраторов, допускаемых к работе в ДБО, с закреплением за каждым пользователем конкретных функций и полномочий;
- руководством Клиента должен быть назначен работник ответственный за обеспечение безопасности ДБО;
- пользователи ДБО должны быть ознакомлены с правилами эксплуатации согласно документации, к ДБО и с настоящими методическими рекомендациями;
- данные для входа в ДБО и носители ключевой информации должны быть защищены от несанкционированного доступа (НСД).

1.3. Использование защищенного носителя USB-токен для хранения закрытых ключей ЭЦП защищает секретные ключи от копирования, но не освобождает от выполнения изложенных требований.

1.4. Для обеспечения безопасной среды на своем компьютере Клиентну надлежит:

- Установить ПО для фильтрации электронных писем, блокирующее потенциально опасные вложения .exe .cmd .bat .dll;
- Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки;
- Проверять рабочие станции в случае подозрения заражения компьютера вирусом.

2. Требования по защите ДБО от несанкционированного доступа (НСД)

2.1. Защита данных для входа в ДБО и носителей ключевой информации от несанкционированного доступа осуществляется с целью исключения возможностей:

- появления в компьютерах, на которых установлены средства ДБО, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию ПО ДБО, либо на перехват информации;
- внесения несанкционированных изменений в технические и программные средства ДБО, а также в их состав;
- внесения несанкционированных изменений в Электронный документ (ЭД).

2.2. ДБО рекомендуется использовать на отдельном выделенном персональном компьютере. Должна быть обеспечена в обязательном порядке защита данного компьютера от сетевых атак и антивирусная защита.

2.3. В целях защиты ДБО от несанкционированного доступа на компьютеры рекомендуется установить программно-аппаратный комплекс защиты от несанкционированного доступа.

2.4. Рекомендуется сформировать с помощью комплекса защиты от НСД функционально замкнутую среду, обеспечивающую контроль целостности ДБО и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий. Защите подлежат системные и загрузочные файлы, а также файлы, связанные с работой средств криптографической защиты информации (СКЗИ).

2.5. На персональном комьпютере, используемом для работы с ДБО не должны устанавливаться средства разработки ПО и отладчики.

2.6. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков персональных компьютеров, используемых для работы с ДБО.
2.7. Права администратора программно-аппаратных средств защиты от НСД предоставляются работнику, ответственному за обеспечение безопасности ДБО. Указанный работник формирует права доступа для каждого пользователя ДБО, участвующего в приеме-передаче ЭД, формировании ЭД и использовании носителей ключевой информации//OTP устройства.
2.8. Для защиты компьютеров от НСД также должны использоваться штатные возможности операционной системы.

3. Требования по организации хранения и использования носителей ключевой информации

3.1. Клиент должен самостоятельно генерировать закрытые криптографические ключи.
3.2. Носители ключевой информации/OTP устройства должны храниться только у тех лиц, которым они принадлежат.
3.3. Порядок хранения и использования носителей ключевой информации с секретными ключами должен исключать возможность несанкционированного доступа к ним.
3.4. Список лиц, имеющих доступ к носителям ключевой информации/OTP устройства, определяется приказом или распоряжением руководства Клиента, согласно закрепленными за ними функциями и полномочиями.
3.5. Во время работы с носителями ключевой информации/OTP устройства доступ к ним посторонних лиц должен быть исключен.
3.6. Для хранения носителей ключевой информации/OTP устройства должны устанавливаться надежные металлические сейфы.
3.7. По окончании рабочего дня, а также вне времени сеансов связи с Банком носители ключевой информации//OTP устройства должны храниться в сейфе.
3.8. Хранение носителей ключевой информации/OTP устройства допускается в одном сейфе с другими документами, отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.
3.9. Не разрешается:

- передавать носители ключевой информации/OTP устройства лицам, к ним не допущенным;
- выводить секретные ключи на дисплей или принтер;
- вставлять носитель ключевой информации в считывающее устройство компьютера в режимах, не предусмотренных функционированием ДБО, а также в считывающие устройства других компьютеров;
- оставлять носитель ключевой информации без присмотра на рабочем месте;
- записывать на носитель ключевой информации посторонние файлы.

4. Практические рекомендации по защите ДБО от несанкционированного доступа

4.1. Рекомендуется полностью блокировать сетевой доступ к ДБО (в том числе и удаленный вход в сеть) с других рабочих станций локальной сети и в особенности из внешних сетей.
4.2. Рекомендуется ограничить использование сети Интернет пользователями ДБО. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное программное обеспечение.
4.3. Пользователи ДБО, работающие с системой не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на компьютере. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.
4.4. Пользователи ДБО, должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований безопасности, и в особенности по вопросам использования антивирусных программ.
4.5. Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

4.6. Рекомендуется ограничить или полностью отказаться от приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.
4.7. На компьютере должна быть установлена только одна ОС.
4.8. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. отключить загрузку с дискет, CD/DVD приводов и т.п.
4.9. Доступ к изменению настроек BIOS должен быть защищен паролем.
4.10. Пользователям операционной системы должны быть назначены пароли. Длина паролей должна составлять не менее шести символов. Срок действия паролей должен быть ограничен.
4.11. Рекомендуется опечатать системный блок компьютера для предотвращения его несанкционированного вскрытия.
4.12. Для ограничения доступа к компьютеру, проверки целостности используемого ПО, рекомендуется установить и настроить на компьютер программно-аппаратный комплекс защиты от НСД («Аккорд», «Соболь» и т.п.).
4.13. Рекомендуется хранить ключи только на отдельных съемных носителях информации, и не использовать их для других целей. Вставлять носители в дисководы только непосредственно при работе с ДБО в моменты выполнения операций подписания или обмена с Банком, по завершении операции необходимо извлечь данный носитель. Не подключайте носители с ключевой информаций к другим компьютерам.
4.14. Не рекомендуется подключать к компьютеру внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

5. Общие требования по учету СКЗИ

5.1. Необходимо вести Журнал поэкземплярного учета СКЗИ и ключевых носителей//ОТР устройства к ним.
5.2. Уничтожение секретных ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания без повреждения ключевого носителя.
5.3. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭЦП со всех магнитных носителей не позднее чем через 10 (десять) дней после момента вывода ключей из действия. Об уничтожении ключей делается соответствующая запись в Журнале учета.

☐ **ҚБҚ пайдаланушысын алып тастау/оқшаулау. Криптопрофильді оқшаулау, тіркеу куәлігін кері қайтарып алу (бар болса) және ОТР құрылғыны шешіп жіберу (бар болса)/Отключить/блокировать пользователя ДБО. Заблокировать криптопрофиль, отозвать регистрационное свидетельства (при наличии) и отвязать ОТР устройства (при наличии)**

ТАӘ /ФИО	Себебі /Причина	Қол қою құқығы /Право подписи	№ ОТР

«Клиент»:
Т.А.Ә. /Ф.И.О _____
Лауазымы /Должность _____
Қолы /Подпись _____
М.О /М.П.

Күні /Дата____/_____/_____ Уақыты /Время_____ сағ /ч/_____мин

Банктің белгілері/Отметки Банка:

Өтінішті қабылдаған /Заявление принял _____ _____

Қолы/Подпись *Т.А.Ә./Ф.И.О.* М.О./М.Ш.

Фронт – офис бөлімшесінің басшысы:/Руководитель подразделения фронт – офиса: _____

20___ жылғы «___» _____
/«____» _____20__ г.