ЦЕНТРАЛЬНЫЙ РЕСПУБЛИКАНСКИЙ БАНК ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ПОСТАНОВЛЕНИЕ

от 10 декабря 2015г. № 164

г. Донецк

Об утверждении
Временных правил организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

С целью повышения уровня организации защиты электронных банковских документов при осуществлении обмена информацией в электронной форме, в соответствии с абзацем 19 подпункта 3, абзацем 3 подпункта 8, подпунктом 26 пункта 10 раздела III Положения о Центральном Республиканском Банке Донецкой Народной Республики, утвержденного Постановлением Совета Министров Донецкой Народной Республики от 6 мая 2015г. № 8-2, Правление Центрального Республиканского Банка Донецкой Народной Республики **ПОСТАНОВЛЯЕТ:**

1. Утвердить Временные правила организации защиты электронных банковских документов в Центральном Республиканском Банке (прилагаются).

2. Контроль за выполнением данного постановления возложить на директора Департамента безопасности Дремова А.Г.

3. Это Постановление вступает в силу со дня, следующего за днем его официального опубликования.

Председатель **И.П. Никитина**

УТВЕРЖДЕНО
Постановление Правления
Центрального Республиканского Банка
Донецкой Народной Республики
от 10 декабря 2015 г. № 164

Временные правила организации защиты электронных банковских документов в Центральном Республиканском Банке Донецкой Народной Республики

I. Общие положения

1. Настоящие Временные правила организации защиты электронных банковских документов в Центральном Республиканском Банке Донецкой Народной Республики (далее – Правила) устанавливают требования по организации защиты электронных банковских документов при осуществлении обмена информацией в электронной форме между Центральным Республиканским Банком Донецкой Народной Республики (далее – Центральный Республиканский Банк, Банк) и клиентом для защиты от несанкционированного доступа и внесения несанкционированных изменений в электронные банковские документы.

2. Основные понятия, используемые в настоящих Правилах:

1) **электронные банковские документы** – любые платежные, бухгалтерские, технологические, текстовые и другие документы, которые формируются, обрабатываются, передаются, хранятся с использованием программно-технических

комплексов автоматизации банковской деятельности, которые обрабатывают информацию с грифом «Банковская тайна», «Коммерческая тайна» и другую конфиденциальную информацию, которая не является собственностью государства и перечень которой определяется Центральным Республиканским Банком;

2) **средства защиты информации** – совокупность программных и аппаратных средств (средства криптографической защиты информации), используемых для решения задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации;

3) **клиент** – физическое лицо – предприниматель, юридическое лицо или физическое лицо;

4) **закрытый (или секретный, личный) ключ электронной подписи** – сохраняемый в тайне компонент ключевой пары, состоящий из уникальной последовательности символов, с помощью которой формируется подпись;

5) **открытый ключ электронной подписи** – уникальная последовательность символов, доступная любому пользователю для подтверждения подписи. Любое заинтересованное лицо может проверить с помощью опубликованного открытого ключа, что документ подписал именно владелец, что документ не искажен;

6) **сертификат открытого ключа электронной подписи (сертификат ключа подписи)** – документ, содержащий информацию о принадлежности открытого ключа определенному пользователю, оформленный соответствующим ответственным органом - удостоверяющим центром. Для исключения внесения изменений в сертификаты ключей со стороны пользователей сертификат в виде электронных данных подписывается электронной подписью удостоверяющего центра, а сам сертификат выдается его владельцу в бумажной форме;

7) **персонифицированный ключ** – индивидуальный ключ, владельцем которого является конкретное физическое лицо.

3. Центральный Республиканский Банк предоставляет клиентам средства защиты информации на основании договора/дополнительного договора (соглашения) об использовании средств защиты информации в информационных задачах между участниками электронного взаимодействия.

4. Требования этих Правил распространяются на участников электронного взаимодействия.

5. Клиент обязан согласовывать с Центральным Республиканским Банком действия в случае возникновения ситуаций, которые могут возникать во время работы со средствами защиты информации и которые не предусмотрены Правилами, в рабочем порядке.

6. Ответственность за работоспособность средств защиты информации, осуществление учета и контроля их использования в Центральном Республиканском Банке возлагается на отдел информационной безопасности Департамента безопасности (далее – Служба защиты информации). В Службе защиты информации назначается администратор, который подписывает Обязательство администратора защиты информации (Приложение 4).

7. Ответственность за выполнение требований по организации защиты электронных банковских документов в Центральном Республиканском Банке в части исключения возможности доступа посторонних лиц к информации, хранящейся на персональных компьютерах и к средствам защиты информации возлагается на руководителей структурных подразделений, в которых обрабатываются электронные банковские документы, у клиентов юридических лиц – на руководителя или уполномоченное им лицо, у клиентов физических лиц – предпринимателей и физических лиц - непосредственно на физическое лицо или уполномоченных ими лиц.

8. Информация в электронной форме, подписанная усиленной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе.

II. Принципы построения системы защиты информации

1. В состав системы защиты электронных документов Центрального Республиканского Банка входят:

1) программные модули криптографической защиты информации, встроенные в программно-технические комплексы и обеспечивающие аутентификацию, шифрование, наложение/проверку электронной подписи (далее – ЭП);

2) программный модуль генерации ключей (далее – ПМГК);

3) пара ключей (закрытый и открытый ключи) и сертификат открытого ключа ответственного лица;

4)пара сертификатов, которые состоят из зашифрованного контейнера и сертификата открытого ключа для шифрования и проверки ЭП. Зашифрованный контейнер содержит сертификат открытого ключа и закрытый ключ для расшифровки и наложения ЭП.

5) технологические и организационные мероприятия.

2. Система защиты информации построена по принципу персонификации работника, который назначен ответственным лицом и работает с системой защиты.

3. При передаче электронных банковских документов с помощью электронной почты и других средств связи между Центральным Республиканским Банком и клиентом используется усиленная электронная подпись.

4. Служба защиты информации обеспечивает условия для генерации и получения ключей (сертификатов) участников электронного взаимодействия. Служба защиты информации проводит инструктаж с ответственными работниками участников электронного взаимодействия по использованию средств защиты информации.

5. Служба защиты информации обеспечивает аннулирование выданных ключей (сертификатов).

6. Служба защиты информации определяет тип носителей для хранения ключей (сертификатов).

7. Ответственный работник участника электронного взаимодействия во время генерации ключей с помощью ПМГК создает закрытый и открытый ключи или пару сертификатов.

8. Все открытые ключи подлежат сертификации, в соответствии с действующим законодательством Донецкой Народной Республики.

9. Служба защиты информации осуществляет учет выданных и аннулированных ключей (сертификатов) в Журнале учета средств защиты информации, использующихся в Центральном Республиканском Банке (Приложение 5) и в Журнал учета средств защиты информации, использующихся клиентами Центрального Республиканского Банка (Приложение 6).

10. Ответственным работникам участников электронного взаимодействия (владельцам ключей) запрещается передавать персонифицированные ключи системы защиты и пароли к ним другим лицам.

11. Ответственным работникам участников электронного взаимодействия и Службе защиты информации запрещается делать копии персонифицированных ключей системы защиты.

12. Клиент, который получил в Банке аппаратные и программные средства защиты информации, не имеет права передавать их другим лицам.

III. Порядок формирования и использования усиленной электронной подписи

1. Создание усиленной электронной подписи реализуется аппаратными, программными или аппаратно-программными средствами защиты информации Центрального Республиканского Банка.

2. Порядок получения средств защиты информации осуществляется в соответствии с требованиями разделов IV и V этих Правил.

3. Срок действия ключа (сертификата) составляет 12 месяцев со дня его создания.

4. По истечении срока действия ключа (сертификата) получение нового ключа (сертификата) осуществляется в соответствии с требованиями разделов IV и V настоящих Правил.

IV. Порядок получения средств защиты информации ответственным работником Центрального Республиканского Банка

1. Ответственный работник Центрального Республиканского Банка обязан прибыть в Службу защиты информации с удостоверением банковского работника для идентификации личности и заполненным в двух экземплярах бланком Заявки на генерацию и выпуск ключа (сертификата) для работников Центрального Республиканского Банка (Приложение 1).

2. Один экземпляр заполненного бланка Заявки на генерацию и выпуск ключа (сертификата) для работников Центрального Республиканского Банка с отметкой о приеме-передаче хранится в Службе защиты информации, второй

экземпляр хранится у ответственного работника Центрального Республиканского Банка.

V. Порядок получения средств защиты информации клиентом

1. Клиент или уполномоченное лицо клиента обязано прибыть в Службу защиты информации Центрального Республиканского Банка с документами, которые удостоверяют личность, и заполненным в двух экземплярах бланком Заявки на генерацию и выпуск ключа (сертификата) (Приложение 2).

2. Один экземпляр заполненного бланка Заявки на генерацию и выпуск ключа (сертификата) с отметкой о приеме-передаче хранится в Службе защиты информации, второй экземпляр хранится у клиента.

3. По запросу клиента Служба защиты информации предоставляет ПМГК для самостоятельной генерации ключей системы защиты информации. Сертификация ключей осуществляется Службой защиты информации на основании Заявки на генерацию и выпуск ключа (сертификата).

VI. Требования к размещению рабочих мест ответственных работников Центрального Республиканского Банка, которые используют средства защиты информации

1. Служба защиты информации должна быть размещена в отдельном(ых) помещении(ях) с ограниченным доступом.

2. Помещения с ограниченным доступом – помещения, в которых расположены рабочие места с компьютерной техникой и обрабатываются электронные банковские документы, которые содержат сведения с грифом

«Банковская тайна», и другая электронная информация, доступ к которой ограничен.

3. Рабочие места, на которых формируются и обрабатываются платежные документы и электронные документы, содержащие информацию с грифом «Банковская тайна», размещаются в помещениях с ограниченным доступом

VII. Требования к размещению рабочих мест клиентов которые используют средства защиты информации

1. Рабочие места, на которых формируются и обрабатываются платежные электронные документы с использованием средств криптозащиты, рекомендуется размещать в помещениях с ограниченным доступом. Посторонние лица не должны иметь доступ в помещения, в которых размещены криптографические средства защиты информации.

2. Расположение рабочего места в помещении должно обеспечивать сохранность конфиденциальных документов и сведений, выводимых на экран монитора рабочего места ответственного работника Центрального Республиканского Банка или клиента.

3. На рабочем месте обязательно должно быть установлено антивирусное программное обеспечение.

4. Клиенту необходимо предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочего места с установленными средствами криптозащиты, например, опечатывание.

5. При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 8 символов.

6. Установленное на рабочее место программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

7.

Клиент несет полную персональную ответственность за лиц, осуществляющих администрирование программного обеспечения рабочего места, а именно у клиентов юридических лиц – руководитель или уполномоченное им лицо, у клиентов физических лиц – предпринимателей и физических лиц - непосредственно физическое лицо.

8. Помещение должно быть оборудовано сейфами или хранилищами с надежными запирающими устройствами для хранения носителей ключевой информации. Режим хранения должен исключать возможность несанкционированного доступа к ним.

VIII. Порядок работы со средствами защиты информации

1. Все лица, которые работают со средствами защиты информации, подписывают Обязательство (Приложение 3). Подписанное Обязательство хранится в Службе защиты информации.

2. Ответственный работник Центрального Республиканского Банка, клиент или уполномоченное лицо клиента вводит пароль при генерации своего ключа (сертификата).

3. Ответственному работнику Центрального Республиканского Банка, клиенту или уполномоченному лицу клиента запрещено разглашать пароль своего ключа (сертификата). Запрещается записывать пароль ключа (сертификата) на носителе или в любом доступном другим работникам месте.

4. Служба защиты информации обеспечивает необходимые условия для ввода ключа (сертификата) в действие.

5. Ответственный работник Центрального Республиканского Банка, клиент или уполномоченное лицо клиента самостоятельно обеспечивает невозможность бесконтрольного доступа к носителю ключа (сертификата) во время его хранения. В случае потери носителя с ключом ответственный работник Центрального Республиканского Банка, клиент или уполномоченное лицо клиента обязан безотлагательно обратиться в Службу защиты информации с письменным заявлением о его утрате. Служба защиты информации проводит анализ ситуации по факту утраты носителя.

6. Ответственный работник Центрального Республиканского Банка, клиент или уполномоченное лицо клиента самостоятельно следит за сроком действия ключа (сертификата) и осуществляет своевременную генерацию нового.

7. Ответственный работник Центрального Республиканского Банка, клиент или уполномоченное лицо клиента в случае прекращения работы со средствами защиты информации обязан вернуть носитель Службе защиты информации для аннулирования ключа (сертификата).

8. Заявление об аннулировании ключа (сертификата) в случае нарушения его конфиденциальности подается ответственным работником Центрального Республиканского Банка, клиентом или уполномоченным лицом клиента в Службу защиты информации.

9. Служба защиты информации аннулирует ключи (сертификаты), в том числе срок действия которых закончился, в течение одного дня.

10. Ответственным работникам Центрального Республиканского Банка, клиентам или уполномоченным лицам клиента не допускается:

1) Разглашать содержимое носителей ключевой информации, выводить ключевую информацию на дисплей или принтер.

2) Передавать пароли и сами носители ключевой информации лицам, к ним не допущенным.

3) Записывать на ключевой носитель постороннюю информацию.

4) Использовать ключевые носители в режимах, не предусмотренных их функционированием.

5) Вносить какие-либо изменения в программное обеспечение криптографических средств защиты информации.

IX. Контроль за выполнением правил организации защиты информации

1. Служба защиты информации осуществляет контроль за использованием средств защиты информации в Центральном Республиканском Банке. Служба защиты информации при выявлении случаев неудовлетворительного использования ключа (сертификата), которые могут привести к нарушениям в работе или к компрометации средств защиты информации, несанкционированного их использования, обязана в течение одного рабочего дня доложить об этом в форме служебной записки Директору Департамента безопасности Центрального

Республиканского Банка с целью оперативного устранения недостатков, которые были выявлены.

К компрометации ключей можно отнести следующие события: утрата ключевого носителя (в том числе с последующим обнаружением); хищение; несанкционированное копирование информации с ключевого носителя; передача ключевой информации по каналам связи в открытом виде; использование ключевого носителя работников, имевших доступ к ключевой информации после их увольнения; любые другие виды разглашения ключевой информации, в результате которых ключи могут стать доступны лицам, к ним не допущенным.

2. В случае компрометации ключа (сертификата) его действие блокируется Службой защиты информации и инициируется служебное расследование. В результате проведения служебного расследования рассматривается вопрос о принятии решения о компрометации ключей (сертификатов). В случае принятия решения о компрометации ключей (сертификатов). они признаются недействительными и аннулируются Службой защиты информации.

Директор
Департамента безопасности **А.Г. Дремов**

Приложение 1
к Временным правилам организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

Заявка на генерацию и выпуск ключа (сертификата) ответственного лица Центрального Республиканского Банка

Данные о владельце ключа (сертификата):

ФИО	
Идентификационный код (за отсутствием ИК заполнить данные паспорта: серия, номер, где, когда и кем выдан)	
Мобильный телефон	
Должность	
Полное наименование подразделения Банка	
Почтовый адрес подразделения Банка	
Внутренний телефон	
Внутрибанковский e-mail	

Ответственный работник _____ _____
Фамилия, инициалы Подпись

Руководитель _____ _____
Фамилия, инициалы Подпись

Набор ключей (сертификатов):

Выдал _____ Получил _____

Дата _____ Подпись _____ Дата _____ Подпись _____

Директор
Департамента безопасности **А.Г. Дремов**

Приложение 2
к Временным правилам организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

Заявка на генерацию и выпуск ключа (сертификата) Клиента Центрального Республиканского Банка Донецкой Народной Республики

Данные о Клиенте:

Полное наименование/ФИО	
Сокращенное наименование	
Местонахождение/адрес	
Почтовый адрес	
Сведения о регистрации	
Идентификационный код	
Контактный телефон	
E-mail	

Заполняется, если клиент - юридическое лицо или предприниматель

Данные о владельце ключа (сертификата):

ФИО	
Должность	
Идентификационный код (за отсутствием ИК заполнить данные паспорта: серия, номер, где, когда и кем выдан)	
Контактный телефон	
E-mail	

Ответственный работник _____ _____
Фамилия, инициалы Подпись

Руководитель _____ _____
Фамилия, инициалы Подпись

М П

Набор ключей (сертификатов):

Выдал _____ Получил _____

Дата _____ Подпись _____ Дата _____ Подпись _____

Директор
Департамента безопасности **А.Г. Дремов**

Идентификационный код Клиента

Приложение 3
к Временным правилам организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

ОБЯЗАТЕЛЬСТВО

Я, _____,
(Фамилия, Имя, Отчество)

_____,
(должность)

_____,
(полное наименование Клиента или подразделения Банка)

работник, назначенный ответственным за работу со средствами защиты, знаком с Временными правилами организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики и

обязуюсь:

1. Принимать все меры предосторожности для защиты носителя с ключом (сертификатом) от несанкционированного доступа, модификации, а также потери носителя.
2. Хранить свой ключ (сертификат) в зашифрованном виде (в том числе и на носителе), принимать все меры защиты (не записывать и не передавать другому лицу свой пароль ключа (сертификата), сетевой пароль и т.д.).
3. В течение 48 часов с момента изменения сведений, содержащихся в сертификате открытого ключа, информировать Службу защиты информации.
4. В случае попытки других работников получить от меня пароли, обнаружения компрометации или подозрения на компрометацию своего ключа (сертификата) или его потери немедленно сообщить об этом Службе защиты информации.
5. Подавать заявление на аннулирование своего ключа (сертификата) немедленно в случае увольнения, снятия полномочий в части работы со средствами защиты информации или других случаях.
6. Обеспечивать конфиденциальность системы защиты.

Я, _____ предупрежден(а) о том, что
(фамилия, инициалы)

все электронные банковские документы, которые имеют электронную подпись, сделанную с использованием моего ключа (сертификата), считаются подтвержденными мной, а электронная подпись – наложенная мной. Электронная подпись, наложенная мной, придает электронным банковским документам юридическую значимость.

Ответственный работник Клиента
или подразделения Банка

Дата _____ Подпись _____

Знание Правил организации защиты электронных банковских документов по вопросам защиты проверено.

_____
Дата

Администратор защиты информации _____ _____
Фамилия, инициалы Подпись

Директор
Департамента безопасности **А.Г. Дремов**

Приложение 4
к Временным правилам организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

ОБЯЗАТЕЛЬСТВО

АДМИНИСТРАТОРА ЗАЩИТЫ ИНФОРМАЦИИ

Я, _____ ,
(Фамилия, Имя. Отчество)

_____ ,
(должность)

_____ ,
(полное наименование подразделения Банка)

работник, который назначен администратором защиты информации согласно распорядительного документа

_____ № _____ от _____ ,
Наименование распорядительного документа — Дата распорядительного документа

знаком с Временными правилами организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики и

обязуюсь:

1. Принимать все меры предосторожности для защиты от несанкционированного доступа всех используемых мной аппаратно-программных средств криптозащиты.
2. Обеспечивать получение ответственными работниками криптографических средств защиты информации, постоянный учет и контроль их использования.
3. Выполнять Временные правила организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики и осуществлять постоянный контроль технологий обработки электронных банковских документов.
4. Знать нормативно-правовые акты Центрального Республиканского Банка Донецкой Народной Республики по вопросам защиты информации.
5. Предоставлять информацию по криптографической защите информации в Службу защиты информации по первому требованию.
6. Поддерживать связь с ответственными работниками Банка и Клиентами по вопросам криптозащиты информации.
7. Обеспечивать конфиденциальность системы криптозащиты.
8. Передать все средства защиты информации, ключи от сейфов, личных печатей и т. п. в установленном порядке в последний день работы в случае увольнения с работы.

(Дата) (Фамилия, инициалы АЗИ) (Подпись)

Знание Правил организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики и других нормативно-правовых актов Центрального Республиканского Банка Донецкой Народной Республики по вопросам защиты проверено.

Начальник отдела
информационной безопасности
Департамента безопасности _____ _____
Фамилия, инициалы — Подпись

Директор
Департамента безопасности **А.Г. Дремов**

Приложение 5
к Временным правилам организации
защиты электронных банковских
документов в системе Центрального
Республиканского Банка
Донецкой Народной Республики

Журнал учета средств защиты информации, использующихся в Центральном Республиканском Банке

№ п/п	№ сеанса ключа	Имя файла ключа	Носитель ключа (имя носителя, серийный номер)	Подразделение Банка ответственного работника Банка	ФИО ответственного работника Банка	Дата генерации/ сертификации ключа	Время генерации/ сертификации ключа	Подпись ответственного работника Банка за получение ключа	Дата аннулирования ключа (сертификата)	Время аннулирования ключа (сертификата)	Подпись ответственного работника за аннулирование ключа (сертификата)	Примечание*
1.												
2.												
3.												

* Поле «Примечание» заполняется в случае увольнения работника, изменения служебных обязанностей работника либо компрометации ключа.

Директор
Департамента безопасности **А.Г. Дремов**

Приложение 6
к Временным правилам организации защиты электронных банковских документов в системе Центрального Республиканского Банка Донецкой Народной Республики

Журнал учета средств защиты информации,

использующихся Клиентами Центрального Республиканского Банка

№ п/п	№ сеанса ключа	Имя файла ключа	Носитель ключа (имя носителя, серийный номер)	Краткое наименование организации	Идентификационный код организации	ФИО ответственного работника организации	Дата генерации/ сертификации ключа	Время генерации/ сертификации ключа	Подпись ответственного работника организации за получение ключа	Дата аннулирования ключа (сертификата)	Время аннулирования ключа (сертификата)	Подпись работника, осуществившего аннулирование ключа (сертификата)	Примечание*
1.													
2.													
3.													

* Поле «Примечание» заполняется в случае увольнения работника, изменения служебных обязанностей работника либо компрометации ключа на основании заявки организации

Директор
Департамента безопасности **А.Г. Дремов**