**ЦЕНТРАЛЬНЫЙ РЕСПУБЛИКАНСКИЙ БАНК ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

**ПОСТАНОВЛЕНИЕ**

от 17 августа 2017 г. г. Донецк № 240

МИНИСТЕРСТВО ЮСТИЦИИ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 2169
от «04» сентября 2017 г.

**Об утверждении Правил организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики**

В соответствии с подпунктом 3 пункта 10 раздела III, пунктом 11 раздела III, подпунктом 2 пункта 13 раздела IV, подпунктом 11 пункта 24 раздела VI Положения о Центральном Республиканском Банке Донецкой Народной Республики, утвержденного Постановлением Президиума Совета Министров Донецкой Народной Республики от 06 мая 2015 г. № 8-2, с целью повышения уровня защиты электронных документов с использованием средств защиты информации и автоматизации процессов создания и проверки электронной подписи, Правление Центрального Республиканского Банка Донецкой Народной Республики

ПОСТАНОВЛЯЕТ:

1. Утвердить Правила организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики (прилагаются).

2. Признать утратившим силу Постановление Правления Центрального Республиканского Банка Донецкой Народной Республики от 10 декабря 2015 г. № 164 «Об утверждении Временных правил организации защиты электронных банковских документов в системе Центрального Республиканского Банка

Донецкой Народной Республики» (зарегистрировано в Министерстве юстиции Донецкой Народной Республики 28 декабря 2015 г., регистрационный № 859).

3. Контроль выполнения настоящего Постановления возложить на заместителя Председателя Дрёмова А.Г.

4. Настоящее Постановление вступает в силу со дня, следующего за днем его официального опубликования.

**Председатель** **И.П. Никитина**

УТВЕРЖДЕНЫ
Постановлением Правления
Центрального
Республиканского Банка
Донецкой Народной
Республики
от 17 августа 2017 г. № 240

**Правила организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики**

Термины и сокращения:

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

**ключевая информация** – специальным образом организованная совокупность данных закрытого ключа ЭП и сертификата открытого ключа ЭП, предназначенная для осуществления криптографической защиты информации в течение определённого срока;

**ключевой носитель** – защищённое аппаратно-программное устройство, предназначенное для хранения ключевых данных пользователя, с помощью которого осуществляется формирование и проверка электронной подписи, шифрование данных, аутентификация;

**ответственный работник** – работник структурного подразделения Центрального Республиканского Банка Донецкой Народной Республики, работник участника или уполномоченное участником лицо, которое использует средства защиты информации удостоверяющего центра;

**открытый ключ ЭП (ключ проверки электронной подписи)** – уникальная последовательность символов, однозначно связанная с закрытым ключом ЭП, доступная любому пользователю для проверки электронной подписи владельца и подтверждения целостности электронного документа;

**сертификат открытого ключа ЭП** – электронный документ, выданный удостоверяющим центром Центрального Республиканского Банка Донецкой Народной Республики, содержащий информацию о принадлежности открытого ключа ЭП владельцу сертификата открытого ключа ЭП;

**система защита информации** – совокупность методов и средств, включая аппаратно-программные, программные средства защиты информации, ключевую информацию и систему распределения ключевой информации, технологические средства контроля и организационные мероприятия, обеспечивающие защиту электронных документов;

**средства защиты информации УЦ** – средства криптографической защиты информации, которые представляют собой совокупность программных

и аппаратных средств, используемых для решения задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации, предоставляемые удостоверяющим центром Центрального Республиканского Банка Донецкой Народной Республики;

**средства ЭП** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи (для хранения личных сертификатов, ключей электронной подписи и ключей проверки электронной подписи используется ключевой носитель);

**технологическое рабочее место Центрального Республиканского Банка Донецкой Народной Республики** – программно-технический комплекс, предназначенный для автоматизации процесса наложения и/или снятия электронной подписи, шифрования и/или расшифровки подписанных электронных документов;

**участник электронного взаимодействия (участник)** – осуществляющий обмен информацией в электронной форме государственный орган, орган местного самоуправления, юридическое лицо, физическое лицо – предприниматель или физическое лицо, которое использует средства защиты информации, предоставленные удостоверяющим центром Центрального Республиканского Банка Донецкой Народной Республики.

## I. Общие положения

1. Правила организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики (далее – Правила) разработаны в соответствии с Законом Донецкой Народной Республики «Об электронной подписи» (далее – Закон), Положением о Центральном Республиканском Банке Донецкой Народной Республики, утвержденным Постановлением Президиума Совета Министров Донецкой Народной Республики от 06 мая 2015 г. № 8-2, Регламентом удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики, утверждённый Постановлением Правления Центрального Республиканского Банка Донецкой Народной Республики 27 мая 2016 г. № 123 (зарегистрировано в Министерстве юстиции Донецкой Народной Республики 16 июня 2016 г., регистрационный № 1359) (далее – Регламент), другими нормативными правовыми актами Донецкой Народной Республики, в том числе нормативными правовыми актами Центрального Республиканского Банка Донецкой Народной Республики (далее – Центральный Республиканский Банк), а также международными стандартами и нормами права.

2. Настоящие Правила устанавливают требования к организации защиты электронных документов с использованием средств защиты информации,

предоставляемых удостоверяющим центром Центрального Республиканского Банка (далее – УЦ).

3. Требования настоящих Правил распространяются на работников Центрального Республиканского Банка, которые используют средства защиты информации УЦ, и участников.

## II. Организация системы защиты информации

1. Информация в электронной форме, подписанная усиленной электронной подписью (далее – ЭП) в соответствии с Законом, признаётся электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

2. ЭП используется при передаче электронных документов, предусмотренных договором на оказание банковских услуг, заключённым между Центральным Республиканским Банком и участником, с помощью электронной почты, других средств связи и средств передачи данных (флэш-накопители, диски и так далее).

3. Все открытые ключи ЭП подлежат сертификации в соответствии с действующим законодательством Донецкой Народной Республики.

4. Создание ЭП реализуется аппаратными, программными или аппаратно-программными средствами защиты информации УЦ.

5. С целью обеспечения защиты электронных документов Центрального Республиканского Банка и участников Центральный Республиканский Банк организует систему защиты информации, которая включает:

1) программные модули криптографической защиты информации, встроенные в программно-технические комплексы и обеспечивающие аутентификацию, шифрование, наложение и/или проверку ЭП;

2) средства ЭП, которые состоят из зашифрованного контейнера и сертификата открытого ключа ЭП (далее – сертификат) для проверки ЭП и шифрования подписанного электронного документа. Зашифрованный контейнер содержит сертификат и закрытый ключ ЭП для наложения ЭП и для расшифровки подписанного электронного документа;

3) персонификацию ответственных работников;

4) технологические и организационные мероприятия.

6. Центральный Республиканский Банк создаёт из числа своих работников Службу защиты информации (далее – СЗИ), которая несёт ответственность за функционирование системы защиты информации в соответствии с настоящими Правилами, в том числе:

1) обеспечивает работоспособность средств защиты информации УЦ;

2) обеспечивает необходимые условия для генерации закрытых ключей ЭП, получения участниками сертификатов и ввода сертификатов в действие;

3) определяет тип ключевых носителей для хранения сертификатов;

4) осуществляет учёт выданных и аннулированных ключей (сертификатов) в журнале учёта средств защиты информации УЦ, использующихся в Центральном Республиканском Банке Донецкой Народной Республики (приложение 1) и в журнале учёта средств защиты информации УЦ, использующихся участниками (приложение 2) (далее – журналы учёта);

5) осуществляет контроль использования средств защиты информации УЦ в Центральном Республиканском Банке в соответствии с настоящими Правилами и Регламентом. При выявлении случаев неудовлетворительного использования сертификатов, которые могут привести к нарушениям в работе или к компрометации ключей, несанкционированного их использования, использования ключевых носителей в условиях, не предусмотренных режимом их функционирования, СЗИ принимает меры с целью оперативного устранения недостатков, которые были выявлены;

6) проводит служебные расследования при возникновении компрометации ключа. На время проведения служебного расследования действие сертификата приостанавливается, о чём уведомляется владелец сертификата с указанием обоснованных причин, и делается запись в журнале учёта с указанием даты, времени и причин приостановления. По результатам служебного расследования составляется заключение, на основании которого принимается решение о возобновлении сертификата или об установлении факта компрометации ключа и признании сертификата недействительным.

7. Работник СЗИ, на которого возлагаются обязанности администратора защиты информации, подписывает обязательство администратора защиты информации (приложение 3).

## III. Порядок получения средств защиты информации УЦ

1. Центральный Республиканский Банк предоставляет участнику (ответственному работнику участника) средства защиты информации УЦ после получения письма о намерениях на бумажном носителе, удостоверенного

подписью руководителя и скреплённого оттиском печати участника, с указанием адреса электронной почты контактных лиц, на основании соглашения об использовании электронной подписи при обмене электронными документами (далее – соглашение), составленного в соответствии с формой, утверждённой Центральным Республиканским Банком.

2. Для получения средств защиты информации УЦ участник предоставляет следующие документы:

1) паспорт или другой документ, удостоверяющий личность ответственного работника в соответствии с законодательством Донецкой Народной Республики;

2) копию приказа о назначении ответственного работника, заверенную участником в установленном порядке;

3) копию доверенности, подтверждающей полномочия ответственного работника представлять интересы участника при использовании средств защиты информации УЦ (далее – доверенность), заверенную участником в установленном порядке;

4) заявку на генерацию и выпуск ключа (сертификата) ответственного работника участника (приложение 4) (далее – заявка участника) в двух экземплярах, удостоверенную подписью руководителя и скреплённую оттиском печати участника;

5) заявление о присоединении к Регламенту удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики (приложение к Регламенту удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики, утверждённому Постановлением Правления Центрального Республиканского Банка Донецкой Народной Республики 27 мая 2016 г. № 123 (зарегистрировано в Министерстве юстиции Донецкой Народной Республики 16 июня 2016 г., регистрационный № 1359), удостоверенное подписью руководителя и скреплённое оттиском печати участника.

3. Ответственному работнику Центрального Республиканского Банка средства защиты информации УЦ предоставляются на основании приказа о назначении работника Центрального Республиканского Банка ответственным за работу со средствами защиты информации УЦ.

4. Для получения средств защиты информации УЦ ответственный работник Центрального Республиканского Банка предоставляет следующие документы:

1) служебное удостоверение работника Центрального Республиканского Банка;

2) заявку на генерацию и выпуск ключа (сертификата) ответственного работника Центрального Республиканского Банка Донецкой Народной Республики (приложение 5) (далее – заявка), удостоверенную подписью руководителя структурного подразделения;

3) копию приказа о назначении работника Центрального Республиканского Банка ответственным за работу со средствами защиты информации УЦ, заверенную в установленном порядке;

4) копию доверенности, подтверждающей полномочия ответственного работника представлять интересы Центрального Республиканского Банка при использовании средств защиты информации УЦ, заверенную в установленном порядке, за исключением случаев получения средств защиты информации УЦ для работы на технологическом рабочем месте.

5. Администратор СЗИ до передачи ответственному работнику ключевого носителя проводит с ним инструктаж по использованию средств защиты информации УЦ. Инструкции по работе с программным обеспечением и средствами защиты информации УЦ размещаются на официальном сайте УЦ.

6. Перед получением средств защиты информации УЦ ответственный работник подписывает обязательство (приложение 6), которое хранится в СЗИ.

7. Ответственный работник вводит пароль при генерации закрытого ключа ЭП на ключевой носитель.

8. СЗИ проводит необходимые мероприятия для ввода сертификата в действие.

9. Получение ответственным работником средства защиты информации УЦ подтверждается его подписью в заявке участника и в журнале учёта.

10. Срок действия сертификата составляет 12 месяцев со дня его создания, по окончании которого сертификат аннулируется в соответствии с Регламентом.

Участник и ответственный работник Центрального Республиканского Банка самостоятельно следят за соблюдением срока действия сертификата и принимает меры для своевременного получения нового сертификата в порядке, установленном разделом III настоящих Правил.

11. Участник и ответственный работник Центрального Республиканского Банка самостоятельно следят за соблюдением срока действия доверенности и принимает меры для своевременного предоставления в УЦ копии новой

доверенности для продолжения работы с сертификатом в случае, если срок действия доверенности оканчивается раньше срока действия сертификата.

В случае окончания срока действия доверенности, если копия новой доверенности не была предоставлена, СЗИ может осуществить приостановление действия сертификата, о чём уведомляется участник или ответственный работник Центрального Республиканского Банка с указанием причины. После получения копии новой доверенности действие сертификата возобновляется, о чём уведомляется участник или ответственный работник Центрального Республиканского Банка. О приостановлении и возобновлении действия сертификата делаются соответствующие записи в журналах учёта с указанием даты, времени, причины приостановления и возобновления.

## IV. Требования по обеспечению сохранности средств защиты информации УЦ и неразглашению ключевой информации

1. Администраторы СЗИ, ответственные работники Центрального Республиканского Банка, участники и ответственные работники участников обеспечивают сохранность полученных средств защиты информации УЦ, а также принимают меры для исключения возможности доступа к ним других лиц.

2. Участники обязаны предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочих мест ответственных работников с установленными средствами криптографической защиты информации и модификации ключевых носителей (опечатывание, опломбирование и тому подобное).

3. Рабочие места администраторов СЗИ, ответственных работников Центрального Республиканского Банка и ответственных работников участников должны быть размещены в помещениях с ограниченным доступом.

4. Рабочие места администраторов СЗИ, ответственных работников Центрального Республиканского Банка и ответственных работников участников должны быть оборудованы таким образом, чтобы исключить возможность доступа к электронным документам, которые формируются, обрабатываются, хранятся на их рабочих местах, другим лицам.

5. Ответственным работникам запрещается:

1) разглашать содержимое ключевых носителей; выводить пароли, закрытый ключ ЭП на дисплей или принтер;

2) передавать ключевые носители и пароли к ним другим лицам;

3) записывать на ключевой носитель постороннюю информацию;

4) делать копии закрытых ключей ЭП;

5) использовать ключевые носители в условиях, не предусмотренных режимом их функционирования;

6) вносить какие-либо изменения в программное обеспечение средств криптографической защиты информации.

6. В случае прекращения работы со средствами защиты информации УЦ, в том числе в связи с увольнением, ответственный работник в сроки, определённые соглашением, обязан вернуть ключевой носитель в СЗИ.

7. В случае утраты ключевого носителя ответственный работник обязан немедленно предоставить в СЗИ письменное заявление об утрате.

## V. Порядок обработки электронных документов с использованием средств защиты информации УЦ на рабочем месте ответственного работника Центрального Республиканского Банка

1. При шифровании и расшифровке подписанных электронных документов, создании и/или проверке ЭП с использованием средств защиты информации УЦ на рабочем месте ответственного работника Центрального Республиканского Банка владельцем сертификата выступает ответственный работник Центрального Республиканского Банка.

2. При получении подписанного и зашифрованного электронного документа ответственный работник Центрального Республиканского Банка расшифровывает своим закрытым ключом ЭП и проверяет действительность ЭП с помощью сертификата открытого ключа ЭП ответственного работника участника средствами защиты информации УЦ.

3. В случае невозможности расшифровки подписанного электронного документа или отрицательного результата проверки ЭП ответственный работник Центрального Республиканского Банка формирует сообщение об ошибке с указанием причины неполучения электронного документа (ошибка шифрования или ошибка ЭП) и направляет ответственному работнику участника. В случае расшифровки и положительного результата проверки ЭП ответственный работник Центрального Республиканского Банка формирует отчёт о проверке ЭП, который подписывается, зашифровывается и направляется ответственному работнику участника, а сам электронный документ принимается к исполнению.

## VI. Порядок обработки электронных документов с использованием средств защиты информации УЦ на технологическом рабочем месте Центрального Республиканского Банка

1. Для автоматического шифрования и расшифровки подписанных электронных документов, автоматического создания и/или автоматической проверки ЭП с использованием средств защиты информации УЦ Центральный Республиканский Банк организует технологическое рабочее место Центрального Республиканского Банка (далее – технологический АРМ), при этом владельцем сертификата выступает Центральный Республиканский Банк.

2. При шифровании и расшифровке подписанных электронных документов, создании и/или проверке ЭП с использованием средств защиты информации УЦ на технологическом АРМе владельцем сертификата выступает Центральный Республиканский Банк.

3. Для бесперебойной работы технологического АРМа создаётся резервный технологический АРМ и выпускается дубликат сертификата. В случае технического сбоя основного технологического АРМа или ключевого носителя функции автоматического создания и/или автоматической проверки ЭП, автоматического шифрования и расшифровки выполняет резервный технологический АРМ с использованием дубликата сертификата до выяснения причин сбоя.

4. Технологический АРМ устанавливается в помещении с ограниченным доступом.

5. Центральный Республиканский Банк определяет работников, ответственных за функционирование средств ЭП на технологическом АРМе (далее – ответственный работник АРМа).

6. Для персонификации ответственными работниками АРМа делаются соответствующие записи о времени работы технологического АРМа в журнале учёта времени использования средств защиты информации УЦ (приложение 7).

7. При получении подписанного и зашифрованного электронного документа на технологическом АРМе происходит расшифровка электронного документа и проводится проверка ЭП. Наименование входящих электронных документов должно соответствовать кодификатору ответственного работника участника, присвоенного УЦ.

8. В случае невозможности расшифровки подписанного электронного документа или отрицательного результата проверки ЭП на технологическом АРМе формируется квитанция об ошибке с указанием причины неполучения электронного документа (ошибка шифрования или ошибка ЭП) и направляется

ответственному работнику участника. В случае расшифровки и положительного результата проверки ЭП на технологическом АРМе формируется отчёт о проверке ЭП, который подписывается, зашифровывается и направляется ответственному работнику участника, а сам электронный документ принимается к исполнению.

## VII. Заключительные положения

Работники СЗИ, ответственные работники Центрального Республиканского Банка и участники несут ответственность за соблюдение требований к организации защиты электронных документов с использованием средств защиты информации УЦ в соответствии с настоящими Правилами.

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 1
к Правилам организации защиты
электронных документов с использованием
средств защиты информации
удостоверяющего центра Центрального
Республиканского Банка Донецкой Народной
Республики
(подпункт 4 пункта 6 раздела II)

**Журнал учёта средств защиты информации УЦ, использующихся в Центральном Республиканском Банке Донецкой Народной Республики**

| № п/п | № сеанса ключа | Имя файла ключа | Носитель ключа (имя носителя, серийный номер) | Наименование подразделения ответственного работника | ФИО ответственного работника | Дата генерации/ сертификации ключа |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| Время генерации/ сертификации ключа | Подпись ответственного работника за получение ключа | Дата аннулирования ключа (сертификата) | Время аннулирования ключа (сертификата) | Подпись ответственного работника за аннулирование ключа (сертификата) | Примечание |
|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 |

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 2
к Правилам организации защиты
электронных документов с использованием
средств защиты информации
удостоверяющего центра Центрального
Республиканского Банка Донецкой Народной
Республики
(подпункт 4 пункта 6 раздела II)

**Журнал учёта средств защиты информации УЦ,
использующихся участниками**

| № п/п | № сеанса ключа | Имя файла ключа | Носитель ключа (имя носителя, серийный номер) | Краткое наименование участника | Идентификационный код участника | ФИО ответственного работника участника |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| Дата генерации/ сертификации ключа | Время генерации/ сертификации ключа | Подпись ответственного работника участника за получение ключа | Дата аннулирования ключа (сертификата) | Время аннулирования ключа (сертификата) | Подпись ответственного работника за аннулирование ключа (сертификата) | Примечание |
|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 3
к Правилам организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики
(пункт 7 раздела II)

**ОБЯЗАТЕЛЬСТВО**
**АДМИНИСТРАТОРА ЗАЩИТЫ ИНФОРМАЦИИ**

Я, _____ ,
(фамилия, имя, отчество)

_____ ,
(должность)

_____ ,
(полное наименование подразделения Центрального Республиканского Банка)

работник, который назначен администратором защиты информации согласно

_____ ,
(наименование, номер и дата распорядительного документа)

ознакомлен(а) с Правилами организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики, утверждёнными Постановлением Правления Центрального Республиканского Банка Донецкой Народной Республики от 27 июня 2017 г. № ____ (зарегистрировано в Министерстве юстиции Донецкой Народной Республики «____» _____ 2017 г., регистрационный № _____) (далее – Правила), и обязуюсь выполнять следующие обязанности администратора защиты информации:

1. Принимать меры для исключения возможности доступа к используемым мной аппаратно-программным средствам криптографической защиты информации другим лицам.

2. Обеспечивать конфиденциальность средств криптографической защиты информации.

3. Обеспечивать своевременное получение ответственными работниками Центрального Республиканского Банка криптографических средств защиты информации, а также систематический учёт и контроль их использования.

4. Осуществлять систематический контроль обработки электронных документов в соответствии с Правилами.

5. Предоставлять актуальную информацию о системе защиты информации УЦ начальнику отдела информационной безопасности Департамента безопасности по первому требованию.

Продолжение приложения 3

6. Оказывать консультационную и другую помощь ответственным работникам Центрального Республиканского Банка и участникам по вопросам криптографической защиты информации в рамках своей компетенции.

7. Систематически изучать и анализировать законодательство Донецкой Народной Республики по вопросам защиты информации.

8. Передать начальнику отдела информационной безопасности Департамента безопасности средства криптографической защиты информации, ключи от сейфов, личных печатей и так далее в установленном порядке в случае прекращения работы с ними, в том числе в связи с увольнением, в последний день работы.

| _____ | _____ | _____ |
|---|---|---|
| (дата) | (фамилия, инициалы администратора защиты информации) | (подпись) |

Знание Правил проверено.

Начальник отдела
информационной безопасности
Департамента безопасности

| _____ | _____ |
|---|---|
| (фамилия, инициалы) | (подпись) |

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 4
к Правилам организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики
(подпункт 4 пункта 2 раздела III)

**Заявка на генерацию и выпуск ключа (сертификата) ответственного работника участника**

**Данные об участнике:**

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

**Данные об ответственном работнике участника:**

| | |
|---|---|
| ФИО | |
| Должность | |
| Регистрационный номер учётной карточки налогоплательщика<br>(при его отсутствии заполняются данные паспорта: серия, номер, где, когда и кем выдан) | |
| Контактный телефон | |
| E-mail | |

Ответственный работник участника _____ (фамилия, инициалы) _____ (подпись)

Руководитель _____ (фамилия, инициалы) _____ (подпись)

М П

**Ключ (сертификат):**

Выдал _____ (фамилия, инициалы) Получил _____ (фамилия, инициалы)

Дата _____ Подпись _____ Дата _____ Подпись _____

| | |
|---|---|
| код ответственного работника участника, присвоенный УЦ | |

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 5
к Правилам организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики
(подпункт 2 пункта 4 раздела III)

**Заявка на генерацию и выпуск ключа (сертификата) ответственного работника Центрального Республиканского Банка Донецкой Народной Республики**

**Данные об ответственном работнике – получателе ключа (сертификата):**

| | |
|---|---|
| ФИО | |
| Регистрационный номер учётной карточки налогоплательщика<br>(за его отсутствием заполнить данные паспорта: серия, номер, где, когда и кем выдан) | |
| Номер мобильного телефона | |
| Должность | |
| Полное наименование подразделения Центрального Республиканского Банка | |
| Почтовый адрес подразделения Центрального Республиканского Банка | |
| Номер внутреннего телефона | |
| Персональный электронный адрес | |

Ответственный работник _____ _____
(фамилия, инициалы) (подпись)

Руководитель _____ _____
(фамилия, инициалы) (подпись)

**Набор ключей (сертификатов):**

Выдал _____ Получил _____
(фамилия, инициалы) (фамилия, инициалы)

Дата _____ Подпись _____ Дата _____ Подпись _____

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 6
к Правилам организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики
(пункт 6 раздела III)

# ОБЯЗАТЕЛЬСТВО

Я, _____,
(фамилия, имя, отчество)

_____,
(должность)

_____,
(полное наименование участника или подразделения Центрального Республиканского Банка)

_____,
(регистрационный номер учётной карточки налогоплательщика, в случае его отсутствия заполняются данные паспорта: серия, номер, где, когда и кем выдан)

работник, назначенный ответственным за работу со средствами защиты информации УЦ, ознакомлен(а) с Правилами организации защиты электронных документов с использованием средств защиты информации удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики, утверждёнными Постановлением Правления Центрального Республиканского Банка Донецкой Народной Республики от 27 июля 2017 г. № ____ (зарегистрировано в Министерстве юстиции Донецкой Народной Республики «____» _____ 2017 г., регистрационный № _____) (далее – Правила) и Регламентом удостоверяющего центра Центрального Республиканского Банка Донецкой Народной Республики, утверждённым Постановлением Правления Центрального Республиканского Банка Донецкой Народной Республики 27 мая 2016 г. № 123 (зарегистрировано в Министерстве юстиции Донецкой Народной Республики 16 июня 2016 г., регистрационный № 1359) (далее – Регламент), и обязуюсь использовать средства защиты информации УЦ в соответствии с Правилами и Регламентом, в том числе:

1. Принимать все меры предосторожности для защиты ключевого носителя от несанкционированного доступа, модификации, а также потери ключевого носителя.

2. Хранить свой сертификат в зашифрованном виде (в том числе и на ключевом носителе), принимать все меры защиты (не записывать и не передавать другому лицу пароль к ключевому носителю, сетевой пароль и так далее).

3. В течение 48 часов с момента изменения сведений, содержащихся в сертификате открытого ключа ЭП, информировать Службу защиты информации.

Продолжение приложения 6

4. В случае попытки других лиц получить от меня пароли, обнаружения компрометации или подозрения на компрометацию своего ключа или его потери немедленно сообщить об этом Службе защиты информации.

5. Подавать заявление на аннулирование своего сертификата немедленно в случае увольнения, снятия полномочий в части работы со средствами защиты информации УЦ или других случаях.

6. Обеспечивать конфиденциальность системы защиты информации УЦ.

Я, _____, подтверждаю,
(фамилия, инициалы)

что все электронные документы, которые имеют электронную подпись, сделанную с использованием моего ключа (сертификата), считаются подтверждёнными мной, а электронная подпись – наложенной мной.

Ответственный работник участника / Центрального Республиканского Банка

_____ _____
(фамилия, инициалы) (подпись)

Инструктаж по использованию средств защиты информации УЦ провёл_____.
(дата)

Администратор защиты информации _____ _____
(фамилия, инициалы) (подпись)

**Заместитель Председателя** **А.Г. Дрёмов**

Приложение 7
к Правилам организации защиты
электронных документов с использованием
средств защиты информации
удостоверяющего центра Центрального
Республиканского Банка Донецкой Народной
Республики
(пункт 6 раздела VI)

**Журнал учёта времени использования средств защиты информации УЦ**

| № п/п | Дата | Имя сертификата | ФИО ответственного работника | Время начала использования | Подпись ответственного работника | Время окончания использования | Подпись ответственного работника | Примечание |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

**Заместитель Председателя** **А.Г. Дрёмов**