«First Heartland Bank» АҚ -да
« Internet Banking » Жүйесі бойынша
Клиенттерге қашықтықтан банктік
қызмет көрсету шартының Типтік
талаптарына № 2 Қосымша

Appendix 2
To Typical conditions of Online Banking
Agreement on
the ”Internet Banking” System
in JSC «First Heartland Bank»

Приложение №2 к Типовым условиям
Договора дистанционного
банковского обслуживания Клиентов
по Системе «Internet Banking» в АО
«First Heartland Bank»

**Требования и рекомендации по обеспечению информационной безопасности Рабочего места Клиента в Системе/**
**Жүйедегі Клиенттің Жұмыс орнын ақпараттық қауіпсіздікпен қамту жөніндегі талаптар мен ұсыныстар /**
**Requirements and Recommendations on Ensuring Information Security of Client's Work Place in the System**

| | | |
|---|---|---|
| **1.Жалпы ережелер**<br>1.1.Жүйе Web–интерфейсінің ақпараттық қауіпсіздігі кешенді (ұйымдастырушылық, әкімшілік, техникалық және бағдарламалық) шаралар мен құралдарды пайдаланумен қамтамасыз етілуі тиіс.<br>1.2.Ақпараттық қауіпсіздікті қамтамасыз ету мақсатында:<br>• КЛИЕНТТІҢ басшылығы әрбір пайдаланушыға бекітілген нақтылы міндеттер мен өкілеттіктерді бекіте отырып, Жүйеде жұмыс істеуге рұқсат етілетін пайдаланушылар мен әкімшілердің тізімін белгілеуі тиіс;<br>• КЛИЕНТТІҢ басшылығы Жүйе қауіпсіздігін қамтамасыз етуге жауапты қызметкерді тағайындауы тиіс;<br>• Жүйе пайдаланушылары Жүйедегі құжаттамаларға сәйкес пайдалану ережелерін оқытудан өтуі және осы әдістемелік ұсыныстармен таныс болуы тиіс;<br>• Жүйеге кіруге арнаған деректер мен ақпараттық кілттік тасымалдаушылар санкциясыз қол жетімділіктен (СҚЖ) қорғалуы тиіс.<br>1.3. ЭСҚ жабық (құпия) кілттерін сқтау үшін Кілттің тасығышын пайдалану құпия кілтті көшірмелеуден қорғайды, бірақ мазмұндалған талаптарды орындаудан босатпайды.<br>1.4. Клиенттің компьютерінде орындаудың қауіпсіздік ортасын қамтамасыз ету үшін Клиент:<br>• Вирусқа қарсы бағдарламалық құралды орнатыңыз және оны үнемі жаңартып отыру;<br>• *.exe; *.cmd; *.bat; *.dll; *.vbs әлеуетті қауіпсіз салымдарды оқшауландыратын, электронды хаттарды сүзу үшін БҚ орнатуы;.<br>• Пайдаланушылардың енуін және бағдарламалардың қосылуын, қателердің туындауын тіркейтін оқиғалардың жүйелі аудитін енгізуі, журналды кезеңімен қарауы және қателерге әрекет жасауы;<br>• Компьютердің вирус жұқтыруына күмән туған жағдайда вирусқа қарсы бағдарламамем жұмыс станцияларын тексеруі тиіс. | **1. General Provisions**<br>1.1. Information Security of System WEB–interface must be ensured with complex (organizational, administrative, technical and software) means and tools.<br>1.2. In order to ensure information security:<br>• The Client management must approve a list of users and administrators allowed to work within the System with indication of precise functions and powers of each user;<br>• The Client management must assign the employee in charge of the System security maintenance;<br>• The System users must be acquainted with service instructions according to documentation for the System and these methodological recommendations;<br>• The Data for System access and the Tokens must be protected from the unauthorized access.<br>1.3. Use of the Token (USB-token) for storage of privacy keys of DS protects privacy keys from copying, but does not release a user from fulfillment of these requirements.<br>1.4. In order to ensure secure environment at his computer Client shall:<br>• Install antivirus software and keep it updated regularly<br>• Install software for filtwering of electronic mails which will block potentially hazardous attachments like *.exe; *.cmd; *.bat; *.dll; *.vbs<br>• Initiate systemic audit of events registering all appearing errors, logging in of users and launch of programs; regularly review the log and respond to errors.<br>• Check working stations antivirus by software virus scan in case of suspecting viruses in computer. | **1. Общие положения**<br>1.1. «Информационная безопасность Web–интерфейса Системы должна обеспечиваться комплексными (организационными, административными, техническими и программными) мерами и средствами.<br>1.2. С целью обеспечения безопасности информации:<br>• руководством Клиента должен быть утвержден список пользователей и администраторов, допускаемых к работе в Системе, с закреплением за каждым пользователем конкретных функций и полномочий;<br>• руководством Клиента должен быть назначен сотрудник ответственный за обеспечение безопасности Системы;<br>• пользователи Системы должны быть ознакомлены с правилами эксплуатации согласно документации к Системе и с настоящими методическими рекомендациями;<br>• данные для входа в Систему и Носители ключевой информации должны быть защищены от несанкционированного доступа (НСД).<br>1.3. Использование защищенного Носителя ключевой информации (USB-токен) для хранения закрытых (секретных) ключей ЭЦП защищает секретные ключи от копирования, но не освобождает от выполнения изложенных требований.<br>1.4. Для обеспечения безопасной среды на своем ПК Клиенту надлежит:<br>• Установить антивирусное программное обеспечение и поддерживать его регулярное обновление.<br>• Установить программное обеспечение для фильтрации электронных писем, блокирующее потенциально опасные вложения с расширениями: *.exe; *.cmd; *.bat; *.dll; *.vbs<br>• Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.<br>• Проверять ПК антивирусунным программным обспечением на вирусы в случае подозрения заражения компьютера вирусом. |
| **2. Санкцияландырылмаған қатынаудан (СҚЖ) қорғау бойынша талаптар**<br>2.1. Жүйеге кірүге арналған деректерді және ақпараттың кілттің тасығыштарын санкциясыз қолжетімділіктен қорғау келесі мүмкіншілктерді болдырмау мақсатында жүзеге асырылады:<br>• Жүйе құралдарына бекітілген компьютерлерде Жүйенің БҚ бұзушылыққа, жаңарту немесе жұмысқа қабілеттілігін бұзуға немесе ақпаратты ұстап алуға бағытталған компьютерлік вирустар мен бағдарламалардың пайда | **2. Requirements on System protection from unauthorized access**<br>2.1. Protection of data used for System access and the Tokens from unauthorized access is performed in order to exclude the possibility of the following:<br>• Emergence at computers with System installed of computer viruses and programs aimed at destruction, disturbance of operability or modification of System software or aimed at information capturing;<br>• Introduction of unauthorized changes to technical and software means of System and into | **2. Требования по защите Системы от несанкционированного доступа (НСД)**<br>2.1. Защита данных для входа в Систему и Носителей ключевой информации от НСД осуществляется с целью исключения возможностей:<br>• появления в ПК, на которых установлены средства Системы, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения Системы, либо |

болуы;
- Жүйенің техникалық және бағдарламалық құралдарына, сондай-ақ олардың құрамына санкцияландырылмаған өзгерістерді енгізу;
- Электронды құжатқа (ЭҚ санкцияландырылмаған өзгертулерді енгізу.

2.2. Жүйені осы мақсат үшін арнайы бөлінген жеке, дербес компьютерге орнату ұсынылады. **Осы компьютер желілік шабуылдар мен вирусқа қарсы қорғаныспен міндетті түрде қамтамасыз етілуі тиіс.**

2.3. Жүйені санкцияландырылмаған қолжетімділіктен қорғау мақсатында компьютерлерде санкцияландырылмаған қол жетімділіктен қорғаудың бағдарламалық-аппараттық кешенін бекіту ұсынылады.

2.4.СҚҚ-дан қорғаныс кешені арқылы БҚ тұтастығын бақылауды қамтамасыз ететін және пайдаланушыларға оларға ұсынылған мүмкіндіктер мен өкілеттіктердің қатаң шеңберінде жұмыс істеуге рұқсат беретін функциональдық тұйықталған ортаны қалыптастыру ұсынылады. Жүйелік және жүктемелік файлдар, сондай-ақ ақпараттардың криптографиялық қорғаныс құралдарының (АКҚҚ) жұмысымен байланысты файлдар қорғалуы тиіс.

2.5.ЭЕМ-да БҚ жетілдіру құралдары мен жөндеушілер бекітілмеуі тиіс.

2.6. Жүйеде жұмыс істейтін дербес компьютерлердің жүйелік блоктарын санкцияландырылмаған ашуға кедергі келтіретін шаралар қолдануы тиіс.

2.7.СҚҚ-дан қорғаудың бағдарламалық-аппараттық құралдарының әкімшісінің құқығы Жүйенің қауіпсіздігін қамтамасыз етуге жауапты қызметкерге беріледі. Аталған қызметкер ЭҚ қалыптастыруға, ЭҚ қабылдау-тапсыруға және ақпараттың кілттік тасымалдаушысын пайдалануға қатысатын Жүйенің әрбір пайдаланушысы үшін қол жетімділік құқығын қалыптастырады.

2.8.Дербес компьютерлерді СҚҚ-дан қорғау үшін операциялық жүйенің штаттық мүмкіндіктері де пайдаланылуы тиіс.

**3. Кілттік ақпарат тасығыштарын сақтау мен пайдалануды ұйымдастыру жөніндегі талаптар**

3.1. Кілттік ақпарат тасығыштары өздері тиесілі тұлғаларда ғана сақталуы тиіс.

3.2.Құпия кілті бар кілттік ақпарат тасығыштарын сақтау мен пайдалану тәртібі оларға санкциясыз қол жетімділіктің мүмкіндігін алып тастауы тиіс.

3.3.Кілттік ақпарат тасығыштарына қол жетімділігі бар тұлғалардың тізімі оларға осындай тиісті міндеттер мен өкілеттіктер бекітілген Клиенттің бұйрығымен немесе өкімімен анықталады.

3.4.Кілттік ақпарат тасығыштарымен жұмыс істеген кезде оларға бөгде тұлғалардың қол жетімділігіне жол берілмеуі тиіс.

3.5. Кілттік ақпарат тасығыштарын сақтау үшін сенімді металл сейфтер орнатылуы тиіс.

3.6.Жұмыс күні аяқталғаннан кейін, сонымен бірге Банкпен байланысты сеанстардан тыс уақытта Кілттік ақпарат тасығыштары сейфте сақталуы тиіс.

3.7.Кілттік ақпарат тасығыштарын басқа құжаттармен бір сейфте, бұл ретте олардан бөлек және оларға бөгде тұлғалардың құпия қол жетімділігі мүмкіндігін болдырмайтындай орамада сақтауға рұқсат етіледі.

3.8.Келесіні іске асыруға рұқсат етілмейді:

their content;
- Introduction of unauthorized changes to Electronic Document (ED).

2.2. It is recommended to use the System on a separate PC specially allocated for this purpose. **Protection of this PC from network attacks and antivirus protection shall be in place.**

2.3. In order to protect the System from unauthorized access a software and hardware complex of protection from unauthorized access must be installed on PC.

2.4. With this complex of protection from unauthorized access it is recommended to form a closed environment ensuring the control over System integrity and allowing users' operation only within the scope of options and powers provided for them. Protection must be applied to systemic and loading files, and files relating to operation of cryptographic information protection means (CIPM).

2.5. There shall be no debuggers and software development means installed on PC used for work with the System.

2.6. Measures must be taken in order to prevent the unauthorized opening of cases of PCs used for work with the System.

2.7. The rights of administrator of software and hardware tools used for protection from unauthorized access shall be entitled to employee in charge of System security ensuring. This employee shall form the access rights for each System user participating in receipt of the ED, execution of the ED and the use of the Tokens.

2.8. In order to protect PCs from unauthorized access inbuilt tools of operating system shall also be employed.

**3. Requirements to Arrangement of Storage and Use of the Tokens**

3.1. The Tokens shall be kept only by persons owning them.

3.2. The order of storing and use of the Tokens with privacy keys shall exclude the possibility of unauthorized access to those.

3.3. The list of persons with access to the Tokens shall be established by decree or order of Client management according to functions and powers assigned to those.

3.4. During work with the Tokens the access of strangers to those shall be excluded.

3.5. Burglar-proof metal safes shall be installed for storing of the Token.

3.6. By the end of Business Day and also out of connections sessions with Bank the Tokens shall be stored in safe.

3.7. It is allowed to store the Tokens in a safe with other documents, but separately from those and in a special package preventing the unauthorized access by strangers.

3.8. It is not allowed to:
- pass the Token to persons not entitled to use them;
- produce privacy keys at display or printer;
- insert the Token into computer reading device in modes not provided for by System functioning and also into reading devices of other computers;
- leave the Token unattended at one's work place;

на перехват информации;
- внесения несанкционированных изменений в технические и программные средства Системы, а также в их состав;
- внесения несанкционированных изменений в Электронный документ (ЭД).

2.2. Систему рекомендуется использовать на отдельном, специально выделенном для этих целей ПК. **Должна быть обеспечена в обязательном порядке защита данного ПК от сетевых атак и антивирусная защита.**

2.3. В целях защиты Системы от НСД на ПК рекомендуется установить программно-аппаратный комплекс защиты от НСД.

2.4. Рекомендуется сформировать с помощью комплекса защиты от НСД функционально замкнутую среду, обеспечивающую контроль целостности Системы 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 ПК, используемом для работы с Системой не должны устанавливаться средства разработки программного обеспечения и отладчики.

2.6. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков персональных компьютеров, используемых для работы с Системой.

2.7. Права администратора программно-аппаратных средств защиты от НСД предоставляются сотруднику, ответственному за обеспечение безопасности Системы. Указанный сотрудник формирует права доступа для каждого пользователя Системы, участвующего в приеме-передаче ЭД, формировании ЭД и использовании Носителей ключевой информации.

2.8. Для защиты ПК от НСД также должны использоваться штатные возможности операционной системы.

**3. Требования по организации хранения и использования Носителей ключевой информации**

3.1. Носители ключевой информации должны храниться только у тех лиц, которым они принадлежат.

3.2. Порядок хранения и использования Носителей ключевой информации с секретными ключами должен исключать возможность НСД к ним.

3.3. Список лиц, имеющих доступ к Носителям ключевой информации, определяется приказом или распоряжением руководства Клиента, согласно закрепленными за ними функциями и полномочиями.

3.4. Во время работы с Носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

3.5. Для хранения Носителей ключевой информации должны устанавливаться надежные металлические сейфы.

3.6. По окончании рабочего дня, а также вне времени сеансов связи с Банком Носители ключевой информации должны храниться в сейфе.

3.7. Хранение Носителей ключевой информации допускается в одном сейфе с другими документами, при этом отдельно от них и в упаковке, исключающей возможность несанкционированного

- Негізгі ақпарат тасығыштарын оларға рұқсат етілмеген тұлғаларға беруге;
- құпия кілттерді дисплейге немесе принтерге шығаруға;
- Кілттік ақпарат тасығыштарын Жүйенің функционалдалануы қарастырылмаған режімде компьютердің есептегіш құрылғысына, сондай-ақ басқа компьютерлердің есептегіш құрылғыларына орнатуға;
- Кілттік ақпарат тасығыштарын жұмыс орнында қараусыз қалдыруға;
- Кілттік ақпарат тасығыштарында бөгде файлдарды жазуға;
- Парольді рұқсат етілмеген тұлғаларға, тіпті Банк қызметкерлеріне де хабарлауға.

**4. Жүйені санкцияландырылмаған қол жетімділіктен қорғау бойынша практикалық ұсынымдар**

4.1. Басқа жергілікті жұмыс станцияларынан және әсіресе, сыртқы желілерден ерекше, Жүйе ресурстарына (оның ішінде желіге алыстан енуді де) желілік қол жетімділікті толықтай оқшауландыру ұсынылады. Осы мақсатта тиісті түрде желіаралық дербес экранды орнату және қосу ұсынылады.

4.2. Жүйе пайдаланушыларына желіні пайдалануды шектеу ұсынылады, яғни мекен-жайларды қосу үшін рұқсат берілетін тізімдерді шектеу, мысалы, банктің серверімен ғана қосуға рұқсат ету. Осы мақсатта да ең дұрысы – орнатылған желіаралық дербес экранды пайдалану.

4.3. Вирусқа қарсы бағдарламалық қамтым міндетті тәртіпте орнатылуы және тұрақты жаңартылып отыруы тиіс. Қауіпсіздік саясатының ең жоғарғы деңгейін жасырын түрде, яғни вирустар табылған кезде пайдаланушылардың жауабын талап етпейтінін орнату ұсынылады.

4.4. Компьютерде бағдарламалық қамтымның осы есептік жазбаларына қондырғының мүмкіндігін шектеу мақсатында, жүйемен жұмыс істеуші Жүйе пайдаланушыларының әкімшілікке құқығы болмауы тиіс. Компьютердің файлдық ресурстарына қолжетімділік, әсіресе, жазуға қолжетімділік, ең төменгі қажетті құқықтармен шектелуі тиіс. Пайдаланушылар тек қана оларға рұқсат берілген қосымшаларға ғана жіберілуі тиіс.

4.5. Жүйе пайдаланушылары негізгі қауіпсіздік талаптарын сақтау мәселелері бойынша және әсіресе, вирусқа қарсы бағдарламаларды пайдалану мәселелері бойынша міндетті түрде нұсқау беруі тиіс.

4.6. Компьютерде жергілікті (немесе домендік) саясаткерлермен операциялық жүйеге ену мүмкіндігі бар пайдаланушылардың тізімін шектеу ұсынылады.

4.7. Сыртқы электронды поштаны (Интернет желісінен) қабылдауды шектеу немесе толықтай бас тарту ұсынылады. Алынатын пошта міндетті түрде вирусқа қарсы құралдармен тексерілуі тиіс.

4.8. Компьютерде тек қана бір ОЖ орнатылуы тиіс.

4.9. Компьютердің BIOS құралдарымен қатқыл дискіде орнатылғаннан ерекшеленетін операциялық жүйені жүктеу мүмкіндігін алып тастау, яғни дискеттен жүктемені, CD/DVD жетектерінен, дискілердің USB flash-інен, желілік үстемені және т.б. ажырату.

4.10. BIOS баптауларын өзгертуге қолжетімділік парольмен қорғалуы тиіс.

4.11. Операциялық жүйенің пайдаланушыларына парольдер белгіленуі тиіс. Парольдердің ұзындығы алты

- record unauthorized files on the Token;
- inform passwords to unauthorized persons, even employees of the Bank.

**4. Practical Recommendations on Protection of System from Unauthorized Access**

4.1. It is recommended to fully block network access to System (including the remote access to network) from other working stations of local network and especially from external networks. For this purpose it is recommended to install and correspondingly customize personal Internet firewall.

4.2. It is recommended to limit the use of Internet network for System users, that is, limit the list of addresses allowed, for example, allowing only for connection with bank server. For this purpose it would be best to use the installed personal Internet firewall.

4.3. It is mandatory to install and regularly update the antivirus software. It is recommended to install the maximum level of security policy by default that will not require any response from user in case of virus detection.

4.4. System users working with the system must not have administrator rights in order to restrict the installation capacities of software on PC under those user accounts records. Access to PC file resources, especially for recording, must be limited to minimum required rights. Users must launch only those applications they are allowed to.

4.5. System users must be obligatorily instructed on issues of complying with the main security requirements, especially in regards to antivirus programs use.

4.6. It is recommended to limit the list of users with access to operating system with local (or domain) policies on PC.

4.7. It is recommended to limit or totally restrict the receipt of external (from Internet) electronic mail. It is obligatory to scan the received mail for viruses with antivirus tools.

4.8. Only one OS must be installed on PC.

4.9. The possibility of uploading of operating system different from the one installed on hard drive must be prevented with use of computer BIOS tools, that is, loading capacity from flop disks, CD/DVD drives, USB flash disks, network uploads, etc. must be restricted.

4.10. Access to change of BIOS settings must be protected with password.

4.11. Operating system users must be assigned with passwords. Password length must be at least 6 digits. Term of password validity must be limited.

4.12. It is recommended to seal computer case in order to prevent its unauthorized opening.

4.13. In order to limit the access to computer, to check the integrity of PC used it is recommended to install and customize software and hardware complex for protection from unauthorized access (“Accord”, “Sobol”, etc.).

4.14. It is recommended to keep the keys only on separate removable media and not use it for other purposes. One must insert removable media to USB ports only during working with

доступа к ним посторонних лиц.

3.8. Не разрешается:

- передавать Носители ключевой информации лицам, к ним не допущенным;
- выводить секретные ключи на дисплей или принтер;
- вставлять Носитель ключевой информации в считывающее устройство ПК в режимах, не предусмотренных функционированием Системы, а также в считывающие устройства других компьютеров;
- оставлять Носитель ключевой информации без присмотра на рабочем месте;
- записывать на Носитель ключевой информации посторонние файлы;
- сообщать пароли неуполномоченным лицам, даже сотрудникам Банка.

**4. Практические рекомендации по защите Системы от НСД**

Рекомендуется полностью блокировать сетевой доступ к Системе (в том числе и удаленный вход в сеть) с других рабочих станций локальной сети и в особенности из внешних сетей. С этой целью рекомендуется установить и настроить соответствующим образом персональный межсетевой экран.

4.2. Рекомендуется ограничить использование сети Интернет пользователями Системы, т.е. ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером Банка. С этой целью также лучше всего использовать установленный персональный межсетевой экран.

4.3. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов.

4.4. Пользователи Системы, работающие с системой не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на ПК. Доступ к файловым ресурсам ПК, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

4.5. Пользователи Системы, должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований безопасности, и в особенности по вопросам использования антивирусных программ.

4.6. Локальными (или доменными) политиками на ПК рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

4.7. Рекомендуется ограничить или полностью отказаться от приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.

4.8. На ПК должна быть установлена только одна ОС.

4.9. Средствами BIOS ПК следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. отключить загрузку с дискет, CD/DVD приводов, USB-flash дисков, сетевую загрузку и т.п.

4.10. Доступ к изменению настроек BIOS должен быть защищен паролем.

| | | |
|---|---|---|
| таңбадан кем құрастырылмауы тиіс. Парольдердің қолданылу мерзімі шектелуі тиіс.<br>4.12. Компьютердің жүйелік блогына, оны санкцияландырылмаған ашудың алдын алу үшін сүргі салу ұсынылады.<br>4.13. Компьютерге қатынауды шектеу үшін, БҚ пайдаланудың тұтастығын тексеруде СҚҚ-ден қорғаудың бағдарламалық-аппараттық кешенін компьютерде орнату және құру ұсынылады («Аккорд», «Соболь» және т.б.).<br>4.14. Кілтте тек жекеленген алынатын ақпараттың тасымалдаушыларын ғана сақтау және оны басқа мақсаттар үшін пайдаланбау ұсынылады. Тасығыштарды USB салатын жерлерге тікелей тек жүйемен жұмыс кезінде операцияларға қол қоюды орындау сәтінде немесе Банкпен алмасқанда ғана салады, операциялар аяқталғаннан кейін осы тасығышты алып тастау қажет. Кілттік ақпараты бар тасығыштарды басқа компьютерлерге қоспаңыз.<br>4.15. Компьютерге сыртқы қондырғыны, оның ішінде өндірістік қажеттіліктермен қарастырылмаған ақпаратты тасығыштарды қосуға кеңес берілмейді.<br>4.16. Вирусқа қарсы қорғауды қамтитын зиянды бағдарламалардың бар-жоғын білу үшін алынатын тасушы медианы (USB-флэш дискілері, USB қатты дискілері, USB арқылы жалғанған ұялы телефондар, CD / DVD дискілері, SD карталар және т.б.) тексеріңіз.<br>4.17. Гиперсілтемелер арқылы өтпеңіз және күдікті электрондық пошталарда және сыртқы сақтау құралдарында қолданбаларды ашпаңыз.<br><br>**5. АҚКҚ есебі жөніндегі жалпы талаптар**<br>5.1. АҚКҚ данасы бойынша және оларға Кілттік тасығыштарының Есебінің журналын жүргізу қажет.<br>5.2. Құпия кілттерді жою, кілттің тасығышын олар орналасқан жерде Кілттік тасығышына зиян келтірмей өшіру жолымен жүргізілуі мүмкін.<br>5.3. Кілттерді жоспарлы ауыстырғаннан немесе кілттерге нұқсан келтіргеннен кейін АҚКҚ пайдаланушыларынан құпия кілтті шифрлеу әрекеттерінен шығарылғандарды және Кілттік ақпарат тасығыштарының ЭСҚ кілттерді әрекеттен шығару сәтінен кейін он күннен кешіктірмей жояды. Кілттердің жойылғаны туралы тиісті жазу Есеп журналына жазылады. | System and during operations of signing or exchange with Bank; after finishing the operation the removable media must be removed. Do not connect key information carriers to other computers.<br>4.15. It is recommended not to connect any external devices to computer including information carriers not required by production necessity.<br>4.16. Always check the removable storage media (USB-flash disks, USB hard drives, mobile phones connected via USB, CD / DVD drives, SD cards, etc.) for the presence of malicious software with anti-virus protection.<br>4.17. Do not go through hyperlinks and do not open applications in suspicious emails and on external storage media.<br><br>**5. General Requirements on CIPM Registration**<br>5.1. It is necessary to maintain the CIPM Registration Log and their Tokens.<br>5.2. Destruction of privacy keys may be performed by erasing (formatting) without damaging of the Token.<br>5.3. After scheduled replacement of keys or compromise of keys CIPM users must destroy the disabled privacy encryption keys and DS of Tokens not later than ten days after the keys were disabled. The corresponding record must be done in the Registration Log on the matter of key destruction. | 4.11. Пользователям операционной системы должны быть назначены пароли. Длина паролей должна составлять не менее 6 (шести) символов. Срок действия паролей должен быть ограничен.<br>4.12. Рекомендуется опечатать системный блок ПК для предотвращения его несанкционированного вскрытия.<br>4.13. Для ограничения доступа к компьютеру, проверки целостности используемого программного обеспечения, рекомендуется установить и настроить на ПК программно-аппаратный комплекс защиты от НСД («Аккорд», «Соболь» и т.п.).<br>4.14. Рекомендуется хранить ключи только на отдельных съемных носителях информации, и не использовать их для других целей. Вставлять носители в USB-разъемы только непосредственно при работе с Системой в моменты выполнения операций подписания или обмена с Банком, по завершении операции необходимо извлечь данный носитель. Не подключайте Носители ключевой информации к другим компьютерам.<br>4.15. Не рекомендуется подключать к компьютеру внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.<br>4.16. Всегда проверяйте подключаемые внешение носители информации (USB-flash диски; USB жесткие диски; мобильные телефоны, подключенные через USB; CD/DVD диски; SD карты и т.п.) на наличе вредоносного программного обеспечения антивруснными средствами защиты.<br>4.17. Не переходите по гиперссылкам и не открывайте приложения в подозрительных электронных письмах и на внешних носителях информации.<br><br>**5. Общие требования по учету СКЗИ**<br>5.1. Необходимо вести Журнал поэкземплярного учета СКЗИ и Носителей ключевой информации к ним.<br>5.2. Уничтожение секретных ключей может производиться путем стирания (форматирования) без повреждения Носителя ключевой информации.<br>5.3. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭЦП Носителей ключевой информации не позднее чем через 10 (десять) дней после момента вывода ключей из действия. Об уничтожении ключей делается соответствующая запись в Журнале учета. |