



**АДМИНИСТРАЦИЯ
ГОРОДСКОГО ОКРУГА ХАРЦЫЗСК
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

ПОСТАНОВЛЕНИЕ

24 декабря 2015 г.

№ 868-17

**Об утверждении Инструкции по работе со средствами
криптографической защиты информации
в Администрации городского округа Харцызск
Донецкой Народной Республики**

В целях обеспечения защиты информации и персональных данных в деятельности Администрации городского округа Харцызск Донецкой Народной Республики, исполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Федеральной антимонопольной службы от 16 июля 2020 г. № 658/20 «Об обращении со средствами криптографической защиты информации», приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66, руководствуясь Уставом муниципального образования городской округ Харцызск Донецкой Народной Республики, принятым решением Харцызского городского совета Донецкой Народной

Республики первого созыва от 25 октября 2023 г. № 5/1, Положением об Администрации городского округа Харцызск Донецкой Народной Республики, утвержденным решением Харцызского городского совета Донецкой Народной Республики первого созыва от 10 ноября 2023 г. № 8/3,

ПОСТАНОВЛЯЕТ:

1. Утвердить Инструкцию по работе со средствами криптографической защиты информации в Администрации городского округа Харцызск Донецкой Народной Республики (далее – Инструкция) (прилагается).

2. Ответственность за организацию работы со средствами криптографической защиты информации в Администрации городского округа Харцызск Донецкой Народной Республики возложить на заведующего сектором программно-компьютерного обеспечения Администрации городского округа Харцызск Донецкой Народной Республики Басулу Сергея Анатольевича (далее - Ответственный).

3. Ответственность за соблюдение норм Инструкции возложить на руководителей структурных подразделений Администрации городского округа Харцызск Донецкой Народной Республики в пределах выполняемых этими структурными подразделениями функций.

4. Ответственному ознакомить с Инструкцией всех пользователей средств криптографической защиты информации в Администрации городского округа Харцызск Донецкой Народной Республики, согласно приложению 2 к Инструкции.

5. Опубликовать настоящее постановление в сетевом издании Государственная информационная система нормативных правовых актов Донецкой Народной Республики, доменное имя сайта – gisnra-dnr.ru.

6. Заведующему сектором информационно-аналитической деятельности Администрации городского округа Харцызск Донецкой Народной Республики Поляченко Е.А. обнародовать настоящее постановление на официальном сайте муниципального образования городской округ Харцызск Донецкой Народной Республики, доменное имя сайта — khartsyzsk.gosuslugi.ru.

7. Контроль за исполнением настоящего постановления оставляю за собой.

8. Настоящее постановление вступает в силу со дня его официального опубликования.

Врип главы муниципального образования
городского округа



Е.В. Поплавский

УТВЕРЖДЕНА

постановлением Администрации
городского округа Харцызск
Донецкой Народной Республики
от 24.12.2015 № 868-П

**Инструкция
по работе со средствами криптографической защиты информации
в Администрации городского округа Харцызск Донецкой Народной
Республики**

1. Общие положения

1.1. Инструкция по работе со средствами криптографической защиты информации в Администрации городского округа Харцызск Донецкой Народной Республики (далее - Инструкция) разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) в Администрации городского округа Харцызск Донецкой Народной Республики (далее - Администрация).

1.2. Под работами с применением СКЗИ в Инструкции понимаются:
защищенное подключение к информационным системам;
подписание электронных документов электронной подписью;
проверка подлинности электронной подписи на электронных документах;
шифрование файлов и работа с зашифрованными данными;
другие работы, выполняемые посредством специализированного программного обеспечения для работы с СКЗИ.

Под обращением с СКЗИ в Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

1.3. Инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

1.4. Требования Инструкции не распространяются на следующие случаи:
осуществляется неавтоматизированная обработка информации;
осуществляется хранение, комплектование, учет и использование архивных документов, содержащих сведения конфиденциального характера, в соответствии с законодательством об архивном деле в Российской Федерации;

осуществляется обработка сведений, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

2. Термины и определения

2.1. В Инструкции используются следующие термины и определения:

средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для однозначной идентификации лица, подписавшего информацию;

персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Администрации в рамках исполнения должностных обязанностей;

пользователи СКЗИ - работники Администрации, непосредственно допущенные к работе с СКЗИ;

информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

компрометация - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

3. Допуск пользователей к работе с СКЗИ

3.1. Для получения допуска к работе с СКЗИ работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний. Обучение проводится работниками сектора программно-компьютерного обеспечения Администрации в форме инструктажа с соответствующей записью в журнал об инструктаже. Форма журнала прохождения инструктажа по правилам работы с СКЗИ приведена в приложении 1 к Инструкции. Проверка знаний проводится в форме устного опроса по окончании инструктажа.

3.2. Основанием для допуска пользователя к работе с СКЗИ является внесение его в Перечень пользователей СКЗИ Администрации по форме согласно приложению 2 к Инструкции.

4. Права и обязанности ответственного за организацию работы с СКЗИ

4.1. При реализации мероприятий, связанных с обеспечением в Администрации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, ответственный за организацию работы со средствами криптографической защиты информации в Администрации (далее - Ответственный) должен руководствоваться действующим законодательством Российской Федерации, а также Инструкцией.

4.2. На Ответственного возлагается проведение следующих мероприятий:
ведение Журнала учета ключей и ключевых носителей для СКЗИ Администрации по форме согласно приложению 3 к Инструкции;

ведение Журнала прохождения инструктажа по правилам работы с СКЗИ по форме согласно приложению 1 к Инструкции;

хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним;

принятие ключевых документов к СКЗИ от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

своевременная актуализация перечня пользователей СКЗИ Администрации;

ежегодная проверка наличия ключей и ключевых носителей для СКЗИ Администрации, согласно Журналу учета ключей и ключевых носителей для СКЗИ Администрации.

4.3. Ответственный обязан:

не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключях;

обеспечивать резервное копирование ключей и ключевых носителей;

немедленно уведомлять непосредственного руководителя о фактах утраты

или недостатки СКЗИ, фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

обеспечивать сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

обеспечить соблюдение требований к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

4.4. В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

требовать от пользователей СКЗИ соблюдения положений Инструкции;

обращаться к непосредственному руководителю с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

инициировать проведение служебных расследований по фактам нарушения в Администрации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

4.5. В случае смены Ответственного, изменения вносятся в постановление Администрации, которым он был назначен.

4.6. За нарушение установленных требований по эксплуатации СКЗИ предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

5. Обязанности пользователей СКЗИ

5.1. Пользователи СКЗИ обязаны:

соблюдать конфиденциальность информации ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;

обеспечивать сохранность вверенных ключевых носителей и ключевой документации на них;

незамедлительно сообщать Ответственному о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;

при увольнении или отстранении от исполнения обязанностей сдать Ответственному носители с ключевой документацией;

при подозрении на компрометацию ключевой документации, а также при обнаружении факта утраты или недостатка СКЗИ, ключевых носителей, ключевой документации незамедлительно уведомлять Ответственного.

5.2. Пользователям СКЗИ запрещается:

выводить ключевую информацию на средствах отображения информации

(дисплей монитора, печатающие устройства, проекторы и т.п.) или оставлять ее в бумажном виде в зоне общего доступа;

оставлять ключевые носители с ключевой документацией без присмотра;

записывать на ключевой носитель информацию, не связанную с работой СКЗИ (текстовые и мультимедиа файлы, служебные файлы и т.п.);

вносить любые изменения в программное обеспечение СКЗИ и в информацию на ключевых носителях.

5.3. За нарушение установленных требований по эксплуатации СКЗИ пользователь СКЗИ несет ответственность в соответствии с действующим законодательством Российской Федерации.

6. Действия в случае компрометации ключей

6.1. О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

6.2. К компрометации ключей относятся следующие события:

утрата носителей ключа;

утрата иных носителей ключа с последующим обнаружением;

возникновение подозрений на утечку ключевой информации или ее искажение;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

доступ посторонних лиц к ключевой информации;

другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

6.3. В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

6.4. Визуальный осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

Приложение 1
к Инструкции
по работе со средствами
криптографической
защиты информации
в Администрации городского
округа Харцызск
Донецкой Народной Республики
(пункт 3.1)

Журнал прохождения инструктажа
по правилам работы с СКЗИ

№ п/п	ФИО	Должность	Отметка	Подпись, дата
			Инструктаж по правилам работы с СКЗИ прошел	

Приложение 2
к Инструкции
по работе со средствами
криптографической
защиты информации
в Администрации городского
округа Харцызск
Донецкой Народной Республики
(пункт 3.2)

Перечень пользователей СКЗИ Администрации
городского округа Харцызск Донецкой Народной Республики

№ п/п	ФИО	Должность
1	2	3
1	Поплавский Евгений Валентинович	Врип главы муниципального образования городского округа Харцызск Донецкой Народной Республики
2	Захаров Олег Михайлович	Первый заместитель главы администрации муниципального образования
3	Михайленко Юлия Александровна	Заместитель главы администрации муниципального образования
4	Рогожина Виктория Сергеевна	Заместитель главы администрации муниципального образования
5	Легчилин Виталий Сергеевич	Заместитель главы администрации муниципального образования
6	Костюченко Александр Григорьевич	Заместитель главы администрации муниципального образования
7	Бабанов Александр Владимирович	Управляющий делами администрации муниципального образования
8	Дорошилова Елена Владимировна	Начальник Управления земельных отношений
9	Высоцкая Татьяна Викторовна	Заместитель начальника Управления земельных отношений
10	Новикова Виктория Олеговна	Заместитель начальника Управления имущественных отношений
11	Пикалова Татьяна Владимировна	Главный специалист отдела бухгалтерского учета
12	Новицкая Марина Ивановна	Начальник отдела экономики
13	Гаевая Татьяна Валерьевна	Заместитель начальника отдела кадров и муниципальной службы
14	Басула Сергей Анатольевич	Заведующий сектором программно-компьютерного обеспечения
15	Артюх Сергей Владимирович	Главный специалист сектора программно-компьютерного обеспечения

1	2	3
16	Басула Юлия Владимировна	Начальник Управления опеки и попечительства
17	Гаврушова Алла Владимировна	Заведующий сектором опеки и попечительства в отношении совершеннолетних лиц Управления опеки и попечительства
18	Савелова Ольга Григорьевна	Заведующий сектором обеспечения деятельности муниципальной комиссии по делам несовершеннолетних и защите их прав (государственные полномочия ДНР)
19	Жеменюк Руслан Игоревич	Начальник отдела капитального строительства
20	Хавиков Дмитрий Анатольевич	Начальник отдела по выявлению и учету бесхозного (выморочного) имущества Управления имущественных отношений
21	Милюхина Ирина Юрьевна	Заместитель начальника отдела бухгалтерского учета

Приложение 3
к Инструкции
по работе со средствами
криптографической
защиты информации
в Администрации городского
округа Харцызск
Донецкой Народной Республики
(пункт 4.2)

Журнал учета ключей и ключевых носителей для СКЗИ Администрации
городского округа Харцызск Донецкой Народной Республики

Начат: « » 20 г.

Окончен: « » 20 г.

[illegible]