Kyrgyz Republic - Digital Code No. 178 of 2025 (current official text)

Publisher: https://reestr.dpa.gov.kg/ru/npa/59

This PDF is a faithful text snapshot prepared from the current official government consolidated HTML page because that portal did not expose a publisher-issued PDF download.

ЦИФРОВОЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Режим для слабовидящих

KYR

RU

ENG

Связаться с нами

Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики

при Кабинете Министров Кыргызской Республики

Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики

при Кабинете Министров Кыргызской Республики

Главная

Об Агентстве

Гражданам

Организациям

Полезные документы

НПА и локальные акты

Проекты НПА

Обучающие материалы

Реестр

Учебный центр

Модули

Генератор политики конфиденциальности

Модуль самооценки

Онлайн-чат

Главная

Полезные документы

ЦИФРОВОЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ

от 31 июля 2025 года № 178

ЦИФРОВОЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ

(Вводится в действиеЗакономКР от 31 июля 2025 года N 179

по истечении шести месяцев со дня официального опубликования указанногоЗакона)

ОБЩАЯ ЧАСТЬ

РАЗДЕЛ I. ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ЦИФРОВОЙ СРЕДЕ

Глава 1. Общие положения

Статья 1. Определение основных понятий, содержащихся в настоящем Кодексе

В настоящем Кодексе применяются следующие основные понятия и их определения:

1)автоматическое решение- решение, принятое на основе цифровых данных таким образом, чтобы результаты обработки цифровых данных формировались и использовались для возникновения, изменения или прекращения правоотношений без участия человека;

2)автор цифрового документа- субъект правоотношений в цифровой среде, цифровая подпись или идентификатор которого относится к цифровому документу;

3)аккредитация удостоверяющего центра- признание отраслевым регулятором Национальной цифровой экосистемы (далее - нацэкосистема) удостоверяющего центра соответствующим требованиям, установленным настоящим Кодексом и принятым на его основе нормативным правовым актам;

4)вещательные сервисы- телекоммуникационные сервисы, предназначенные исключительно для распространения теле-, радиоканалов, включая пакетирование теле-, радиоканалов в вещательные мультиплексы;

5)виртуальный оператор- поставщик телекоммуникационного сервиса, использующий для целей его предоставления цифровой ресурс нумерации или цифровой радиочастотный ресурс Кыргызской Республики, но не являющийся владельцем телекоммуникационных сетей в Кыргызской Республике;

6)владелец персональных записей- субъект правоотношений в цифровой среде, который самостоятельно или совместно с другими лицами определяет цели и способы обработки персональных данных;

7)владелец сертификата ключа проверки цифровой подписи- субъект правоотношений в цифровой среде, которому в порядке, установленном настоящим Кодексом, удостоверяющим центром выдан сертификат ключа проверки цифровой подписи;

8)владелец цифрового ресурса- субъект правоотношений в цифровой среде, который самостоятельно или совместно с другими лицами создал такой цифровой ресурс или получил на основании закона или договора право разрешать или ограничивать доступ к цифровому ресурсу;

9)владелец цифровой технологической системы- субъект правоотношений в цифровой среде, который самостоятельно или совместно с другими лицами создал такую систему либо получил право на ее эксплуатацию в соответствии с нормативным правовым актом или договором;

10)владелец цифровой экосистемы- субъект правоотношений в цифровой среде, самостоятельно или совместно с другими лицами определяющий правила цифровой экосистемы;

11)владелец цифровых записей- субъект правоотношений в цифровой среде, который самостоятельно или совместно с другими лицами создал такие записи или получил на основании закона или договора право разрешать или ограничивать доступ к цифровым записям;

12)высокочастотные устройства- устройства, предназначенные для физического воздействия на объекты посредством радиоизлучения;

13)государственный цифровой сервис (далее - госсервис)- цифровой сервис, используемый для выполнения функций, обязанностей и полномочий государственных органов и органов местного самоуправления;

14)государственный (муниципальный) цифровой ресурс- цифровой ресурс, созданный в целях предоставления госсервисов государственными органами или органами местного самоуправления;

15)дипфейк- создание или изменение изображений или аудио-, видеоматериалов, демонстрирующих значительное сходство с существующими лицами, объектами, явлениями или событиями и способных создать у физических лиц ложное впечатление о достоверности таких изображений или материалов;

16)доверенная третья сторона- лицо, обеспечивающее совместное признание подлинности цифровых подписей, созданных в соответствии с нормами права иностранного государства, и цифровых подписей, созданных в соответствии с настоящим Кодексом;

17)доверенный цифровой сервис- цифровой сервис, направленный на удостоверение возникновения, изменения или прекращения отношений в цифровой среде;

18)идентификатор- любая информация, в том числе код, шифр, номер или адрес, позволяющая связывать цифровые записи, содержащие такую информацию, между собой и с субъектом правоотношений в цифровой среде;

19)идентичность- тождество субъекта самому себе на протяжении правоотношений;

20)информация- содержание (контент) цифровых данных, цифровых записей, непосредственно доступное для восприятия человеком;

21)информация персонального характера- информация (независимо от ее достоверности) о физическом лице, которое может быть идентифицировано либо на основании этой информации, либо на основании этой информации в совокупности с другой информацией, к которой владелец записей имеет доступ или может его получить;

22)инфраструктура- земли (земельные участки), здания, строения, сооружения и иные аналогичные объекты;

23)инцидент в цифровой среде- событие или действие, приводящее к неполноте, недостоверности, неактуальности цифровых записей, недоступности или нарушению функционирования цифровых сервисов или цифровых технологических систем;

24)квалифицированный сертификат ключа проверки цифровой подписи (квалифицированный сертификат)- сертификат ключа проверки цифровой подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо отраслевым регулятором, осуществляющим функции корневого удостоверяющего центра;

25)ключ- любая информация (код, шифр), имеющаяся у лица, к которому относится идентификатор, и однозначно связывающая такое лицо с используемым им идентификатором;

26)ключ проверки цифровой подписи- уникальная последовательность символов, однозначно связанная с ключом цифровой подписи и предназначенная для проверки подлинности цифровой подписи;

27)ключ цифровой подписи- уникальная последовательность символов, предназначенная для создания цифровой подписи;

28)конверсия радиочастот- процесс перевода полос радиочастот, определенных в Национальной таблице распределения радиочастот, или их частей:

а) из категории правительственного использования в категорию гражданского или совместного правительственного и гражданского использования;

б) из категории совместного правительственного и гражданского использования в категорию гражданского использования;

29)конструктивная защита данных- защита данных на основе конструкции технологических систем, ориентированной на интересы их пользователей и учитывающей жизненный цикл обрабатываемых системой цифровых записей и предоставляемых с ее помощью цифровых сервисов;

30)контактная информация- идентификатор, предназначенный для связи в цифровой среде с лицом, к которому он относится;

31)координирующий орган- уполномоченный государственный орган, осуществляющий межотраслевую и межведомственную координацию деятельности государственных органов, органов местного самоуправления, юридических лиц в процессе цифровой трансформации Кыргызской Республики;

32)метаданные- структурированные цифровые данные, характеризующие любые цифровые объекты правоотношений в цифровой среде для их идентификации, поиска и управления ими;

33)мобильное устройство- цифровое устройство, имеющее международный идентификационный код (IMEI);

34)нацэкосистема- национальная (общегосударственная) цифровая экосистема, владельцем которой является Кыргызская Республика;

35)обработка- любое действие (операция) или совокупность действий (операций), совершаемых с цифровыми данными (цифровыми записями), включая сбор, запись, организацию, структурирование, накопление, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение, обмен или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение;

36)обработчик- субъект правоотношений в цифровой среде, которому иные субъекты поручили на основании договора или правового акта осуществлять обработку цифровых записей, эксплуатацию цифровых технологических систем или предоставление цифровых сервисов, а равно осуществлять доступ к объектам правоотношений в цифровой среде;

37)общедоступная цифровая технологическая система- цифровая технологическая система, доступ к которой не ограничен в соответствии с законом, договором или решением владельца;

38)общедоступные цифровые записи- цифровые записи, в том числе содержащие открытые данные, доступ к которым не ограничен в соответствии с законом, договором или решением владельца;

39)открытые данные- цифровые данные, доступные в машиночитаемом формате без ограничений на их повторное использование;

40)отраслевой регулятор- уполномоченный государственный орган, осуществляющий проведение проверок и принятие решений, обязательных для субъектов правоотношений в соответствующей сфере деятельности, а в случаях, предусмотренных настоящим Кодексом, также выдачу разрешений (лицензий);

41)охраняемые блага- жизнь и здоровье людей, права и свободы человека и гражданина, окружающая среда, обороноспособность государства, национальная безопасность государства, общественный порядок и нравственность;

42)персональные данные- цифровые данные, содержащие информацию персонального характера;

43)персональные записи- цифровые записи, содержащие информацию персонального характера;

44)персональные ресурсы- цифровые ресурсы, состоящие из персональных записей;

45)пользователь- субъект правоотношений в цифровой среде, запрашивающий или осуществляющий доступ к цифровым записям, цифровым ресурсам, цифровым сервисам или технологическим системам;

46)поставщик цифрового сервиса- субъект правоотношений в цифровой среде, самостоятельно или совместно с другими лицами предоставляющий цифровой сервис пользователям;

47)потребитель- физическое лицо, пользующееся цифровой технологической системой или цифровым сервисом в личных целях, не связанных с извлечением прибыли;

48)правительственная сеть связи Кыргызской Республики (правительственная сеть)- специальная интегрированная засекреченная телекоммуникационная сеть, предназначенная для ведения секретных переговоров и обмена секретной информацией между государственными органами, органами местного самоуправления, учреждениями и организациями (предприятиями) Кыргызской Республики, в том числе, находящимися за ее пределами, имеющими соответствующий допуск на осуществление деятельности с использованием информации, составляющей государственные секреты, в интересах государственного управления, национальной безопасности, обороны, охраны правопорядка и при чрезвычайных ситуациях, а также для ведения секретных переговоров и обмена секретной информацией с иностранными компетентными государственными органами;

49)применимое законодательство- законодательство, подлежащее применению к правоотношениям в цифровой среде с участием иностранных физических или юридических лиц либо осложненным иным иностранным элементом, определенное в соответствии с Гражданским кодексом Кыргызской Республики, иными законами Кыргызской Республики, международными договорами, вступившими в силу в соответствии с законодательством Кыргызской Республики, признаваемыми международными обычаями, а также на основании соглашения сторон;

50)принципал данных (записей)- субъект правоотношений в цифровой среде, к которому относятся цифровые данные или записи (то есть содержат информацию о нем);

51)пространственные данные- данные о пространственных объектах, в том числе включающие сведения об их форме, местоположении и свойствах;

52)пространственные метаданные- данные, которые позволяют описывать содержание и другие характеристики пространственных данных, необходимые для их идентификации и поиска;

53)пространственные объекты- природные, искусственные и иные объекты (в том числе здания, сооружения), местоположение которых может быть определено;

54)публичные обязательства- обязанность совершать определенные действия или осуществлять определенную деятельность, связанную с использованием радиочастотного спектра, возложенная решением отраслевого регулятора или иного уполномоченного государственного органа;

55)радиослужба- использование радиочастотного спектра для определенных целей;

56)радиочастотный спектр Кыргызской Республики- ограниченный государственный ресурс, представляющий собой упорядоченную совокупность радиочастот, которые расположены в пределах, установленных Международным союзом электросвязи, и могут быть использованы для функционирования радиоэлектронных средств или высокочастотных устройств на территории Кыргызской Республики;

57)радиоэлектронные средства- устройства, предназначенные для передачи и/или приема данных, телеметрии, радиолокации, коммуникаций индукционного типа, измерения различных параметров посредством радиоволн;

58)распределенный цифровой ресурс- цифровой ресурс, в котором создание и обработка цифровых записей осуществляется по общим правилам, а именно в соответствии с общими для используемых цифровых технологических систем протоколами обработки данных с использованием двух и более технических средств, распределенных в пространстве и принадлежащих различным владельцам такого ресурса;

59)риск (в цифровой среде)- сочетание вероятности и тяжести инцидентов в цифровой среде;

60)сайт- цифровой ресурс, идентифицируемый с использованием доменного имени или адреса в интернете;

61)сервис цифрового благополучия- сервис, направленный на улучшение качества жизни физического лица на основе обработки цифровых данных о его физиологических особенностях;

62)сертификат ключа проверки цифровой подписи- цифровой документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки цифровой подписи владельцу сертификата ключа проверки цифровой подписи;

63)система искусственного интеллекта- цифровая технологическая система, которая на основе цифровых данных и заданного человеком набора целей, способна с определенной степенью автономности формировать прогнозы, рекомендации или принимать решения, оказывающие влияние на состояние субъектов или объектов внешней среды;

64)система искусственного интеллекта повышенной опасности- система искусственного интеллекта, использование которой повышает вероятность причинения вреда охраняемым благам;

65)смарт-контракт- совокупность цифровых записей, в том числе программа для цифровых устройств, в виде которых изложены все или часть условий сделки между субъектами правоотношений в цифровой среде, которая исполняется независимо от участия сторон при поступлении цифровых данных, предусмотренных сторонами сделки;

66)собственник материальных носителей с информацией персонального характера- лицо, в собственности которого находятся материальные носители с информацией персонального характера, представленной не в форме персональных данных;

67)средства удостоверяющего центра- программные и (или) аппаратные средства, используемые для реализации функций создания, хранения и выдачи сертификатов ключа проверки цифровой подписи, а также ведения реестра сертификатов ключа проверки цифровой подписи;

68)средства цифровой подписи- шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание цифровой подписи, проверка цифровой подписи, создание ключей цифровой подписи и ключей проверки цифровой подписи;

69)субъект персональных данных- физическое лицо, являющееся принципалом персональных данных;

70)субъект правоотношений в цифровой среде- участник регулируемых настоящим Кодексом отношений, к которому относятся Кыргызская Республика, другие государства, государственные органы, органы местного самоуправления и их должностные лица, а также физические и юридические лица. Правила, установленные настоящим Кодексом, применяются к отношениям с участием иностранных граждан, лиц без гражданства, иностранных юридических лиц, иностранных государств, если иное не предусмотрено настоящим Кодексом или законом;

71)телекоммуникации- обмен цифровыми данными с другими пользователями посредством телекоммуникационного сервиса, в том числе путем доступа к цифровым данным, загруженным или созданным другими пользователями, а также голосовые соединения с другими пользователями посредством телекоммуникационного сервиса;

72)телекоммуникационная сеть- цифровая технологическая система, предназначенная для предоставления телекоммуникационного сервиса;

73)телекоммуникационное сооружение- инфраструктура оператора телекоммуникаций, созданная или приспособленная для размещения телекоммуникационных сетей и (или) их элементов (включая базовые станции, антенно-мачтовые сооружения, антенно-фидерные устройства, линейно-кабельные сооружения, но не ограничиваясь ими), не являющаяся объектом капитального строительства;

74)телекоммуникационный сервис- доступные пользователям возможности использования цифровых технологических систем в целях обмена цифровыми данными с другими пользователями, в том числе путем доступа к цифровым данным, загруженным или созданным другими пользователями, а также возможности голосовых соединений по телекоммуникационной сети;

75)трансграничная передача персональных данных- передача персональных данных владельцам записей, находящимся под юрисдикцией других государств;

76)удостоверяющий центр- юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки цифровой подписи;

77)устройства цифрового благополучия- цифровые технологические системы и их элементы, используемые в рамках сервисов цифрового благополучия;

78)утечка персональных данных- разновидность неправомерной обработки персональных данных, в результате которой персональные данные становятся доступны лицам, не имеющим законного основания для доступа к ним;

79)цифровая аутентификация- подтверждение связи между идентификатором и лицом, к которому относится идентификатор, с использованием ключа;

80)цифровая запись - цифровые данные, которые могут быть идентифицированы с использованием метаданных;

81)цифровая идентификация- поиск цифровой записи с целью установления связи между принципалом данных и такой цифровой записью;

82)цифровая подпись- информация в цифровой форме, которая присоединена к другой информации в цифровой форме и (или) логически связана с ней и используется для обеспечения неизменности цифрового документа и определения автора цифрового документа;

83)цифровая среда- не имеющая территориальных границ система общественных отношений по обработке цифровых данных с использованием цифровых устройств;

84)цифровая технологическая система- система цифровых устройств, программ для них и баз данных, предназначенных для обработки цифровых данных;

85)цифровая устойчивость- состояние цифровой среды, характеризуемое непрерывностью предоставления цифровых сервисов и пользования ими, обеспечиваемое за счет реализации мер по кибербезопасности, а также эффективного управления рисками и ресурсами;

86)цифровая экосистема- совокупность общедоступных цифровых технологических систем, цифровых ресурсов и цифровых сервисов, используемых для обеспечения взаимодействия субъектов правоотношений в цифровой среде по единым правилам;

87)цифровое приложение (приложение)- цифровой ресурс, представляющий собой программу для электронных вычислительных машин и иных цифровых устройств, используемый для доступа к цифровым данным;

88)цифровое сообщество- объединение субъектов правоотношений в цифровой среде независимо от наличия у него статуса юридического лица, созданное ими по их собственной инициативе и на началах добровольности для реализации задач его участников на основании общих правил по развитию и (или) использованию объектов правоотношений в цифровой среде;

89)цифровое устройство- техническое устройство, предназначенное для обработки цифровых данных, в том числе электронная вычислительная машина (ЭВМ);

90)цифровой- термин, характеризующий любое явление, необходимым признаком которого является использование цифровых данных (в большинстве случаев - данных, выраженных посредством двоичного кода);

91)цифровой архив- цифровая технологическая система, обеспечивающая целостность и неизменность обрабатываемых с ее помощью цифровых записей и ограниченный доступ к ним;

92)цифровой документ- цифровая запись, неизменность которой обеспечивается с помощью цифровой подписи или идентификатора, используемых в соответствии с правилами системы идентификации;

93)цифровой дубликат документа- цифровая запись, воспроизводящая в полном объеме информацию, изначально содержащуюся в подлиннике документа на бумажном или ином материальном носителе, подписанном собственноручной подписью, включая его реквизиты;

94)цифровой реестр- цифровой ресурс, состоящий из записей, подтверждающих принадлежность прав на использование перечисленных в настоящем Кодексе объектов учета;

95)цифровой ресурс- упорядоченная совокупность цифровых записей, в том числе база данных, предназначенная для хранения и использования цифровых записей и (или) цифровых данных и доступа к ним;

96)цифровой сервис- возможность использования цифровой технологической системы для создания, передачи, хранения цифровых данных или доступа к ним;

97)цифровой сервис идентификации мобильных устройств- цифровой сервис идентификации и проверки подлинности идентификационного кода действующих и ввозимых на территорию Кыргызской Республики мобильных устройств;

98)цифровые данные- пригодные для обработки с использованием цифровых устройств данные независимо от формы и способа их хранения и передачи;

99)цифровые права- права на объект правоотношений в цифровой среде, включающие в себя право на доступ к объекту правоотношений в цифровой среде и право устанавливать условия доступа к нему;

100)шлюз- цифровое устройство, обеспечивающее передачу данных между телекоммуникационными сервисами по передаче данных и предоставлению голосовых соединений;

101)Национальный оператор телекоммуникаций- юридическое лицо с государственной долей участия не менее 80 процентов, определенное постановлением Кабинета Министров Кыргызской Республики (далее - Кабинет Министров).

Статья 2. Основы отношений в цифровой среде

1. Настоящий Кодекс закрепляет правила, которым субъекты правоотношений обязаны следовать в цифровой среде.

2. Предметом регулирования настоящего Кодекса является цифровая среда на следующих уровнях:

1) отношения, связанные с обработкой цифровых данных, созданием и использованием цифровых записей, в том числе в виде цифровых документов и цифровых ресурсов;

2) отношения, связанные с созданием и использованием цифровых сервисов, построением цифровых экосистем и участием в них;

3) отношения, связанные с созданием цифровых технологических систем, в том числе центров обработки данных и телекоммуникационных сетей;

4) отношения, касающиеся доступа владельцев цифровых технологических систем к инфраструктуре (землям, зданиям, строениям, сооружениям и иным аналогичным объектам).

3. Отношения по распространению отдельных видов информации или доступу к ней в зависимости от ее содержания регулируются законодательством в сфере информации и не входят в предмет регулирования настоящего Кодекса.

4. Отношения, вытекающие в рамках контрразведывательной и разведывательной деятельности, а также оперативно-розыскной деятельности, регулируются законодательством в соответствующих сферах и не входят в предмет регулирования настоящего Кодекса.

5. В рамках регулирования цифровой среды настоящий Кодекс предусматривает исключительный перечень случаев, в которых допускается:

1) ограничение доступа к объектам правоотношений в цифровой среде;

2) принудительное установление недискриминационного доступа к объектам правоотношений в цифровой среде.

Статья 3. Принципы регулирования цифровой среды

1. Регулирование цифровой среды основано на общеправовых, организационных и отраслевых принципах.

2. К общеправовым принципам, применяемым для регулирования цифровой среды, относятся:

1) справедливость и соразмерность регулирования, приоритет интересов человека как единственного конечного пользователя цифровых технологий (принцип справедливости);

2) доступность, понятность и предсказуемость правового регулирования (принцип определенности);

3) участие в выработке правил для цифровой среды всех лиц, на которых распространяются правила, напрямую или через представителей (принцип участия).

3. К организационным принципам, на реализацию которых направлено регулирование цифровой среды, относятся:

1) возможность субъектов правоотношений в цифровой среде по своему выбору использовать любые цифровые технологии, если при их использовании выполняются требования, установленные настоящим Кодексом (принцип технологической нейтральности);

2) применение норм настоящего Кодекса без какой-либо дискриминации в отношении всех субъектов правоотношений в цифровой среде вне зависимости от качества, востребованности и иных содержательных характеристик, обрабатываемых ими цифровых данных (принцип контентной нейтральности);

3) долговременная устойчивость правил и правоотношений, определяемых настоящим Кодексом, бесперебойность, непрерывность сервисов и процессов, защищенность объектов и субъектов правоотношений в цифровой среде (принцип устойчивости);

4) поощрение конкуренции на цифровых рынках, открытость и совместимость форматов данных и записей с возможностью их переноса между поставщиками разных цифровых сервисов и владельцами разных цифровых технологических систем, доступность цифровых данных и принятие решений на их основе, в том числе при их повторном использовании (принцип открытости);

5) хранение на протяжении всего жизненного цикла соответствующей технологии необходимых цифровых данных, подтверждающих выполнение обязанностей субъектами правоотношений, в том числе устранение ими нарушений и (или) соблюдение прав в цифровой среде (принцип подотчетности).

4. Отраслевые принципы, составляющие основу регулирования отношений в отдельных сферах, закреплены в соответствующих главах настоящего Кодекса.

Статья 4. Цифровой кодекс и иные нормативные правовые акты

1. Настоящий Кодекс имеет приоритет при регулировании отношений в цифровой среде. Нормы других законов и принятых в соответствии с ними нормативных правовых актов, определяющие правила регулирования отношений в цифровой среде, не могут противоречить положениям настоящего Кодекса. В случае возникновения противоречий между настоящим Кодексом и другим нормативным правовым актом, действуют и применяются нормы настоящего Кодекса с учетом правил о разрешении коллизий, установленных законодательством о нормативных правовых актах.

2. Нормативные правовые акты по вопросам правового регулирования в цифровой среде могут приниматься исключительно в случаях, прямо установленных настоящим Кодексом.

3. Проект закона о внесении изменений в настоящий Кодекс подлежит обязательному согласованию с координирующим органом в целях обеспечения единства цифровой среды на всех уровнях, установленных настоящим Кодексом, и соответствия принципам регулирования отношений в цифровой среде. Внесение изменений в настоящий Кодекс допускается не более одного раза в год.

Статья 5. Цифровой кодекс и правила цифровых сообществ

1. Цифровые сообщества создаются субъектами правоотношений в цифровой среде по их инициативе и на началах добровольности. Цифровые сообщества могут иметь любую организационную форму и порядок управления, не запрещенные законодательством. Субъекты правоотношений, являющиеся участниками цифровых сообществ, самостоятельно определяют правила таких сообществ. В Кыргызской Республике государственные органы, органы местного самоуправления, их должностные лица, физические и юридические лица при определении правил цифровых сообществ, в которых они участвуют, обязаны руководствоватьсяКонституциейКыргызской Республики, настоящим Кодексом и законами Кыргызской Республики.

2. При применении правил цифровых сообществ государственные органы, органы местного самоуправления и должностные лица Кыргызской Республики обязаны обеспечивать соблюдение требований законодательства Кыргызской Республики и несут ответственность за его несоблюдение.

Статья 6. Общепризнанная международная практика

1. Положения стандартов и рекомендаций, опубликованные международными организациями, экспертными сообществами зарубежных стран и активно применяемые субъектами правоотношений в цифровой среде, образуют общепризнанную

международную практику.

2. В случаях, предусмотренных настоящим Кодексом, субъекты правоотношений в цифровой среде при выборе технологий или способов осуществления своих прав и исполнения обязанностей в цифровой среде учитывают общепризнанную международную практику, утвержденную отраслевым регулятором в соответствующей сфере, предусмотренной настоящим Кодексом. При отсутствии утвержденной отраслевым регулятором общепризнанной международной практики субъекты правоотношений в цифровой среде вправе учитывать общепризнанную международную практику, не противоречащую утвержденным стандартам и нормативным правовым актам Кыргызской Республики.

3. Субъекты правоотношений в цифровой среде должны продемонстрировать, что выбранные технологии соответствуют общепризнанной международной практике или требованиям, которые эквивалентны или выше требований общепризнанной международной практики, путем опубликования деклараций соответствия.

Глава 2. Государственное регулирование в цифровой среде

Статья 7. Формы государственного регулирования

В Кыргызской Республике государственное регулирование отношений в цифровой среде осуществляется в формах:

1) межотраслевого и межведомственного координирования деятельности государственных органов, органов местного самоуправления, юридических лиц в цифровой среде;

2) отраслевого регулирования и надзора.

Статья 8. Координирование деятельности в цифровой среде

1. Межотраслевое и межведомственное координирование деятельности государственных органов, органов местного самоуправления, юридических лиц в цифровой среде осуществляется путем:

1) определения общегосударственных целей и задач, программ и планов деятельности в цифровой среде;

2) планирования и мониторинга бюджетов деятельности государственных органов, органов местного самоуправления в цифровой среде с учетом обеспечения режима секретности, защиты государственной или иной охраняемой законом тайны;

3) стратегического руководства цифровыми реформами и программами, координации региональной и международной помощи, выделяемой на осуществление деятельности в цифровой среде;

4) сотрудничества всех заинтересованных сторон, в том числе объединений и ассоциаций субъектов правоотношений в цифровой среде, в разработке и реализации целей и задач, общенациональных инициатив, планов, программ;

5) координирования деятельности по созданию архитектуры государственной цифровой экосистемы, общих цифровых платформ и сервисов, пилотированию инновационных решений;

6) обеспечения бесперебойности, интеграции и согласованности в деятельности всех субъектов правоотношений для достижения целей государственного управления в цифровой среде.

2. Координирующий орган в цифровой среде определяется Кабинетом Министров.

Статья 9. Отраслевое регулирование и надзор

1. Регулирование и надзор в цифровой среде осуществляются путем проведения проверок, принятия решений (административных актов), обязательных для субъектов правоотношений в цифровой среде, а в случаях, предусмотренных настоящим Кодексом, выдачи разрешений (лицензий).

2. Настоящий Кодекс устанавливает полномочия государственных органов по осуществлению регулирования и надзора (отраслевых регуляторов) в следующих сферах:

1) персональные данные;

2) национальная цифровая экосистема;

3) телекоммуникации.

3. Положения об отраслевых регуляторах утверждаются Кабинетом Министров.

4. Порядок формирования и осуществления деятельности отраслевого регулятора должен обеспечивать независимость проводимого им регулирования.

5. Один и тот же отраслевой регулятор не может осуществлять полномочия в нескольких сферах, предусмотренных настоящим Кодексом.

6. Каждый отраслевой регулятор обязан ежегодно представлять отчет о состоянии отношений в сфере, относящейся к его компетенции, своих решениях, кадровых и финансовых ресурсах, их объемах и использовании, планируемых действиях и мерах. Отчет подлежит опубликованию на сайте отраслевого регулятора.

7. Отраслевые регуляторы создают учебные центры в соответствующих сферах и обеспечивают их деятельность. Учебные центры отраслевых регуляторов на возмездной или грантовой основе проводят образовательные и просветительские

мероприятия, научные исследования и практические разработки.

Статья 10. Экспертные советы

1. Отраслевой регулятор вправе создать экспертный совет.

Экспертный совет - консультативно-совещательный орган, созданный на общественных началах из представителей экспертных, научных кругов, профессиональной среды в соответствующей отрасли регулирования, для подготовки предложений и рекомендаций по вопросам развития и соблюдения принципов регулирования цифровой среды.

Решение отраслевого регулятора о созыве экспертного совета с указанием срока начала деятельности экспертного совета и срока его полномочий подлежит опубликованию на сайте отраслевого регулятора.

2. Экспертный совет и эксперты не вправе вмешиваться в деятельность отраслевого регулятора, участвовать в проведении проверок или принятии решений, обязательных для субъектов правоотношений в цифровой среде.

3. Регламент работы экспертного совета, включая процедуры его формирования, утверждается отраслевым регулятором.

Статья 11. Аккредитация субъектов для осуществления проверок в соответствующей сфере

1. Отраслевой регулятор соответствующей сферы осуществляет аккредитацию физических и (или) юридических лиц на право осуществления проверок субъектов регулирования в случаях, предусмотренных настоящим Кодексом. Аккредитованные лица вправе осуществлять проверки при наличии согласия субъекта регулирования.

2. Требования к аккредитованным лицам, порядок аккредитации и вид документа, выдаваемого по результатам проведения проверок аккредитованными лицами, устанавливаются актами Кабинета Министров в соответствии с настоящим Кодексом.

3. За аккредитацию аккредитованные лица ежегодно вносят плату, рассчитываемую по методике, утверждаемой Кабинетом Министров и учитывающей:

1) доход от предоставления услуг аккредитованными лицами;

2) количество проверок;

3) весовой коэффициент, включающий в себя социальный фактор;

4) расчетный показатель;

5) коэффициент эффективности деятельности аккредитованного лица.

Статья 12. Правила и стандарты профессиональной деятельности в цифровой среде

1. Профессиональные объединения субъектов правоотношений в цифровой среде вправе утверждать регламент, обязательный для их участников. Регламент может включать в себя правила и стандарты профессиональной деятельности участников объединения, не противоречащие настоящему Кодексу.

2. Профессиональные объединения обязаны осуществлять контроль за соблюдением таких регламентов своими участниками.

3. Сведения о членстве в таких профессиональных объединениях, результатах контроля за соблюдением обязательных регламентов и допущенных нарушениях, а также устранении таких нарушений являются общедоступной информацией. Данные сведения должны публиковаться профессиональными объединениями на их сайтах.

Статья 13. Предоставление телекоммуникационных сетей и сооружений для целей государственного управления

1. Отраслевой регулятор телекоммуникаций, государственные органы и органы местного самоуправления Кыргызской Республики, эксплуатирующие внутренние, закрытые и засекреченные телекоммуникационные сети, а также операторы телекоммуникаций независимо от форм собственности обязаны обеспечивать предоставление телекоммуникационных сетей и сооружений в интересах государственного управления, национальной безопасности, обороны, охраны правопорядка и при чрезвычайных ситуациях.

2. При наступлении чрезвычайных ситуаций отраслевой регулятор телекоммуникаций принимает меры по обеспечению предоставления необходимых телекоммуникационных сервисов. Отраслевой регулятор телекоммуникаций может создать особые временные органы для эксплуатации телекоммуникационных сетей и предоставления телекоммуникационных сервисов полностью или частично на территории, где сложилась чрезвычайная или кризисная ситуация.

3. Кабинет Министров может использовать телекоммуникационные сервисы и сооружения в интересах государственного управления, национальной безопасности, обороны, охраны правопорядка и при чрезвычайных ситуациях (природные катастрофы, карантины и т.д.). Уполномоченные государственные органы могут пользоваться приоритетным правом на эксплуатацию или приостановление эксплуатации телекоммуникационных сетей и сооружений только в указанных исключительных обстоятельствах.

4. Правительственная сеть организуется и предоставляется уполномоченным государственным органом в сфере обеспечения национальной безопасности. Правительственная сеть должна обеспечивать защищенность информации, передаваемой по данной сети.

Статья 14. Приостановление и возобновление эксплуатации телекоммуникационных сетей

1. Приостановление эксплуатации телекоммуникационных сетей и оказания телекоммуникационных сервисов в случае, предусмотренном частью 3статьи 13настоящего Кодекса, осуществляется операторами телекоммуникаций на основании мотивированного решения в письменной форме уполномоченного должностного лица государственного органа в сфере обеспечения национальной безопасности в случаях, установленных законодательством Кыргызской Республики.

2. Операторы телекоммуникаций не вправе предоставлять доступ к своей телекоммуникационной сети, а также обязаны обеспечить невозможность пользования соответствующим телекоммуникационным сервисом мобильным устройствам, если его международный идентификационный код (IMEI) включен в "Черный список" Государственной системы идентификации мобильных устройств в порядке, установленном Кабинетом Министров.

3. Операторы телекоммуникаций обязаны возобновить эксплуатацию телекоммуникационных сетей и предоставление телекоммуникационных сервисов на основании решения суда или мотивированного решения в письменной форме уполномоченного должностного лица государственного органа в сфере обеспечения национальной безопасности, который принял решение о приостановлении эксплуатации сети или оказания телекоммуникационных сервисов.

4. Кабинет Министров в установленном им порядке компенсирует убытки, понесенные оператором телекоммуникаций вследствие такого приостановления его деятельности.

Глава 3. Специальное регулирование в цифровой среде

Статья 15. Цели и принципы специального регулирования

1. Временное освобождение субъектов отдельных видов деятельности в цифровой среде от отдельных обязанностей, установленных настоящим Кодексом и принятыми в соответствии с ним нормативными правовыми актами (специальное регулирование), может быть введено в порядке, установленном настоящей главой Кодекса.

2. Целями специального регулирования являются:

1) выработка передовых форм, методов и способов осуществления экономической и социальной деятельности;

2) безопасное тестирование цифровых инноваций в реальных условиях;

3) улучшение качества и доступности объектов правоотношений в цифровой среде;

4) стимулирование добросовестной конкуренции;

5) привлечение инвестиций в цифровую экономику;

6) повышение эффективности государственного управления и местного самоуправления;

7) снижение регуляторной неопределенности в отношении инновационных продуктов и сервисов.

3. Специальное регулирование основывается на принципах:

1) временного характера вводимых специальных правил;

2) четкого соответствия специальных правил целям их введения;

3) запрета лишения граждан их прав и свобод специальными правилами;

4) сохранения цифровой устойчивости;

5) равенства субъектов специального регулирования;

6) добровольного участия в специальном регулировании;

7) транспарентности содержания специальных правил и их целей;

8) эффективного контроля отраслевого регулятора за реализацией специальных правил.

4. Порядок создания и участия, требования к участникам специальных регулятивных режимов на рынке банковских и платежных систем устанавливаются Национальным банком Кыргызской Республики.

5. Специальное регулирование вводится только для отношений, связанных с цифровой средой, и не может ограничивать конкуренцию и равенство субъектов, а равно освобождать от обязанности по уплате налогов и иных неналоговых платежей или по возмещению причиненного вреда.

Статья 16. Введение специального регулирования

1. Специальное регулирование вводится решением Президента Кыргызской Республики (далее - Президент) по инициативе субъектов правоотношений в цифровой среде, в том числе государственных органов и органов местного самоуправления, одобренной отраслевым регулятором, предусмотренным настоящим Кодексом, в сфере деятельности которого вводится специальное регулирование.

2. Субъект правоотношений в цифровой среде, выступающий с инициативой введения специального регулирования (инициатор), обращается к отраслевому регулятору с заявлением о введении специального регулирования, содержащим следующие данные:

1) указание на положения настоящего Кодекса и принятых в соответствии с ним нормативных правовых актов, устанавливающих обязанности субъектов правоотношений в цифровой среде в виде совершения определенных действий, соблюдения определенных процедур, запретов или ограничений;

2) указание на круг субъектов, которые будут затронуты специальным регулированием;

3) описание целей и задач предлагаемого специального регулирования, значимости отношений, применительно к которым вводится специальное регулирование, обоснование преимуществ введения специального регулирования;

4) обоснование того, что освобождение инициатора и иных субъектов, занимающихся аналогичной деятельностью, от перечисленных обязанностей будет способствовать достижению одной или нескольких целей специального регулирования, установленных настоящим Кодексом;

5) описание возможных негативных последствий от введения специального регулирования, мер, необходимых для их минимизации, методики оценки успешности результатов.

3. Отраслевой регулятор, получивший заявление о введении специального регулирования, публикует его на своем сайте. Срок публикации заявления на сайте не может превышать 5 рабочих дней с момента получения заявления.

4. Одновременно с публикацией заявления о введении специального регулирования отраслевой регулятор публикует на сайте контактную информацию для направления замечаний.

5. Отраслевой регулятор по результатам рассмотрения заявления о введении специального регулирования и полученных замечаний по нему принимает решение, содержащее одну из следующих рекомендаций:

1) одобрить введение специального регулирования;

2) возвратить заявление о введении специального регулирования на доработку с учетом замечаний, которые должны быть перечислены в решении отраслевого регулятора;

3) отклонить заявление о введении специального регулирования.

6. Решение об одобрении введения специального регулирования отраслевого регулятора должно содержать выводы о соответствии заявления целям специального регулирования и требованиям, установленным настоящей статьей.

7. Отраслевой регулятор в десятидневный срок направляет предложение о введении специального регулирования Президенту для принятия решения о введении специального регулирования вместе с проектом соответствующего решения Президента и приложением иных необходимых документов от инициатора.

8. Решение Президента о введении специального регулирования включает:

1) указание на цель (цели) введения специального регулирования из числа указанных в настоящем Кодексе;

2) указание на конкретные положения законов и иных нормативных правовых актов Кыргызской Республики, применительно к которым вводится специальное регулирование;

3) описание вводимых специальных правил, заключающихся в освобождении от обязанностей совершения определенных действий, соблюдения определенных процедур, запретов или ограничений;

4) указание на круг субъектов правоотношений в цифровой среде, в отношении которых вводится специальное регулирование;

5) описание видов деятельности, в отношении которых вводится специальное регулирование;

6) перечень мер, которые субъекты правоотношений в цифровой среде обязаны принимать в целях снижения возможных негативных последствий от введения специального регулирования;

7) периодичность и перечень данных, которые субъекты правоотношений в цифровой среде, применяющие специальное регулирование, должны передавать отраслевому регулятору в целях мониторинга специального регулирования;

8) другие условия, определяющие порядок действия режима специального регулирования для данного субъекта.

9. Решение о введении специального регулирования вступает в силу через 30 дней после его официального опубликования, если решением не установлен более продолжительный срок. Специальное регулирование вводится на три года, если менее продолжительный срок не запрошен инициатором, обратившимся с заявлением о введении специального регулирования.

10. Иные процедуры и условия введения специального регулирования, в том числе процедуры подачи, оценки заявлений участников, порядок мониторинга специального регулирования и отчетности участников, устанавливаются Кабинетом Министров.

Статья 17. Применение специального регулирования

1. Субъект правоотношений в цифровой среде, применяющий специальное регулирование, обязан предупреждать об этом других субъектов, с которыми он вступает в правоотношения в цифровой среде, путем указания на это на своем сайте, в приложениях, текстах договоров и иным аналогичным образом.

2. Субъект правоотношений в цифровой среде, применяющий специальное регулирование, обязан предоставлять отраслевому регулятору в обезличенной форме данные, необходимые для мониторинга специального регулирования в сроки, установленные в решении о введении специального регулирования.

3. Отраслевой регулятор в пределах своей компетенции проводит мониторинг специального регулирования, в рамках которого собирает и обобщает данные, полученные от субъектов, применяющих специальное регулирование, а также выявляет и обобщает факты нарушения прав и законных интересов субъектов правоотношений в цифровой среде в результате применения специального регулирования, в том числе на основании поступающих жалоб субъектов.

4. Если по результатам мониторинга специального регулирования отраслевой регулятор выявляет несоответствие применения специального регулирования принципам, предусмотренным настоящим Кодексом, а равно недостаточность мер, которые субъекты правоотношений в цифровой среде обязаны принимать в целях снижения возможных негативных последствий от введения специального регулирования, отраслевой регулятор вносит предложение о завершении или изменении специального регулирования.

5. Обобщенные данные мониторинга специального регулирования включаются в ежегодный отчет отраслевого регулятора.

Статья 18. Изменение и завершение специального регулирования

1. Изменение специального регулирования осуществляется в пределах срока его действия путем внесения изменений в соответствующее решение Президента.

2. Специальное регулирование завершается:

1) по истечении его срока;

2) в случае исключения из настоящего Кодекса или принятого в соответствии с ним нормативного правового акта обязанностей, временное освобождение от которых было предметом специального регулирования;

3) в случае отмены решения Президента, которым было введено специальное регулирование.

3. Президент отменяет решение о введении специального регулирования, если после его принятия выявлено несоответствие применения специального регулирования принципам и целям его введения, установленным настоящим Кодексом, а равно отсутствует результат от мер по снижению негативных последствий от его введения.

4. Если специальное регулирование завершается в связи с истечением его срока, отраслевой регулятор обязан не позднее чем за шесть месяцев до дня истечения срока опубликовать на своем сайте и направить Президенту отчет о результатах специального регулирования, содержащий предложения по внесению изменений в законодательство в целях исключения обязанностей, освобождение от которых было предметом специального регулирования, либо предложение о сохранении существующего законодательного регулирования.

Глава 4. Взаимодействие в цифровой среде

Статья 19. Правовые основы взаимодействия в цифровой среде

1. Субъекты правоотношений в цифровой среде вправе взаимодействовать с использованием объектов правоотношений в цифровой среде, владельцами (поставщиками) которых они являются. В случаях, установленных законом, субъекты правоотношений в цифровой среде обязаны взаимодействовать в порядке, установленном настоящим Кодексом, принятыми в соответствии с ним нормативными правовыми актами или правилами соответствующего цифрового сообщества.

2. Взаимодействие в цифровой среде может являться публичным, частно-публичным или частным.

3. Взаимодействие является публичным, если один из участников может принимать решения или предъявлять требования об обработке данных, обязательные для выполнения другими участниками взаимодействия. Порядок публичного взаимодействия, в том числе порядок обработки данных в ходе публичного взаимодействия, определяется законом, предусматривающим такое публичное взаимодействие.

4. Взаимодействие является частно-публичным в следующих случаях:

1) при осуществлении государственно-частного партнерства в соответствии с законодательством Кыргызской Республики о государственно-частном партнерстве;

2) при участии в нацэкосистеме;

3) при взаимодействии операторов телекоммуникаций с использованием их телекоммуникационных сетей (далее - межсетевое соединение) с оператором телекоммуникаций, признанным хозяйствующим субъектом, занимающим доминирующее положение в соответствии с антимонопольным законодательством, в случаях, установленных частью 6статьи 189настоящего Кодекса;

4) при предоставлении телекоммуникационных сервисов в особых условиях в соответствии с настоящим Кодексом.

5. Взаимодействие в случаях, не указанных в частях 3 и 4 настоящей статьи, в том числе межсетевое соединение без участия оператора телекоммуникаций, признанного хозяйствующим субъектом, занимающим доминирующее положение в соответствии с антимонопольным законодательством, является частным. Частное взаимодействие осуществляется на основании соглашений между субъектами правоотношений в цифровой среде.

6. Частно-публичное взаимодействие осуществляется на основании соглашения, заключаемого в порядке, установленном настоящей главой Кодекса с учетом положений законодательства о государственно-частном партнерстве (для взаимодействия при осуществлении государственно-частного партнерства) и положений настоящего Кодекса о взаимодействии в соответствующих сферах отношений в цифровой среде.

7. Сделки между участниками взаимодействия по поводу товаров, работ, услуг, интеллектуальной собственности или объектов правоотношений в цифровой среде совершаются в соответствии с гражданским законодательством. Осуществление закупок государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями, фондами и иными юридическими лицами, созданными за счет государственных средств, средств государственных органов или органов местного самоуправления (публичными участниками взаимодействия), регулируется законодательством Кыргызской Республики в сфере государственных закупок.

Статья 20. Принципы регулирования взаимодействия

1. Взаимодействие в цифровой среде должно опираться на заранее определенные, понятные и однозначные правила (принцип определенности отношений).

2. Срок взаимодействия в цифровой среде должен позволять каждому из участников достичь своих целей и задач на основе такого взаимодействия (принцип долгосрочного характера взаимодействия).

3. Взаимодействие в цифровой среде должно быть выгодным для всех его участников, включая тех, для кого оно является обязательным (принцип взаимной выгоды).

4. Взаимодействие в цифровой среде не может иметь целью или фактически приводить к ограничению прав и свобод граждан (принцип недопустимости ограничения прав и свобод).

5. Взаимодействие в цифровой среде не может иметь целью или фактически приводить к ограничению конкуренции в цифровой среде (принцип недопустимости ограничения конкуренции).

6. Взаимодействие с другими участниками не должно приводить к снижению цифровой устойчивости ни одного из них (принцип сохранения цифровой устойчивости).

7. Характер, правила и цели взаимодействия в цифровой среде должны быть открыты и доступны для остальных субъектов правоотношений в цифровой среде (принцип транспарентности взаимодействия).

Статья 21. Соглашение о взаимодействии

1. Предметом соглашения о взаимодействии является сотрудничество сторон в следующих областях:

1) обработка цифровых данных, записей и документов;

2) создание и использование цифровых ресурсов, сайтов и приложений, а также предоставление доступа к ним;

3) создание и предоставление цифровых сервисов, в том числе доверенных сервисов;

4) межсетевое соединение и взаимодействие с использованием других цифровых технологических систем.

2. Если иное не установлено настоящим Кодексом или соглашением о взаимодействии, стороны в равной степени участвуют в достижении результатов взаимодействия.

3. Если соглашение о взаимодействии предусматривает обязательства сторон по предоставлению права использования интеллектуальной собственности, условия соглашения о взаимодействии и форма его заключения должны соответствовать требованиям гражданского законодательства, предъявляемым к лицензионным договорам.

4. Условия соглашения о взаимодействии, обязывающие стороны воздерживаться от определенных действий, не могут противоречить требованиям антимонопольного законодательства.

Статья 22. Заключение соглашения о частно-публичном взаимодействии

1. Заключение соглашения является обязательным:

1) для владельцев государственных и муниципальных цифровых технологических систем - при взаимодействии в рамках нацэкосистемы;

2) для оператора телекоммуникаций, признанного хозяйствующим субъектом, занимающим доминирующее положение в соответствии с антимонопольным законодательством - при межсетевом соединении в случаях, установленных частью 6статьи 189настоящего Кодекса;

3) для операторов телекоммуникаций - при предоставлении телекоммуникационных сервисов в особых условиях в соответствии с настоящим Кодексом.

2. Соглашение о взаимодействии в цифровой среде в рамках государственно-частного партнерства заключается в порядке, предусмотренном законодательством о государственно-частном партнерстве.

3. Предложение о заключении соглашения о взаимодействии может быть направлено субъектом правоотношений в цифровой среде, имеющим право на заключение такого соглашения (управомоченной стороной) в адрес субъекта, для которого заключение такого соглашения является обязательным (обязанной стороны).

4. Обязанная сторона заключает соглашения о частно-публичном взаимодействии на равных условиях с любыми управомоченными субъектами, в том числе со своими аффилированными лицами.

5. Если соглашение о взаимодействии не заключено в течение 3 месяцев со дня получения обязанной стороной предложения от управомоченной стороны, любая из сторон вправе обратиться к отраслевому регулятору за разрешением спора о взаимодействии.

6. Соглашение о взаимодействии заключается без ограничения срока, если в предложении управомоченной стороны не указан срок, на который предлагается заключить соглашение.

Статья 23. Изменение и прекращение соглашения о взаимодействии

1. Соглашение о взаимодействии изменяется или прекращается по соглашению его сторон, а если стороны не достигли соглашения - по решению отраслевого регулятора или суда.

2. Соглашение сторон или решение о прекращении взаимодействия должно содержать:

1) указание на принадлежность прав (в том числе цифровых прав) на объекты правоотношений в цифровой среде, созданные или измененные в результате взаимодействия;

2) обязанность сторон по передаче друг другу технической документации и иных сопроводительных материалов на объекты правоотношений в цифровой среде, созданные или измененные в результате взаимодействия;

3) порядок правопреемства в отношениях с пользователями, затрагиваемыми в результате прекращения взаимодействия.

3. Соглашение о взаимодействии, заключенное на определенный срок, должно содержать условия, предусмотренные частью 2 настоящей статьи.

4. После прекращения взаимодействия стороны обязаны прекратить обработку данных в той части, в которой соглашение о взаимодействии являлось основанием для их обработки.

РАЗДЕЛ II. ПРАВООТНОШЕНИЯ В ЦИФРОВОЙ СРЕДЕ

Глава 5. Объекты правоотношений в цифровой среде

Статья 24. Виды объектов правоотношений в цифровой среде

1. К объектам правоотношений в цифровой среде относятся:

1) цифровые данные, цифровые записи (в том числе в виде цифровых документов) и цифровые ресурсы;

2) цифровые сервисы и цифровые экосистемы;

3) цифровые технологические системы, в том числе центры обработки данных и телекоммуникационные сети;

4) земли, здания, строения, сооружения и иные аналогичные объекты в части доступа к ним владельцев цифровых технологических систем.

2. В случаях, предусмотренных настоящим Кодексом, на объекты правоотношений в цифровой среде устанавливаются цифровые права, включающие в себя право доступа к объекту правоотношений в цифровой среде и право устанавливать условия доступа к нему. Цифровые права являются отчуждаемыми и могут передаваться от одного субъекта правоотношений в цифровой среде другому на основании договора. Цифровые права охраняются настоящим Кодексом.

3. Цифровые права на один и тот же объект могут принадлежать нескольким субъектам правоотношений в цифровой среде совместно. В этом случае порядок осуществления цифровых прав и распоряжения ими определяется соглашением о взаимодействии между всеми субъектами, которым они принадлежат.

4. Цифровые права осуществляются при условии соблюдения прав принципалов данных и ограничений, установленных в отношении соответствующих цифровых записей.

5. Ограничения цифровых прав, в том числе права свободного доступа к объектам цифровых прав, устанавливаются настоящим Кодексом в отношении отдельных видов объектов в целях реализации принципов регулирования отношений в цифровой среде.

6. Принудительное отчуждение или ограничение цифровых прав в отношении конкретного объекта допускается только на основании решения суда в случаях, прямо предусмотренных законодательством Кыргызской Республики.

Статья 25. Цифровые данные и цифровые записи

1. Цифровые данные свободно передаются между любыми субъектами и обрабатываются в этих целях без ограничений и не могут сами по себе являться объектом цифровых прав. Цифровые персональные данные обрабатываются по правилам, установленным настоящим Кодексом. Цифровые записи являются объектом цифровых прав их владельца, если иное не установлено настоящим Кодексом или договором между субъектами правоотношений в цифровой среде.

2. В отношении цифровых записей их владельцу принадлежат следующие цифровые права:

1) разрешать или ограничивать доступ к цифровым записям, определять порядок и условия такого доступа;

2) использовать цифровые записи, а также распространять их;

3) предоставлять цифровые записи другим лицам по договору или на ином установленном законом основании;

4) защищать свои права установленными законом способами в случае незаконного получения доступа к цифровым записям или их незаконного использования иными лицами.

3. Права на цифровые записи, представляющие собой виртуальные активы, определяются законодательством Кыргызской Республики о виртуальных активах. Права на цифровые записи, представляющие собой интеллектуальную собственность, определяются законодательством Кыргызской Республики в сфере интеллектуальной собственности.

4. Требования, относящиеся к составу или представлению цифровых данных или метаданных, либо цифровых записей, образуют соответственно формат данных или формат записи. Формат данных или формат записи могут быть предусмотрены нормативными правовыми актами или соглашением субъектов правоотношений в цифровой среде.

5. Требования к формату данных и формату записи цифровых документов определяются автором цифрового документа. Требования к формату данных и формату записи цифровых документов государственных органов, органов местного самоуправления, а также цифровых документов, являющихся обращениями в государственные органы и органы местного самоуправления, устанавливаются в соответствии с настоящим Кодексом.

Статья 26. Цифровые ресурсы

1. Владельцу цифрового ресурса принадлежат следующие цифровые права:

1) разрешать или ограничивать доступ к цифровому ресурсу, определять порядок и условия такого доступа;

2) распространять цифровые данные из цифрового ресурса;

3) использовать для идентификации цифрового ресурса любые обозначения, не запрещенные законодательством;

4) защищать свои права установленными законом способами в случае незаконного доступа к цифровому ресурсу или его незаконного использования.

2. Правила, установленные настоящим Кодексом для цифровых ресурсов, распространяются на цифровые (в том числе мобильные) приложения.

Статья 27. Цифровые сервисы

1. К цифровым сервисам относятся доступные пользователям возможности использования цифровых технологических систем в целях:

1) создания, обработки, хранения цифровых данных или доступа к ним;

2) обмена цифровыми данными с другими пользователями, в том числе путем доступа к цифровым данным, загруженным или созданным другими пользователями.

2. Предоставление цифровых сервисов и пользование ими осуществляется в соответствии с правилами, утверждаемыми поставщиком цифрового сервиса.

3. Требования к госсервисам устанавливаются настоящим Кодексом.

Статья 28. Цифровые экосистемы

1. Участниками цифровой экосистемы и соответствующего ей цифрового сообщества являются владелец цифровой экосистемы, владельцы цифровых ресурсов, поставщики цифровых сервисов и пользователи (потребители).

2. Участники цифровой экосистемы имеют право участвовать в определении правил цифровой экосистемы в порядке, определенном настоящим Кодексом и правилами цифровой экосистемы.

3. Отраслевые регуляторы и государственные органы Кыргызской Республики, уполномоченные осуществлять антимонопольное регулирование в соответствующей сфере, принимают меры, направленные на защиту и развитие конкуренции в цифровых экосистемах, в том числе путем:

1) разработки методики оценки состояния конкуренции в цифровых экосистемах;

2) определения особенностей применения общих правил конкуренции в отраслях экономики, в которых нарушения владельцами цифровых экосистем требований антимонопольного законодательства создают препятствия для развития конкуренции.

4. Пункты 1 и 2 части 3 настоящей статьи реализуются нормативными правовыми актами Кабинета Министров.

Статья 29. Цифровые технологические системы

1. К цифровым технологическим системам относятся системы обработки цифровых данных (в том числе центры обработки данных и системы искусственного интеллекта) и телекоммуникационные сети. Отношения по созданию, построению, размещению, эксплуатации цифровых технологических систем регулируются настоящим Кодексом. Настоящий Кодекс применяется также к отношениям по размещению и использованию технических средств, входящих в цифровые технологические системы (элементов цифровых технологических систем), и к регулированию сервисов, предоставляемых с использованием цифровых технологических систем.

2. Цифровые технологические системы могут являться государственными, муниципальными или частными. Государственные и муниципальные цифровые технологические системы создаются для предоставления госсервисов государственными органами и органами местного самоуправления. Цифровые технологические системы, созданные в иных целях, являются частными системами.

3. Цифровые технологические системы создаются и эксплуатируются их владельцем (владельцами) либо пользователями совместно на основании согласованных ими правил.

4. Если иное не установлено настоящим Кодексом, установление обязательных требований к цифровым технологическим системам, а также подтверждение соответствия установленным требованиям регулируются законодательством Кыргызской Республики в сфере технического регулирования.

5. Размещение и эксплуатация цифровых технологических систем, а также предоставление сервисов с их использованием регулируются гражданским законодательством с учетом особенностей, установленных настоящим Кодексом.

Глава 6. Субъекты правоотношений в цифровой среде

Статья 30. Правовой статус субъектов правоотношений в цифровой среде

1. Кыргызская Республика и другие государства, государственные органы, органы местного самоуправления и должностные лица, а также физические и юридические лица имеют неотъемлемое право быть субъектами правоотношений в цифровой среде, а также иные права, предусмотренные настоящим Кодексом и правилами цифровых сообществ, и несут связанные с этим обязанности.

2. Субъекты правоотношений в цифровой среде обладают следующими цифровыми правами:

1) право на доступ к цифровым данным, принципалами которых они являются;

2) право создавать, распространять и использовать цифровые данные, обрабатывать их любым способом, не запрещенным законодательством, цифровые права на созданные или полученные иным образом объекты правоотношений в цифровой среде;

3) право создавать цифровые сообщества и участвовать в определении правил для них;

4) право определять свою идентичность (в том числе путем указания имени, наименования, иных идентификаторов) в рамках цифрового сообщества;

5) право по своему выбору продолжать участвовать в цифровом сообществе или выйти из него с возможностью удалить любые данные, относящиеся к их идентичности в рамках цифрового сообщества, если обязанность сообщества хранить некоторые данные не установлена законом.

3. Субъекты правоотношений в цифровой среде могут выступать в качестве владельцев цифровых записей, цифровых ресурсов, цифровых технологических систем или экосистем, поставщиков цифровых сервисов, принципалов данных, пользователей, обработчиков либо ином статусе, предусмотренном настоящим Кодексом, правилами цифровых сообществ или договорами субъектов правоотношений в цифровой среде.

4. Все субъекты правоотношений в цифровой среде имеют право на защиту своих прав, предусмотренных настоящим Кодексом.

5. Субъекты правоотношений в цифровой среде не вправе допускать незаконную дискриминацию других субъектов правоотношений в цифровой среде и незаконное ограничение конкуренции в цифровой среде.

Статья 31. Владелец цифровых записей

1. Владелец цифровых записей обязан обеспечить полноту, достоверность и актуальность цифровых записей в той мере, в которой это необходимо для целей их использования.

2. Владельцу цифровых записей принадлежат цифровые права на его цифровые записи, предусмотренные настоящим Кодексом.

3. Владелец цифровых записей обязан:

1) содействовать иным лицам в осуществлении принадлежащего им права на доступ к цифровым данным;

2) ограничивать доступ к цифровым записям, если такая обязанность установлена законом, иными нормативными правовыми актами или соглашением сторон;

3) размещать цифровые записи на материальных носителях, расположенных на территории Кыргызской Республики в случаях, предусмотренных настоящим Кодексом.

4. Владелец цифровых записей вправе, если иное не предусмотрено законом, обусловить предоставление доступа к цифровым записям другому лицу с обязанностью этого лица не раскрывать содержание таких цифровых записей третьим лицам и не распространять их (требование о соблюдении конфиденциальности). Пользователь, нарушивший требование о соблюдении конфиденциальности, обязан возместить владельцу цифровых записей убытки, причиненные таким нарушением, за исключением случаев, когда:

1) содержащаяся в цифровых записях информация является общедоступной или она стала таковой не вследствие нарушения пользователем своих обязанностей;

2) содержащаяся в цифровых записях информация была ранее самостоятельно разработана пользователем или получена от третьих лиц без требования о соблюдении ее конфиденциальности.

5. Владелец цифровых записей определяет место их обработки по своему выбору, за исключением случаев, когда место обработки цифровых записей или место нахождения цифрового ресурса прямо предусмотрено законом.

Статья 32. Владелец цифрового ресурса

1. Владельцу цифрового ресурса принадлежат цифровые права на него, предусмотренные настоящим Кодексом.

2. Владелец цифрового ресурса определяет правила использования цифрового ресурса, включающие в себя правила доступа к нему.

3. Владелец цифрового ресурса обязан соблюдать ограничения доступа к цифровым данным или ресурсам, установленные настоящим Кодексом.

4. Правила использования государственных и муниципальных цифровых ресурсов устанавливаются нормативными правовыми актами Кабинета Министров. Если иное не установлено законом, устанавливающим правила использования конкретного государственного или муниципального цифрового ресурса, доступ к нему не ограничивается.

Статья 33. Поставщик цифрового сервиса

1. Поставщик цифрового сервиса самостоятельно определяет условия пользования цифровым сервисом, если иное не установлено настоящим Кодексом.

2. Поставщик цифрового сервиса обязан сделать общедоступными на своем сайте или в приложении следующие метаданные о цифровом сервисе:

1) наименование поставщика;

2) юридический адрес поставщика;

3) контактная информация поставщика, позволяющая осуществлять прямое и эффективное обращение к поставщику;

4) сведения о регистрации поставщика в государственном или подобном публичном реестре, его регистрационный номер, или эквивалентное средство идентификации в этом реестре;

5) ссылка на применимое законодательство, устанавливающее требования к цифровому сервису;

6) меры, необходимые для подключения цифрового сервиса;

7) существующие ограничения на использование цифрового сервиса.

Статья 34. Владелец цифровой экосистемы

Владелец цифровой экосистемы обязан:

1) обеспечивать соблюдение прав и законных интересов участников цифровой экосистемы, в том числе установленных настоящим Кодексом, цифровых прав и прав принципалов данных;

2) обеспечивать возможность участия в определении правил цифровой экосистемы всем участникам цифровой экосистемы;

3) обеспечивать возможность свободного присоединения к цифровой экосистеме и свободного выхода из цифровой экосистемы с возможностью удаления всех данных, относящихся к участнику, покидающему цифровую экосистему, если обязанность хранения таких данных не предусмотрена законом;

4) обеспечивать участнику, покидающему цифровую экосистему, возможность получить копию относящихся к нему данных или, при наличии у обработчика цифровой экосистемы такой технической возможности, перенести их на другой цифровой ресурс, указанный таким участником;

5) обеспечивать равный и недискриминационный доступ для всех участников экосистемы к цифровым записям, цифровым сервисам и цифровым технологическим системам в рамках цифровой экосистемы;

6) защищать конкуренцию внутри цифровой экосистемы и не вести монополистическую деятельность в отношении других субъектов правоотношений в цифровой среде;

7) обеспечивать возможность рассмотрения споров между участниками цифровой экосистемы по равным для всех участников правилам и исполнение решений, принятых по таким спорам.

Статья 35. Владелец цифровой технологической системы

1. Права и обязанности владельцев цифровых технологических систем устанавливаются настоящим Кодексом.

2. Для владения цифровой технологической системой и ее эксплуатации не требуется получение разрешения (лицензии), за исключением случаев, установленных настоящим Кодексом.

Статья 36. Пользователь

1. Права пользователя возникают на основании нормативных правовых актов или договоров с владельцами цифровых записей, цифровых ресурсов, цифровых технологических систем, поставщиками цифровых сервисов.

2. Пользователь обязан соблюдать правила пользования, в том числе ограничения доступа, установленные законом, владельцем цифровых записей, цифрового ресурса, цифровой технологической системы, поставщиком цифрового сервиса.

Статья 37. Принципал данных

1. Принципал данных имеет право на доступ к относящимся к нему цифровым записям, а также право участвовать в определении правил доступа к таким записям и их использования в составе других объектов правоотношений в цифровой среде. Права принципала данных осуществляются и охраняются независимо от прав на эти цифровые записи. Права принципала данных неотчуждаемы и не могут быть переданы другим лицам. Права принципала данных могут быть ограничены только на основании закона и исключительно с учетом принципов регулирования отношений в цифровой среде.

2. Принципал данных в целях реализации своих прав, предусмотренных настоящим Кодексом, обязан предоставлять сведения, подтверждающие, что соответствующие цифровые записи относятся именно к нему.

Статья 38. Обработчик

1. Обработчик действует в интересах лица, поручившего осуществлять обработку цифровых записей, эксплуатацию цифровых технологических систем или предоставление цифровых сервисов, а равно осуществлять доступ к объектам правоотношений в цифровой среде (поручение на обработку).

2. Субъект правоотношений в цифровой среде, поручивший обработчику осуществление действий в своих интересах, несет ответственность за действия обработчика как за свои собственные действия.

3. В поручении на обработку должны быть определены перечень действий (операций) с цифровыми записями, цели обработки, должна быть установлена обязанность обработчика соблюдать установленные ограничения доступа к цифровым записям, цифровым технологическим системам или цифровым сервисам, а также должны быть указаны требования к обеспечению защиты объектов правоотношений в цифровой среде в соответствии с настоящим Кодексом.

Глава 7. Цифровая идентификация

Статья 39. Право на идентичность

1. Субъекты правоотношений в цифровой среде имеют неотъемлемое право определять свою идентичность (идентифицировать или не идентифицировать себя), в том числе путем выбора идентификатора.

2. В случаях, установленных законом, субъекты правоотношений в цифровой среде обязаны идентифицировать себя в порядке, установленном настоящим Кодексом, принятыми в соответствии с ним нормативными правовыми актами или правилами соответствующего цифрового сообщества.

Статья 40. Защита права на идентичность

1. Никто не может быть принужден к идентификации (в том числе путем указания конкретного идентификатора), кроме случаев, установленных настоящим Кодексом или законом.

2. Субъекты правоотношений в цифровой среде не обязаны сохранять идентичность дольше, чем это необходимо для осуществления прав и исполнения обязанностей другими участниками того же правоотношения в цифровой среде.

3. Не допускается объединение цифровых записей, содержащих идентификаторы, если такое объединение нарушает право на идентичность или лишает субъектов возможности защиты такого права.

4. Кыргызская Республика наделяет каждого своего гражданина уникальным публичным идентификатором на протяжении всей жизни, а также в соответствии со своими международными обязательствами обеспечивает возможность идентификации для граждан других государств, лиц без гражданства и организаций.

Статья 41. Отраслевые принципы цифровой идентификации

1. Государственная политика Кыргызской Республики в области цифровой идентификации направлена на выявление и устранение административных барьеров для использования цифровой идентификации, создание условий физическим и юридическим лицам для доступа к цифровой идентификации. Наличие или отсутствие у гражданина возможности цифровой идентификации не может быть условием для осуществления прав и исполнения обязанностей в цифровой среде (принцип недискриминации).

2. Цифровая идентификация должна быть доступна каждому на разумных условиях, а все связанные с цифровой идентификацией издержки должны быть пропорциональны приобретаемым в результате благам (принцип доступности).

3. Системы цифровой идентификации должны строиться на основе открытых стандартов и соответствовать принципам совместимости, переносимости данных и цифровой устойчивости, обрабатывая только те цифровые данные, которые необходимы для целей цифровой идентификации (принцип достаточности).

4. Цифровая идентификация осуществляется на основе доверия и подотчетности между субъектами правоотношений в цифровой среде. Субъекты правоотношений в цифровой среде должны иметь возможность осуществлять контроль за использованием своих данных, а также иметь гарантии независимого контроля и справедливого рассмотрения споров (принцип доверия).

Статья 42. Идентификаторы и источники цифровых данных

1. Идентификаторы и содержащие их цифровые записи обрабатываются по правилам, установленным настоящим Кодексом для персональных данных, с особенностями, предусмотренными настоящей главой Кодекса.

2. Уникальным публичным идентификатором в Кыргызской Республике является:

1) для физических лиц - персональный идентификационный номер;

2) для юридических лиц - идентификационный номер налогоплательщика.

3. Уникальные публичные идентификаторы являются общедоступными данными, обрабатываемыми в соответствии с настоящим Кодексом.

4. Выбор идентификатора для включения в цифровую запись осуществляется:

1) принципалом данных - при сборе данных о нем владельцем записей;

2) владельцем записей - при создании данных самим владельцем записей, в том числе при создании или присвоении идентификатора;

3) третьим лицом - при получении данных владельцем записей не от принципала данных.

5. Владелец записей обязан обеспечивать уникальность идентификаторов, используемых в цифровых записях.

Статья 43. Использование идентификаторов в цифровых записях

1. Цифровая запись, в которой идентификатор использован в соответствии с правилами системы цифровой идентификации, считается цифровым документом, аналогичным документу на бумажном носителе, подписанному собственноручной подписью, при выполнении одного из следующих условий:

1) идентификатор содержится в самой цифровой записи и в соответствии с правилами системы цифровой идентификации однозначно указывает на согласие лица, к которому относится идентификатор, с содержанием цифровой записи или однозначно указывает на ознакомление такого лица с содержанием цифровой записи;

2) указание идентификатора в соответствии с правилами системы цифровой идентификации было необходимым условием создания цифровой записи с использованием системы цифровой идентификации и в метаданных цифровой записи содержится однозначное указание на лицо, от имени которого была создана цифровая запись.

2. Для обращения в государственные органы и органы местного самоуправления Кыргызской Республики, в том числе для получения госсервисов, идентификаторы должны использоваться в соответствии с правилами Единой системы идентификации, утверждаемыми Кабинетом Министров.

3. Обращение и приложенные к нему материалы, образующие цифровой документ, признаются равнозначными обращению и иным материалам, подписанным собственноручной подписью и представленным на бумажном носителе, за исключением случаев, когда законом установлен запрет на обращение в государственные органы и органы местного самоуправления в форме цифровой записи.

Статья 44. Контактная информация

1. Идентификатор, являющийся контактной информацией, может использоваться для направления уведомлений в целях возникновения, изменения, прекращения правоотношений только с предварительного согласия лица, к которому относится такой идентификатор.

2. Цифровая аутентификация может осуществляться путем контакта с лицом, к которому относится контактная информация, исключительно в случаях и порядке, предусмотренных правилами системы идентификации в соответствии с настоящим Кодексом.

Статья 45. Цифровая идентификация в цифровых сообществах

1. Цифровая идентификация в цифровых сообществах осуществляется в соответствии с правилами сообщества.

2. Передача идентификаторов и содержащих их цифровых записей лицам, не являющимся участниками сообщества, не допускается, за исключением случаев, установленных законом.

Статья 46. Системы цифровой идентификации

1. Цифровая идентификация осуществляется по правилам системы цифровой идентификации, которые также должны предусматривать возможность цифровой аутентификации.

2. Правила системы цифровой идентификации должны содержать следующие положения:

1) виды участников системы цифровой идентификации;

2) виды отношений, в которых осуществляется цифровая идентификация в соответствии с данной системой цифровой идентификации;

3) перечень используемых в системе цифровой идентификации идентификаторов и способы их получения;

4) указание на владельца (владельцев) цифровых записей, содержащих идентификаторы и данные о результатах цифровой идентификации и цифровой аутентификации, либо указание на то, что такие записи представляют собой распределенный цифровой ресурс;

5) способы цифровой аутентификации (способы получения и предъявления ключа) и процедуру цифровой аутентификации;

6) порядок учета результатов цифровой идентификации и порядок обеспечения целостности информации о фактах цифровой идентификации;

7) способы и порядок публикации или иного предоставления неограниченного доступа к правилам системы цифровой идентификации;

8) запрет на передачу цифровых записей с идентификаторами лицам, не являющимся участниками системы цифровой идентификации, за исключением случаев, установленных законодательством.

3. Цифровая идентификация и цифровая аутентификация в соответствии с правилами системы цифровой идентификации являются основанием для возникновения, изменения, прекращения правоотношений, в том числе для целей доказывания.

4. Цифровая аутентификация считается подтверждением личности физического лица в случаях, когда использование соответствующей системы цифровой идентификации предусмотрено законом или соглашением сторон. При обращении за получением госсервисов или при совершении сделки цифровая аутентификация признается надлежащим волеизъявлением лица на получение такого госсервиса или совершение сделки.

5. Цифровые записи о цифровой идентификации или цифровой аутентификации не могут быть признаны не имеющими юридической силы только на том основании, что они представлены в виде цифровых данных.

Статья 47. Сервис цифровой аутентификации

1. Цифровой сервис, в рамках которого его поставщик по запросу пользователя сервиса осуществляет цифровую аутентификацию третьих лиц в соответствии с правилами системы цифровой идентификации, является сервисом цифровой аутентификации.

2. Сервис цифровой аутентификации предоставляется на основании соглашения, заключаемого между поставщиком сервиса и пользователем. Такое соглашение должно предусматривать:

1) перечень используемых идентификаторов;

2) порядок доступа к цифровым записям, необходимым для осуществления цифровой аутентификации;

3) порядок доступа к цифровым записям, содержащим данные о результатах цифровой аутентификации;

4) порядок обновления цифровых записей, на основе которых осуществляется цифровая аутентификация;

5) сферы применения или виды отношений, в которых используется сервис цифровой аутентификации, если он может использоваться в ограниченной сфере применения или в отдельных видах отношений;

6) требования, реализация которых необходима для корректной работы сервиса и использования его результатов;

7) порядок обновления и изменения сервиса;

8) порядок уведомления о несанкционированном доступе к идентификаторам, ключам или иным данным, необходимым для работы сервиса;

9) требования к обеспечению цифровой устойчивости сервиса;

10) условия о размере или порядке определения вознаграждения поставщику сервиса либо безвозмездности пользования сервисом;

11) ответственность за нарушение условий соглашения.

3. Сервисы цифровой аутентификации должны регулярно проходить аудит кибербезопасности. Информация о прохождении аудита с указанием срока прохождения следующего аудита должны быть опубликованы на сайте поставщика сервиса.

Статья 48. Государственная система биометрической идентификации Кыргызской Республики

1. Каждое физическое лицо имеет право на биометрическую регистрацию в целях цифровой идентификации и цифровой аутентификации в соответствии с настоящим Кодексом.

2. Государственная система биометрической идентификации формируется для цифровой аутентификации граждан Кыргызской Республики при проведении выборов и референдумов, получения и предоставления госсервисов и может быть использована в иных целях исключительно в случаях, прямо предусмотренных законом. В указанных случаях обработка

биометрических данных допускается только в целях цифровой аутентификации физического лица путем сравнения с его биометрическими данными, хранящимися в базах данных. Обработка биометрических данных физических лиц в целях цифровой идентификации путем их сравнения со всеми имеющимися в базах данных биометрическими данными запрещается.

3. Обработке подлежат следующие биометрические данные граждан Кыргызской Республики:

1) цифровое графическое изображение лица;

2) графическое строение папиллярных узоров пальцев обеих рук;

3) собственноручная подпись.

4. Кроме биометрических данных в Государственной системе биометрической идентификации обрабатываются следующие персональные данные:

1) персональный идентификационный номер;

2) фамилия, имя, отчество;

3) национальность (этническая принадлежность);

4) серия и номер паспорта;

5) свидетельство о рождении (для лиц, ранее не получавших паспорт гражданина Кыргызской Республики);

6) пол;

7) число, месяц, год рождения;

8) место жительства.

5. Персональные данные граждан Кыргызской Республики в Государственной системе биометрической идентификации образуют государственный цифровой ресурс биометрических данных. Владельцем государственного цифрового ресурса биометрических данных является Кыргызская Республика. Порядок биометрической регистрации и цифровой идентификации с использованием Государственной системы биометрических данных определяется Кабинетом Министров. Обработка биометрических данных в целях, не указанных в части 2 настоящей статьи, не допускается.

6. Порядок обеспечения безопасности биометрических данных при их обработке в государственном цифровом ресурсе биометрических данных, требования к материальным носителям биометрических данных и технологиям хранения таких данных вне государственного цифрового ресурса биометрических данных определяются Кабинетом Министров.

Статья 49. Единая система идентификации Кыргызской Республики

1. Единая система идентификации Кыргызской Республики используется государственными органами, органами местного самоуправления, их должностными лицами для цифровой идентификации и цифровой аутентификации должностных лиц и пользователей госсервисов. Сервис цифровой аутентификации на основе Единой системы идентификации Кыргызской Республики может использоваться юридическими лицами и индивидуальными предпринимателями в не запрещенных законом целях.

2. В Единой системе идентификации используются следующие идентификаторы:

1) для физических лиц - фамилия, имя, отчество (при наличии), дата рождения, персональный идентификационный номер, квалифицированная цифровая подпись, контактная информация (адрес электронной почты, номер мобильного устройства физического лица);

2) для юридических лиц - наименование, идентификационный номер налогоплательщика, регистрационный номер или код иностранной организации, квалифицированная цифровая подпись.

3. Идентификаторы вносятся в Единую систему идентификации в процессе их сбора от лица, к которому они относятся, а при их отсутствии присваиваются такому лицу в порядке, установленном законодательством.

4. Владельцем цифрового ресурса Единой системы идентификации является Кыргызская Республика, от имени которой действует отраслевой регулятор нацэкосистемы.

5. Порядок и процедура цифровой идентификации и цифровой аутентификации с использованием Единой системы идентификации, порядок учета результатов цифровой идентификации и порядок обеспечения целостности информации о фактах цифровой идентификации, порядок использования сервиса цифровой аутентификации на основе Единой системы идентификации определяются положением о Единой системе идентификации, утверждаемым Кабинетом Министров.

6. Обмен цифровыми записями, необходимыми для цифровой идентификации в Единой системе идентификации либо содержащими результаты цифровой аутентификации с использованием Единой системы идентификации, осуществляется в порядке межведомственного взаимодействия. При цифровой аутентификации с использованием Единой системы идентификации могут использоваться цифровые записи из Государственной системы биометрической идентификации.

Статья 50. Обезличивание персональных записей

1. Цифровые записи, не содержащие идентификаторы, считаются обезличенными и могут обрабатываться в научных, статистических и иных исследовательских целях без получения согласия принципала данных на их обработку. Обезличивание персональных записей осуществляется таким образом, чтобы для владельца записей была уничтожена связь между этими цифровыми записями и этим принципалом данных.

2. Владелец обезличенных персональных записей, обрабатывающий их в научных, статистических и иных исследовательских целях, считается действующим в своих законных интересах и должен соблюдать требования настоящего Кодекса, относящиеся к обработке персональных записей.

3. Принципал данных в целях реализации своих прав, предусмотренных настоящим Кодексом, обязан предоставлять владельцу записей сведения, подтверждающие, что соответствующие обезличенные цифровые записи относятся непосредственно к нему.

Статья 51. Ответственность за нарушение права на идентичность

1. Субъекты правоотношений в цифровой среде имеют право на возмещение вреда (в том числе морального вреда, причиненного физическим лицам) в случае нарушения их права на идентичность или лишения возможности защиты такого права, в том числе в случае их неправомерной цифровой идентификации (цифровой аутентификации), принуждения к цифровой идентификации (цифровой аутентификации) или отказа в цифровой идентификации (цифровой аутентификации). Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом правоотношений в цифровой среде убытков.

2. Субъект правоотношений в цифровой среде вправе вместо возмещения имущественного вреда и понесенных убытков требовать от нарушителя выплаты компенсации за нарушение его права на идентичность. Моральный вред возмещается в случаях и порядке, предусмотренных гражданским законодательством.

3. Размер компенсации должен составлять не менее ста расчетных показателей и может быть увеличен судом в зависимости от характера и длительности нарушения права на идентичность.

4. Порядок рассмотрения требований, предусмотренных настоящей статьей, устанавливается гражданским процессуальным законодательством.

Глава 8. Основания возникновения, изменения, прекращения правоотношений в цифровой среде

Статья 52. Цифровые записи как основания возникновения, изменения, прекращения правоотношений в цифровой среде

1. Основаниями возникновения, изменения, прекращения правоотношений в цифровой среде являются юридические факты, выраженные в цифровых записях, в том числе представленные в виде цифровых документов или в составе цифровых ресурсов.

2. Удостоверение возникновения, изменения, прекращения правоотношений в цифровой среде осуществляется в том числе с помощью доверенных сервисов.

Статья 53. Возникновение, изменение, прекращение цифровых прав

1. Цифровые права возникают в случаях, предусмотренных настоящим Кодексом, в силу создания или получения соответствующего объекта правоотношений в цифровой среде. Для возникновения цифровых прав не требуется регистрация или уведомление либо совершение иных действий.

2. Цифровые права субъектов на созданные ими объекты правоотношений в цифровой среде принадлежат каждому из этих субъектов, самостоятельно создавших одинаковые или сходные объекты. Тождество или сходство объектов цифровых прав, принадлежащих разным субъектам, само по себе не является нарушением цифровых прав другого субъекта.

3. Принадлежность цифровых прав может подтверждаться метаданными, в том числе содержащимися в составе распределенных цифровых ресурсов. В случае спора о принадлежности цифровых прав на цифровые записи или цифровые ресурсы обязанность доказывать наличие цифровых прав возлагается на владельца соответственно цифровых записей или цифровых ресурсов.

4. При отчуждении цифровых прав, в том числе на основании решения суда, они не прекращаются, а переходят к новому владельцу.

Статья 54. Возникновение, изменение, прекращение прав принципала данных

1. Права принципала данных возникают в силу наличия связи между ним и относящимися к нему данными.

2. Для возникновения и осуществления принципалом данных своих прав не требуются уведомление, регистрация или совершение иных действий, однако владелец цифровых записей вправе потребовать от принципала данных доказательств того, что такие цифровые записи относятся к этому принципалу.

3. Права принципала данных прекращаются в случаях:

1) уничтожения цифровых записей, которые относятся к этому принципалу;

2) обезличивания цифровых записей таким образом, чтобы была уничтожена связь между этими цифровыми записями и этим принципалом данных.

Статья 55. Доверенные цифровые сервисы

1. К доверенным цифровым сервисам относятся:

1) сервисы цифровой аутентификации;

2) сервисы цифровых подписей;

3) сервисы цифровых архивов;

4) сервисы гарантированной доставки сообщений;

5) сервисы аутентификации сайтов.

2. Требования к доверенным цифровым сервисам устанавливаются настоящим Кодексом.

Статья 56. Признание иностранных доверенных цифровых сервисов

1. Доверенные цифровые сервисы, соответствующие требованиям, установленным в других государствах (далее - иностранные доверенные сервисы), признаются доверенными сервисами в соответствии с настоящим Кодексом в случаях, если:

1) иностранный доверенный сервис включен в Реестр иностранных доверенных цифровых сервисов, который формируется и ведется отраслевым регулятором нацэкосистемы;

2) судом в решении по делу установлено, что иностранный доверенный сервис, использованный стороной, соответствует критериям, установленным частью 3 настоящей статьи.

2. Решение о включении иностранного доверенного сервиса в реестр принимается отраслевым регулятором нацэкосистемы. В решении отраслевого регулятора нацэкосистемы о включении или отказе во включении иностранного доверенного сервиса в реестр должны быть указаны основания такого решения. Отказ от признания иностранного доверенного сервиса доверенным может быть обжалован в суде.

3. Основанием для решения отраслевого регулятора нацэкосистемы о включении в Реестр иностранных доверенных цифровых сервисов, а также основанием для вынесения судом решения о соответствии иностранного доверенного сервиса установленным требованиям является его соответствие одновременно следующим критериям:

1) фактическое соответствие иностранного доверенного сервиса требованиям настоящего Кодекса, в том числе по результатам проведенной экспертизы;

2) соответствие цифрового сервиса общепризнанной международной практике, относящейся к доверенным сервисам и содержащей требования, эквивалентные или более высокие, чем требования настоящего Кодекса, прежде всего в части раскрытия информации, документирования, цифровой устойчивости, технического контроля и надзора;

3) наличие сертификатов или заключений о соответствии, выданных другими государствами или организациями;

4) наличие соглашения между субъектами правоотношений в цифровой среде, предусматривающего использование иностранного доверенного сервиса и последствия такого использования.

4. Решение суда о признании иностранного доверенного сервиса фактически соответствующим требованиям, установленным настоящим Кодексом, является основанием для включения в Реестр иностранных доверенных цифровых сервисов.

5. Признание иностранных доверенных сервисов цифровых подписей осуществляется только если в отношении них обеспечивается признание подлинности цифровой подписи в соответствии состатьей 140настоящего Кодекса.

Статья 57. Особенности автоматического принятия решений на основе цифровых данных

1. Субъекты правоотношений в цифровой среде вправе автоматизировать принятие решений на основе цифровых данных таким образом, чтобы результаты обработки цифровых данных формировались и использовались для возникновения, изменения, прекращения правоотношений без участия человека (автоматические решения).

2. Принципалы данных, интересы которых затрагиваются автоматическими решениями, порождающими правовые последствия для принципала или схожим образом существенно влияющими на него, вправе потребовать от субъекта, использующего автоматические решения:

1) прекратить принятие автоматических решений в отношении данного принципала данных;

2) пересмотреть с участием человека автоматические решения, принятые ранее в отношении этого принципала данных.

3. Субъект правоотношений в цифровой среде, использующий автоматическое решение, обязан выполнять требования, установленные настоящим Кодексом в отношении принятия автоматических решений в соответствующих сферах деятельности.

Статья 58. Смарт-контракт

1. Субъекты правоотношений в цифровой среде вправе на основании договора изложить все или часть условий этого договора на специальном языке программирования в виде кода, который впоследствии будет исполнен без участия сторон

при наступлении определенных условий, согласованных сторонами, подтвержденных соответствующими цифровыми данными (смарт-контракт), что влечет возникновение, изменение или прекращение отношений между сторонами.

2. Договор, предусматривающий использование смарт-контракта, должен содержать правила разрешения споров между сторонами, предусматривающие принятие решения по спору человеком.

3. Требования в отношении использования смарт-контрактов в отдельных сферах деятельности устанавливаются настоящим Кодексом и законодательством о виртуальных активах.

Глава 9. Осуществление прав и исполнение обязанностей в цифровой среде

Статья 59. Общедоступные и открытые данные

1. Цифровые данные могут использоваться любыми лицами по их усмотрению при условии соблюдения исключительных прав на объекты интеллектуальной собственности, а также ограничений, установленных законом на распространение, предоставление, использование, иную обработку отдельных видов данных или доступ к ним.

2. Цифровые записи предполагаются общедоступными, если в их метаданных не содержится указаний на ограничение доступа к ним в соответствии с законом, договором или решением обладателя.

3. Владелец цифровых записей вправе, указав это в метаданных цифровой записи, обусловить дальнейшее распространение цифровой записи обязанностью указывать себя в качестве источника данных.

Статья 60. Распространение цифровых записей и доступ к ним

1. Распространение цифровых записей осуществляется по инициативе их владельца или владельца цифрового ресурса. Доступ к цифровым записям осуществляется по инициативе пользователя.

2. Распространение цифровых записей осуществляется свободно при соблюдении требований, установленных настоящим Кодексом. Доступ к цифровым записям осуществляется на условиях, определенных владельцем соответствующих цифровых записей или владельцем цифрового ресурса.

3. Метаданные цифровых записей, которые распространяются или к которым осуществляется доступ, должны включать в себя достоверные сведения об их владельце в форме и объеме, которые достаточны для цифровой идентификации такого лица или для возможности связаться с ним в цифровой среде.

4. Лицо, распространяющее цифровые записи, обязано обеспечить пользователю возможность отказа от получения цифровых записей, если иное не установлено законом.

5. Случаи и условия обязательного распространения цифровых записей или доступа к ним устанавливаются законом.

Статья 61. Ограничение распространения цифровых записей и доступа к цифровым записям

1. Доступ к цифровым записям или их распространение могут быть ограничены в соответствии с метаданными таких записей на основании закона исключительно в следующих случаях:

1) если ограничение доступа является осуществлением цифровых прав;

2) если метаданные цифровых записей указывают на их отнесение к охраняемой законом тайне;

3) если распространение цифровых записей или доступ к ним запрещены в соответствии с законом или решением суда.

2. Вводимые ограничения должны соответствовать принципам регулирования отношений в цифровой среде. Не допускается произвольное ограничение доступа к цифровым записям и их распространение.

3. Исследователи и научные организации имеют право осуществлять доступ к цифровым записям, содержащим персональные данные или отнесенным к охраняемой законом тайне, в научных, статистических или иных исследовательских целях при условии обеспечения их конфиденциальности.

4. Уполномоченные лица, в том числе научные организации, исследователи и отраслевые регуляторы, осуществляющие в соответствии с настоящим Кодексом доступ к цифровым записям, содержащим персональные данные или отнесенным к охраняемой законом тайне, обязаны соблюдать порядок такого доступа, установленный Кабинетом Министров.

5. Лица, нарушившие установленные в соответствии с законом или решением владельца записей ограничения доступа к записям, несут установленную законом ответственность.

Статья 62. Доступ к цифровым записям в государственных и муниципальных цифровых ресурсах

Цифровые записи из государственных и муниципальных цифровых ресурсов предоставляются пользователям бесплатно и без ограничений, если иное не установлено законом. Пользователь, направляющий запрос о предоставлении таких записей, не обязан обосновывать необходимость их получения.

Статья 63. Цифровая устойчивость

1. Государственное регулирование цифровой устойчивости осуществляется в целях обеспечения непрерывности деятельности объектов и субъектов и их восстановления после инцидентов в цифровой среде с учетом практической невозможности полной защиты от них.

2. Цифровая устойчивость достигается путем реализации субъектами правоотношений в цифровой среде следующих мер:

1) обеспечение целостности и доступности объектов правоотношений в цифровой среде, конфиденциальности обрабатываемых цифровых данных;

2) осуществление мониторинга и предупреждение инцидентов в цифровой среде и обмена данными о них;

3) управление рисками в цифровой среде на основе системы управления рисками;

4) управление ресурсами, необходимыми для обеспечения непрерывности деятельности субъектов правоотношений в цифровой среде.

3. Порядок и способы обеспечения целостности, доступности и конфиденциальности объектов критической информационной инфраструктуры, порядок мониторинга инцидентов в цифровой среде и обмена данными о них устанавливаются законодательством Кыргызской Республики в сфере обеспечения кибербезопасности.

4. Отраслевые регуляторы в пределах своих полномочий обеспечивают обмен данными об инцидентах в цифровой среде, а также другими данными, влияющими на цифровую устойчивость, между субъектами правоотношений в цифровой среде. Отраслевые регуляторы в пределах своих полномочий обобщают данные, полученные в соответствии с частью 5 настоящей статьи, и обеспечивают принятие мер по предупреждению инцидентов в цифровой среде. Участники правоотношений в цифровой среде обязаны реализовывать меры, указанные соответствующим отраслевым регулятором, в целях предупреждения инцидентов в цифровой среде и снижения их негативных последствий.

5. О каждом инциденте в цифровой среде, влияющем на цифровую устойчивость или права и законные интересы субъектов правоотношений в цифровой среде, владелец записей или поставщик цифрового сервиса обязан уведомить отраслевого регулятора не позднее чем через 72 часа после обнаружения инцидента. В случае если уведомление не было сделано в течение 72 часов, его необходимо сопроводить объяснением причин задержки.

6. Обработчик обязан уведомлять владельца записей об инцидентах в срок, установленный договором между ними или правовым актом, но не позднее чем через 48 часов после обнаружения инцидента.

7. Уведомление должно содержать:

1) описание инцидента и оценку числа пользователей, на права и законные интересы которых он влияет;

2) контактную информацию ответственного за обработку персональных данных или другого лица, уполномоченного предоставлять данные об инциденте;

3) описание последствий инцидента;

4) описание принятых мер по устранению инцидента, в том числе мер, направленных на минимизацию его возможных негативных последствий.

8. Владелец записей или поставщик цифрового сервиса обязан обновлять данные в уведомлении по мере обнаружения новых сведений об инциденте или его последствиях.

Статья 64. Система управления рисками в цифровой среде

1. Система управления рисками в цифровой среде должна определять для каждого объекта правоотношений в цифровой среде, на которого она распространяется:

1) перечень рисков, включающий оценку вероятности и масштаба негативных последствий;

2) меры по управлению рисками, то есть по снижению вероятности и масштаба негативных последствий в отношении каждого из выявленных рисков;

3) порядок оценки эффективности существующей системы управления рисками и внесения в нее изменений на основе собранных данных о ее реализации.

2. Если иное не установлено законом, система управления рисками разрабатывается и реализуется владельцем (поставщиком) объекта правоотношений в цифровой среде по методике, определенной им самостоятельно с учетом общепризнанной мировой практики.

3. В случаях, установленных настоящим Кодексом и законодательством Кыргызской Республики в сфере обеспечения кибербезопасности, владельцы (поставщики) объектов правоотношений в цифровой среде обязаны провести испытания для определения наиболее подходящих мер по управлению рисками. Испытания признаются успешными, если по их результатам объект может использоваться по назначению и соответствует предъявляемым к нему требованиям.

4. Все данные о системе управления рисками, методике их внедрения и результаты испытаний системы искусственного интеллекта повышенной опасности должны быть представлены в виде цифровых записей. В части, не отнесенной законом к государственным секретам, такие сведения относятся к общедоступным цифровым данным и должны быть опубликованы на сайте владельца (поставщика) объекта правоотношений в цифровой среде.

Статья 65. Управление ресурсами

1. Субъекты правоотношений в цифровой среде самостоятельно определяют ресурсы (человеческие, финансовые, технические и др.), необходимые для обеспечения цифровой устойчивости.

2. Запрещается устанавливать требования к субъектам правоотношений в цифровой среде, выполнение которых создает угрозу для их цифровой устойчивости.

3. При принятии решений о необходимых ресурсах для обеспечения цифровой устойчивости принимаются во внимание следующие факторы:

1) уровень развития науки и техники;

2) уровень знаний и навыков людей, участвующих в создании и использовании соответствующего объекта;

3) характер, объем и цели обработки цифровых данных, предоставления цифровых сервисов или эксплуатации цифровых технологических систем;

4) жизненный цикл объектов правоотношений в цифровой среде, начиная с этапа проектирования соответствующего объекта;

5) права и законные интересы субъектов правоотношений в цифровой среде, являющихся владельцами, пользователями или потребителями соответствующего объекта.

Статья 66. Способы защиты прав субъектов правоотношений в цифровой среде

1. Защита прав субъектов правоотношений в цифровой среде осуществляется путем:

1) использования технических, организационных и правовых мер защиты принадлежащих им объектов правоотношений в цифровой среде;

2) восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения;

3) принуждения пользователя к исполнению его обязанности или законного требования обладателя;

4) возмещения убытков, в том числе причиненных нарушением законно установленных ограничений доступа к цифровым записям, а также требований о соблюдении конфиденциальности информации и об указании источника цифровых данных;

5) компенсации морального вреда;

6) неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону;

7) иными способами, предусмотренными настоящим Кодексом.

2. Меры, предусмотренные пунктами 4 и 5 части 1 настоящей статьи, не применяются в отношении поставщиков, цифровые сервисы которых заключаются:

1) в передаче цифровых данных, предоставленных другим лицом, при условии их передачи без изменений и исправлений;

2) в хранении цифровых данных и обеспечении доступа к ним при условии, что этот поставщик не знал о незаконности обрабатываемой информации.

Статья 67. Рассмотрение споров в цифровой среде

1. Решения и действия (бездействие) государственных органов и органов местного самоуправления, организаций, должностных лиц, нарушающие права субъектов правоотношений в цифровой среде, могут быть обжалованы в порядке, установленном законодательством об основах административной деятельности и административных процедурах.

2. Споры, связанные с нарушением правил цифровых сообществ, рассматриваются по правилам цифровых сообществ, которые должны предусматривать:

1) обязанность уведомления всех лиц, затрагиваемых спором, и обязанность предоставления им доступа ко всем относящихся к ним и к сути спора цифровым записям;

2) возможность для любого лица, которого затрагивает спор, высказать свои возражения относительно сути предъявляемых к нему претензий или иным образом представить свои аргументы и соответствующие доказательства относительно сути спора;

3) рассмотрение спора по существу лицом, не заинтересованным в том или ином исходе спора (независимым арбитром), либо принятие решения по спору всеми участниками цифровых сообществ путем голосования, если это предусмотрено правилами цифровых сообществ.

3. Решение по спору, вынесенное в рамках цифрового сообщества в соответствии с правилами этого цифрового сообщества, обязательно для всех участников цифрового сообщества. Сообщество участников цифровой экосистемы обеспечивает исполнение решений на базе цифровой экосистемы.

Статья 68. Ответственность за правонарушения в цифровой среде

1. Совершение правонарушений в цифровой среде влечет ответственность в соответствии с применимым законодательством. Отдельными главами настоящего Кодекса устанавливаются особенности ответственности за правонарушения, совершенные в соответствующих сферах деятельности в цифровой среде.

2. Если в результате неправомерного отказа в доступе к объектам правоотношений в цифровой среде, несвоевременного предоставления доступа, предоставления заведомо неполных, недостоверных или неактуальных цифровых записей, нарушения установленных настоящим Кодексом или договором требований по доступности и надежности цифровых сервисов и цифровых технологических систем, нарушения цифровых прав были причинены убытки, то они подлежат возмещению в соответствии с гражданским законодательством.

3. Возмещение физическому лицу морального вреда, причиненного нарушениями, указанными в части 2 настоящей статьи, осуществляется независимо от возмещения имущественного вреда и понесенных убытков.

ОСОБЕННАЯ ЧАСТЬ

РАЗДЕЛ III. ОБРАБОТКА ЦИФРОВЫХ ДАННЫХ. ЦИФРОВЫЕ РЕСУРСЫ

Глава 10. Общие положения об обработке цифровых данных

Статья 69. Основы правового регулирования обработки цифровых данных

1. Отраслевыми принципами регулирования отношений по обработке цифровых данных в Кыргызской Республике являются:

1) совокупность прав владельцев записей по своему усмотрению определять состав обрабатываемых цифровых данных, цели и способы их обработки, с одной стороны, и прав принципалов данных на доступ к своим данным, а в случаях, установленных настоящим Кодексом, также и прав на возражение против обработки и удаления данных, с другой (принцип добровольности участия);

2) обязанность субъектов правоотношений в цифровой среде при определении ими объемов обрабатываемых цифровых данных и выборе целей и способов обработки цифровых данных заботиться о соблюдении прав и законных интересов других субъектов (принцип добросовестности);

3) возможность обработки цифровых данных, созданных для определенных целей, в других целях при условии совместимости новых целей обработки с первоначальными (принцип повторного использования);

4) возможность использования цифровых данных из разных источников и переноса по усмотрению принципала данных цифровых записей между владельцами записей в силу использования совместимых форматов данных и форматов записей, обеспечивающих возможность взаимодействия без каких-либо дополнительных ограничений (принцип совместимости и переносимости).

2. Регулирование отношений по обработке цифровых данных в отдельных видах правоотношений в цифровой среде осуществляется по правилам настоящей главы с учетом требований и ограничений, установленных соответствующими главами настоящего Кодекса. Субъекты всех видов правоотношений в цифровой среде пользуются всеми правами, предусмотренными настоящей главой, и несут связанные с ними обязанности.

Статья 70. Обработка цифровых данных с использованием технологий больших данных и интернета вещей

1. Технологии, предполагающие обработку большого количества не связанных между собой и постоянно обновляющихся цифровых данных с целью анализа связей между ними (технологии больших данных), могут создаваться и использоваться в Кыргызской Республике без ограничений. Принципалы таких данных пользуются всеми правами, установленными настоящим Кодексом, в том числе в случае обезличивания данных.

2. Цифровые права на цифровые записи, создаваемые цифровыми устройствами в автоматическом режиме без участия человека (устройствами интернета вещей), принадлежат владельцам таких цифровых устройств, если иное не установлено соглашением владельца устройства с другими субъектами правоотношений в цифровой среде.

3. Лица, применяющие технологии больших данных и интернета вещей, обязаны учитывать общепризнанную международную практику при выборе форматов записей, создаваемых при использовании таких технологий.

Статья 71. Запрет недобросовестной обработки

1. Недобросовестная обработка цифровых данных не допускается.

2. Обработка цифровых данных является недобросовестной, если:

1) осуществляется обработка неполных, неточных и (или) неактуальных цифровых данных, принятие решений на основании которых будет незаконным или несправедливым для принципала данных;

2) осуществляется обработка цифровых данных, нарушающих право на идентичность и (или) ставящих принципалов данных в нарушение законодательства в неравное положение по критериям пола, расы, языка, инвалидности, этнической принадлежности, вероисповедания, возраста, политических или иных убеждений, образования, происхождения, имущественного или иного положения;

3) обработка цифровых данных нарушает принцип добровольности и приводит к избыточной обработке данных о принципале, в частности, при заключении с ним договора или предоставлении доступа к цифровому сервису;

4) возможность обработки для пользователя обусловливается действиями, которые не связаны с целями и задачами такого доступа, в том числе в случае навязывания услуг или параметров обработки данных;

5) принципалы данных и (или) пользователи не имеют полной, достоверной и актуальной информации об обработке и действиях, необходимых для ее осуществления, до начала такой обработки.

Статья 72. Обработка цифровых данных в цифровых сообществах

1. Обработка цифровых данных в цифровых сообществах осуществляется в соответствии с правилами цифрового сообщества.

2. В целях организации обработки цифровых данных в цифровом сообществе может быть определен обработчик цифровых записей. Деятельность обработчика регламентируется общедоступным правовым актом сообщества, соответствующим требованиям настоящего Кодекса. Порядок утверждения такого правового акта и порядок внесения изменений в него определяется правилами цифрового сообщества.

Статья 73. Информация об обработке и доступ к данным

1. Принципал данных имеет право на получение от владельца записей следующей информации (далее - информация об обработке):

1) подтверждение факта обработки цифровых данных, относящихся к этому принципалу;

2) правовые основания и цели обработки относящихся к нему цифровых данных;

3) наименование и место нахождения владельца записей;

4) место или места обработки относящихся к нему цифровых данных;

5) контактная информация ответственного за обработку персональных данных (если он назначен владельцем записей);

6) о лицах, которые имеют доступ к цифровым данным, относящимся к этому принципалу или которым передаются такие цифровые данные (кроме работников владельца записей);

7) о сроках обработки цифровых данных, относящихся к этому принципалу, или порядке их определения;

8) о правах принципала данных, в том числе являющегося субъектом персональных данных;

9) о последствиях отказа принципала от обработки относящихся к нему цифровых данных;

10) об автоматическом принятии решений на основе цифровых данных, включая информацию об алгоритме, а также о значимости и предполагаемых последствиях решений для принципала данных.

2. Владелец записей обязан предоставить принципалу данных информацию об обработке в следующих случаях и следующие сроки:

1) при сборе персональных данных от субъекта персональных данных - до момента получения персональных данных;

2) при получении цифровых данных из иных источников - в течение семи рабочих дней со дня получения данных владельцем записей;

3) при получении запроса принципала данных о предоставлении информации об обработке - в течение семи рабочих дней со дня получения запроса.

3. Информация об обработке должна быть предоставлена принципалу данных владельцем записей в понятной форме. Информация об обработке не может содержать персональные данные других лиц, за исключением случаев, когда имеются основания для доступа принципала данных к таким данным.

4. Принципал данных имеет право запросить доступ ко всем относящимся к нему цифровым данным, обрабатываемым владельцем записей, а владелец записей обязан предоставить такой доступ в течение семи рабочих дней со дня получения запроса от принципала данных. По выбору владельца записей в указанный срок вместо предоставления доступа к цифровым записям принципалу данных может быть предоставлена копия всех цифровых записей, относящихся к нему.

5. Владелец записей не обязан предоставлять принципалу данных информацию об обработке или доступ к относящимся к нему цифровым записям, если он может доказать, что они уже были предоставлены принципалу данных.

Статья 74. Ограничения прав принципала данных

1. Ограничение прав принципала данных на получение информации об обработке и доступе к данным о себе устанавливается законом в отношении:

1) цифровых данных, полученных в рамках оперативно-розыскной, внешней разведывательной и контрразведывательной деятельности, за исключением случаев, когда эта деятельность проводится с нарушением законодательства Кыргызской Республики;

2) цифровых данных, обработка которых осуществляется в соответствии с уголовно-процессуальным законодательством;

3) цифровых данных, обработка которых осуществляется в соответствии с законодательством Кыргызской Республики в сфере защиты государственных секретов.

2. Ограничение прав принципала данных на получение информации об обработке и доступе к данным о себе, не предусмотренное частью 1 настоящей статьи, не допускается.

3. Если владелец записей обнаружил, что при получении цифровых данных в рамках оперативно-розыскной, разведывательной или контрразведывательной деятельности было допущено нарушение законодательства Кыргызской Республики, подтвержденное судебным актом или актом органа прокуратуры, он обязан в течение семи рабочих дней направить принципалу таких данных информацию об обработке в порядке, предусмотренном настоящим Кодексом.

Статья 75. Исправление и дополнение цифровых записей

1. Владелец записей обязан вносить исправления в цифровые записи и с учетом целей их обработки дополнять их в случаях:

1) получения запроса принципала данных на исправление или дополнение относящихся к нему цифровых записей;

2) получения требования соответствующего уполномоченного государственного органа о необходимости исправления или дополнения цифровых записей;

3) получения владельцем записей новых данных, указывающих на неполноту и недостоверность цифровых записей, утрату ими актуальности.

2. Владелец записей вправе не вносить исправления и дополнения в цифровые записи, если содержащиеся в них данные являются полными, достоверными и актуальными с точки зрения целей их обработки владельцем записей.

3. Владелец записей обязан предоставить принципалу данных информацию об исправлении или дополнении относящихся к нему цифровых записей в течение семи рабочих дней со дня получения запроса принципала данных или внесения изменений и дополнений в данные по другим основаниям.

Статья 76. Перенос цифровых записей

1. Владелец цифровых записей в случае получения требования принципала данных о переносе относящихся к нему записей к другому владельцу обязан предпринять одно из следующих действий:

1) передать такие цифровые записи новому владельцу, указанному в требовании;

2) передать принципалу данных относящиеся к нему цифровые записи в формате, допускающем их перенос к новому владельцу.

2. При выборе формата для передачи владелец записей должен учитывать рекомендуемые стандарты цифровых записей, сведения о форматах, используемых новым владельцем, а также иные доступные владельцу записей сведения о форматах записей, используемых для переноса данных, в том числе указанные в запросе от принципала данных.

3. Запрос о переносе записей к другому владельцу может касаться только записей, обрабатываемых на основании договора с принципалом данных или согласия принципала данных на обработку относящихся к нему данных.

4. Отраслевой регулятор нацэкосистемы разрабатывает и публикует на своем сайте рекомендации о форматах цифровых записей и их метаданных, технических и (или) организационных решениях, направленных на обеспечение переносимости цифровых записей.

Глава 11. Обработка персональных данных

Статья 77. Правовое регулирование обработки персональных данных

1. Настоящий Кодекс применяется к любым отношениям по обработке персональных данных, в том числе в составе цифровых записей и цифровых ресурсов. Настоящий Кодекс предусматривает особенности обработки информации персонального характера, не являющейся цифровыми персональными данными.

2. Настоящий Кодекс не применяется к отношениям по обработке персональных данных физическим лицом исключительно в связи с его личными или семейными делами.

3. Нормативные правовые акты, регулирующие обработку персональных данных, противоречащие настоящему Кодексу или не опубликованные в установленном порядке, не подлежат применению.

Статья 78. Отраслевые принципы обработки персональных данных

1. Персональные данные должны обрабатываться на законных основаниях, справедливым и открытым образом в отношении субъекта персональных данных (принцип законности, справедливости, прозрачности).

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Изменение или расширение цели обработки персональных данных владельцем записей без согласия субъекта не допускается, за исключением случаев, установленных законодательством (принцип ограничения цели).

3. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки (принцип минимизации данных).

4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Владелец записей должен принимать необходимые меры по удалению или уточнению неполных или неточных персональных данных (принцип точности).

5. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством или обязательным для субъекта договором. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством (принцип ограничения хранения).

6. Обработка персональных данных должна осуществляться способом, обеспечивающим их безопасность, то есть с обязательным принятием организационных и технических мер, предотвращающих несанкционированную или незаконную обработку персональных данных, их случайное или преднамеренное уничтожение, потерю, повреждение или изменение (принцип целостности и конфиденциальности).

7. Владелец записей несет ответственность за соблюдение принципов, предусмотренных настоящей статьей, и должен быть способен подтвердить их соблюдение.

Статья 79. Основания обработки персональных данных

1. Обработка персональных данных допускается при наличии хотя бы одного из следующих оснований обработки:

1) обработка необходима для заключения или исполнения договора, в котором субъект персональных данных является стороной, представителем или иным лицом, действующим от имени стороны по договору, или выгодоприобретателем, либо для принятия мер по инициативе субъекта до заключения договора;

2) обработка необходима для выполнения владельцем записей обязанностей (полномочий), установленных законом или принятыми в соответствии с ним нормативными правовыми актами, в том числе актами в сфере официальной статистики и правилами нацэкосистемы;

3) обработка необходима для защиты жизненно важных интересов субъекта персональных данных либо иного физического лица;

4) обработка необходима для реализации владельцем записей публичных или иных общественно полезных задач, включая защиту человеческой жизни, интересы общества, гуманитарные, экологические и иные значимые цели;

5) обработка необходима для реализации законных интересов владельца записей или третьего лица и при этом не нарушаются законные интересы, права и свободы субъекта персональных данных.

2. Получение согласия субъекта на осуществление отдельных видов обработки его данных при наличии оснований обработки, предусмотренных частью 1 настоящей статьи, осуществляется в случаях, предусмотренных законом. При отсутствии оснований, предусмотренных частью 1 настоящей статьи, обработка осуществляется при условии получения согласия субъекта на обработку персональных данных и только для тех целей обработки, в отношении которых было получено согласие субъекта персональных данных.

3. Согласие ничтожно, если оно получено в ответ на запрос, который:

1) не выделен из других запросов к субъекту, в частности, в котором прямо не указано, что этот запрос является запросом на согласие;

2) не понятен и не доступен субъекту, изложен сложным языком;

3) направлен субъекту при наличии других оснований обработки, предусмотренных частью 1 настоящей статьи.

4. Согласие на обработку персональных данных должно быть добровольным, конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных в любой форме, позволяющей подтвердить факт его получения, если иное не установлено законодательством.

5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Процедура отзыва согласия не должна быть более обременительной, чем процедура предоставления согласия.

6. Выдача и отзыв согласия на обработку персональных данных могут быть совершены представителем субъекта, действующим от его имени на основании доверенности, договора, указания закона либо акта уполномоченного государственного органа или органа местного самоуправления. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает и отзывает законный представитель субъекта персональных данных. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают и отзывают наследники субъекта персональных данных.

Статья 80. Обработка специальных категорий персональных данных

1. Запрещается обработка следующих специальных категорий персональных данных:

1) раскрывающих расовое или этническое происхождение, политические взгляды, религиозные или философские воззрения либо членство в профсоюзе;

2) содержащих генетическую информацию;

3) биометрических данных для цифровой идентификации физического лица;

4) данных, касающихся здоровья, половой жизни или сексуальной ориентации физического лица.

2. Установленный частью 1 настоящей статьи запрет обработки перечисленных специальных категорий персональных данных не применяется в указанных ниже случаях, если при этом закреплены в законе и применяются меры защиты от недобросовестной обработки данных и меры предотвращения вреда субъекту персональных данных:

1) обработка необходима для заключения или исполнения договора, в котором субъект персональных данных является стороной, представителем или иным лицом, действующим от имени стороны по договору, или выгодоприобретателем, либо для принятия мер по инициативе субъекта до заключения договора;

2) обработка осуществляется на основании закона, прямо предусматривающего необходимость обработки таких персональных данных и определяющего цели их обработки;

3) обработка является необходимой для защиты жизненно важных интересов субъекта персональных данных или иного физического лица, или группы лиц;

4) осуществляется обработка персональных записей, которые субъект данных явным образом сделал общедоступными;

5) обработка осуществляется в медико-профилактических целях, целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством сохранять врачебную тайну;

6) обработка осуществляется для защиты интересов в области общественного здравоохранения, в том числе для мониторинга и защиты от опасной для жизни эпидемии и ее распространения, или в целях гуманитарной помощи;

7) обработка персональных записей членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством, для достижения законных целей, предусмотренных их учредительными документами;

8) обработка необходима в связи с осуществлением правосудия, в том числе в рамках третейского производства;

9) обработка осуществляется для защиты национальной безопасности, обороны, общественной безопасности или предотвращения, расследования и судебного рассмотрения уголовных преступлений и исполнения уголовных наказаний;

10) обработка осуществляется в соответствии с актами в сфере официальной статистики и правилами нацэкосистемы;

11) обработка осуществляется в научных или иных исследовательских целях при условии обезличивания персональных записей.

Статья 81. Особенности обработки персональных данных детей

1. Обработка персональных данных детей допускается только в случаях, перечисленных в части 2 настоящей статьи, при следующих условиях:

1) обработка осуществляется в интересах ребенка;

2) в отношении обработки применяются установленные настоящей статьей гарантии защиты основных прав и свобод детей.

2. Обработка персональных данных детей допускается, если:

1) обработка осуществляется на основании закона, прямо предусматривающего необходимость обработки персональных данных детей и определяющего цели их обработки;

2) обработка является необходимой для защиты жизненно важных интересов ребенка (субъекта персональных данных) или иного физического лица, или группы лиц;

3) обработка осуществляется в медико-профилактических целях, целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством сохранять врачебную тайну;

4) обработка осуществляется для защиты интересов в сфере общественного здравоохранения, в частности в целях защиты от опасной для жизни эпидемии и ее распространения, или в целях гуманитарной помощи;

5) обработка необходима в связи с осуществлением правосудия, в том числе в рамках третейского разбирательства;

6) обработка осуществляется для защиты национальной безопасности, обороны, общественной безопасности или предотвращения, расследования и судебного рассмотрения уголовных преступлений и исполнения уголовных наказаний;

7) обработка осуществляется в научных, статистических или иных исследовательских целях при условии принятия надлежащих мер для защиты данных и учета интересов детей либо обезличивания персональных записей.

3. При отсутствии оснований, предусмотренных частью 2 настоящей статьи, обработка персональных данных ребенка допускается только при условии получения согласия законного представителя ребенка на обработку персональных данных ребенка и для тех целей обработки, в отношении которых было получено согласие. Дети, достигшие четырнадцатилетнего возраста, вправе самостоятельно давать согласие на обработку своих персональных данных при осуществлении своих прав и исполнении обязанностей в рамках дееспособности, установленной гражданским законодательством.

4. Запрос согласия на обработку персональных данных детей и информация, связанная с обработкой персональных данных детей, должны быть изложены ясным и доступным языком, понятным для ребенка.

5. Владельцы записей обязаны принимать меры, необходимые для предотвращения незаконной обработки персональных данных детей.

Статья 82. Оценка воздействия

1. В случаях, предусмотренных частью 2 настоящей статьи, владелец записей перед обработкой персональных данных должен провести оценку воздействия. Применительно к набору схожих операций по обработке персональных данных может быть проведена единая оценка.

2. Оценка воздействия на защиту персональных данных проводится в следующих случаях:

1) при систематической и комплексной оценке личных аспектов физических лиц для целей автоматического принятия решений в отношении субъекта персональных данных, порождающих правовые последствия для физического лица или схожим образом существенно влияющих на физическое лицо;

2) при обработке специальных категорий персональных данных в отношении более чем тысячи субъектов персональных данных;

3) при систематическом автоматическом наружном мониторинге общественных мест техническими средствами.

3. Отраслевой регулятор в сфере персональных данных определяет перечень операций по обработке, для которых требуется оценка воздействия на защиту персональных данных, а также перечень операций по обработке, для которых оценка воздействия на защиту данных не требуется.

4. Оценка воздействия на защиту персональных данных включает в себя:

1) описание системы планируемых операций и целей обработки;

2) оценку соответствия целям обработки по критериям необходимости и пропорциональности операций по обработке, а также достаточности или избыточности персональных данных;

3) описание системы управления рисками.

5. Система управления рисками должна учитывать мнения субъектов персональных данных из соответствующей целевой аудитории о запланированной обработке их персональных данных.

6. Владелец записей обязан осуществить пересмотр оценки воздействия при существенном изменении набора операций или перечней персональных данных.

Статья 83. Удаление персональных записей

1. Владелец записей обязан, в том числе на основании запроса субъекта персональных данных, немедленно удалить персональные записи при наличии хотя бы одного из следующих оснований:

1) персональные записи больше не нужны для целей их обработки;

2) прекратило действие основание для обработки персональных данных (в том числе субъект персональных данных отозвал свое согласие и при этом иные основания обработки отсутствуют);

3) по результатам рассмотрения возражения субъекта персональных данных против обработки цифровых данных о нем всеми способами и для всех целей осуществления обработки, владельцем записей принято решение об удалении данных.

2. В случаях, предусмотренных частью 1 настоящей статьи, владелец записей вправе не удалять персональные данные и хранить их в целях:

1) осуществления принадлежащего ему права на свободу слова;

2) научных, в том числе исторических или статистических исследований, и архивных целях;

3) предъявления претензий и требований, их исполнения или защиты от них;

4) если обязанность хранения таких данных предусмотрена законодательством.

Статья 84. Возражение против обработки

1. Субъект персональных данных вправе направить владельцу записей возражение против обработки персональных данных о нем определенными способами или в определенных целях. Владелец записей обязан немедленно прекратить обработку персональных данных указанными способами или в указанных целях при наличии хотя бы одного из следующих оснований:

1) обработка осуществляется в целях автоматического принятия решений в отношении субъекта персональных данных;

2) обработка несправедлива по отношению к субъекту персональных данных или приводит к дискриминации по расовым, национальным, половым, возрастным, религиозным, политическим признакам;

3) возражение против обработки заявлено в рамках отказа от получения цифровых записей;

4) возражение против обработки связано с выходом субъекта из цифрового сообщества;

5) если обработка нарушает право субъекта персональных данных определять свою идентичность в рамках цифрового сообщества, кроме случаев, установленных законом.

2. Владелец записей обязан рассмотреть возражение против обработки и в течение семи рабочих дней со дня его получения направить субъекту персональных данных мотивированное решение.

3. Субъект персональных данных вправе обжаловать решение владельца записей в отраслевой регулятор в сфере персональных данных или в суд.

Статья 85. Ограничение обработки

1. Владелец записей обязан ограничить обработку цифровых записей в отношении субъекта персональных данных:

1) при получении возражения против обработки - на время рассмотрения возражения;

2) при получении требования отраслевого регулятора в сфере персональных данных об ограничении обработки - на срок, указанный в требовании;

3) при возникновении оснований для исправления или удаления персональных записей - до их исправления или удаления.

2. Владелец записей обязан с использованием имеющейся у него контактной информации проинформировать субъекта персональных данных об установлении или снятии ограничений на обработку персональных записей не позднее одного рабочего дня, следующего за днем, когда были установлены или сняты ограничения.

Статья 86. Участие обработчика

1. Обработчик осуществляет обработку персональных записей в соответствии с правовым актом или договором с их владельцем на тех же основаниях обработки персональных данных, предусмотренных настоящим Кодексом, что и владелец персональных записей.

2. Владелец записей обязан обеспечить соблюдение обработчиком требований настоящего Кодекса.

3. Обработчик не вправе привлекать другого обработчика без предварительного письменного разрешения владельца записей.

4. Договор обработчика с владельцем записей или правовой акт, в соответствии с которым привлекается обработчик, должен содержать следующие положения:

1) период, в течение которого осуществляется обработка;

2) характер и цель обработки;

3) тип персональных данных и категории субъектов персональных данных;

4) обязанность обрабатывать персональные записи только на основании письменных распоряжений владельца записей;

5) обязанность обеспечить ограничение доступа к персональным записям, в том числе путем возложения обязательств по ограничению доступа на работников обработчика и третьих лиц, имеющих доступ к цифровым технологическим системам обработчика;

6) процедуры взаимодействия владельца записей и обработчика в рамках исправления, дополнения, удаления персональных данных и ограничения их обработки;

7) порядок учета операций с персональными записями, позволяющий подтвердить исполнение обязанностей, установленных настоящим Кодексом.

5. Отраслевой регулятор в сфере персональных данных разрабатывает и публикует на своем сайте типовые (рекомендуемые) формы договора обработчика с владельцем записей и правового акта, в соответствии с которым привлекается обработчик.

Статья 87. Совместные владельцы записей

1. Владельцы записей, которым совместно принадлежат цифровые права на одни и те же персональные записи (персональные ресурсы) и которые совместно определяют цели и средства обработки, считаются совместными владельцами записей.

2. Совместные владельцы записей должны открытым образом, в том числе путем заключения договора или издания правового акта определить и опубликовать порядок совместного осуществления своих прав и исполнения обязанностей, предусмотренных настоящим Кодексом в отношении владельцев записей. Одновременно с публикацией порядка совместного осуществления прав и исполнения обязанностей должна быть опубликована контактная информация,

достаточная для того, чтобы связаться с владельцами записей в цифровой среде.

3. Обработка данных в цифровых сообществах осуществляется в соответствии с правилами сообщества, в которых должно быть определено лицо, ответственное за обработку персональных данных в цифровом сообществе.

4. Обработка данных в цифровых экосистемах осуществляется в соответствии с правилами цифровой экосистемы. Владелец цифровой экосистемы обязан обеспечить соблюдение требований настоящего Кодекса в отношении обработки персональных данных в цифровой экосистеме, должен быть способен подтвердить их соблюдение и несет ответственность за их несоблюдение.

5. Субъект персональных данных может осуществлять свои права в отношении любого из владельцев записей по своему выбору независимо от договоренностей между совместными владельцами записей.

Статья 88. Защита персональных данных

1. Владелец записей обязан осуществлять защиту персональных данных, персональных записей, персональных ресурсов.

2. В целях обеспечения цифровой устойчивости в ходе обработки персональных данных владелец записей:

1) реализует конструктивную защиту данных при проектировании цифровых технологических систем;

2) ведет учет операций с персональными записями в соответствии с рекомендациями отраслевого регулятора в сфере персональных данных;

3) определяет лицо, ответственное за обработку персональных данных в организации (для организаций с количеством работников более десяти человек), из числа работников организации или привлекаемое на основании договора;

4) организует обучение правилам и рекомендациям в сфере обработки персональных данных и факторам их эффективного применения.

3. Кабинет Министров устанавливает требования по защите персональных данных при их обработке в цифровых технологических системах в соответствии с установленными уровнями защищенности персональных данных.

Статья 89. Трансграничная передача

1. Отраслевой регулятор в сфере персональных данных утверждает и публикует на своем сайте перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. Иностранное государство может быть включено в указанный перечень при условии соответствия действующих в таком государстве норм права и применяемых мер по обеспечению защиты персональных данных положениям настоящего Кодекса.

2. Трансграничная передача персональных данных на территории иностранных государств, включенных в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Кодексом и не может быть запрещена или ограничена.

3. Владелец записей обязан до начала осуществления трансграничной передачи персональных данных убедиться в том, что иностранное государство, на территорию которого осуществляется передача персональных данных, включено в перечень, предусмотренный настоящей статьей.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами, вступившими в силу в соответствии с законодательством Кыргызской Республики;

3) предусмотренных законодательством Кыргызской Республики, если это необходимо в целях защиты основ конституционного строя Кыргызской Республики, обеспечения обороны страны и безопасности государства;

4) заключения и (или) исполнения договора, выгодоприобретателем или стороной (представителем или иным лицом, действующим от имени стороны по договору) которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия субъекта персональных данных;

6) обеспечения условиями договора, заключенного между владельцами записей или владельцем записей и обработчиком, адекватной защиты прав субъектов персональных данных. Необходимые условия договора, обеспечивающие адекватную защиту прав субъектов персональных данных, определяются отраслевым регулятором в сфере персональных данных.

5. В случае трансграничной передачи персональные данные обрабатываются в соответствии с законодательством страны, в которую они переданы.

Статья 90. Отраслевой регулятор в сфере персональных данных

1. Регулирование и надзор в сфере персональных данных осуществляются уполномоченным государственным органом, создаваемым в порядке, установленномстатьей 9настоящего Кодекса (отраслевым регулятором в сфере персональных данных). Отраслевой регулятор в сфере персональных данных должен быть независим от лиц, в отношении которых он

осуществляет свои полномочия.

2. Руководитель отраслевого регулятора в сфере персональных данных должен обладать квалификацией, опытом и знаниями, в том числе в сфере защиты персональных данных, необходимыми для осуществления полномочий и выполнения обязанностей.

3. Отраслевой регулятор в сфере персональных данных осуществляет следующие полномочия:

1) обеспечение применения настоящего Кодекса и надзор за его применением в соответствующей сфере;

2) повышение осведомленности субъектов персональных данных относительно рисков, норм, гарантий и прав, касающихся обработки персональных данных, в том числе персональных данных детей;

3) повышение осведомленности владельцев и обработчиков персональных данных об их обязательствах в соответствии с настоящим Кодексом;

4) консультирование государственных органов и организаций в отношении законодательных и административных мер, относящихся к обработке персональных данных;

5) осуществление в порядке, установленном Кабинетом Министров, аккредитации физических или юридических лиц на проведение проверок соблюдения требований в сфере персональных данных;

6) информирование субъектов данных по вопросам осуществления их прав, предусмотренных настоящим Кодексом, в том числе если это требует сотрудничества с надзорными органами других государств в этих целях;

7) рассмотрение жалоб и проведение проверок в ходе применения настоящего Кодекса в сфере персональных данных, в том числе по своей инициативе и на основе информации, полученной от другого надзорного органа или другого государственного органа. Проведение проверок субъектов предпринимательства осуществляется в соответствии с законодательством Кыргызской Республики о порядке проведения проверок субъектов предпринимательства;

8) использование профилактических, корректирующих и принудительных мер по фактам нарушений принципов и правил обработки персональных данных, прав и обязанностей в соответствии с настоящим Кодексом;

9) публикация руководств и рекомендаций по обработке персональных данных, соответствующих мерам безопасности и соблюдению настоящего Кодекса.

4. Отраслевой регулятор в сфере персональных данных ведет реестр владельцев записей, куда по мере получения вносит данные:

1) об инцидентах с персональными данными;

2) о проверках соблюдения владельцами записей и обработчиками положений настоящего Кодекса и вынесении обязательных для исполнения решений по результатам проверок;

3) о привлечении к ответственности за нарушения в сфере персональных данных.

5. Порядок ведения реестра владельцев записей определяется отраслевым регулятором самостоятельно. Доступ к реестру осуществляется посредством сайта отраслевого регулятора.

6. Отраслевой регулятор в сфере персональных данных публикует годовой отчет о деятельности и результаты своих расследований на своем сайте.

7. Отраслевой регулятор в сфере персональных данных имеет право:

1) запрашивать у физических лиц и организаций информацию, в том числе относящуюся к государственным секретам или к иной охраняемой законом тайне, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) для целей установления фактов, имеющих значение для проводимых контрольно-надзорных мероприятий, осуществлять доступ во все помещения, к документам, оборудованию, сотрудникам и контрагентам владельца персональных записей, имеющим отношение к их обработке;

3) осуществлять мониторинг обработки персональных данных государственными органами и их подведомственными организациями за исключением данных, полученных в процессе разведывательной и контрразведывательной деятельности и деятельности, связанной с обороной;

4) требовать от владельца записей уточнения, блокирования или удаления недостоверных либо полученных незаконным путем персональных данных;

5) требовать приостановления обработки персональных данных, осуществляемой с нарушением требований настоящего Кодекса;

6) обращаться в суд с исковыми заявлениями в защиту нарушенных прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

7) направлять материалы, связанные с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Кабинет Министров предложения о совершенствовании нормативного правового регулирования в сфере персональных данных. Нормативные правовые акты, принимаемые во исполнение настоящего Кодекса, направленные на осуществление проверок организаций, деятельность которых регулируется банковским законодательством, подлежат обязательному согласованию с Национальным банком Кыргызской Республики;

9) привлекать к ответственности лиц, виновных в нарушении требований настоящего Кодекса в соответствующей сфере.

8. Отраслевой регулятор в сфере персональных данных обязан исключить незаконный доступ к персональным записям, обрабатываемым в ходе осуществления им своей деятельности, и несет ответственность в случае неправомерной обработки таких персональных записей.

9. Отраслевой регулятор в сфере персональных данных обязан:

1) организовывать соблюдение прав субъектов персональных данных в соответствии с положениями настоящего Кодекса;

2) проверять соблюдение владельцами записей и обработчиками положений настоящего Кодекса в сфере обработки персональных данных и выносить обязательные для исполнения решения по результатам проверок;

3) взаимодействовать с другими государственными органами Кыргызской Республики, в том числе заключать меморандумы о совместных действиях по контролю и надзору, в целях исключения дублирования контрольно-надзорных мероприятий и учета особенностей ведения деятельности в соответствующей сфере;

4) рассматривать жалобы и обращения физических и юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий обязательные для исполнения решения по результатам рассмотрения указанных жалоб и обращений;

5) давать разъяснения по вопросам применения законодательства в сфере персональных данных по запросу физических лиц и организаций с опубликованием таких разъяснений на своем сайте;

6) разрабатывать и публиковать рекомендации по вопросам учета операций по обработке персональных данных, проведения обучающих и просветительских мероприятий в сфере персональных данных, а также примерные формы договоров, правовых актов и иных документов в сфере персональных данных.

10. Отраслевой регулятор в сфере персональных данных осуществляет сотрудничество с аналогичными органами в иностранных государствах, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

Статья 91. Особенности обработки информации персонального характера, не являющейся персональными данными

1. Информация персонального характера, не являющаяся цифровыми данными и обрабатываемая без использования цифровых устройств, должна обрабатываться с соблюдением принципов обработки, установленных настоящим Кодексом, и только при наличии предусмотренных настоящим Кодексом оснований обработки.

2. Если для реализации требований, предъявленных субъектом персональных данных, требуется изготовление копий информации персонального характера на бумажном носителе, субъект персональных данных обязан оплатить стоимость изготовления таких копий.

3. Собственник материальных носителей, содержащих информацию персонального характера, не обязан соблюдать требования настоящего Кодекса по защите персональных данных, однако обязан ограничить доступ к таким носителям и вести учет таких носителей и лиц, имеющих доступ к ним.

Глава 12. Пространственные данные

Статья 92. Пространственные данные в цифровой среде

1. Пространственные данные обеспечивают связь правоотношений в цифровой среде с инфраструктурой.

2. Пространственные данные состоят из следующих видов цифровых данных:

1) цифровые геодезические данные, то есть пригодные для обработки с использованием цифровых устройств результатов геодезической деятельности;

2) цифровые картографические данные, то есть пригодные для обработки с использованием цифровых устройств результатов картографической деятельности;

3) цифровые данные о местоположении, то есть пригодные для обработки с использованием цифровых устройств данных, включающих в себя координаты пространственных объектов.

3. Настоящий Кодекс регулирует обработку пространственных данных в рамках правоотношений в цифровой среде с учетом ограничений, установленных настоящим Кодексом и законодательством Кыргызской Республики об отдельных видах тайн. Деятельность в области геодезии и картографии, включая порядок функционирования и взаимодействия органов государственной власти Кыргызской Республики в области геодезии и картографии, регулируется законодательством Кыргызской Республики о геодезии и картографии.

4. Порядок создания и использования результатов геодезической и картографической деятельности, отнесенных к государственным секретам, устанавливается законодательством Кыргызской Республики о защите государственных

секретов.

Статья 93. Отраслевые принципы регулирования отношений по обработке пространственных данных

1. Результаты геодезической и картографической деятельности и иные данные о местоположении пространственных объектов используются субъектами правоотношений в цифровой среде в случае приведения их в форму, пригодную для обработки с использованием цифровых устройств (принцип оцифровки).

2. Пространственные данные являются основой для развития инфраструктуры Кыргызской Республики, восполнения и бережного использования природных ресурсов, охраны окружающей среды, что требует обработки полных, актуальных и достоверных пространственных данных (принцип качества).

3. Пространственные данные обрабатываются субъектами правоотношений в цифровой среде на основе доступа к ним всех заинтересованных лиц с учетом ограничений, установленных законодательством Кыргызской Республики в сфере защиты государственных секретов (принцип совместного участия в обработке).

4. Обработка пространственных данных не может нарушать неприкосновенность частной жизни, жилища, ограничивать свободу передвижения человека (принцип личной неприкосновенности).

Статья 94. Пространственные метаданные

1. Обработка пространственных записей, доступ к ним и их распространение осуществляются на основе пространственных метаданных.

2. Доступ к пространственным метаданным не может быть ограничен, если иное не установлено законодательством.

3. Владельцы картографо-геодезических фондов в Кыргызской Республике обязаны формировать и публиковать пространственные метаданные о принадлежащих им фондах в формате открытых данных, а также передавать пространственные метаданные для включения в национальный ресурс пространственных данных Кыргызской Республики.

4. Требования к пространственным метаданным устанавливаются уполномоченным государственным органом, осуществляющим функции по выработке государственной политики в сфере геодезии и картографии.

Статья 95. Национальный ресурс пространственных данных

1. Национальный ресурс пространственных данных Кыргызской Республики (далее - георесурс) является базой цифровых пространственных данных о территории Кыргызской Республики и пространственных метаданных, а также стандартов обработки и форматов цифровых пространственных данных, обеспечивающих их доступность и совместимость.

2. Георесурс не содержит данных, относящихся к государственным секретам.

3. Цифровые права на георесурс принадлежат Кыргызской Республике. От имени Кыргызской Республики права владельца георесурса осуществляет уполномоченный государственный орган, осуществляющий функции по выработке государственной политики в сфере геодезии и картографии.

4. Владелец георесурса обеспечивает полноту, достоверность и актуальность данных в георесурсе и в этих целях осуществляет взаимодействие с владельцами других государственных цифровых ресурсов.

5. Георесурс включает в себя следующие виды цифровых данных:

1) пространственные данные государственного картографо-геодезического фонда Кыргызской Республики, в том числе полученные в ходе оцифровки материалов картографо-геодезического фонда Кыргызской Республики;

2) пространственные данные, полученные в результате выполнения лицензионных договоров об использовании георесурса;

3) пространственные данные, полученные из других государственных цифровых ресурсов;

4) пространственные метаданные;

5) стандарты обработки и форматы пространственных данных.

6. Доступ к георесурсу предоставляется на основании лицензионного договора об использовании георесурса, заключаемого владельцем георесурса с пользователями в соответствии с гражданским законодательством на следующих условиях:

1) плата за предоставление доступа к георесурсу не взимается;

2) право на использование цифровых данных из георесурса предоставляется пользователю на условии предоставления им прав на использование любых пространственных данных, производных от данных, полученных из георесурса (производные пространственные данные) владельцу георесурса;

3) пользователь обязан передать владельцу георесурса производные пространственные данные в срок, не превышающий одного года с момента их создания, в формате, утвержденном уполномоченным государственным органом, осуществляющим функции по выработке государственной политики в сфере геодезии и картографии;

4) пользователь обязан передать владельцу георесурса метаданные производных пространственных данных вместе с производными пространственными данными.

Статья 96. Геосайт

1. Сайт, посредством которого осуществляется доступ к пространственным записям Кыргызской Республики и их распространение (далее - геосайт), предназначен для осуществления следующих функций:

1) поиск пространственных данных с использованием пространственных метаданных;

2) получение данных о местоположении в формате открытых данных;

3) получение доступа к форматам, стандартам и иным нормативно-техническим данным в сфере геодезии и картографии.

2. Перечень данных о местоположении, доступ к которым предоставляется в формате открытых данных с использованием геосайта, утверждается Кабинетом Министров.

3. Доступ к геосайту предоставляется бесплатно.

4. Цифровые права на геосайт принадлежат Кыргызской Республике. От имени Кыргызской Республики права владельца геосайта осуществляет уполномоченный государственный орган, осуществляющий функции по выработке государственной политики в сфере геодезии и картографии.

Статья 97. Обработка пространственных записей

1. При обработке пространственных записей их владельцы должны соблюдать права принципалов данных, в том числе:

1) право принципала на получение относящихся к нему пространственных метаданных;

2) право принципала на внесение изменений в пространственные данные в части, относящейся к такому принципалу данных, или к принадлежащим ему пространственным объектам или цифровым устройствам;

3) право требовать от владельца пространственных данных удаления относящихся к принципалу цифровых записей либо удаления любых связанных с ним идентификаторов.

2. Создание производных пространственных данных осуществляется при условии соблюдения цифровых и иных прав владельца пространственных записей, использованных для создания таких производных данных.

3. Обработка пространственных записей осуществляется независимо от прав на инфраструктуру, к которой относятся пространственные данные.

Статья 98. Обеспечение совместимости и переносимости пространственных записей

1. В целях обеспечения совместимости и переносимости цифровых пространственных записей их обработка осуществляется в соответствии с общепризнанной международной практикой и с учетом мнения участвующих субъектов правоотношений в цифровой среде.

2. Обработка пространственных записей в рамках госсервисов осуществляется в соответствии со стандартами и форматами, содержащимися в георесурсе.

3. Уполномоченный государственный орган, осуществляющий функции по выработке государственной политики в сфере геодезии и картографии, публикует на георесурсе перечень стандартов и форматов, используемых при обработке пространственных записей.

Глава 13. Цифровые реестры

Статья 99. Регулирование цифровых реестров

1. Настоящий Кодекс регулирует создание и использование цифровых реестров, подтверждающих принадлежность прав на использование следующих объектов учета:

1) элементы нацэкосистемы;

2) радиочастотный спектр;

3) нумерация.

2. Кыргызская Республика является владельцем:

1) цифрового реестра нацэкосистемы;

2) цифрового радиочастотного реестра;

3) цифрового реестра нумерации.

3. От имени Кыргызской Республики права владельца цифрового реестра нацэкосистемы осуществляет отраслевой регулятор нацэкосистемы, права владельца цифрового радиочастотного реестра и цифрового реестра нумерации - отраслевой регулятор телекоммуникаций.

4. Порядок внесения и изменения записей в цифровые реестры, владельцем которых является Кыргызская Республика, устанавливается законодательством Кыргызской Республики с учетом положений международных договоров и общепризнанной международной практики.

5. Пользователи радиочастотного спектра, нумерации, владельцы (поставщики) элементов нацэкосистемы являются принципалами записей в соответствующих цифровых реестрах.

Статья 100. Отраслевые принципы ведения цифровых реестров

1. Записи в цифровых реестрах являются общедоступными (кроме записей, отнесенных в установленном законом порядке к государственным секретам), создаются и изменяются на основе правил, установленных в соответствии с законом, и являются основанием для возникновения, изменения, прекращения правоотношений в цифровой среде (принцип публичности).

2. Записи в цифровых реестрах создаются и изменяются только по воле принципалов таких записей, изменение записи в цифровых реестрах помимо воли ее принципала возможно только на основании решения суда (принцип неотчуждаемости).

3. В отношении одного объекта учета на одной территории может быть создана только одна запись (принцип уникальности).

4. Если целевой характер прав не был зафиксирован при создании записи в цифровом реестре, подтверждаемые записью права можно осуществлять в любых целях и с использованием любых технологий (целевой принцип).

5. Записи в цифровых реестрах создаются таким образом, чтобы осуществление прав одних принципалов записей не мешало осуществлению прав других принципалов записей (принцип гармонизации).

6. Цифровые реестры должны обеспечить наиболее справедливое и эффективное распределение прав, подтверждаемых записями в них (принцип эффективности).

Статья 101. Радиочастотный реестр

1. Кыргызской Республике принадлежит исключительное право на распределение радиочастотного спектра, выделение и присвоение радиочастот в Кыргызской Республике. Распределение, выделение и присвоение частот осуществляются в соответствии с вступившими в установленном законодательством порядке в силу международными договорами, участницей которых является Кыргызская Республика, и законодательством Кыргызской Республики. Результаты распределения радиочастотного спектра закрепляются в Национальной таблице распределения радиочастот, цифровые записи о принадлежности прав на использование радиочастотного спектра, полученных в результате выделения и присвоения радиочастот, составляют радиочастотный реестр.

2. Право на использование радиочастотного спектра предоставляется на основании решения отраслевого регулятора телекоммуникаций о выделении или присвоении радиочастот, принятого в порядке, предусмотренном настоящим Кодексом, и подтверждается записью в радиочастотном реестре. Запись в реестре о праве на использование радиочастотного спектра формируется из данных, указанных в соответствующем решении отраслевого регулятора телекоммуникаций и обновляемых в случае необходимости в порядке, установленном настоящим Кодексом. В запись в реестре не включаются данные о координатах местонахождения радиоэлектронного средства или высокочастотного устройства, а равно об их технических характеристиках.

3. Право на использование радиочастотного спектра изменяется или прекращается с момента внесения изменений в соответствующую запись в порядке, предусмотренном настоящим Кодексом.

4. Владелец радиочастотного реестра обеспечивает полноту, достоверность и актуальность данных в нем и в этих целях осуществляет взаимодействие с владельцами других государственных цифровых ресурсов и с принципалами записей в радиочастотном реестре.

5. Цифровые записи в радиочастотном реестре являются общедоступными. Отраслевой регулятор телекоммуникаций обеспечивает доступ к радиочастотному реестру посредством системы цифрового взаимодействия, а также через приложение и сайт госсервисов.

Статья 102. Распределение радиочастотного спектра

1. Распределение радиочастотного спектра между радиослужбами осуществляется в соответствии с Регламентом радиосвязи Международного союза электросвязи. Результаты распределения отражаются в Национальной таблице распределения радиочастот между радиослужбами Кыргызской Республики (Национальная таблица распределения радиочастот), гармонизированной с Международной таблицей распределения радиочастот как частью Регламента радиосвязи. В любой полосе радиочастот либо ее части могут функционировать только те радиослужбы, которые указаны для данной полосы частот в Национальной таблице распределения радиочастот.

2. Изменение Национальной таблицы распределения радиочастот производится решением Национальной комиссии по радиочастотам. Изменения в Национальной таблице распределения радиочастот вступают в силу с 1 января года, следующего за истечением двух лет со дня вынесения положительного решения Национальной комиссии по радиочастотам.

3. Полосы радиочастот или их части, определенные в Национальной таблице распределения радиочастот, могут использоваться в соответствии с одной из трех следующих категорий:

1) исключительно для правительственного использования;

2) исключительно для гражданского использования;

3) для совместного правительственного и гражданского использования.

4. Настоящий Кодекс не регулирует выделение и присвоение радиочастот в полосах радиочастот для правительственного использования. Выделение и присвоение радиочастот в полосах радиочастот для совместного правительственного и гражданского использования осуществляется решением отраслевого регулятора телекоммуникаций по результатам межведомственного согласования. Выделение и присвоение радиочастот в полосах радиочастот для гражданского использования осуществляется решением отраслевого регулятора телекоммуникаций.

5. Национальная комиссия по радиочастотам осуществляет конверсию радиочастот. Меры административного, экономического или технического характера, необходимые для реализации решения Национальной комиссии по радиочастотам о конверсии, определяет и реализует отраслевой регулятор телекоммуникаций.

Статья 103. Обеспечение электромагнитной совместимости

1. Обеспечение электромагнитной совместимости является услугой отраслевого регулятора телекоммуникаций, включающей в себя:

1) проведение анализа электромагнитной совместимости радиоэлектронных средств с использованием цифрового радиочастотного реестра и при необходимости Национальной таблицы радиочастот;

2) межведомственное согласование для полос (номиналов) радиочастот совместного правительственного и гражданского использования;

3) международную координацию полосы (номинала) радиочастот или радиочастотного присвоения в случаях, предусмотренных международными договорами Кыргызской Республики;

4) выявление фактической ситуации с помехами применительно к номиналам или полосам радиочастот.

2. По результатам предоставления услуги составляется заключение отраслевого регулятора телекоммуникаций с указанием полос или номиналов радиочастот и территории, на которых они могут использоваться. Заключение является действительным в течение 180 календарных дней.

3. Проведение радиомониторинга для управления использованием радиочастотного спектра не может приводить к увеличению платы за обеспечение электромагнитной совместимости.

4. Обеспечение электромагнитной совместимости проводится однократно при выделении и частном присвоении радиочастот. При общем присвоении радиочастот обеспечение электромагнитной совместимости осуществляется ежеквартально. В заключении по результатам обеспечения электромагнитной совместимости уточняются условия, на которых допускается эксплуатация радиоэлектронных средств, закрепленные в общем присвоении.

5. Номиналы и (или) полосы радиочастот не могут использоваться на соответствующей территории в случаях электромагнитной несовместимости, отказа в межведомственном согласовании и (или) международной координации.

6. Порядок определения размера оплаты за обеспечение электромагнитной совместимости определяется Кабинетом Министров.

7. Принципалы записей, использующие радиочастотный спектр для выполнения публичных обязательств либо осуществляющие использование радиочастотного спектра для радиолюбительской службы и радиолюбительской спутниковой службы, освобождаются от платы за обеспечение электромагнитной совместимости.

Статья 104. Выделение радиочастот

1. Право использования радиочастоты или полосы радиочастот на определенной территории предоставляется решением отраслевого регулятора телекоммуникаций об их выделении.

2. Решение о выделении должно содержать:

1) номиналы или полосы радиочастот, в отношении которых предоставляется право использования радиочастотного спектра;

2) пространственные данные, однозначно определяющие территорию, в отношении которой предоставляется право использования радиочастотного спектра;

3) указание на радиослужбу в соответствии с Национальной таблицей распределения радиочастот.

3. Выделение радиочастот осуществляется по результатам торгов, если запрашиваемые радиочастоты относятся к сервисным в соответствии с решением отраслевого регулятора телекоммуникаций.

4. Отраслевой регулятор телекоммуникаций принимает решение о признании радиочастот сервисными, если они одновременно соответствуют всем следующим критериям:

1) радиочастоты относятся к категории гражданского назначения;

2) радиочастоты не используются действующими радиоэлектронными средствами;

3) право на использование радиочастоты полностью или частично не принадлежит другим лицам;

4) право на использование радиочастот не оспаривается или в отношении них не установлены ограничения или обременения, препятствующие их использованию в соответствии с назначением;

5) радиочастоты не перераспределяются в порядке, установленном настоящим Кодексом;

6) радиочастоты не предназначены для трансляции государственного телерадиовещания;

7) радиочастоты выделяются для использования в рамках технологии, предусматривающей доступ неограниченного числа пользователей к телекоммуникационным сервисам.

5. Радиочастоты выделяются сроком на 10 лет с возможностью продления. Для целей, не связанных с предоставлением телекоммуникационных сервисов, радиочастоты выделяются на срок не более 5 лет с возможностью продления.

6. Право на использование радиочастот не может быть отчуждено принципалом записи другим лицам, кроме как в порядке, предусмотренном настоящим Кодексом.

Статья 105. Присвоение радиочастот

1. Эксплуатация радиоэлектронного средства или высокочастотного устройства допускается только при наличии решения отраслевого регулятора телекоммуникаций о присвоении радиочастоты, за исключением радиоэлектронных средств и высокочастотных устройств, внесенных в перечень радиоэлектронных средств и высокочастотных устройств, для эксплуатации которых не требуется выделения или присвоения радиочастот, утверждаемый Кабинетом Министров. Решение о присвоении принимается в отношении радиочастот, распределенных в соответствии с Национальной таблицей распределения радиочастот.

2. Присвоение радиочастот радиоэлектронным средствам и высокочастотным устройствам осуществляется решением отраслевого регулятора телекоммуникаций и является частным или общим.

3. Отраслевой регулятор принимает решение об общем присвоении радиочастоты радиоэлектронным средствам, основанным на технологии, предупреждающей вредные помехи при их одновременной работе (сотовые сети, сети широкополосного доступа и иные аналогичные цифровые устройства). Во всех остальных случаях отраслевой регулятор принимает решение о частном присвоении. Использование радиоэлектронных средств в случаях, требующих международного признания таких средств, осуществляется на основании частного присвоения вне зависимости от наличия решения об общем присвоении.

4. Решение о присвоении радиочастот закрепляет следующие, указанные владельцем радиоэлектронных средств (высокочастотных устройств), условия, на которых допускается эксплуатация таких средств (устройств):

1) телекоммуникационные сервисы, для предоставления которых используются радиоэлектронные средства;

2) данные о допустимом местоположении радиоэлектронных средств (высокочастотных устройств) путем указания на координаты (для частного присвоения) или территорию (для общего присвоения), а также максимальное и минимальное количество радиоэлектронных средств на территории;

3) технические параметры радиоэлектронного средства (высокочастотного устройства).

5. Владелец радиоэлектронных средств, эксплуатирующий их в соответствии с общим присвоением, взаимодействует с отраслевым регулятором телекоммуникаций путем обмена цифровыми данными, имеющими значение для оценки электромагнитной обстановки вокруг радиоэлектронных средств, а именно:

1) данными о применяемых технологиях;

2) координатами установки радиоэлектронных средств;

3) данными о рабочих частотах;

4) данными о мощности излучения радиоэлектронного средства и параметрах антенны.

6. Присвоение радиочастоты осуществляется на срок не менее 5 лет с возможностью продления, за исключением сервисных радиочастот, в которых присвоение радиочастоты осуществляется на срок действия права на использование радиочастот в соответствии с решением об их выделении.

Статья 106. Плата за использование радиочастотного спектра

1. За использование радиочастотного спектра принципалы записей должны ежегодно вносить плату, рассчитываемую по методике, установленной Кабинетом Министров. Плата за использование радиочастотного спектра должна стимулировать принципалов записей на:

1) эффективное и экономное использование радиочастотного спектра;

2) внедрение новых цифровых технологий.

2. Методика расчета платы прямо или опосредованно учитывает следующие факторы:

1) местонахождение радиоэлектронного средства или заявленную территорию использования;

2) плотность населения;

3) ширину используемой полосы радиочастот или номинала радиочастот;

4) весовой коэффициент, включающий в себя коммерческую цену и социальный фактор;

5) расчетный показатель;

6) коэффициент эффективности использования номинала или полосы радиочастот.

3. В случаях выделения новой полосы частот или применения в пределах выделенных полос частот новых технологий, использующих радиочастотный спектр, требующих замены радиоэлектронных средств эксплуатируемой сети, для расчета ежегодной платы применяется дополнительный понижающий коэффициент, учитывающий время (не более трех лет), необходимое для развития телекоммуникационной сети.

4. Плата за использование радиочастотного спектра направляется в республиканский бюджет и принимается во внимание при определении объема финансирования деятельности отраслевого регулятора телекоммуникаций.

5. Принципалы записей освобождаются от внесения платы за определенные полосы радиочастот при использовании их исключительно для:

1) радиолюбительской службы и радиолюбительской спутниковой службы;

2) выполнения публичных обязательств, возложенных на них в соответствии с законодательством.

6. Плата за использование частотных присвоений в рамках радиочастот, выделенных в соответствии с частью 3статьи 104настоящего Кодекса, не взимается.

Статья 107. Использование радиочастотного спектра

1. Использование радиочастотного спектра в Кыргызской Республике осуществляется принципалами записей в соответствии с параметрами записей в цифровом радиочастотном реестре.

2. Принципалы записей обязаны ограничивать количество частот и ширину используемого радиочастотного спектра до минимума, требующегося для достижения целей использования радиочастотного спектра.

3. Сигналам о бедствии должен предоставляться абсолютный приоритет, на все такие данные должен быть дан немедленный ответ и незамедлительно приняты требуемые меры. Субъекты правоотношений в цифровой среде должны принимать меры по предотвращению распространения ложных или вводящих в заблуждение сигналов бедствия, срочности, безопасности или опознавания и сотрудничать в случае необходимости с другими субъектами правоотношений в цифровой среде при определении местоположения источников таких сигналов.

4. Порядок использования радиочастотного спектра в интересах национальной безопасности и обороны определяется Президентом. При использовании радиочастотного спектра в указанных целях должны соблюдаться:

1) положения части 3 настоящей статьи относительно сигналов бедствия и принятия мер для предотвращения помех;

2) положения Регламента радиосвязи Международного союза электросвязи.

Статья 108. Национальная комиссия по радиочастотам

1. Национальная комиссия по радиочастотам является коллегиальным органом, осуществляющим межведомственное согласование в процессе распределения радиочастотного спектра. Состав Национальной комиссии по радиочастотам и порядок ее работы определяются Кабинетом Министров. Председателем Национальной комиссии по радиочастотам является руководитель отраслевого регулятора телекоммуникаций.

2. Национальная комиссия по радиочастотам осуществляет ведение Национальной таблицы распределения радиочастот путем выполнения следующих задач:

1) распределение радиочастот на основе разумного баланса между гражданским и правительственным использованием радиочастотного спектра, имеющими равное значение для страны;

2) гармонизация Национальной таблицы распределения радиочастот с Международной таблицей распределения частот;

3) конверсия радиочастот;

4) формирование принципов использования радиочастотного ресурса на территории Кыргызской Республики.

3. Национальная комиссия по радиочастотам готовит предложения Кабинету Министров по внесению изменений в нормативные правовые акты для решения задач, возложенных на Национальную комиссию по радиочастотам.

4. Проекты нормативных правовых актов Кабинета Министров, затрагивающие использование радиочастотного спектра, подлежат обсуждению на Национальной комиссии по радиочастотам.

5. Национальная комиссия по радиочастотам при принятии решений руководствуется:

1) положениями настоящего Кодекса и других нормативных правовых актов Кыргызской Республики, затрагивающих использование радиочастотного спектра;

2) межправительственными и региональными соглашениями, затрагивающими использование радиочастотного спектра;

3) решениями всемирных и региональных конференций радиосвязи;

4) текущими и перспективными потребностями Кабинета Министров в радиочастотном спектре для целей национальной безопасности, обороны, охраны правопорядка и ликвидации последствий чрезвычайных ситуаций, а также для иных правительственных целей;

5) существующими и будущими потребностями операторов телекоммуникаций, средств массовой информации и других пользователей радиочастотного спектра.

6. Деятельность Национальной комиссии по радиочастотам осуществляется на безвозмездной основе. Подготовка необходимых документов, оказание организационной, методической и иной помощи Национальной комиссии по радиочастотам осуществляются отраслевым регулятором телекоммуникаций.

7. Решения Национальной комиссии по радиочастотам оформляются решением Кабинета Министров или актом государственного органа, определяемого Кабинетом Министров, и публикуются на сайте отраслевого регулятора телекоммуникаций не позднее трех рабочих дней после их принятия.

Статья 109. Цифровой реестр нумерации

1. Исключительное право на распределение нумерации, включенной в соответствии с международными обязательствами Кыргызской Республики в Национальный план нумерации, утверждаемый Кабинетом Министров, принадлежит Кыргызской Республике. Цифровые записи о принадлежности прав на использование нумерации, полученной в результате выделения диапазонов нумерации, составляют реестр нумерации.

2. Право на использование нумерации возникает, изменяется или прекращается с момента создания соответствующей записи в реестре нумерации или внесения в нее изменений в порядке, предусмотренном настоящим Кодексом.

3. Владелец цифрового реестра нумерации обеспечивает полноту, достоверность и актуальность данных в цифровом реестре нумерации и в этих целях осуществляет взаимодействие с владельцами других государственных цифровых ресурсов.

4. Цифровые записи в цифровом реестре нумерации являются общедоступными. Отраслевой регулятор телекоммуникаций обеспечивает доступ к цифровому реестру нумерации посредством системы цифрового взаимодействия, а также через приложение и сайт госсервисов.

Статья 110. Использование нумерации

1. За использование нумерации принципалы записей должны ежегодно вносить плату в размере, установленном Кабинетом Министров. Плата не взимается при использовании коротких номеров экстренными оперативными службами.

2. Использование нумерации, не внесенной в цифровой реестр нумерации, либо использование нумерации лицом, не являющимся принципалом записи, запрещается. Информация о выделении, изменении, переоформлении или изъятии нумерации не может относиться к коммерческой тайне.

3. В случае полного или частичного прекращения права на использование нумерации плата за использование нумерации не возвращается.

4. В случае принятия решения об изменении национального плана нумерации, влекущего за собой массовое изменение структуры или формата номера или кода, такое решение должно быть опубликовано не менее, чем за 2 года до даты введения планируемых изменений, а отраслевой регулятор телекоммуникаций обязан сообщить о порядке переоформления соответствующих решений о выделении нумерации всем принципалам записей, затрагиваемых решением, не позднее 3 рабочих дней после принятия такого решения.

5. Принятие решений, указанных в части 4 настоящей статьи, является основанием для изменения номеров пользователей телекоммуникационного сервиса без их согласия, с уведомлением их о сроках и причине такой замены через сайт или приложение оператора телекоммуникаций (виртуального оператора), а также путем рассылки сообщений. Уведомление должно быть сделано не менее чем за 6 месяцев до планируемого изменения номеров пользователей.

Статья 111. Цифровой реестр нацэкосистемы

1. Цифровой реестр нацэкосистемы обеспечивает возможность использования элементов нацэкосистемы, возможность их взаимодействия, а также их совместимость.

2. Цифровой реестр нацэкосистемы состоит из цифровых записей об элементах нацэкосистемы, каждая из которых содержит данные:

1) о владельце (поставщике) элемента нацэкосистемы;

2) о пользователях (потребителях) элемента нацэкосистемы;

3) о госсервисах, в рамках которых используется элемент нацэкосистемы;

4) о других элементах нацэкосистемы, с которыми данный элемент нацэкосистемы взаимодействует (взаимодействующие элементы);

5) о способах использования элемента нацэкосистемы;

6) о результатах использования элемента нацэкосистемы, в том числе во взаимодействующих элементах;

7) о лицах, ответственных за обеспечение защиты элемента нацэкосистемы, их контактную информацию;

8) о показателях, характеризующих доступность элемента нацэкосистемы (предельный период недоступности в год, сроки восстановления доступности в случае сбоя, одновременное количество пользователей);

9) об используемых форматах данных и интерфейсах обмена данными.

3. Включение объекта правоотношений в цифровой среде в цифровой реестр нацэкосистемы осуществляется на добровольной основе и без взимания платы. Владелец (поставщик) объекта правоотношений в цифровой среде обладает правами и обязанностями участника нацэкосистемы со дня включения принадлежащего ему объекта учета в цифровой реестр нацэкосистемы и до внесения в запись о соответствующем элементе нацэкосистемы данных о его исключении из числа элементов нацэкосистемы.

4. Условиями включения объекта правоотношений в цифровой среде в цифровой реестр нацэкосистемы являются:

1) обеспечение совместимости и взаимодействия объекта правоотношений в цифровой среде с другими элементами нацэкосистемы;

2) представление положительных результатов тестирования функциональности и цифровой устойчивости объекта правоотношений в цифровой среде с использованием фабрики госсервисов;

3) предоставление данных, указанных в части 2 настоящей статьи, необходимых для создания цифровой записи об элементе нацэкосистемы.

5. Отраслевой регулятор нацэкосистемы создает в цифровом реестре нацэкосистемы цифровую запись о новом элементе в течение 5 рабочих дней с момента получения от владельца объекта правоотношений в цифровой среде данных, подтверждающих выполнение условий включения объекта правоотношений в цифровой среде в цифровой реестр нацэкосистемы.

6. Изменение цифровой записи в цифровом реестре нацэкосистемы осуществляется отраслевым регулятором нацэкосистемы по обращению владельца (поставщика) соответствующего элемента нацэкосистемы. В случае исключения объекта правоотношений в цифровой среде из числа элементов нацэкосистемы соответствующие данные вносятся в запись об этом элементе.

7. Цифровые записи в цифровом реестре нацэкосистемы являются общедоступными. Отраслевой регулятор нацэкосистемы обеспечивает доступ к цифровому реестру нацэкосистемы посредством системы цифрового взаимодействия, а также через приложение и сайт госсервисов.

РАЗДЕЛ IV. ЦИФРОВЫЕ СЕРВИСЫ И ЭКОСИСТЕМЫ

Глава 14. Общие положения о цифровых сервисах

Статья 112. Правовое регулирование цифровых сервисов

1. Цифровые сервисы предоставляются пользователям по правилам, установленным поставщиками таких сервисов, с соблюдением обязательных требований, предусмотренных настоящим Кодексом.

2. Правила цифровых сервисов, установленные их поставщиками, обязаны учитывать общепризнанную международную практику при выборе технологий или способов цифровой идентификации и цифровой аутентификации пользователей и их доступа к своим данным.

3. Регулирование отношений по предоставлению сервисов цифрового благополучия, телекоммуникационных сервисов, доверенных сервисов и госсервисов осуществляется по правилам настоящей главы с учетом дополнительных требований и ограничений, установленных соответствующими главами настоящего Кодекса. Субъекты таких правоотношений пользуются всеми правами, предусмотренными настоящей главой, и несут связанные с ними обязанности.

Статья 113. Отраслевые принципы регулирования цифровых сервисов

1. Возможность пользования цифровыми сервисами должна быть доступна для всех нуждающихся в этом лиц, в том числе лиц с ограниченными возможностями здоровья (принцип инклюзивности).

2. Правовое регулирование цифровых сервисов защищает взаимосвязанные интересы поставщиков и пользователей таких сервисов в получении благ от обработки цифровых данных (принцип обоюдной защиты).

3. Деятельность поставщиков цифровых сервисов не может требовать лицензии или иного предварительного согласования со стороны уполномоченных государственных органов (принцип отсутствия предварительного разрешения).

4. Возможность пользования цифровыми сервисами не может быть обусловлена приобретением цифрового устройства пользователем у поставщика сервиса (принцип свободы пользовательских устройств).

5. Возможность пользования цифровыми сервисами не может быть обусловлена местом нахождения пользовательских данных (принцип географической недискриминации).

6. Правила пользования сервисом не должны допускать дискриминации пользователей по признаку пола, расы, языка, инвалидности, этнической принадлежности, вероисповедания, возраста, политических или иных убеждений, образования,

происхождения, имущественного или иного положения, других обстоятельств, а также, если это прямо не оговорено в пользовательском соглашении, - местонахождения пользователей или пользовательских данных, используемых пользователями цифровых устройств (принцип недискриминации пользователей).

7. Обеспечение цифровой устойчивости цифрового сервиса является совместной обязанностью поставщиков цифровых сервисов и их пользователей (принцип взаимности).

Статья 114. Пользовательское соглашение

1. Пользование цифровым сервисом осуществляется на основании соглашения между поставщиком и пользователем сервиса (пользовательское соглашение), в рамках которого пользователь обязуется соблюдать правила пользования цифровым сервисом. Пользование цифровым сервисом без пользовательского соглашения не допускается, за исключением случаев, когда правила пользования сервисом устанавливаются законом или принятыми в соответствии с ним нормативными правовыми актами.

2. Вся информация, которую поставщик цифрового сервиса обязан предоставить пользователю в соответствии с законодательством, должна быть доступна до заключения пользовательского соглашения.

3. Пользовательское соглашение в соответствии с применимым законодательством может заключаться в любой форме, позволяющей идентифицировать пользователя, а также подтвердить факт заключения соглашения и условия, на которых оно было заключено.

4. Поставщик цифрового сервиса обязан в течение всего срока действия пользовательского соглашения и трех лет после его прекращения хранить цифровые записи, позволяющие подтвердить условия пользовательского соглашения в отношении конкретного пользователя и факт исполнения пользовательского соглашения сторонами. Условия пользовательского соглашения и иные цифровые записи, относящиеся к заключению и исполнению пользовательского соглашения, должны быть доступны пользователю таким образом, чтобы он мог хранить и воспроизводить их.

5. При необходимости внесения изменений в пользовательское соглашение поставщик обязан любым доступным способом уведомить пользователя о вносимых изменениях и установить срок не менее одного месяца. Пользовательское соглашение считается измененным с даты, указанной в уведомлении, за исключением случаев получения до этого момента отказа пользователя от изменения пользовательского соглашения. Если пользователь до истечения указанного срока заявляет о своем несогласии с предложенными изменениями, пользовательское соглашение прекращается, а поставщик цифрового сервиса обязан вернуть уплаченные пользователем денежные средства, за вычетом стоимости цифрового сервиса до момента получения заявления пользователя о несогласии с вносимыми изменениями с учетом особенностей, установленных иными нормативными правовыми актами для отдельных видов цифровых сервисов.

6. Поставщик цифрового сервиса не вправе ограничивать доступ к цифровым записям, относящимся к пользовательскому соглашению или его исполнению сторонами таким образом, чтобы содержимое этих записей нельзя было автоматически перевести на государственный или официальный язык, если только эта информация уже не представлена на государственном и официальном языках.

Статья 115. Поставщики цифровых сервисов

1. Субъект правоотношений в цифровой среде, предоставляющий цифровой сервис и определяющий правила пользования таким сервисом, обязан однозначно и в понятной пользователям форме идентифицировать себя в качестве поставщика цифрового сервиса и сделать общедоступной информацию о цифровом сервисе, предусмотренную настоящим Кодексом.

2. Если в предоставлении цифрового сервиса или определении правил пользования им участвуют несколько субъектов, они обязаны определить, кто из них уполномочен на заключение пользовательского соглашения. Если иное не установлено в пользовательском соглашении, все субъекты правоотношений в цифровой среде, предоставляющие цифровой сервис и определяющие правила пользования таким сервисом, отвечают перед пользователем солидарно.

3. Поставщику цифрового сервиса запрещается:

1) осуществлять обработку цифровых данных пользователей в целях, не предусмотренных пользовательским соглашением, за исключением случаев, установленных применимым законодательством;

2) заниматься недобросовестной конкуренцией, осуществлять действия, ограничивающие конкуренцию;

3) ограничивать права пользователей, предусмотренные настоящим Кодексом и иным законодательством Кыргызской Республики, в том числе путем принятия технических мер, затрудняющих доступ к цифровым данным, необходимым пользователям для осуществления и защиты своих прав.

Статья 116. Пользователи и потребители цифровых сервисов

1. Пользователь обязан сохранять свою идентичность в течение действия пользовательского соглашения. Цифровая идентификация и цифровая аутентификация пользователя осуществляются в соответствии с правилами системы цифровой идентификации, используемой поставщиком сервиса в соответствии с настоящим Кодексом.

2. Цифровые права на цифровые записи, создаваемые пользователем при использовании цифрового сервиса, принадлежат пользователю, если иное не предусмотрено пользовательским соглашением.

3. Пользователи обязаны соблюдать права интеллектуальной собственности иных лиц при пользовании цифровыми сервисами и несут ответственность за их несоблюдение.

4. Потребителям предоставляются следующие дополнительные права:

1) право на отказ от цифрового сервиса в любое время по усмотрению потребителя с правом на возврат всех уплаченных денежных средств за вычетом стоимости цифрового сервиса до отказа потребителя от него с учетом особенностей, установленных иными нормативными правовыми актами для отдельных видов цифровых сервисов;

2) право на бесплатное получение информации, достаточной для настройки цифрового устройства потребителя в целях получения цифрового сервиса и устранения неисправностей, вызванных настройками цифрового устройства потребителя (потребительская поддержка);

3) право на удаление всех цифровых записей, относящихся к потребителю, после отказа от цифрового сервиса, за исключением цифровых записей, которые поставщик сервиса обязан хранить в соответствии с законодательством Кыргызской Республики.

Статья 117. Защита конкуренции в цифровых сервисах

1. При предоставлении цифровых сервисов к запрещенным действиям, помимо предусмотренных антимонопольным законодательством Кыргызской Республики, относятся:

1) манипуляция алгоритмом поисковой выдачи;

2) создание приоритета для собственных цифровых сервисов или товаров, работ, услуг данного поставщика;

3) возможность получения цифрового сервиса только при условии приобретения определенных товаров (цифровых устройств), работ, услуг или цифровых сервисов поставщика или иных лиц;

4) требование передачи прав на интеллектуальную собственность как условие использования цифрового сервиса;

5) ограничение возможности использовать другие цифровые сервисы или переносить цифровые записи пользователя на другие цифровые сервисы;

6) требование обязательного участия в маркетинговых акциях или иных аналогичных активностях поставщика цифровых сервисов или иных лиц;

7) создание приоритета для одних пользователей перед другими по критерию местонахождения пользователя или его цифровых данных;

8) удаление сообщений и комментариев, не содержащих информацию, распространение которой запрещено законодательством;

9) демпинг или перекрестное субсидирование.

2. Поставщик цифрового сервиса не приобретает цифровых прав или прав интеллектуальной собственности на принадлежащие пользователям объекты правоотношений в цифровой среде. Использование таких объектов допускается только при условии заключения договора на их использование в порядке, установленном настоящим Кодексом или гражданским законодательством Кыргызской Республики. Поставщик обязан хранить цифровые записи, подтверждающие факт заключения договора на использование соответствующих объектов и условия их использования.

Статья 118. Право на отказ от сервиса

1. Если пользователь в соответствии с пользовательским соглашением, настоящим Кодексом или применимым законодательством заявил о своем отказе от цифрового сервиса, поставщик цифрового сервиса обязан:

1) произвести расчет полученной по пользовательскому соглашению оплаты, расчет стоимости цифрового сервиса до момента получения сообщения об отказе и определить сумму, подлежащую возврату пользователю, либо сумму, подлежащую оплате поставщику за использованный цифровой сервис;

2) предоставить пользователю данные о цифровых записях пользователя, имеющихся у поставщика цифрового сервиса;

3) сообщить пользователю о возможных вариантах получения копии всех цифровых записей пользователя, имеющихся у поставщика цифрового сервиса, а также о возможности переноса цифровых записей на другие цифровые сервисы;

4) предоставить пользователю возможность удалить его цифровые записи и гарантировать такое удаление;

5) до момента получения решения пользователя относительно его цифровых записей - хранить все цифровые записи пользователя в неизменном виде.

2. Если поставщик цифрового сервиса после отказа пользователя не получил решения пользователя относительно его цифровых записей, поставщик цифрового сервиса обязан удалить все записи пользователя по истечении одного календарного года, следующего за годом получения отказа пользователя от цифрового сервиса.

3. Поставщик не вправе удалять цифровые записи пользователей, содержащие информацию, которую поставщик обязан хранить в соответствии с законодательством Кыргызской Республики. Поставщик обязан уведомить пользователя о составе цифровых записей, хранение которых будет продолжено.

Статья 119. Рассмотрение споров

1. Поставщик цифрового сервиса обязан обеспечить с использованием своего сайта или приложения возможность направления жалоб:

1) относительно качества цифрового сервиса;

2) на нарушения прав интеллектуальной собственности или цифровых прав;

3) на нарушения правил пользования сервисом;

4) относительно распространения цифровых записей или предоставления доступа к ним, если такие действия ограничены в соответствии с законодательством Кыргызской Республики;

5) на иные нарушения действующего законодательства Кыргызской Республики.

2. Если жалоба относится к действиям пользователей цифрового сервиса, поставщик сервиса обязан информировать каждого из них о получении жалобы и предоставить все данные, относящиеся к полученной жалобе.

3. Поставщик цифрового сервиса обязан принять меры, необходимые для устранения указанных в жалобе нарушений в срок, не превышающий пяти рабочих дней. Если для устранения указанных в жалобе нарушений требуется больший срок, поставщик сообщает об этом пользователю в течение пяти рабочих дней с обоснованием срока, требуемого для устранения нарушений. О принятых мерах поставщик цифрового сервиса обязан проинформировать заявителя тем же способом, каким была направлена жалоба, если заявитель не запросил иную форму информирования.

4. Поставщик цифрового сервиса, предоставляющего пользователям возможность обмена цифровыми данными с другими пользователями, обязан обеспечить рассмотрение споров между пользователями по правилам пользования сервисом, указанным в пользовательском соглашении и (или) опубликованным на сайте или в приложении поставщика.

5. Решения поставщика цифрового сервиса по жалобе или спору могут быть обжалованы в обязательном досудебном порядке в отраслевом регуляторе, а в случае несогласия с решением отраслевого регулятора - в суде, в соответствии с законодательством Кыргызской Республики или иным применимым законодательством на основании соглашения сторон. Отраслевой регулятор в рамках рассмотрения жалоб и споров проверяет соответствие действий сторон пользовательскому соглашению и соответствие пользовательского соглашения законодательству Кыргызской Республики. Отраслевой регулятор при вынесении решения по жалобе или спору не вправе руководствоваться положениями пользовательского соглашения, противоречащими законодательству Кыргызской Республики.

Статья 120. Ответственность

1. Поставщик цифрового сервиса вправе приостановить возможность использования сервиса пользователем, нарушающим пользовательское соглашение, до момента устранения нарушения.

2. Если иное не установлено пользовательским соглашением, поставщик цифрового сервиса несет ответственность перед пользователем за отсутствие возможности пользования цифровым сервисом в размере двойной цены сервиса, рассчитанной за каждый полный час, в течение которого цифровой сервис был недоступен пользователю. При определении размера ответственности поставщика не учитывается время проведения аварийных или ремонтно-профилактических работ в объемах и порядке, предусмотренных пользовательским соглашением.

3. При задержке в предоставлении цифрового сервиса или предоставлении цифрового сервиса ненадлежащего качества поставщик цифрового сервиса несет ответственность перед пользователем соразмерно периоду задержки или ухудшению качества цифрового сервиса в размере, не превышающем цену соответствующего цифрового сервиса за этот период.

4. В случае непредоставления пользователю данных, необходимых для расчетов за цифровой сервис в соответствующем периоде, поставщик несет ответственность перед пользователем в размере цены цифрового сервиса за этот период.

5. Вред, причиненный пользователю недоступностью для него информации, предусмотренной настоящим Кодексом, а также предоставлением цифрового сервиса ненадлежащего качества, в том числе приведшего к потере цифровых записей пользователя, подлежит возмещению в полном объеме поставщиком цифрового сервиса на основании судебного решения.

Глава 15. Сервисы цифрового благополучия

Статья 121. Правовое регулирование сервисов цифрового благополучия

1. Сервисы цифрового благополучия могут свободно создаваться и использоваться в Кыргызской Республике с учетом ограничений, установленных настоящим Кодексом.

2. Использование сервисов цифрового благополучия медицинскими организациями и частнопрактикующими медицинскими работниками регулируется законодательством Кыргызской Республики об охране здоровья граждан. Использование сервисов цифрового благополучия в рамках медицинской деятельности не должно приводить к ущемлению прав и законных интересов физических лиц.

3. В случаях если в соответствии с законодательством Кыргызской Республики оказание медико-санитарной помощи допускается при условии установления личности физического лица, цифровая аутентификация потребителя сервиса осуществляется с использованием сервисов цифровой аутентификации в соответствии с настоящим Кодексом.

4. Не допускается ограничение использования сервисов цифрового благополучия по критерию места нахождения их поставщиков, пользователей или мест обработки цифровых записей.

Статья 122. Отраслевые принципы регулирования сервисов цифрового благополучия

1. Решения, касающиеся здоровья физического лица, в том числе о диагнозе, могут приниматься только человеком (принцип принятия решения человеком).

2. Потребитель сервиса цифрового благополучия должен иметь полные данные о возможностях и ограничениях сервиса, а также условиях его использования, до начала пользования сервисом (принцип информированности потребителя).

3. Результаты работы сервиса цифрового благополучия, в том числе реализуемые автоматически, должны сопровождаться доступными для потребителя данными о последствиях использования или неиспользования каждого из результатов работы сервиса (принцип предсказуемости результата).

4. Данные, распространяемые о сервисе цифрового благополучия, не могут содержать необоснованные гарантии или заверения в улучшении качества жизни и здоровья потребителя (принцип обоснованности результата).

5. Данные о работе сервиса цифрового благополучия в отношении конкретного потребителя должны быть доступны для потребителя в виде цифровых записей (принцип подотчетности).

Статья 123. Использование цифровых сервисов для целей оказания медико-санитарной помощи

1. За исключением случаев, когда это прямо запрещено законодательством, цифровые сервисы могут использоваться в рамках оказания медико-санитарной помощи в следующих целях:

1) проведение консультаций;

2) мониторинг состояния пациента;

3) обмен опытом и взаимные консультации между медицинскими работниками;

4) проведение обучения медицинских работников;

5) соблюдение санитарно-гигиенического, санитарно-противоэпидемического режимов.

2. Цифровые записи должны учитываться при оказании медико-санитарной помощи, если они созданы в рамках цифровых сервисов.

Статья 124. Обработка данных в рамках сервисов цифрового благополучия

1. Кыргызская Республика обеспечивает обработку цифровых данных о состоянии здоровья граждан Кыргызской Республики в рамках нацэкосистемы.

2. Цифровые данные потребителей сервиса цифрового благополучия могут использоваться в целях улучшения этого сервиса для всех его потребителей.

3. Обработка поставщиком сервиса цифрового благополучия цифровых данных потребителей этого сервиса для целей других цифровых сервисов, а также передача таких данных поставщиком сервиса цифрового благополучия другим лицам (кроме обработчика) допускается только при наличии основания для обработки, предусмотренного настоящим Кодексом, а если таким основанием выступает законный интерес - исключительно при условии обезличивания данных.

4. Поставщик сервиса цифрового благополучия обязан обеспечить качество данных на основе утвержденной им методики, включающей:

1) описание способов обработки цифровых данных в целях подготовки их к использованию;

2) описание моделей и гипотез, в рамках которых используются цифровые данные;

3) предварительную оценку доступности, достаточности и пригодности необходимых цифровых данных;

4) способы проверки выборки на предвзятость (на смещение выборки и на ошибку отбора);

5) методы выявления недостатков по количеству и качеству данных, а также способы устранения этих недостатков.

5. Цифровые данные для сервисов цифрового благополучия должны быть релевантными, репрезентативными, свободными от ошибок и полными. Они должны в необходимой мере учитывать назначение цифрового сервиса и предполагаемые условия его использования, включая статистические характеристики лиц и групп потребителей сервиса.

6. Поставщик сервиса обязан сделать общедоступной методику обеспечения качества данных на своем сайте или в приложении, посредством которых осуществляется доступ к цифровому сервису.

Статья 125. Устройства цифрового благополучия

1. Требования к цифровым технологическим системам и их элементам, используемым в рамках сервисов цифрового благополучия (устройствам цифрового благополучия), а также формы подтверждения соответствия устанавливаются в соответствии с законодательством Кыргызской Республики о техническом регулировании.

2. Устройства цифрового благополучия, использование которых не связано с проникновением через естественные внешние барьеры организма (неинвазивные цифровые устройства) могут использоваться потребителями без предварительного одобрения или подтверждения соответствия.

3. Поставщик сервиса цифрового благополучия обязан сделать общедоступными на своем сайте или в приложении следующие данные об устройствах цифрового благополучия:

1) перечень цифровых устройств, которые могут быть использованы в рамках сервиса, или требования к таким устройствам;

2) правила пользования устройствами цифрового благополучия в рамках сервиса;

3) ссылки на стандарты, спецификации или иные аналогичные документы, которым соответствуют устройства и информация о подтверждении соответствия устройств положениям таких документов.

4. Поставщик сервиса цифрового благополучия обязан обеспечивать возможность использования потребителями любых устройств, соответствующих опубликованным поставщиком требованиям, без какой-либо дискриминации относительно их производителя или модели.

5. Поставщик сервиса цифрового благополучия обязан учитывать общепризнанную международную практику при определении форматов и интерфейсов обмена данными с устройствами, а также требований к устройствам.

Статья 126. Использование систем искусственного интеллекта для обеспечения цифрового благополучия

Системы искусственного интеллекта, используемые для обеспечения цифрового благополучия, относятся к системам искусственного интеллекта повышенной опасности. Поставщик сервиса цифрового благополучия, использующий системы искусственного интеллекта в рамках сервиса, обязан соблюдать требования к системам искусственного интеллекта повышенной опасности, установленные настоящим Кодексом.

Статья 127. Защита прав потребителей сервисов цифрового благополучия

1. Потребитель сервиса цифрового благополучия имеет право на возмещение вреда (в том числе морального вреда), причиненного ему в результате использования сервиса цифрового благополучия, а равно вследствие недоступности данных, которые должны быть доступны потребителям в соответствии с настоящим Кодексом. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных потребителем убытков.

2. Потребитель сервиса цифрового благополучия вправе вместо возмещения вреда и (или) компенсации морального вреда требовать от поставщика выплаты компенсации в размере от ста до четырехсот расчетных показателей. Компенсация подлежит взысканию при доказанности факта нарушения, совершенного поставщиком, и возникновения вреда у потребителя. Размер компенсации определяется по усмотрению суда исходя из характера нарушения и иных обстоятельств дела и должен быть разумным и справедливым.

3. Поставщик сервиса цифрового благополучия освобождается от возмещения вреда, если докажет, что отсутствует причинно-следственная связь между использованием его цифрового сервиса и возникновением вреда у потребителя.

Глава 16. Телекоммуникационные сервисы

Статья 128. Правовое регулирование телекоммуникационных сервисов

1. Кыргызская Республика регулирует телекоммуникационные сервисы на основе международных договоров и решений международных организаций в сфере телекоммуникаций, участницей которых является Кыргызская Республика. Термины, относящиеся к телекоммуникационным сервисам, используются в значении, установленном в документах Международного союза электросвязи, если иное не установлено настоящим Кодексом.

2. Предоставление телекоммуникационных сервисов и их регулирование должны осуществляться с учетом общепризнанной международной практики в сфере телекоммуникаций. Если законодательством Кыргызской Республики требуется подтверждение соответствия требованиям, установленным настоящим Кодексом, могут использоваться документы, полученные в соответствии с законодательством иностранных государств, если они подтверждают соответствие требованиям, которые эквивалентны или выше требований, установленных настоящим Кодексом.

Статья 129. Отраслевые принципы регулирования телекоммуникационных сервисов

1. Субъекты правоотношений в цифровой среде вправе свободно предоставлять телекоммуникационные сервисы и пользоваться ими в Кыргызской Республике (принцип свободы телекоммуникаций).

2. Регулирование телекоммуникационных сервисов обеспечивает непрерывность их предоставления для поставщиков и пользователей и недопустимость произвольного прекращения телекоммуникационных сервисов (принцип непрерывности).

3. Регулирование деятельности по предоставлению телекоммуникационных сервисов и пользованию ими обеспечивает их постоянное развитие и внедрение перспективных технологий их предоставления в соответствии с общепризнанной международной практикой (принцип развития).

4. Телекоммуникационные сервисы и их регулирование должны быть организованы таким образом, чтобы увеличивать количество пользователей, имеющих возможность взаимодействия между собой с использованием телекоммуникационных сервисов (принцип взаимодействия).

5. Устойчивое развитие телекоммуникационных сервисов и реализация принципов их регулирования возможны только при условии обеспечения совместимости сервисов и цифровых устройств, используемых для предоставления сервисов и пользования ими (принцип совместимости).

6. При предоставлении телекоммуникационных сервисов и пользовании ими обеспечивается целостность и неприкосновенность передаваемых цифровых данных, при этом поставщики телекоммуникационных сервисов не должны контролировать содержание передаваемых цифровых данных и нести ответственность в связи с их содержанием (принцип неприкосновенности).

7. Поставщики телекоммуникационных сервисов самостоятельно устанавливают цены и тарифы на телекоммуникационные сервисы с учетом требований, установленных законодательством Кыргызской Республики в сфере ценообразования (принцип свободы ценообразования).

Статья 130. Охрана тайны цифровых данных, передаваемых с помощью телекоммуникационного сервиса

1. Тайна переписки, телефонных и иных переговоров, а также других сообщений, передаваемых с помощью телекоммуникационного сервиса, охраняетсяКонституциейи настоящим Кодексом.

2. Доступ к данным, составляющим такую тайну, осуществляется только отправителями и получателями таких данных (сообщений), а также, при наличии технической возможности, лицами, задействованными в функционировании и эксплуатации телекоммуникационной сети и (или) предоставлении телекоммуникационных сервисов.

Доступ иных лиц к данным, составляющим такую тайну, допускается только в соответствии с законом и на основании судебного акта. Доступ к данным предоставляется отдельно в отношении каждого пользователя на основании, вынесенного относительно него судебного акта и на указанный в таком акте срок.

3. Запрещается несанкционированное подключение и иное вмешательство в телекоммуникационные сервисы с целью получения, изменения или иной обработки передаваемых с их использованием данных.

4. Если телекоммуникационный сервис используется в целях предоставления общего доступа к данным (в частности, при вещании или размещении на сайте), такие данные не относятся к тайне переписки, телефонных и иных переговоров, а также других сообщений, передаваемых с помощью телекоммуникационного сервиса.

Статья 131. Предоставление телекоммуникационных сервисов

1. Телекоммуникационные сервисы предоставляются круглосуточно, если иное прямо не указано в пользовательском соглашении. Поставщики телекоммуникационных сервисов обязаны принимать меры по обеспечению цифровой устойчивости телекоммуникационных сервисов, а также по своевременному выявлению и устранению перебоев в их предоставлении.

2. Поставщики телекоммуникационных сервисов обязаны информировать пользователей на своем сайте или в приложении о ремонтно-профилактических работах, которые могут повлечь перебои в предоставлении телекоммуникационного сервиса, не менее чем за 3 рабочих дня до начала их проведения.

3. При возникновении аварий или иных инцидентов, влияющих на предоставление телекоммуникационного сервиса, поставщик сервиса должен информировать пользователей на своем сайте или в приложении об инциденте, его влиянии на сервис и планируемых сроках его устранения.

4. Пользователям телекоммуникационных сервисов предоставляется круглосуточная техническая поддержка. Поставщик обязан разместить контактную информацию службы технической поддержки на своем сайте или в приложении.

5. Если стоимость телекоммуникационного сервиса рассчитывается в зависимости от объема его использования, поставщик обязан опубликовать на своем сайте или в приложении сведения об изготовителе и модели расчетной системы, используемой для расчета объема использования телекоммуникационного сервиса.

6. При предоставлении телекоммуникационных сервисов на территории Кыргызской Республики применяется бишкекское учетно-отчетное время, если иное не установлено международным договором, вступившим в силу в соответствии с законодательством Кыргызской Республики.

Статья 132. Цели использования телекоммуникационных сервисов

1. Пользователь имеет право использовать телекоммуникационные сервисы в любых целях, если настоящей статьей или пользовательским соглашением не предусмотрено, что использование телекоммуникационного сервиса в определенных целях может осуществляться только с прямого согласия поставщика сервиса.

2. Пользователь обязан хранить цифровые записи, позволяющие подтвердить согласие поставщика сервиса на использование сервиса в любой из следующих целей:

1) проведение лотерей, голосований, конкурсов, викторин, опросов других пользователей этого телекоммуникационного сервиса;

2) распространение рекламы среди пользователей этого телекоммуникационного сервиса или массовая рассылка им цифровых записей;

3) установка шлюзов между разными телекоммуникационными сервисами;

4) исследование телекоммуникационного сервиса, в том числе путем тестирования его защиты.

3. Поставщик или пользователь телекоммуникационного сервиса, использующий его для распространения рекламы среди пользователей данного телекоммуникационного сервиса, обязан получить предварительное согласие пользователей на это и хранить цифровые записи, позволяющие подтвердить согласие пользователей на получение рекламы.

Статья 133. Вещательные сервисы

1. Вещательные сервисы используются для распространения в Кыргызской Республике:

1) телерадиоканалов, зарегистрированных на территории Кыргызской Республики в качестве средств массовой информации и имеющих соответствующее разрешение на размещение в аналоговом вещании и (или) в цифровом пакете вещания, выданное в соответствии с законодательством о телевидении и радиовещании;

2) иностранных телерадиоканалов.

2. Формирование телерадиоканалов осуществляется в соответствии с законодательством Кыргызской Республики о телевидении и радиовещании и другими нормативными правовыми актами Кыргызской Республики в сфере средств массовой информации.

3. Поставщики вещательных сервисов обязаны распространять получаемые телерадиоканалы в неизменном виде. Внесение изменений в телерадиоканалы возможно только при условии регистрации в качестве вещательной организации в соответствии с законодательством о телевидении и радиовещании.

Статья 134. Предоставление телекоммуникационных сервисов в особых условиях

1. Телекоммуникационные сервисы используются в приоритетном порядке для передачи сообщений при:

1) угрозе жизни и здоровью людей;

2) чрезвычайных ситуациях и аварийно-спасательных работах.

2. Условия рассылки сообщений для нужд государственного управления, национальной безопасности, обороны, охраны правопорядка и иных аналогичных целей устанавливаются законом.

3. Передача сообщений, предусмотренных частью 1 настоящей статьи, а также вызов экстренных оперативных служб осуществляются операторами телекоммуникаций на безвозмездной основе.

4. Оператор телекоммуникаций обязан предоставить диспетчерам экстренных оперативных служб (пожарно-спасательной службы, службы охраны общественного порядка, скорой медицинской помощи, службы спасения) пространственные данные пользовательского оборудования (оконечного оборудования), с которого были осуществлены вызовы или передача сообщения о происшествии, и иные данные, необходимые для обеспечения реагирования по вызову или сообщению о происшествии.

5. Кабинет Министров определяет национальных операторов телекоммуникаций, которые:

1) выполняют особый порядок работы и взаимодействия с субъектами правоотношений в цифровой среде в соответствии с возложенными обязательствами и правами, утвержденный Кабинетом Министров;

2) обеспечивают бесперебойность действующей телекоммуникационной инфраструктуры, создают и поддерживают необходимый резерв телекоммуникационного оборудования и материалов при чрезвычайных ситуациях для целей государственного управления, национальной безопасности, обороны, охраны правопорядка за счет средств республиканского бюджета;

3) предоставляют телекоммуникационные сервисы для целей реализации государственных социальных проектов по обеспечению доступности телекоммуникационных сервисов по всей территории Кыргызской Республики, в том числе в труднодоступных и малонаселенных местах;

4) не вправе приостанавливать и прерывать работу телекоммуникационных сетей или предоставление телекоммуникационных сервисов без предварительного разрешения отраслевого регулятора телекоммуникаций для целей государственного управления, национальной безопасности, обороны, охраны правопорядка и при чрезвычайных ситуациях.

Глава 17. Доверенные сервисы

Статья 135. Правовое регулирование доверенных сервисов

1. Отношения по использованию цифровых подписей и цифровых архивов регулируются настоящим Кодексом и принимаемыми в соответствии с ним нормативными правовыми актами.

2. Порядок использования цифровой подписи в цифровой экосистеме устанавливается владельцем этой системы или соглашением участников цифрового взаимодействия в цифровой экосистеме.

3. Виды цифровых подписей, используемых органами исполнительной власти и органами местного самоуправления, а также требования по обеспечению совместимости таких цифровых подписей устанавливаются Кабинетом Министров.

4. Законами Кыргызской Республики могут устанавливаться особенности использования доверенных сервисов в следующих видах отношений:

1) подготовка и проведение выборов и референдума;

2) совершение гражданско-правовых сделок;

3) предоставление госсервисов;

4) осуществление платежей и банковских операций;

5) ведение бухгалтерского и налогового учета.

Статья 136. Сервисы цифровых подписей и цифровых архивов

1. Сервисы цифровых подписей и сервисы цифровых архивов относятся к доверенным цифровым сервисам, направленным на удостоверение возникновения, изменения, прекращения правоотношений в цифровой среде.

2. Для работы с цифровыми подписями их поставщик и пользователи используют средства цифровой подписи, представляющие собой шифровальные (криптографические) цифровые технологические системы.

3. Цифровые архивы хранят цифровые записи, содержащие цифровые подписи, вместе со средствами цифровой подписи, необходимыми для работы с такими подписями.

Статья 137. Отраслевые принципы регулирования отношений по использованию доверенных сервисов

1. Субъекты правоотношений в цифровой среде вправе по своему усмотрению использовать любой доверенный сервис, если требование об использовании его конкретного вида в соответствии с целями их использования не предусмотрено законодательством либо соглашением субъектов правоотношений в цифровой среде.

2. Субъекты правоотношений в цифровой среде вправе использовать любую технологию и (или) технологическую систему, позволяющую выполнить требования настоящего Кодекса применительно к цифровым подписям, цифровым архивам или иным доверенным сервисам.

3. Требования к использованию конкретного вида цифровой подписи или цифрового архива, установленные в законодательных и иных нормативных правовых актах, должны соответствовать целям их использования.

4. Цифровая подпись и (или) цифровая запись, неизменность которых обеспечивается цифровой подписью, не могут быть признаны не имеющими юридической силы только на том основании, что цифровая подпись не является собственноручной подписью или документ хранится в цифровом архиве.

Статья 138. Виды цифровых подписей

1. Видами цифровых подписей являются неквалифицированная цифровая подпись (далее - неквалифицированная подпись) и квалифицированная цифровая подпись (далее - квалифицированная подпись).

2. Неквалифицированной подписью является цифровая подпись, которая соответствует следующим признакам:

1) получена в результате криптографического преобразования цифровых данных с использованием ключа цифровой подписи;

2) уникальным образом связана с подписантом;

3) позволяет однозначно определить лицо, подписавшее цифровую запись;

4) позволяет обнаружить факт внесения изменений в цифровую запись после ее подписания;

5) создается с использованием средств цифровой подписи, которые лицо, подписавшее цифровую запись, способно сохранять под своим контролем.

3. При использовании неквалифицированной подписи сертификат ключа проверки подписи может не создаваться, если соответствие цифровой подписи признакам неквалифицированной подписи может быть обеспечено без использования сертификата ключа проверки подписи.

4. Квалифицированной подписью является цифровая подпись, которая соответствует всем признакам неквалифицированной подписи и следующим дополнительным признакам:

1) ключ проверки цифровой подписи указан в квалифицированном сертификате;

2) для создания и проверки цифровой подписи используются средства цифровой подписи, получившие подтверждение соответствия требованиям, установленным настоящим Кодексом.

5. Цифровая подпись юридического лица служит подтверждением того, что цифровая запись исходит от юридического лица и служит доказательством неизменности документа после создания цифровой подписи.

6. К квалифицированным сертификатам, выданным аккредитованным удостоверяющим центром, приравниваются сертификаты ключа проверки подписи, в отношении которых проверка осуществляется доверенной третьей стороной Кыргызской Республики, а в случае технической невозможности использовать доверенную третью сторону, иностранным доверенным сервисом, включенным в Реестр иностранных доверенных цифровых сервисов.

Статья 139. Условия признания цифровых записей, подписанных цифровой подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

1. Цифровая запись, подписанная квалифицированной подписью, признается цифровым документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, за исключением случаев, когда законодательством установлен запрет составления такого документа в цифровой форме.

2. Цифровая запись, подписанная неквалифицированной подписью, признается цифровым документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных:

1) нормативными правовыми актами;

2) соглашением субъектов правоотношений в цифровой среде, если нормативными правовыми актами не установлен запрет на составление такого документа в цифровой форме.

Указанные нормативные правовые акты и соглашения субъектов правоотношений в цифровой среде должны предусматривать порядок проверки цифровой подписи.

3. Если в соответствии с нормативными правовыми актами или обычаем делового оборота документ на бумажном носителе должен быть заверен печатью, цифровой документ, подписанный цифровой подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Нормативными правовыми актами или соглашением субъектов правоотношений в цифровой среде могут быть предусмотрены дополнительные требования к цифровому документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

4. Одной цифровой подписью может быть подписан пакет цифровых документов, то есть несколько цифровых документов, связанных между собой. При подписании цифровой подписью пакета цифровых документов каждый документ, входящий в него, считается подписанным цифровой подписью того вида, которым подписан пакет цифровых документов.

5. Если в соответствии с нормативными правовыми актами Кыргызской Республики к оформлению документов на бумажном носителе с использованием бланков строгой отчетности предъявляются особые требования, то цифровой документ, подписанный квалифицированной цифровой подписью, считается соответствующим этим требованиям.

Статья 140. Иностранные цифровые подписи и архивы

1. В Кыргызской Республике могут быть использованы любые методы создания цифровой подписи и цифровых архивов, которые соответствуют установленным настоящим Кодексом требованиям, а также международные стандарты в сфере цифровых подписей и цифровых архивов.

2. Цифровые подписи, созданные в соответствии с нормами права иностранного государства, в Кыргызской Республике признаются цифровыми подписями того вида, признакам которого они отвечают в соответствии с настоящим Кодексом.

3. Цифровая подпись и подписанный ею цифровой документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки подписи выдан в соответствии с нормами права иностранного государства и такая подпись не соответствует установленным настоящим Кодексом требованиям цифровой подписи.

4. Признание подлинности иностранных цифровых подписей производится:

1) доверенной третьей стороной, а в случае технической невозможности использовать доверенную третью сторону, иностранным доверенным сервисом, включенным в Реестр иностранных доверенных цифровых сервисов в порядке, установленном настоящим Кодексом;

2) судом, в рамках решения вопроса о соответствии иностранного доверенного сервиса, использованного стороной, критериям, установленным настоящим Кодексом.

5. Порядок осуществления функций доверенной третьей стороной Кыргызской Республики устанавливается Кабинетом Министров.

Статья 141. Обязанности субъектов правоотношений в цифровой среде при использовании цифровой подписи

Субъекты правоотношений в цифровой среде при использовании цифровой подписи обязаны:

1) обеспечивать конфиденциальность ключа цифровой подписи, в том числе не допускать использования принадлежащих им ключей цифровой подписи без их согласия;

2) проявлять разумную осмотрительность для недопущения несанкционированного использования цифровой подписи или данных, необходимых для ее создания;

3) незамедлительно, но не позднее 1 рабочего дня, следующего за днем получения информации о нарушении конфиденциальности ключа подписи уведомлять удостоверяющий центр, выдавший сертификат ключа проверки подписи, и иных участников правоотношений о таком нарушении;

4) не использовать ключ цифровой подписи при наличии оснований полагать, что его конфиденциальность нарушена;

5) использовать средства цифровой подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Кодексом, для осуществления обмена цифровыми документами, подписанными

квалифицированной подписью;

6) обеспечивать точность и своевременную актуализацию данных, необходимых для использования сертификата ключа проверки цифровой подписи;

7) предпринимать разумные меры для проверки достоверности цифровой подписи.

Статья 142. Признание подлинности квалифицированной подписи

1. До тех пор, пока решением суда не установлено иное, квалифицированная подпись признается подлинной при одновременном соблюдении следующих условий:

1) квалифицированный сертификат, содержащий ключ проверки подписи, создан и выдан аккредитованным удостоверяющим центром, при этом аккредитация такого удостоверяющего центра действительна (не приостановлена, не прекращена, не аннулирована) на день выдачи указанного сертификата;

2) квалифицированный сертификат, содержащий ключ проверки подписи, действителен (не прекратил свое действие, не аннулирован) на день подписания цифрового документа (при наличии достоверной информации о моменте подписания цифрового документа) или на день проверки - если момент подписания не определен;

3) имеется положительный результат проверки принадлежности владельцу указанного сертификата квалифицированной цифровой подписи, с помощью которой подписан данный цифровой документ, и отсутствия изменений, внесенных в этот документ после его подписания, при этом проверка осуществляется с применением средств цифровой подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Кодексом, и с использованием квалифицированного сертификата лица, от имени которого подписан документ.

2. Признание подлинности подписей, основанных на сертификатах, выданных иностранным удостоверяющим центром, осуществляется доверенной третьей стороной или поставщиком соответствующего сервиса, внесенного в Реестр иностранных доверенных сервисов. Результат проверки доверенной третьей стороной отражается в квитанции, подписанной квалифицированной подписью доверенной третьей стороны.

Статья 143. Средства цифровой подписи

1. Для создания и проверки цифровой подписи, создания ключей подписи и ключей проверки подписи должны использоваться средства цифровой подписи, которые:

1) позволяют установить факт изменения подписанного цифрового документа после его подписания;

2) обеспечивают практическую невозможность вычисления ключа подписи из цифровой подписи или ключа ее проверки.

2. При создании цифровой подписи средство цифровой подписи должно:

1) показывать лицу, подписывающему цифровую запись, ее содержание;

2) создавать цифровую подпись лишь после подтверждения операции по созданию цифровой подписи лицом, подписывающим информацию;

3) однозначно и ясно показывать, что цифровая подпись создана.

3. При проверке цифровой подписи средство цифровой подписи должно:

1) показывать содержание цифрового документа, подписанного цифровой подписью;

2) показывать, вносились ли изменения в подписанный цифровой подписью цифровой документ;

3) указывать на лицо, с использованием ключа подписи которого подписаны цифровые документы.

4. Средства цифровой подписи, предназначенные для создания цифровой подписи в цифровых документах, содержащих сведения, составляющие государственные секреты, или предназначенные для использования в цифровом ресурсе, содержащем государственные секреты, подлежат обязательной сертификации на соответствие требованиям по защите сведений соответствующей степени секретности.

5. Средства цифровой подписи, предназначенные для создания цифровой подписи в цифровых документах, содержащих конфиденциальную информацию, не должны нарушать конфиденциальности такой информации.

6. Требования частей 2 и 3 настоящей статьи не применяются к средствам цифровой подписи, используемым для автоматического (без участия человека) создания или проверки цифровых подписей.

Статья 144. Удостоверяющий центр

1. Удостоверяющий центр:

1) создает сертификат ключа проверки цифровой подписи и выдает его лицу, обратившемуся за получением такого сертификата (далее - заявитель);

2) устанавливает сроки действия сертификатов ключа проверки цифровой подписи;

3) аннулирует выданные им сертификаты ключа проверки цифровой подписи;

4) по обращению заявителя выдает средства цифровой подписи, содержащие ключ цифровой подписи и ключ проверки цифровой подписи (в том числе созданные удостоверяющим центром) либо обеспечивающие возможность создания ключа цифровой подписи и ключа проверки цифровой подписи заявителем;

5) ведет реестр выданных и аннулированных им сертификатов ключа проверки подписи (далее - реестр сертификатов), включающий в том числе сведения, содержащиеся в выданных им сертификатах ключа проверки цифровой подписи, а также сведения о дате прекращения действия (аннулирования) сертификата ключа проверки цифровой подписи и его основании;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и доступа к нему, обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием сети Интернет;

7) по обращению заявителей создает ключи цифровой подписи и ключи проверки цифровой подписи;

8) обеспечивает конфиденциальность ключей цифровой подписи (в случае создания таких ключей);

9) проверяет уникальность ключей проверки цифровой подписи в реестре сертификатов данного удостоверяющего центра;

10) осуществляет по обращениям участников цифрового взаимодействия проверку цифровой подписи;

11) осуществляет иную деятельность, связанную с использованием цифровой подписи.

2. Удостоверяющий центр обязан:

1) информировать заявителей об условиях и порядке использования цифровой подписи и средств цифровой подписи, о рисках, связанных с использованием цифровой подписи, и мерах, необходимых для обеспечения безопасности цифровых подписей и их проверки;

2) обеспечивать актуальность цифровых данных, содержащихся в реестре сертификатов, и их защиту от неправомерного доступа, уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации;

3) безвозмездно предоставлять любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов цифровые данные, содержащиеся в реестре сертификатов удостоверяющего центра, в том числе данные об аннулировании сертификата ключа проверки цифровой подписи.

3. Удостоверяющий центр в соответствии с законодательством Кыргызской Республики несет ответственность за вред, причиненный иным лицам в результате:

1) неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора предоставления сервиса удостоверяющим центром;

2) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных пунктом 10 части 1, пунктами 2 и 3 части 2 настоящей статьи.

4. Удостоверяющий центр вправе наделить иных лиц (далее - доверенные лица) полномочиями по созданию и выдаче сертификатов ключа проверки цифровой подписи от имени удостоверяющего центра, подписываемых цифровой подписью, основанной на сертификате ключа проверки цифровой подписи, выданного такому доверенному лицу этим удостоверяющим центром.

5. Удостоверяющий центр, наделивший полномочиями доверенных лиц, является корневым удостоверяющим центром по отношению к таким доверенным лицам и выполняет по отношению к ним следующие функции:

1) осуществляет проверку цифровых подписей, ключи проверки цифровой подписи которых указаны в сертификатах ключей проверки цифровой подписи, выданных доверенными лицами;

2) обеспечивает цифровое взаимодействие между доверенными лицами и доверенных лиц с удостоверяющим центром.

6. Цифровые записи, внесенные в реестр сертификатов, подлежат хранению в течение всего срока деятельности удостоверяющего центра, если нормативными правовыми актами не установлен более короткий срок. В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен заблаговременно, но не позднее чем за 1 месяц до даты прекращения деятельности, уведомить об этом владельцев выданных им сертификатов ключа проверки цифровой подписи, срок действия которых не истек. В указанном случае после завершения деятельности удостоверяющего центра цифровые записи, внесенные в реестр сертификатов, должны быть удалены.

В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен заблаговременно, но не менее чем за один месяц до даты передачи своих функций, уведомить об этом владельцев выданных им сертификатов ключа проверки цифровой подписи, срок действия которых не истек. В указанном случае после завершения деятельности удостоверяющего центра цифровые записи, внесенные в реестр сертификатов, должны быть переданы лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

7. Порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, установленных настоящей статьей, определяется удостоверяющим центром самостоятельно, если иное не установлено

нормативным правовым актом или соглашением субъектов правоотношений в цифровой среде.

8. Договор на предоставление сервиса удостоверяющим центром, реализующим свою деятельность в отношении неограниченного круга лиц, является публичным договором.

Статья 145. Сертификат ключа проверки цифровой подписи

1. Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки цифровой подписи на основании соглашения между удостоверяющим центром и заявителем.

2. Сертификат ключа проверки цифровой подписи должен содержать следующие сведения:

1) даты начала и окончания срока его действия;

2) фамилия, имя, отчество (если имеется) - для физических лиц, наименование - для юридических лиц, или иной идентификатор владельца сертификата ключа проверки цифровой подписи;

3) ключ проверки цифровой подписи;

4) наименование используемого средства цифровой подписи и (или) стандарты, которым соответствуют ключ цифровой подписи и ключ проверки цифровой подписи;

5) наименование удостоверяющего центра, выдавшего сертификат.

3. При выдаче сертификата ключа проверки цифровой подписи юридическому лицу в качестве владельца такого сертификата, наряду с указанием его наименования, указывается и физическое лицо, действующее от его имени на основании учредительных документов или доверенности.

4. Удостоверяющий центр вправе выдавать сертификаты ключа проверки цифровой подписи как в форме цифрового документа, так и в форме документа на бумажном носителе. Владелец сертификата ключа проверки цифровой подписи, выданного в форме цифрового документа, вправе также получить сертификат ключа проверки подписи на бумажном носителе, подписанный удостоверяющим центром.

5. Сертификат ключа проверки цифровой подписи действует со дня его выдачи, если в самом сертификате ключа проверки подписи не указана иная дата.

Сведения о сертификате ключа проверки цифровой подписи должны быть внесены удостоверяющим центром в реестр сертификатов не позднее даты начала действия сертификата ключа проверки подписи, указанной в нем.

6. Сертификат ключа проверки цифровой подписи прекращает свое действие:

1) по истечении срока его действия;

2) по заявлению владельца сертификата ключа проверки цифровой подписи, подаваемому в форме документа на бумажном носителе либо в цифровой форме;

3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

4) в иных случаях, установленных законом или соглашением удостоверяющего центра с владельцем сертификата ключа проверки цифровой подписи.

7. Данные о прекращении действия сертификата ключа проверки цифровой подписи должны быть внесены удостоверяющим центром в реестр сертификатов в течение одного рабочего дня с момента, когда удостоверяющему центру стало известно о наступлении обстоятельств, повлекших прекращение действия сертификата ключа проверки цифровой подписи. Сертификат ключа проверки цифровой подписи прекращает свое действие с момента внесения записи об этом в реестр сертификатов.

8. Удостоверяющий центр незамедлительно, но не позднее 1 рабочего дня, аннулирует сертификат ключа проверки цифровой подписи путем внесения записи об аннулировании в реестр сертификатов по решению суда, вступившему в законную силу, в частности в случае, если решением суда установлено, что сертификат ключа проверки цифровой подписи содержит недостоверные данные.

9. Использование аннулированного сертификата ключа проверки цифровой подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием.

Удостоверяющий центр обязан до внесения в реестр сертификатов сведений об аннулировании сертификата ключа проверки подписи уведомить владельца сертификата ключа проверки подписи об аннулировании его сертификата ключа проверки подписи.

Статья 146. Аккредитованный удостоверяющий центр

1. Удостоверяющий центр, получивший аккредитацию, является аккредитованным удостоверяющим центром.

2. Аккредитованный удостоверяющий центр обязан хранить следующие данные:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего права лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименовании, номере и дате выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если сведения о полномочиях владельца квалифицированного сертификата действовать по поручению третьих лиц включены в квалифицированный сертификат.

3. Указанные в части 2 настоящей статьи данные должны храниться аккредитованным удостоверяющим центром в течение срока его деятельности, если нормативными правовыми актами не предусмотрен более короткий срок.

Цифровые данные должны храниться в форме, позволяющей проверить их целостность и достоверность.

Удостоверяющий центр должен обеспечивать владельцу квалифицированного сертификата доступ к цифровым записям, относящимся к владельцу квалифицированного сертификата и хранящимся в аккредитованном удостоверяющем центре.

4. В случае прекращения деятельности аккредитованного удостоверяющего центра он обязан:

1) сообщить об этом отраслевому регулятору нацэкосистемы не позднее чем за 1 месяц до даты прекращения деятельности удостоверяющего центра;

2) передать отраслевому регулятору нацэкосистемы в установленном порядке реестр сертификатов;

3) передать на хранение отраслевому регулятору нацэкосистемы в установленном порядке цифровые записи, подлежащие хранению в аккредитованном удостоверяющем центре.

Статья 147. Аккредитация удостоверяющего центра

1. Аккредитация удостоверяющего центра осуществляется отраслевым регулятором нацэкосистемы в отношении удостоверяющих центров, являющихся юридическими лицами.

2. Аккредитация удостоверяющего центра осуществляется на добровольной основе.

Аккредитация удостоверяющего центра осуществляется на 5 лет, если меньший срок не указан в заявлении удостоверяющего центра.

3. Аккредитация предоставляется при условии выполнения удостоверяющим центром следующих требований:

1) стоимость чистых активов удостоверяющего центра составляет не менее одного миллиона сомов;

2) наличие финансового обеспечения ответственности за убытки, причиненные иным лицам вследствие их доверия к сведениям, указанным в сертификате ключа проверки цифровой подписи, выданном таким удостоверяющим центром, или данных, содержащихся в реестре сертификатов данного удостоверяющего центра, в размере не менее полутора миллионов сомов;

3) наличие средств цифровой подписи и средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным уполномоченным государственным органом в сфере обеспечения национальной безопасности;

4) наличие в штате удостоверяющего центра не менее 2 сотрудников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключа проверки цифровой подписи, имеющих высшее профессиональное образование в сфере информационных технологий или информационной/кибербезопасности либо высшее или среднее профессиональное образование, прошедших переподготовку или повышение квалификации по вопросам использования цифровой подписи.

4. Аккредитация удостоверяющего центра осуществляется по его заявлению, подаваемому в отраслевой регулятор нацэкосистемы.

К заявлению прилагаются документы, подтверждающие соответствие удостоверяющего центра требованиям, установленным частью 3 настоящей статьи.

5. Отраслевой регулятор нацэкосистемы на основании представленных документов не позднее 30 календарных дней со дня их получения принимает решение об аккредитации удостоверяющего центра или об отказе в аккредитации.

В случае принятия решения об аккредитации удостоверяющего центра отраслевой регулятор нацэкосистемы не позднее 10 дней со дня принятия решения об аккредитации уведомляет удостоверяющий центр о принятом решении и выдает свидетельство об аккредитации по установленной форме. Одновременно с выдачей свидетельства об аккредитации аккредитованному удостоверяющему центру выдается квалифицированный сертификат, созданный с использованием средств корневого удостоверяющего центра.

В случае принятия решения об отказе в аккредитации удостоверяющего центра отраслевой регулятор нацэкосистемы не позднее 10 календарных дней со дня принятия решения об отказе в аккредитации направляет или вручает удостоверяющему центру уведомление о принятом решении с указанием причин отказа.

6. Основанием для отказа в аккредитации является несоответствие удостоверяющего центра требованиям, установленным частью 3 настоящей статьи, либо наличие в представленных документах недостоверной информации.

7. Аккредитованный удостоверяющий центр должен соблюдать требования, на соответствие которым он аккредитован, в течение всего срока его аккредитации. В случае возникновения обстоятельств, делающих невозможным их соблюдение, удостоверяющий центр должен немедленно уведомить об этом отраслевого регулятора нацэкосистемы.

Аккредитованный удостоверяющий центр при осуществлении своих функций и исполнении принятых обязательств должен соблюдать требования, установленные для удостоверяющих центров настоящим Кодексом.

В случае обнаружения несоблюдения аккредитованным удостоверяющим центром указанных требований отраслевой регулятор нацэкосистемы обязан выдать удостоверяющему центру предписание об устранении нарушений с установлением срока их устранения и приостановить действие аккредитации на указанный срок. Аккредитованный удостоверяющий центр письменно уведомляет отраслевой регулятор нацэкосистемы об устранении нарушений, послуживших основанием для приостановления его аккредитации. Отраслевой регулятор нацэкосистемы вправе проверить фактическое устранение нарушений, после чего принимает решение о возобновлении действия аккредитации, а при их неустранении в указанный в предписании срок - аннулирует аккредитацию удостоверяющего центра.

8. На государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, осуществляющие функции удостоверяющего центра, не распространяются требования, установленные пунктами 1 и 2 части 3 настоящей статьи.

9. Корневой удостоверяющий центр, функции которого осуществляет отраслевой регулятор нацэкосистемы, не подлежит аккредитации в соответствии с настоящим Кодексом.

10. За аккредитацию аккредитованные удостоверяющие центры должны ежегодно вносить плату, рассчитываемую по методике, установленной Кабинетом Министров.

Статья 148. Квалифицированный сертификат

1. Квалифицированный сертификат подлежит созданию с использованием средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Кодексом.

2. Квалифицированный сертификат должен содержать следующие сведения:

1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;

2) фамилия, имя и отчество (если имеется), дата и место рождения владельца квалифицированного сертификата - физического лица либо наименование (фирменное наименование), регистрационный номер и место регистрации и (или) фактического нахождения исполнительного органа владельца квалифицированного сертификата - юридического лица;

3) ключ проверки цифровой подписи;

4) наименование средств цифровой подписи и средств удостоверяющего центра, которые использованы для создания ключа цифровой подписи, ключа проверки цифровой подписи и квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Кодексом;

5) наименование и местонахождение удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра и реквизиты свидетельства об аккредитации этого центра;

6) иные сведения о заявителе (по требованию заявителя).

3. Если заявителем представлены в удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат включаются сведения, свидетельствующие о таких правомочиях заявителя и сроке действия указанных правомочий.

4. Квалифицированный сертификат выдается в форме, требования к которой устанавливаются уполномоченным государственным органом в сфере обеспечения национальной безопасности.

5. В случае аннулирования квалифицированного сертификата, выданного аккредитованному удостоверяющему центру, выдавшему квалифицированный сертификат заявителю, а также в случае аннулирования или истечения срока аккредитации удостоверяющего центра квалифицированный сертификат, выданный аккредитованным удостоверяющим центром заявителю, прекращает свое действие.

6. Владелец квалифицированного сертификата при наличии оснований полагать, что конфиденциальность ключа цифровой подписи нарушена, обязан прекратить использование данного ключа и немедленно обратиться в удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата.

Статья 149. Выдача квалифицированного сертификата

1. Аккредитованный удостоверяющий центр при выдаче квалифицированного сертификата обязан осуществлять цифровую идентификацию и цифровую аутентификацию заявителя в соответствии с правилами системы цифровой идентификации, используемой в соответствии с настоящим Кодексом, либо на основании основного документа, удостоверяющего личность заявителя - физического лица.

2. Заявитель, действующий от имени другого лица, представляет в аккредитованный удостоверяющий центр:

1) доверенность (если заявитель действует от имени другого лица на основании доверенности);

2) документ о назначении, учредительные документы и документ о государственной регистрации заявителя - юридического лица (если заявитель действует от имени юридического лица без доверенности).

3. При получении квалифицированного сертификата заявитель должен быть ознакомлен удостоверяющим центром со сведениями, содержащимися в квалифицированном сертификате.

4. Удостоверяющий центр одновременно с выдачей квалифицированного сертификата должен выдать владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной подписи и средств цифровой подписи.

5. При перевыпуске квалифицированного сертификата на новый срок цифровая идентификация и цифровая аутентификация заявителя осуществляются на основании ранее выпущенного квалифицированного сертификата.

Статья 150. Цифровые архивы и сервисы цифровых архивов

1. Цифровой архив как цифровая технологическая система обеспечивает целостность и неизменность обрабатываемых с ее помощью цифровых записей и ограниченный доступ к ним. Виды цифровых записей, подлежащих архивному хранению, порядок их создания и хранения устанавливаются законодательством об архивном деле.

2. Поставщик сервиса цифровых архивов на основании законодательства или соглашения с пользователем обязан обеспечивать целостность и неизменность переданных на хранение в цифровой архив цифровых записей, а также обеспечивать доступ к ним лиц, которые имеют на это право в соответствии с законодательством или соглашением.

3. Видами цифровых архивов в зависимости от используемых технологий являются:

1) простые цифровые архивы, в которых целостность и неизменность цифровых записей обеспечиваются средствами цифровой технологической системы;

2) квалифицированные цифровые архивы, в которых целостность и неизменность цифровых записей обеспечиваются средствами квалифицированной подписи.

4. Субъекты правоотношений в цифровой среде в целях исполнения возложенных на них обязанностей по архивному хранению документов вправе организовывать цифровые архивы цифровых записей либо пользоваться сервисом цифровых архивов. Правила создания и использования госсервисов цифровых архивов являются составной частью правил нацэкосистемы.

5. Юридическая значимость цифровой записи в цифровом архиве признается неизменной, если в цифровом архиве обеспечиваются:

1) неизменность и целостность цифровой записи после включения ее в цифровой архив;

2) возможность доступа к нему лиц, которые имеют на это право в соответствии с законодательством или соглашением;

3) автоматическая регистрация действий, осуществляемых с цифровой записью в течение срока его хранения.

6. Цифровые документы, подписанные квалифицированной подписью, должны храниться в квалифицированных цифровых архивах, которые должны обеспечивать:

1) подписание цифрового документа квалифицированной подписью лица, осуществляющего хранение цифрового документа;

2) подтверждение действительности квалифицированной подписи, которой первоначально подписан переданный на хранение цифровой документ.

Статья 151. Хранение цифрового дубликата документа

1. Цифровая запись, воспроизводящая в полном объеме информацию, изначально содержащуюся в подлиннике документа на бумажном или ином материальном носителе, подписанном собственноручной подписью, включая его реквизиты, признается цифровым дубликатом документа.

2. Цифровой дубликат документа, хранящийся в цифровом архиве в соответствии с настоящим Кодексом, удостоверяет юридические факты, являющиеся основаниями возникновения, изменения, прекращения правоотношений, вместо подлинника документа, если владелец может подтвердить его соответствие следующим требованиям:

1) информация, изначально содержащаяся в подлиннике документа на бумажном или ином материальном носителе, подписанном собственноручной подписью, включая его реквизиты, в полном объеме воспроизведена в цифровом дубликате документа;

2) была обеспечена неизменность и целостность цифрового дубликата документа после его создания.

3. Информация, изначально содержащаяся в нескольких связанных между собой документах на бумажном или ином материальном носителе (пакете документов), может быть включена в состав одного цифрового дубликата документа. При этом информация должна располагаться в хронологическом порядке подписания подлинников документов.

4. Цифровой дубликат документа должен содержать следующую информацию:

1) информацию, изначально содержащуюся в подлиннике документа на бумажном или ином материальном носителе, в полном объеме и без изменений (в некорректируемом виде);

2) изображение собственноручной подписи каждого лица из числа подписавших подлинник документа;

3) метаданные для целей цифровой идентификации и поиска цифрового дубликата документа.

5. При несоответствии между цифровым дубликатом документа и подлинником документа приоритет имеет подлинник документа.

6. Лица, создавшие цифровой дубликат документа, вправе прекратить хранение подлинника документа на материальном носителе. Перечень видов документов, которые должны продолжать храниться в подлиннике после изготовления их цифровых дубликатов, утверждается Кабинетом Министров. Не допускается признание цифрового дубликата документа не имеющим юридической силы только на основании отсутствия (уничтожения) подлинника документа, на основании которого он был создан.

Статья 152. Доверенное хранение цифровых записей

При хранении цифровых записей в распределенных цифровых ресурсах, в том числе с использованием смарт-контрактов, правила хранения цифровых записей и доступа к ним определяются параметрами такого распределенного цифрового ресурса и (или) смарт-контракта.

Статья 153. Полномочия государственных органов в сфере использования цифровой подписи и цифровых архивов

1. Кабинет Министров:

1) устанавливает порядок передачи реестров и иных данных в отраслевой регулятор нацэкосистемы в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) устанавливает порядок формирования и ведения реестров квалифицированных сертификатов, а также предоставления сведений из таких реестров;

3) устанавливает правила аккредитации удостоверяющих центров, в том числе порядок проверки соблюдения аккредитованными удостоверяющими центрами требований, на соответствие которым эти удостоверяющие центры были аккредитованы;

4) определяет перечень видов документов, которые должны продолжать храниться в подлиннике после изготовления их цифровых дубликатов;

5) определяет порядок осуществления функций доверенной третьей стороны Кыргызской Республики, включая порядок ее взаимодействия с доверенными третьими сторонами и удостоверяющими центрами других государств.

2. Отраслевой регулятор нацэкосистемы:

1) осуществляет аккредитацию удостоверяющих центров, в том числе проверку соблюдения аккредитованными удостоверяющими центрами требований, на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае обнаружения их несоблюдения выдает предписания об устранении нарушений;

2) осуществляет функции корневого удостоверяющего центра в отношении аккредитованных удостоверяющих центров;

3) осуществляет функции доверенной третьей стороны Кыргызской Республики.

3. Уполномоченный государственный орган в сфере обеспечения национальной безопасности:

1) устанавливает требования к форме квалифицированного сертификата;

2) устанавливает требования к средствам цифровой подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств цифровой подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Кодексом, и публикует перечень таких средств.

4. Отраслевой регулятор нацэкосистемы обязан обеспечить хранение и беспрепятственный круглосуточный доступ к следующим цифровым записям:

1) наименования, адреса аккредитованных удостоверяющих центров;

2) реестр выданных и аннулированных квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых аннулирована;

4) перечень аккредитованных центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

6) реестры сертификатов, переданные отраслевому регулятору нацэкосистемы.

Глава 18. Госсервисы

Статья 154. Правоотношения по созданию и использованию госсервисов

1. Госсервисы предоставляются в рамках национальной цифровой экосистемы (нацэкосистемы), за исключением госсервисов, оказываемых посредством цифровых технологических систем уполномоченного государственного органа в сфере обеспечения национальной безопасности.

2. Правила создания и использования госсервисов являются частью правил нацэкосистемы и устанавливаются настоящим Кодексом.

3. Поставщиками госсервисов являются государственные органы и органы местного самоуправления Кыргызской Республики, а также юридические лица - участники нацэкосистемы. Поставщики обязаны обеспечивать цифровую устойчивость госсервисов.

4. Пользователями госсервисов являются государственные органы и органы местного самоуправления, юридические лица независимо от их организационно-правовой формы, а также физические лица (потребители). В зависимости от вида пользователей различаются:

1) госсервисы взаимодействия, то есть госсервисы, предназначенные для обработки данных государственными органами, органами местного самоуправления Кыргызской Республики и юридическими лицами, участвующими в предоставлении госсервисов;

2) пользовательские сервисы, то есть госсервисы для пользователей, в том числе физических лиц (потребителей).

Статья 155. Отраслевые принципы создания и использования госсервисов

1. Госсервисы должны создаваться в соответствии с общегосударственными стратегиями и планами по мере цифровой трансформации государственных органов и органов местного самоуправления (принцип пропорциональности).

2. Госсервисы должны основываться на элементах нацэкосистемы, источниках и форматах цифровых данных, используемых в рамках других госсервисов, а также допускать возможность использования цифровых записей другими госсервисами (принцип совместимости).

3. Права и интересы человека и гражданина, удобство пользования сервисами, их безопасность для потребителей являются безусловным приоритетом при создании госсервисов (принцип интересов потребителя).

4. Госсервисы должны проектироваться и создаваться таким образом, чтобы быть максимально доступными для потребителей с учетом их образования и имущественного положения, а также возраста и физических особенностей (принцип доступности).

5. Пользователи госсервисов должны обоснованно доверять их надежности и безопасности, а также тому, что обработка их данных осуществляется на основании закона и в соответствии с ним (принцип уверенности).

6. Госсервисы должны проектироваться таким образом, чтобы основанные на них услуги и функции становились доступными для пользователей в результате цифровой трансформации (принцип упрощения).

7. Данные об использовании госсервисов, включая отзывы и жалобы пользователей, должны храниться в соответствии с законодательством и использоваться для оценки эффективности госсервисов и их постоянного улучшения (принцип обратной связи).

Статья 156. Потребители госсервисов

1. Физическое лицо, данные которого обрабатываются в рамках госсервиса, считается его потребителем независимо от того, осуществляется ли обработка по инициативе физического лица или по инициативе поставщика госсервиса.

2. Основанием для обработки персональных данных в рамках госсервисов является осуществление поставщиком госсервиса обязанностей (полномочий), установленных настоящим Кодексом, законом или принятыми в соответствии с ними нормативными правовыми актами. Получение согласия физического лица на обработку персональных данных, необходимых для осуществления таких обязанностей, не требуется. Запрещается обработка в рамках госсервисов персональных данных, которые не требуются для предоставления госсервисов.

3. Потребители вправе по своему выбору пользоваться госсервисами любыми доступными им способами или не пользоваться ими.

4. Если в предоставлении госсервиса участвуют несколько государственных органов, органов местного самоуправления или юридических лиц, потребитель имеет право взаимодействовать с любым из них по своему выбору, за исключением случаев, когда законом или принятым в соответствии с ним нормативными правовыми актами предусмотрено, что права и обязанности поставщика госсервиса выполняет определенный государственный орган или юридическое лицо.

5. Потребители имеют право на составление отзывов и жалоб относительно пользования госсервисами. Отзывы (жалобы), которые потребитель решил опубликовать, должны быть опубликованы на сайте поставщика госсервиса не позднее одного рабочего дня после их направления потребителем. Поставщик госсервиса обязан предоставить возможность направления ему отзывов и жалоб посредством приложения или сайта госсервисов, а также предоставить потребителю возможность выбора, подлежат ли его отзывы или жалобы опубликованию.

6. Потребитель вправе не предоставлять поставщику госсервиса данные, которые уже содержатся в государственных цифровых ресурсах.

Статья 157. Участие государственных органов, органов местного самоуправления и юридических лиц в создании и использовании госсервисов

1. Координирование деятельности по созданию госсервисов осуществляет координирующий орган в соответствии с настоящим Кодексом.

2. Отраслевой регулятор в сфере нацэкосистемы:

1) обеспечивает создание госсервисов и осуществляет их учет, создает и эксплуатирует государственную цифровую технологическую систему для создания и развития госсервисов (фабрику госсервисов), осуществляет права и обязанности владельца фабрики госсервисов;

2) осуществляет от имени Кыргызской Республики права и обязанности владельца приложений и сайта госсервисов;

3) участвует в разработке документов, оформляющих создание или изменение госсервисов;

4) оказывает содействие государственным органам и органам местного самоуправления в процессе цифровой трансформации, в том числе при разработке и согласовании ими документов и процедур, касающихся госсервисов, предоставления доступа к открытым данным;

5) разрабатывает и публикует на своем сайте требования к технико-экономическим обоснованиям, техническим спецификациям, техническим заданиям на создание цифровых сервисов для государственных органов, органов местного самоуправления и уполномоченных ими юридических лиц;

6) определяет ключевые показатели эффективности госсервисов и осуществляет их мониторинг;

7) проводит оценку цифровой устойчивости госсервисов и выдает обязательные для исполнения поставщиками госсервисов предписания по повышению их цифровой устойчивости;

8) участвует в разработке методик обучения, повышения квалификации государственных и муниципальных служащих и иных лиц в части использования госсервисов.

3. Органы государственной власти, органы местного самоуправления, юридические лица создают госсервисы и используют их в соответствии с их полномочиями, предусмотренными законодательством Кыргызской Республики, нормативными актами и соглашениями между такими органами и юридическими лицами.

Статья 158. Правила создания госсервисов

1. Решение о создании госсервиса или о его изменении принимается участником нацэкосистемы, заинтересованным в его создании или изменении.

2. Решение о создании госсервиса должно содержать:

1) указание на поставщика госсервиса;

2) данные о пользователях и потребителях госсервиса;

3) указание на функции и полномочия, в рамках которых используется госсервис;

4) данные о цифровых технологических системах, с использованием которых предоставляется госсервис;

5) указание на источники данных, обрабатываемых в рамках госсервиса, в том числе являющиеся результатом использования других госсервисов;

6) описание способов доступа к госсервису;

7) описание результатов использования госсервиса и порядка их использования, в том числе в других госсервисах.

3. До начала использования госсервиса его поставщик обязан:

1) обеспечить совместимость и взаимодействие созданного госсервиса с другими госсервисами;

2) провести тестирование функциональности и цифровой устойчивости госсервиса с использованием фабрики госсервисов и предоставить его результаты отраслевому регулятору в сфере нацэкосистемы;

3) при положительном результате тестирования, подтвержденном отраслевым регулятором в сфере нацэкосистемы, предоставить регулятору данные, необходимые для учета госсервиса.

4. Отраслевой регулятор нацэкосистемы в целях учета госсервисов включает в цифровой реестр нацэкосистемы данные, указанные в части 2 настоящей статьи, а также следующие данные:

1) лица, ответственные за обеспечение цифровой устойчивости госсервиса, и их контактная информация;

2) показатели, характеризующие качество госсервиса (предельный период недоступности сервиса в течение года, сроки восстановления доступности сервиса в случае сбоя, одновременное количество пользователей);

3) используемые форматы данных и интерфейсы обмена данными.

5. При внесении изменений в госсервис его поставщик до начала использования обновленного госсервиса обязан выполнить действия, предусмотренные частью 3 настоящей статьи.

Статья 159. Фабрика госсервисов

1. Фабрика госсервисов является государственной цифровой технологической системой для создания и развития госсервисов.

2. Фабрика госсервисов обеспечивает:

1) доступ владельца госсервиса к общему пространству цифровых данных нацэкосистемы;

2) тестирование госсервиса до начала его использования;

3) мониторинг работы госсервиса;

4) взаимодействие госсервиса с другими госсервисами и иными объектами правоотношений в цифровой среде в рамках нацэкосистемы;

5) развитие госсервиса и внесение в него изменений.

3. Правила работы фабрики госсервисов определяются Кабинетом Министров. Правила могут предусматривать иные функции, выполнение которых обеспечивается фабрикой госсервисов.

Статья 160. Правила пользования госсервисом

1. Правила пользования госсервисом утверждаются его поставщиком на основании законодательства, регулирующего выполнение им соответствующих функций или полномочий.

2. При пользовании госсервисами пользовательское соглашение не заключается, если иное не предусмотрено законодательством Кыргызской Республики.

3. В правилах пользования госсервисом должны быть описаны права и обязанности всех категорий его пользователей, а также порядок их действий для достижения каждой из возможных целей его использования.

4. Правила пользования госсервисом должны учитывать возможность обработки данных в рамках госсервиса как по инициативе пользователя, так и в проактивном порядке, по инициативе его поставщика. Правила пользования госсервисом должны предусматривать гарантии прав пользователя при обработке данных о нем по инициативе поставщика госсервиса.

5. Правила пользования госсервисом должны содержать описание порядка и последствий обработки данных в рамках госсервиса:

1) указание на типы, источники исходных данных, обрабатываемых в рамках госсервиса, и их принципалов;

2) описание возможных вариантов обработки данных (создание, обновление, уточнение, изменение, поиск);

3) указание на цифровые ресурсы или цифровые записи, в которые вносятся изменения в результате обработки данных.

6. Правила пользования сервисом размещаются на сайте поставщика госсервиса и должны быть доступны пользователям сервиса на сайте или в приложении до начала использования сервиса.

Статья 161. Приложения и сайт госсервисов

1. Приложения и сайт госсервисов предназначены для доступа к пользовательским госсервисам.

2. Приложения и сайт госсервисов обеспечивают:

1) доступ пользователей к сведениям о госсервисах, правилам пользования ими;

2) возможность использования госсервисов для получения соответствующих услуг;

3) возможность загрузки данных, в том числе цифровых документов и цифровых дубликатов документов, для их обработки в рамках госсервиса;

4) возможность мониторинга хода обработки пользовательских данных, в том числе получения данных о ходе предоставления госсервиса;

5) возможность получения результатов использования госсервиса за исключением случаев, когда такое получение запрещено законом;

6) возможность оплаты госсервисов и совершения других обязательных платежей, если иное не предусмотрено законом;

7) возможность направления жалоб на деятельность поставщиков госсервисов и получения решений по таким жалобам.

3. Положение о приложениях и сайте госсервисов утверждается Кабинетом Министров. Положением могут быть предусмотрены иные функции, выполнение которых обеспечивается приложениями и сайтом госсервисов.

Статья 162. Рассмотрение споров

1. Рассмотрение жалоб и споров, касающихся госсервисов, осуществляется отраслевым регулятором нацэкосистемы с использованием сайта или приложения госсервисов.

2. Отраслевой регулятор в течение трех рабочих дней после получения жалобы обязан проинформировать об этом государственные органы, органы местного самоуправления и юридические лица, участвующие в предоставлении госсервиса, и предоставить все данные, относящиеся к полученной жалобе.

3. Отраслевой регулятор в течение четырнадцати рабочих дней после получения жалобы рассматривает ее и при подтверждении указанных в жалобе сведений выдает обязательные для исполнения поставщиками госсервисов предписания по устранению причин, послуживших основанием для жалобы. При рассмотрении жалобы отраслевой регулятор запрашивает необходимые данные у поставщика сервиса.

4. Поставщик госсервиса обязан принять меры, необходимые для устранения указанных в жалобе нарушений в течение 5 рабочих дней после получения предписания отраслевого регулятора. О принятых мерах поставщик госсервиса обязан проинформировать пользователя.

5. Решения поставщика госсервиса по жалобе или спору могут быть обжалованы в суде по месту нахождения поставщика.

Глава 19. Нацэкосистема

Статья 163. Архитектура нацэкосистемы

1. Нацэкосистема предназначена для предоставления цифровых сервисов, в том числе госсервисов. Нацэкосистема обеспечивает общие правила создания и использования следующих объектов правоотношений в цифровой среде (элементов нацэкосистемы):

1) государственные (муниципальные) цифровые ресурсы, приложения и сайты госсервисов;

2) госсервисы и доверенные сервисы;

3) государственные (муниципальные) цифровые технологические системы и их элементы;

4) земли, здания, строения, сооружения и иные аналогичные объекты в части доступа к ним владельцев государственных цифровых технологических систем.

2. Учет элементов нацэкосистемы осуществляется в цифровом реестре нацэкосистемы в соответствии с настоящим Кодексом. Включение в состав элементов нацэкосистемы цифровых технологических систем уполномоченного государственного органа в сфере обеспечения национальной безопасности осуществляется исключительно по решению руководителя указанного уполномоченного государственного органа.

3. Правила нацэкосистемы устанавливаются в соответствии с настоящим Кодексом и включают в себя правила:

1) развития нацэкосистемы;

2) взаимодействия участников нацэкосистемы;

3) формирования источников данных и обработки данных;

4) создания госсервисов и пользования ими;

5) доверенных сервисов и систем цифровой идентификации;

6) создания и использования государственных и муниципальных цифровых технологических систем.

4. Координацию деятельности по созданию и развитию нацэкосистемы осуществляет координирующий орган. Создание госсервисов в ходе развития нацэкосистемы и пользование ими осуществляются по правилам, установленным соответствующей главой настоящего Кодекса.

5. Владельцем нацэкосистемы является Кыргызская Республика, от имени которой действует отраслевой регулятор нацэкосистемы.

6. Участниками нацэкосистемы являются владелец нацэкосистемы в лице отраслевого регулятора, государственные органы, юридические лица независимо от их организационно-правовой формы, а также физические лица, являющиеся владельцами (поставщиками) элементов нацэкосистемы или их пользователями.

7. Цифровая идентификация и цифровая аутентификация участников нацэкосистемы осуществляются с использованием систем цифровой идентификации по правилам, установленным соответствующей главой настоящего Кодекса.

Статья 164. Принципы нацэкосистемы

1. Каждый субъект правоотношений в цифровой среде вправе стать участником нацэкосистемы при условии соблюдения ее правил (принцип общедоступности).

2. Элементы нацэкосистемы проектируются и эксплуатируются таким образом, чтобы последствия инцидентов в цифровой среде для каждого из элементов, их замена или развитие не оказывали негативного влияния на нацэкосистему в целом (принцип модульности).

3. Элементы нацэкосистемы проектируются и создаются таким образом, чтобы функционировать независимо от конкретных цифровых устройств и их местоположения (облачный принцип).

4. Участники нацэкосистемы исходя из собственных потребностей вправе определять состав создаваемых и используемых ими в своей деятельности элементов нацэкосистемы с учетом положений настоящего Кодекса и правил нацэкосистемы (принцип вариативности).

5. Функции каждого элемента нацэкосистемы могут одновременно выполняться другими элементами нацэкосистемы, если это повышает эффективность нацэкосистемы в целом (принцип параллельности).

6. Элементы нацэкосистемы должны преимущественно основываться на открытых форматах данных (записей) и интерфейсов обмена данными и не зависеть от конкретного поставщика цифровых устройств, форматов данных (записей) и интерфейсов обмена данными, права на которые принадлежат третьим лицам (принцип независимости от поставщика).

Статья 165. Развитие нацэкосистемы

1. Развитие нацэкосистемы осуществляется в соответствии с программами и планами развития нацэкосистемы и ее отдельных элементов, утверждаемыми Кабинетом Министров.

2. Планы и программы развития нацэкосистемы и ее отдельных компонентов должны учитывать потребности в предоставлении госсервисов, а также общепризнанную международную практику в сфере цифрового управления.

3. Участники нацэкосистемы вправе по своей инициативе создавать элементы нацэкосистемы, не предусмотренные планами и программами ее развития, но необходимые для деятельности участников нацэкосистемы. Элементы нацэкосистемы, созданные в инициативном порядке, должны быть внесены в цифровой реестр нацэкосистемы в порядке, установленном настоящим Кодексом.

Статья 166. Взаимодействие участников нацэкосистемы

1. Участники нацэкосистемы обязаны взаимодействовать между собой в рамках нацэкосистемы в соответствии с ее правилами и соглашениями между участниками о взаимодействии.

2. Правила взаимодействия участников нацэкосистемы устанавливаются Кабинетом Министров.

3. Взаимодействие участников нацэкосистемы осуществляется на бесплатной основе.

4. Взаимодействие между государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями и организациями при предоставлении госсервисов осуществляется с использованием системы цифрового взаимодействия, являющейся элементом нацэкосистемы.

5. Владельцем системы цифрового взаимодействия является Кыргызская Республика, от имени которой действует отраслевой регулятор нацэкосистемы.

6. Перечни цифровых данных, передаваемых с использованием системы цифрового взаимодействия, устанавливаются нормативными правовыми актами, определяющими соответствующие полномочия государственных органов Кыргызской Республики.

Статья 167. Обработка данных и источники данных нацэкосистемы

1. Цифровые ресурсы участников нацэкосистемы являются источниками цифровых данных, обрабатываемых в рамках нацэкосистемы, и образуют общее пространство цифровых данных нацэкосистемы.

2. Право участников нацэкосистемы обрабатывать данные в общем пространстве цифровых данных может быть ограничено только законодательством. Участник нацэкосистемы обязан предоставлять доступ к своим цифровым ресурсам для целей обработки данных из них в общем пространстве цифровых данных в случаях, установленных законодательством или соглашением такого участника с другими участниками нацэкосистемы.

3. Обработка цифровых записей в рамках нацэкосистемы осуществляется с учетом их метаданных, определяющих владельцев или принципалов цифровых записей, допустимые цели и способы обработки, форматы цифровых записей и интерфейсы обмена данными, а также иные характеристики, важные для обработки цифровых записей.

4. Цифровые данные подлежат обработке в рамках нацэкосистемы независимо от их формата. Участники нацэкосистемы вправе по своему усмотрению осуществлять обработку цифровых данных в том формате, теми способами и в такой последовательности операций, которые в лучшей степени обеспечивают достижение цели обработки, если иное не установлено законами и принимаемыми в соответствии с ними нормативными правовыми актами или соглашением участников нацэкосистемы.

5. Если иное не установлено законами и принимаемыми в соответствии с ними нормативными правовыми актами или соглашением участников нацэкосистемы, данные в общем пространстве цифровых данных являются открытыми данными.

6. Обработка в рамках нацэкосистемы персональных данных и цифровых записей, отнесенных к охраняемой законом тайне, допускается по основаниям, предусмотренным настоящим Кодексом и законами о соответствующих видах тайны. Участники нацэкосистемы, обрабатывающие такие данные, обязаны реализовывать следующие меры предотвращения вреда субъекту персональных данных или лицу, в интересах которых соблюдается охраняемая законом тайна:

1) доступ уполномоченных лиц к таким данным осуществляется в порядке, установленном Кабинетом Министров;

2) данные обрабатываются исключительно в целях, установленных законодательством, и не передаются одним участником нацэкосистемы другому, кроме случаев, установленных законом;

3) данные, предназначенные для опубликования или иного распространения, представляются в обобщенном виде, не позволяющем отнести их к конкретному принципалу данных без дополнительной информации;

4) на работников, имеющих доступ к таким данным в силу исполнения служебных обязанностей, и на обработчиков таких данных возлагаются обязательства по обеспечению их конфиденциальности и устанавливается ответственность за нарушение этих обязательств;

5) осуществляется учет всех операций с такими данными и всех лиц, осуществляющих доступ к таким данным;

6) обеспечивается свободный доступ (в том числе путем опубликования на сайте или в приложении участника нацэкосистемы) к сведениям о составе обрабатываемых данных, целях и способах их обработки, способах получения принципалами данных информации об обработке в соответствии с настоящим Кодексом.

7. Требования к порядку создания, актуализации и использования государственных (муниципальных) цифровых ресурсов определяются Кабинетом Министров. Сведения о государственных (муниципальных) цифровых ресурсах, цифровых ресурсах других участников нацэкосистемы и порядке доступа к ним включаются в цифровой реестр нацэкосистемы.

Статья 168. Создание и использование государственных и муниципальных цифровых технологических систем

1. В составе нацэкосистемы могут использоваться цифровые технологические системы и соединяющие их телекоммуникационные сети, как построенные за счет средств республиканского и местных бюджетов, так и используемые на договорной основе.

2. Владелец государственной (муниципальной) цифровой технологической системы обязан утвердить ее правила и обеспечить их соответствие положениям настоящего Кодекса, если такие правила или положение о государственной (муниципальной) цифровой технологической системе не утверждены законом или принятыми в соответствии с ним нормативными правовыми актами.

3. Требования к государственным (муниципальным) цифровым технологическим системам устанавливаются Кабинетом Министров.

4. Сведения о государственных (муниципальных) цифровых технологических системах включаются в цифровой реестр нацэкосистемы.

Статья 169. Отраслевой регулятор нацэкосистемы

1. Регулирование деятельности, связанной с нацэкосистемой, и надзор за такой деятельностью осуществляются уполномоченным государственным органом, создаваемым в порядке, установленномстатьей 9настоящего Кодекса (отраслевым регулятором нацэкосистемы). Отраслевой регулятор нацэкосистемы независим в своей деятельности от лиц, в отношении которых он осуществляет свои полномочия.

2. Руководитель отраслевого регулятора нацэкосистемы должен обладать квалификацией, опытом и знаниями, в том числе в сфере цифровых технологий, необходимыми для выполнения обязанностей и осуществления полномочий.

3. Отраслевой регулятор нацэкосистемы осуществляет следующие полномочия:

1) реализует планы развития нацэкосистемы и ее отдельных элементов;

2) осуществляет права и обязанности владельца системы цифрового взаимодействия, единой системы цифровой идентификации, приложения и сайта госсервисов, фабрики госсервисов, цифрового реестра нацэкосистемы, является их обработчиком, а также эксплуатирует, развивает и осуществляет их техническую поддержку и сопровождение, обеспечивает внедрение, мониторинг и бесперебойное функционирование;

3) осуществляет техническую координацию, методологическую поддержку и мониторинг эффективности деятельности участников нацэкосистемы, качества цифровых сервисов;

4) обеспечивает совместимость цифровых технологических систем на технико-технологическом уровне, методологическое обеспечение и развитие архитектуры нацэкосистемы;

5) разрабатывает, тестирует, модернизирует собственные цифровые сервисы, приложения, цифровые технологические системы;

6) осуществляет функции корневого удостоверяющего центра, осуществляет аккредитацию удостоверяющих центров в соответствии с настоящим Кодексом;

7) участвует в разработке документов, определяющих создание, изменение и процедуры предоставления госсервисов в части, касающейся создания или изменения элементов нацэкосистемы;

8) обеспечивает развитие правил нацэкосистемы;

9) оказывает содействие государственным органам и органам местного самоуправления в процессе цифровой трансформации, в том числе при создании, развитии и использовании государственных (муниципальных) цифровых технологических систем и обработке цифровых данных с их использованием;

10) обеспечивает взаимодействие участников нацэкосистемы;

11) разрабатывает, утверждает и публикует на своем сайте рекомендации по форматам цифровых данных и записей, используемых в нацэкосистеме;

12) определяет ключевые показатели работы нацэкосистемы и осуществляет их мониторинг;

13) проводит оценку цифровой устойчивости нацэкосистемы и выдает обязательные для исполнения владельцами государственных (муниципальных) цифровых технологических систем предписания по повышению их цифровой устойчивости;

14) участвует в разработке методик обучения, повышения квалификации государственных и муниципальных служащих и иных лиц в части развития и использования нацэкосистемы;

15) ведет цифровой реестр нацэкосистемы, иные реестры в порядке, установленном настоящим Кодексом.

4. Для достижения прозрачности своих регулирующих функций отраслевой регулятор нацэкосистемы должен публиковать годовой отчет о деятельности и результаты оценки цифровой устойчивости нацэкосистемы на своем сайте.

5. Отраслевой регулятор нацэкосистемы имеет право:

1) запрашивать и безвозмездно получать у физических лиц и организаций необходимую для реализации своих полномочий информацию, в том числе относящуюся к государственным секретам или иной охраняемой законом тайне;

2) требовать от владельца государственной (муниципальной) цифровой технологической системы принятия мер по восстановлению ее цифровой устойчивости;

3) обращаться в суд с исковыми заявлениями в защиту прав участников нацэкосистемы, в том числе прав неопределенного круга лиц, и представлять интересы участников нацэкосистемы в суде;

4) направлять в правоохранительные органы в соответствии с подведомственностью материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением правил нацэкосистемы;

5) вносить в Кабинет Министров предложения о совершенствовании правил нацэкосистемы, планах, программах развития нацэкосистемы и ее отдельных элементов;

6) привлекать к ответственности лиц, виновных в нарушении настоящего Кодекса.

6. Отраслевой регулятор нацэкосистемы обязан:

1) обеспечивать соблюдение правил нацэкосистемы и их развитие в соответствии с положениями настоящего Кодекса;

2) регулярно осуществлять проверки соблюдения владельцами государственных (муниципальных) цифровых технологических систем положений настоящего Кодекса и выносить по результатам проверок обязательные для исполнения решения;

3) рассматривать жалобы и обращения участников нацэкосистемы по вопросам, связанным с их взаимодействием в рамках нацэкосистемы, и по результатам их рассмотрения принимать в пределах своих полномочий обязательные для исполнения решения;

4) давать разъяснения по вопросам применения правил нацэкосистемы по запросу физических лиц и организаций с опубликованием таких разъяснений на своем сайте;

5) разрабатывать и публиковать рекомендации по вопросам развития нацэкосистемы, создания и использования государственных (муниципальных) цифровых технологических систем, разрабатывать и публиковать примерные формы договоров, правовых актов и иных документов для участников нацэкосистемы.

Статья 170. Рассмотрение споров в рамках нацэкосистемы

1. В случае возникновения споров по вопросам взаимодействия участников нацэкосистемы любая из сторон в порядке досудебного рассмотрения обязана обратиться в отраслевой регулятор нацэкосистемы. Отраслевой регулятор нацэкосистемы рассматривает такое обращение в течение 2 месяцев с даты его получения.

2. В целях рассмотрения спора отраслевой регулятор нацэкосистемы имеет право запросить любые данные, в предоставлении которых не может быть отказано.

3. Отраслевой регулятор нацэкосистемы не рассматривает спор в следующих случаях:

1) если предметом спора не является взаимодействие с использованием нацэкосистемы;

2) если спор касается заключения соглашения о взаимодействии и с момента направления запроса о заключении соглашения одним участником нацэкосистемы другому прошло менее 3 месяцев;

3) если прошло более 1 года с даты последнего действия в процессе переговоров.

4. В случаях, предусмотренных пунктами 1 и 3 части 3 настоящей статьи, участники нацэкосистемы вправе обратиться напрямую в суд.

5. Отраслевой регулятор нацэкосистемы в целях разрешения спора имеет право в своем решении установить технические и (или) финансовые условия взаимодействия, обязательные для соблюдения сторонами.

6. Решение отраслевого регулятора нацэкосистемы выносится в виде административного акта и может быть обжаловано в судебном порядке.

7. В случае если отраслевой регулятор нацэкосистемы не вынес решение в срок, указанный в части 1 настоящей статьи, спор считается нерешенным, а руководитель отраслевого регулятора нацэкосистемы подлежит привлечению к ответственности за бездействие в соответствии с законодательством о правонарушениях.

РАЗДЕЛ V. ЦИФРОВЫЕ ТЕХНОЛОГИЧЕСКИЕ СИСТЕМЫ

Глава 20. Общие положения о цифровых технологических системах

Статья 171. Правовое регулирование цифровых технологических систем

1. Цифровые технологические системы в Кыргызской Республике могут создаваться и использоваться без ограничений. Настоящий Кодекс регулирует использование отдельных видов цифровых технологических систем исключительно для предотвращения вреда жизни, здоровью людей, окружающей среде, собственности, общественной и государственной безопасности, а также для обеспечения возможности взаимодействия в цифровой среде с использованием цифровых технологических систем.

2. Настоящий Кодекс регулирует использование следующих видов цифровых технологических систем:

1) телекоммуникационные сети;

2) радиоэлектронные средства и высокочастотные устройства;

3) государственные и муниципальные цифровые технологические системы;

4) системы искусственного интеллекта.

3. Возможность взаимодействия в цифровой среде с использованием цифровых технологических систем в Кыргызской Республике обеспечивается на основе общепризнанной международной практики в порядке, установленном соответствующей главой настоящего Кодекса.

4. Владельцами и пользователями цифровых технологических систем в Кыргызской Республике могут быть любые лица, независимо от их гражданства, страны происхождения или формы собственности, а также технологий, используемых ими в цифровых технологических системах.

Статья 172. Радиоэлектронные средства и высокочастотные устройства

1. Радиоэлектронные средства и высокочастотные устройства независимо от их назначения должны устанавливаться и эксплуатироваться таким образом, чтобы не создавать вредных помех другим действующим радиоэлектронным средствам и высокочастотным устройствам, не затруднять или прерывать использование цифровых сервисов или цифровых технологических систем, в том числе признаваемых в Кыргызской Республике в соответствии с международными договорами, вступившими в силу в соответствии с законодательством Кыргызской Республики.

2. Радиоэлектронные средства должны использоваться в соответствии с условиями, определенными в решении о присвоении радиочастоты. Владелец радиоэлектронных средств, эксплуатирующий их в соответствии с общим присвоением, обязан самостоятельно взаимодействовать с владельцами других действующих радиоэлектронных средств с целью недопущения и устранения вредных помех другим действующим радиоэлектронным средствам, вплоть до выключения своих радиоэлектронных средств, создающих вредные помехи. Если владельцы радиоэлектронных средств самостоятельно не согласовали комплекс мер по устранению вредных помех в течение месяца с даты начала переговоров о таком согласовании, любой из них вправе передать спор на рассмотрение отраслевого регулятора телекоммуникаций.

Статья 173. Доступ владельцев цифровых технологических систем к инфраструктуре

1. Размещение, строительство, эксплуатация элементов цифровых технологических систем осуществляется владельцами цифровых технологических систем по договору с собственниками или иными владельцами зданий, сооружений, опор линий электропередач, контактных сетей железных дорог, столбовых опор, мостов, коллекторов, туннелей, железных и автомобильных дорог и других инженерных объектов и технологических площадок. При этом собственник или иной владелец указанных объектов вправе требовать от владельцев цифровых технологических систем соразмерную плату за пользование этим имуществом, если иное не предусмотрено настоящим Кодексом.

2. Необходимость размещения цифровых технологических систем должна учитываться при территориальном планировании и архитектурно-строительном проектировании в соответствии с законодательством Кыргызской Республики. Требования к зданиям, строениям и сооружениям для размещения цифровых технологических систем устанавливаются уполномоченным государственным органом в сфере архитектуры и строительства.

3. Переустройство и перенос цифровых технологических систем, вызываемые новым строительством, расширением, реконструкцией населенных пунктов и отдельных видов инфраструктуры, переустройством дорог и мостов, освоением новых земель, переустройством систем мелиорации, разработкой полезных ископаемых производятся заказчиком строительства за свой счет в соответствии с действующими стандартами по техническим условиям владельцев указанных объектов. При этом необходимое увеличение характеристик таких цифровых технологических систем осуществляется за

счет их владельцев.

4. Не допускается ввод в эксплуатацию зданий и сооружений, построенных, реконструированных, прошедших капитальный ремонт и не соответствующих утвержденным требованиям к зданиям, строениям и сооружениям в целях размещения цифровых технологических систем.

Статья 174. Цифровая устойчивость технологических систем

1. Операторы телекоммуникаций и владельцы государственных (муниципальных) цифровых технологических систем обязаны обеспечивать цифровую устойчивость принадлежащих им телекоммуникационных сетей и государственных (муниципальных) цифровых технологических систем.

2. Для телекоммуникационных сетей и государственных (муниципальных) цифровых технологических систем устанавливаются охранные зоны в соответствии с земельным и градостроительным законодательствами Кыргызской Республики.

3. Лица, осуществляющие проектирование и строительство, при проектировании, строительстве, ремонте, реконструкции и восстановлении зданий, строений и сооружений обязаны получить письменное разрешение владельцев цифровых технологических систем и телекоммуникационных сооружений, размещенных в зданиях (строениях, сооружениях), на проведение работ и предпринять все необходимые меры по сохранению цифровых технологических систем и телекоммуникационных сооружений, затрагиваемых работами.

4. Нарушение мер по обеспечению цифровой устойчивости технологических систем влечет ответственность в соответствии с законодательством Кыргызской Республики. Ущерб, причиненный в результате несанкционированного подсоединения к цифровым технологическим системам, вмешательства в их работу либо их повреждения, возмещается владельцу системы лицом, причинившим вред, в полном объеме.

Глава 21. Телекоммуникационные сети

Статья 175. Правовое регулирование телекоммуникационных сетей

1. Кыргызская Республика регулирует использование телекоммуникационных сетей на основеКонституции, настоящего Кодекса и законов Кыргызской Республики, международных договоров, участницей которых является Кыргызская Республика, и решений международных организаций в сфере телекоммуникаций. Термины, относящиеся к телекоммуникационным сетям, используются в значении, установленном в документах Международного союза электросвязи, если иное не установлено настоящим Кодексом.

2. Использование телекоммуникационных сетей и их регулирование должны осуществляться с учетом общепризнанной международной практики в сфере телекоммуникаций.

3. Если согласно законодательству Кыргызской Республики необходимо подтверждение соответствия требованиям, установленным настоящим Кодексом, могут быть использованы документы, полученные согласно законодательству иностранных государств, если они подтверждают соответствие требованиям, которые эквивалентны или выше требований, установленных настоящим Кодексом.

Статья 176. Отраслевые принципы регулирования

1. Субъекты правоотношений в цифровой среде вправе свободно создавать телекоммуникационные сети и пользоваться ими в Кыргызской Республике (принцип свободы телекоммуникаций).

2. Регулирование деятельности по созданию телекоммуникационных сетей и пользованию ими обеспечивает непрерывность их эксплуатации и недопустимость произвольного прекращения или приостановления эксплуатации телекоммуникационных сетей или вмешательства в их эксплуатацию (принцип непрерывности).

3. Регулирование деятельности по созданию телекоммуникационных сетей и пользованию ими обеспечивает их постоянное развитие и взаимодействие с телекоммуникационными сетями других стран в соответствии с общепризнанной международной практикой (принцип развития).

4. Телекоммуникационные сети и их регулирование должны быть организованы таким образом, чтобы способствовать увеличению количества пользователей, имеющих возможность взаимодействия между собой с использованием телекоммуникационных сетей (принцип взаимодействия).

5. Устойчивое развитие телекоммуникационных сетей и реализация принципов их регулирования возможны только при условии обеспечения совместимости телекоммуникационных сетей и их элементов (принцип совместимости).

6. При эксплуатации телекоммуникационных сетей и пользовании ими обеспечивается целостность и неприкосновенность передаваемых цифровых данных, при этом владельцы телекоммуникационных сетей не вправе контролировать содержание передаваемых цифровых данных и не несут ответственности за их содержание (принцип неприкосновенности).

7. Кыргызская Республика обеспечивает и поддерживает равные условия конкуренции для всех операторов телекоммуникаций независимо от их форм собственности путем регулирования и пресечения монополистической деятельности, предоставления равноправного доступа к радиочастотному ресурсу и ресурсу нумерации, защиты интересов принципалов записей в таких ресурсах (принцип недискриминации).

Статья 177. Категории телекоммуникационных сетей

1. Телекоммуникационные сети на территории Кыргызской Республики делятся на следующие категории в зависимости от их назначения:

1) общего пользования, предназначенные для предоставления общедоступных телекоммуникационных сервисов неограниченному кругу лиц;

2) внутренние, предназначенные для предоставления телекоммуникационных сервисов ограниченному кругу пользователей в интересах одного или группы юридических лиц;

3) закрытые, предназначенные для предоставления телекоммуникационных сервисов ограниченному кругу пользователей в интересах одного или группы юридических лиц без доступа к ним из телекоммуникационных сетей общего пользования;

4) засекреченные, предназначенные для предоставления телекоммуникационных сервисов ограниченному кругу пользователей в случаях, предусмотренных законодательством Кыргызской Республики в сфере защиты государственных секретов;

5) телерадиовещания, предназначенные для предоставления вещательных сервисов.

2. На закрытые и засекреченные телекоммуникационные сети не распространяется действие статей176,178,181-184настоящего Кодекса.

3. Требования по организации, эксплуатации засекреченных телекоммуникационных сетей и порядок предоставления телекоммуникационных сервисов в таких сетях регулируются нормативными правовыми актами Кыргызской Республики в сфере защиты государственных секретов. Контроль за исполнением требований осуществляется уполномоченным государственным органом в сфере обеспечения национальной безопасности.

4. Правительственная сеть связи Кыргызской Республики относится к засекреченным телекоммуникационным сетям.

Статья 178. Размещение телекоммуникационных сетей

1. Операторы телекоммуникаций имеют право прохода (право на строительство, установку, эксплуатацию, техническое обслуживание и ремонт телекоммуникационных сетей и их элементов, а также телекоммуникационных сооружений) в отношении земельных участков, выделенных под общественные нужды (включая общественные дороги, тротуары или иные общественные земли или сооружения).

2. Операторы телекоммуникаций имеют право строить, устанавливать и эксплуатировать опоры, линии и иные телекоммуникационные сооружения на участках земли, в зданиях и сооружениях, на столбовых опорах, мостах, трубопроводах, дорогах, в коллекторах, железнодорожных туннелях и других местах на основании договора с владельцами таких земельных участков или сооружений. Для владельцев земельных участков, зданий и сооружений заключение договоров, предусмотренных настоящей частью, является обязательным в соответствии с гражданским законодательством.

3. Любое строительство и эксплуатация телекоммуникационных сетей или сооружений должны вестись с учетом норм экологической безопасности и архитектурно-художественных требований к инфраструктуре, в отношении которой производятся такие работы. При этом принимаются меры по уменьшению возможного ущерба имуществу или правам собственника в связи с осуществлением строительства и эксплуатации телекоммуникационных сетей или сооружений, а также в связи с предоставленными правами прохода. По завершении любых работ по строительству, установке или ремонту телекоммуникационных сетей или сооружений оператор телекоммуникаций за свой счет обязан привести затронутую работами инфраструктуру в первоначальное состояние.

4. Оператор телекоммуникаций обязан возместить ущерб, причиненный зданию, земельному участку или сооружениям в результате строительства, установки, ремонта, а также эксплуатации телекоммуникационных сетей или сооружений, включая любое уменьшение стоимости этих объектов.

5. В экстренных случаях при необходимости проведения оператором телекоммуникаций неотложных работ по восстановлению или монтажу телекоммуникационных сетей или сооружений на участке земли, в здании или иных сооружениях, которые не являются собственностью такого оператора, оператор телекоммуникаций обязан приложить все усилия для своевременного уведомления владельца земельного участка, здания или иных сооружений и получения его согласия на проведение таких работ. Отсутствие согласия владельца не является препятствием для проведения этих работ и не освобождает оператора телекоммуникаций от возмещения любого ущерба, причиненного при выполнении таких работ. Стоимость ущерба определяется независимой оценочной комиссией в соответствии с законодательством.

6. Операторы телекоммуникаций обязаны заключать и исполнять соглашения о предоставлении доступа другим операторам телекоммуникаций к кабелепроводам, коллекторам, правам прохода, опорам и другим телекоммуникационным сооружениям там, где это технически возможно. Любой оператор телекоммуникаций, использующий такие кабелепроводы, коллекторы, права прохода, опоры и другие сооружения, обязан:

1) обеспечить, чтобы его собственные сооружения и сервисы не вызывали технических или физических препятствий, а также помех при эксплуатации систем, предоставлении сервисов и ведении иной деятельности владельца указанных сооружений;

2) принимать немедленные меры по устранению любых таких препятствий или помех;

3) полностью компенсировать все затраты, ущерб или иные экономические убытки, понесенные в результате возникновения вышеуказанных препятствий или помех.

7. Оператор телекоммуникаций самостоятельно и за свой счет осуществляет демонтаж телекоммуникационных сетей, сооружений и оборудования. Принудительный демонтаж телекоммуникационных сетей, сооружений и оборудования осуществляется только по решению суда, если иное не установлено договором, предусмотренным частью 2 настоящей статьи.

Статья 179. Отраслевой регулятор телекоммуникаций

1. Регулирование деятельности, связанной с телекоммуникационными сетями, и надзор за такой деятельностью осуществляются уполномоченным государственным органом, создаваемым в порядке, установленномстатьей 9настоящего Кодекса (отраслевым регулятором телекоммуникаций). Отраслевой регулятор телекоммуникаций независим в своей деятельности от лиц, в отношении которых он осуществляет свои полномочия.

2. Руководитель отраслевого регулятора телекоммуникаций должен обладать квалификацией, опытом и знаниями в сфере цифровых технологий, необходимыми для выполнения обязанностей и осуществления полномочий.

3. Отраслевой регулятор телекоммуникаций:

1) реализует государственные программы и планы развития телекоммуникаций в Кыргызской Республике;

2) выполняет функции администрации связи Кыргызской Республики при осуществлении международной деятельности в сфере телекоммуникаций;

3) взаимодействует в порядке, установленном законодательством, с органами саморегулирования в сфере телекоммуникаций;

4) организует сбор статистической и иной информации о деятельности операторов телекоммуникаций;

5) выполняет функции органа лицензирования в сфере телекоммуникаций;

6) принимает предусмотренные антимонопольным законодательством меры для защиты и развития конкуренции в сфере телекоммуникаций, в том числе осуществляет регулирование цен (тарифов) субъектов естественных монополий, включая их установление, пересмотр или утверждение;

7) организует обязательное подтверждение соответствия цифровых устройств, используемых в рамках телекоммуникационных сетей, в том числе радиоэлектронных средств;

8) разрабатывает, актуализирует проекты технических регламентов и национальных стандартов, а также совместно с государственным органом по стандартизации регистрирует национальные стандарты с установлением технических требований и норм применения международных (региональных) стандартов;

9) проводит оценку цифровой устойчивости телекоммуникационных сетей операторов телекоммуникаций и публикует ее результаты;

10) ведет государственный надзор за соответствием деятельности принципалов записей в радиочастотном реестре и реестре нумерации условиям таких записей;

11) создает, развивает и эксплуатирует государственную систему радиоконтроля на территории Кыргызской Республики для проведения общих измерений использования радиочастот, проверки технических и эксплуатационных характеристик передаваемых радиосигналов, обнаружения и опознавания помех, несанкционированных радиопередатчиков и источников высокочастотного электромагнитного излучения;

12) участвует в разработке методик обучения, повышения квалификации государственных и муниципальных служащих и иных лиц в сфере телекоммуникаций;

13) выявляет и устраняет радиопомехи или несанкционированные сигналы на территории Кыргызской Республики, осуществляет взаимодействие с уполномоченными органами в сфере телекоммуникаций других государств, направленное на устранение помехового влияния радиоэлектронных средств других государств на радиоэлектронные средства операторов телекоммуникаций Кыргызской Республики.

4. Финансирование деятельности отраслевого регулятора телекоммуникаций производится за счет бюджетных средств и за счет ежегодных отчислений операторов телекоммуникаций в размере 0,9 процентов от суммы их выручки по предоставлению телекоммуникационных сервисов (в полном объеме подлежащих зачислению в республиканский бюджет, из которых 40 процентов направляются на развитие телекоммуникационной отрасли, 60 процентов - на развитие цифровизации), а также за счет других источников финансирования, не запрещенных законодательством Кыргызской Республики.

5. Для достижения прозрачности своих регулирующих функций отраслевой регулятор телекоммуникаций должен публиковать годовой отчет о деятельности и результаты оценки цифровой устойчивости телекоммуникационных сетей на своем сайте.

6. Отраслевой регулятор телекоммуникаций в связи с его деятельностью имеет право:

1) запрашивать и безвозмездно получать у физических и юридических лиц необходимую для реализации своих полномочий информацию, в том числе отнесенную к государственным секретам или иной охраняемой законом тайне;

2) требовать от оператора телекоммуникаций принятия мер по соблюдению лицензионных требований;

3) обращаться в суд с исковыми заявлениями в защиту прав операторов телекоммуникаций или пользователей телекоммуникационных сервисов, а также принципалов записей в радиочастотном ресурсе и ресурсе нумерации, в том числе в защиту прав неопределенного круга лиц, и представлять интересы указанных лиц в суде;

4) направлять в правоохранительные органы в соответствии с подследственностью материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений в сфере телекоммуникаций;

5) вносить в Кабинет Министров предложения о принятии, изменении или отмене нормативных правовых актов в сфере телекоммуникаций;

6) привлекать к ответственности лиц, виновных в нарушении настоящего Кодекса.

7. Отраслевой регулятор телекоммуникаций обязан:

1) обеспечивать соблюдение лицензионных требований и условий использования радиочастотного ресурса и ресурса нумерации;

2) регулярно осуществлять проверки соблюдения операторами телекоммуникаций и принципалами записей в радиочастотном ресурсе и ресурсе нумерации положений настоящего Кодекса и выносить по результатам проверок обязательные для исполнения решения;

3) обеспечивать выполнение решений Национальной комиссии по радиочастотам;

4) обеспечивать выполнение обязательств, возложенных на операторов телекоммуникаций в интересах национальной безопасности, обороны, охраны правопорядка и при чрезвычайных ситуациях;

5) рассматривать жалобы и обращения операторов телекоммуникаций и пользователей их телекоммуникационных сервисов и по результатам их рассмотрения принимать в пределах своих полномочий обязательные для исполнения решения;

6) давать разъяснения по вопросам применения настоящего Кодекса и принятых в соответствии с ним нормативных правовых актов в сфере телекоммуникаций по запросу физических лиц и организаций с опубликованием таких разъяснений на своем сайте;

7) разрабатывать и публиковать рекомендации по вопросам развития телекоммуникаций, разрабатывать и публиковать типовые формы договоров, правовых актов и иных документов в сфере телекоммуникаций.

Статья 180. Участие в международном регулировании телекоммуникаций

1. Кыргызская Республика является членом Международного союза электросвязи и признает его основные документы:

1) Устав Международного союза электросвязи;

2) Конвенцию Международного союза электросвязи;

3) административные регламенты - Регламент международной электросвязи, Регламент радиосвязи.

2. Отраслевой регулятор телекоммуникаций в рамках своих полномочий и в соответствии с международными договорами, вступившими в силу в соответствии с законодательством Кыргызской Республики:

1) обеспечивает в необходимых случаях международное признание радиочастотных присвоений Кыргызской Республики путем принятия мер по их внесению в Международный справочный регистр радиочастот с положительным заключением;

2) защищает радиочастотные присвоения от вредных помех, создаваемых владельцами радиоэлектронных средств и высокочастотных устройств из других стран, путем анализа международных информационных циркуляров по частотам Бюро радиосвязи Международного союза электросвязи и принятия мер по недопущению помех в соответствии с Регламентом радиосвязи или межправительственными соглашениями об использовании радиочастотного спектра, если таковые имеются;

3) сотрудничает с администрациями связи других стран в сфере координации и (или) взаимного признания выделенных радиочастот и частотных присвоений на основе Регламента радиосвязи или межправительственных соглашений по использованию радиочастотного спектра;

4) гармонизирует Национальную таблицу распределения радиочастот Кыргызской Республики с Международной таблицей распределения радиочастот;

5) гармонизирует Национальный план нумерации с решениями международных организаций;

6) обеспечивает участие специалистов отрасли и научно-образовательных организаций, осуществляющих подготовку кадров в сфере телекоммуникаций, в работе конференций и исследовательских комиссий Международного союза электросвязи.

3. Членские взносы за участие Кыргызской Республики в деятельности международных организаций по телекоммуникациям оплачиваются за счет бюджета отраслевого регулятора телекоммуникаций.

Глава 22. Взаимодействие владельцев цифровых технологических систем между собой и с государственными органами

Статья 181. Лицензирование деятельности операторов телекоммуникаций

1. Субъект правоотношений в цифровой среде признается оператором телекоммуникаций и обязан действовать на основании лицензии, если он одновременно соответствует трем критериям:

1) является или намеревается стать владельцем телекоммуникационной сети общего пользования или телерадиовещания, расположенной на территории Кыргызской Республики;

2) предоставляет или намеревается предоставлять телекоммуникационные сервисы пользователям в Кыргызской Республике с использованием такой телекоммуникационной сети;

3) использует или намеревается использовать для предоставления телекоммуникационных сервисов радиочастотный спектр и (или) нумерацию, и (или) инфраструктуру в Кыргызской Республике.

2. Субъект правоотношений в цифровой среде, намеревающийся осуществлять деятельность оператора телекоммуникаций, обязан обратиться в отраслевой регулятор телекоммуникаций для получения лицензии. Субъект правоотношений в цифровой среде, которому выдана лицензия на деятельность оператора телекоммуникаций, обязан начать предоставление телекоммуникационного сервиса и обеспечить выполнение лицензионных требований в течение двух лет с момента получения лицензии.

3. Порядок получения лицензии на деятельность операторов телекоммуникаций, а также ее приостановления, возобновления, прекращения, переоформления определяется Положением о лицензировании деятельности операторов телекоммуникаций, утверждаемым Кабинетом Министров. При выдаче, переоформлении лицензии и (или) разрешения и выдаче их дубликатов взимается государственная пошлина в соответствии с законодательством Кыргызской Республики о неналоговых доходах. Лицензия на деятельность операторов телекоммуникаций является бессрочной.

4. Лицензионные требования устанавливаются Кабинетом Министров и включают:

1) владение телекоммуникационной сетью на территории Кыргызской Республики и ее эксплуатацию;

2) использование радиочастотного спектра, нумерации или инфраструктуры в соответствии с настоящим Кодексом;

3) взаимодействие с сетями общего пользования в Кыргызской Республике в соответствии с настоящим Кодексом;

4) взаимодействие с государственными органами Кыргызской Республики в соответствии с настоящим Кодексом;

5) перечисление платы за использование радиочастотного спектра и нумерации в соответствии с настоящим Кодексом;

6) ежегодные отчисления в размере 0,9 процентов от выручки за предоставление телекоммуникационных сервисов.

5. Установление иных лицензионных требований, кроме предусмотренных настоящим Кодексом и соответствующими актами Кабинета Министров, не допускается.

6. Виртуальные операторы не могут осуществлять деятельность без взаимодействия с оператором телекоммуникаций.

7. Лицензионный контроль в сфере телекоммуникаций осуществляется в соответствии с Положением о лицензировании, утвержденным Кабинетом Министров.

Статья 182. Торги на право использования радиочастот

1. Отраслевой регулятор телекоммуникаций в своем решении определяет форму проведения торгов в отношении сервисных радиочастот:

1) торги проводятся в форме конкурса, если для реализации принципов регулирования, установленных настоящим Кодексом, радиочастоты должны быть выделены участнику, предложившему лучший инвестиционный проект;

2) во всех остальных случаях выделения сервисных радиочастот торги проводятся в форме онлайн-аукциона.

2. Определение победителя конкурса осуществляется конкурсной комиссией в составе не менее 7 человек, формируемой решением Кабинета Министров из представителей:

1) Жогорку Кенеша Кыргызской Республики;

2) Кабинета Министров;

3) Национальной комиссии по радиочастотам;

4) отраслевого регулятора телекоммуникаций;

5) профессиональных ассоциаций операторов телекоммуникаций.

3. Членами конкурсной комиссии не могут быть лица, лично заинтересованные в результатах конкурса (в том числе физические лица, подавшие заявки на участие в конкурсе либо состоящие в трудовых отношениях с лицами, подавшими указанные заявки), либо физические лица, на которых может быть оказано влияние участниками конкурса (в том числе

физические лица, являющиеся участниками (акционерами) юридических лиц, членами их органов управления, кредиторами участников конкурса).

4. Стартовая цена онлайн-аукциона рассчитывается исходя из:

1) ширины полосы номинала или полосы радиочастот (прием-передача);

2) географической зоны покрытия;

3) коэффициента коммерческой привлекательности;

4) расчетного коэффициента.

5. Для допуска к торгам участники вносят гарантийный взнос в размере 5% от стартовой стоимости лота. Шаг онлайн-аукциона составляет 5% от стартовой стоимости лота.

6. Гарантийный взнос подлежит возврату:

1) при признании торгов несостоявшимися;

2) участникам, которые не были признаны победителями торгов.

7. Дата и условия проведения торгов устанавливаются отраслевым регулятором телекоммуникаций и публикуются на его сайте не позднее чем за 30 календарных дней до дня проведения торгов.

8. Победителем аукциона признается лицо, предложившее наибольшую цену за лот. Победителем конкурса признается лицо, предложившее лучший инвестиционный проект в соответствии с опубликованными условиями оценки инвестиционных проектов.

9. Результаты конкурса оформляются протоколом, подписываемым всеми членами конкурсной комиссии. Результаты онлайн-аукциона определяются на основании отчетной формы системы онлайн-аукционов, имеющей силу протокола.

10. Торги признаются несостоявшимися в следующих случаях:

1) на конкурс не было подано ни одного предложения или ни один участник не зарегистрировался на онлайн-аукцион;

2) ни одно из конкурсных предложений не соответствует условиям конкурса;

3) по итогам онлайн-аукциона не была создана отчетная форма;

4) ни один из зарегистрированных участников онлайн-аукциона не повысил стартовую цену в течение 30 минут с момента начала онлайн-аукциона.

11. Данные о результатах торгов размещаются на сайте отраслевого регулятора телекоммуникаций не позднее 1 рабочего дня, следующего за днем их завершения.

12. Победитель торгов обязан оплатить цену лота в течение 7 банковских дней после дня публикации результатов торгов. В случае неуплаты победителем установленной цены в предусмотренный срок право использования радиочастотного спектра переходит участнику, занявшему второе место. Если установленная цена не уплачена ни одним из участников торгов, торги проводятся повторно.

13. Порядок проведения торгов устанавливается Кабинетом Министров.

Статья 183. Взаимодействие с отраслевым регулятором телекоммуникаций при ведении цифровых реестров

1. Решение о выделении или присвоении радиочастот либо о выделении диапазона нумерации принимается на основании заявления, поданного по форме, утвержденной отраслевым регулятором телекоммуникаций и опубликованной им на своем сайте. Срок принятия решения и создания соответствующей записи в цифровом реестре не может превышать:

1) 1 рабочего дня со дня внесения полной стоимости цены лота, определенной по результатам торгов - при выделении радиочастот по результатам торгов;

2) 90 календарных дней со дня получения заявления (включая срок предоставления услуги по обеспечению электромагнитной совместимости) - при выделении или присвоении радиочастот в остальных случаях;

3) 15 рабочих дней со дня получения заявления - при выделении нумерации.

2. Отраслевой регулятор телекоммуникаций принимает решение об отказе в выделении или присвоении радиочастот в случаях невозможности обеспечения электромагнитной совместимости радиочастоты с характеристиками, указанными в заявлении, и недостоверности данных в поданном заявлении. Если решение принималось по результатам торгов, то решение о выделении радиочастот принимается только в пользу участника торгов, признанного победителем.

3. Отраслевой регулятор вносит изменения в запись в соответствующем реестре не позднее трех рабочих дней, следующих за днем получения данных о:

1) реорганизации юридического лица;

2) изменении наименования юридического лица;

3) изменении фамилии, имени, отчества физического лица;

4) перераспределении, совместном использовании, отчуждении соответствующего объекта учета;

5) изменении радиослужбы в связи с переходом на новые технологии, улучшающие характеристики оказываемых телекоммуникационных сервисов;

6) продлении права на использование радиочастот;

7) изменении условий использования, указанных в записи;

8) внесении изменений в Национальную таблицу распределения радиочастот или Национальный план нумерации;

9) прекращении права использования соответствующего объекта учета полностью или частично;

10) выявлении ошибок после создания записи, в том числе при несоответствии данных в записи решению отраслевого регулятора телекоммуникаций, на основании которого была создана или изменена запись.

4. Если внесение изменений в запись в радиочастотном реестре связано с изменением Национальной таблицы распределения радиочастот, номиналов или полос радиочастот либо с изменением установленных условий их использования, отраслевой регулятор телекоммуникаций проводит мероприятия по обеспечению электромагнитной совместимости радиочастот до внесения изменений в запись. Плата за обеспечение электромагнитной совместимости при этом не взимается. Затраты, понесенные принципалом записи в связи с переходом на другие частоты по решению отраслевого регулятора телекоммуникаций до окончания срока действия выделения или присвоения, компенсируются государством.

5. Изменение радиослужбы в связи с переходом на новые технологии допускается с учетом общепризнанной международной практики и только при обеспечении электромагнитной совместимости.

6. Продление права на использование радиочастотного спектра осуществляется на основании заявления принципала соответствующей записи. Право на использование радиочастотного спектра продлевается на срок не менее 5 и не более 10 лет. При этом право на использование радиочастотного спектра может быть продлено на срок менее 5 лет исключительно по инициативе принципала, если принципал соответствующей записи в заявлении указал срок продления менее чем 5 лет.

7. За продление права на использование радиочастотного спектра взимается плата, рассчитываемая в зависимости от запрашиваемого срока продления, в следующем размере:

1) за каждый полный календарный год - в размере 1% от расчетной стартовой цены таких частот;

2) за каждый календарный день - в размере 0,00273973% от расчетной стартовой цены таких частот (при расчете неполного календарного года).

8. Если запрашиваемый срок продления состоит из полного календарного года (лет), календарных месяцев и календарных дней, то календарные месяцы переводятся в календарные дни, при этом плата за продление рассчитывается согласно пунктам 1 и 2 части 7 настоящей статьи.

Расчетная стартовая цена частот рассчитывается на момент принятия решения о продлении в соответствии с Положением о порядке проведения торгов на право использования радиочастотного спектра, утверждаемым Кабинетом Министров.

9. При продлении права на использование радиочастотного спектра исключительно для целей, не связанных с предоставлением телекоммуникационных сервисов и/или для выполнения публичных обязательств, возложенных в соответствии с законодательством, принципалы соответствующих записей освобождаются от внесения платы, предусмотренной частью 7 настоящей статьи.

10. Право на использование радиочастотного спектра прекращается в случаях:

1) обращения принципала записи с заявлением о прекращении права;

2) прекращения деятельности принципала записи, в том числе при ликвидации юридического лица без правопреемства, смерти физического лица или признания физического лица недееспособным в установленном законом порядке;

3) истечения срока, на который было предоставлено право, при отсутствии заявления принципала записи о его продлении;

4) вступления в законную силу решения суда об отмене решения отраслевого регулятора телекоммуникаций, на основании которого была создана запись в реестре;

5) неиспользования радиочастот в течение двух лет со дня возникновения права на их использование.

11. Право на использование нумерации прекращается полностью в случаях:

1) обращения принципала записи с заявлением о прекращении права;

2) неиспользования выделенного диапазона нумерации в течение одного года со дня создания соответствующей записи в цифровом реестре нумерации;

3) использования нумерации в нарушение Национального плана нумерации Кыргызской Республики.

12. Право на использование нумерации прекращается в отдельной части диапазона нумерации путем внесения соответствующих изменений в запись в цифровом реестре нумерации в случаях:

1) обращения принципала записи с заявлением об отказе от части диапазона нумерации;

2) использования нумерации в объеме менее 20% от диапазона, указанного в соответствующей записи, в течение 2 лет со дня создания соответствующей записи в цифровом реестре нумерации. В таком случае из права на использование исключается 80% неиспользуемой нумерации;

3) использования нумерации в нарушение Национального плана нумерации Кыргызской Республики.

13. Отраслевой регулятор телекоммуникаций по заявлению принципала записи в цифровом реестре обязан создать и передать ему копии относящихся к нему записей в виде документов на бумажном носителе или цифровых документов, подписанных уполномоченным должностным лицом отраслевого регулятора телекоммуникаций. Срок создания и передачи копий не может превышать пяти рабочих дней со дня получения заявления принципала записи.

14. Порядок взаимодействия при ведении цифровых реестров определяется отраслевым регулятором телекоммуникаций с учетом требований настоящего Кодекса.

Статья 184. Взаимодействие операторов телекоммуникаций в процессе перераспределения, совместного использования и передачи радиочастот и нумерации

1. Принципалы записей в цифровых реестрах вправе взаимодействовать в целях:

1) перераспределения между собой выделенных им радиочастот;

2) совместного использования выделенных им радиочастот;

3) отчуждения выделенных (присвоенных) им радиочастот.

2. Перераспределение, совместное использование и передача соответствующих объектов учета осуществляется на основании соглашения между принципалами записей с обязательным уведомлением отраслевого регулятора телекоммуникаций. При перераспределении к уведомлению прилагается проект соглашения с описанием целей и условий такого перераспределения.

3. Отраслевой регулятор телекоммуникаций в течение тридцати дней со дня получения уведомления в соответствии с частью 2 настоящей статьи предпринимает одно из следующих действий:

1) принимает решение о проведении онлайн-аукциона (в случае принятия оператором телекоммуникаций решения об отчуждении радиочастот);

2) вносит изменения в запись в соответствующем реестре (в случае перераспределения или совместного использования радиочастот, отчуждения нумерации);

3) принимает решение о запрете перераспределения, совместного использования или отчуждения соответствующих объектов (в случае несоответствия целей или условий перераспределения, совместного использования или отчуждения объектов учета Национальной таблице распределения радиочастот или Национальному плану нумерации Кыргызской Республики).

4. Отчуждение радиочастот, право на использование которых было получено по результатам торгов, осуществляется единым лотом на онлайн-аукционе в порядке, установленном в соответствии с настоящим Кодексом. Отраслевой регулятор принимает решение о проведении онлайн-аукциона одновременно с согласием на заключение соглашения. Соглашение об отчуждении радиочастот заключается с победителем онлайн-аукциона. Победитель онлайн-аукциона выплачивает цену лота принципалу записи, отчуждающему право на использование радиочастот, а также отчисляет отраслевому регулятору телекоммуникаций плату в размере 5% от итоговой цены лота, направляемую на развитие отраслевого регулятора телекоммуникаций.

Статья 185. Взаимодействие с цифровыми технологическими системами идентификации мобильных устройств

1. Мобильные устройства, используемые для получения сервисов в сетях операторов телекоммуникаций Кыргызской Республики, подлежат обязательной регистрации в государственной цифровой технологической системе идентификации мобильных устройств.

2. Операторы телекоммуникаций обязаны предоставлять телекоммуникационные сервисы на зарегистрированные мобильные устройства.

3. Порядок функционирования государственной цифровой технологической системы идентификации мобильных устройств, их взаимодействия с операторами телекоммуникаций, порядок регистрации мобильных устройств, сроки введения ограничений на обслуживание незарегистрированных мобильных устройств определяются Кабинетом Министров.

Статья 186. Взаимодействие операторов телекоммуникаций в цифровой технологической системе по противодействию мошенничеству

1. В целях защиты прав и законных интересов граждан и юридических лиц от мошеннических действий, совершаемых с использованием телекоммуникационных сетей и сервисов, цифровых финансовых услуг, устанавливается система взаимодействия между операторами телекоммуникаций, правоохранительными органами, коммерческими банками,

микрофинансовыми организациями (микрокредитными и микрофинансовыми компаниями), иными поставщиками платежных услуг (далее - участники взаимодействия).

2. Цифровая технологическая система по противодействию мошенничеству направлена на оперативное выявление, предупреждение, пресечение и расследование случаев мошенничества, связанных с:

а) несанкционированным доступом к системам дистанционного банковского обслуживания или электронным кошелькам;

б) телефонным мошенничеством (вишинг);

в) рассылкой фишинговых или вредоносных сообщений через сети телекоммуникаций (СМС-фишинг, смишинг);

г) созданием поддельных (фишинговых) веб-ресурсов финансовых и иных организаций;

д) иными видами мошенничества с использованием средств телекоммуникаций в целях совершения либо содействия совершению противоправных действий финансового характера.

3. Операторы телекоммуникаций обязаны:

а) внедрять и использовать технические средства и программное обеспечение для выявления и блокировки мошеннического трафика, включая вызовы и сообщения с фальсифицированных номеров, несанкционированные массовые рассылки, а также трафик, перенаправляющий на известные фишинговые ресурсы, в соответствии с процедурами, установленными Кабинетом Министров;

б) предоставлять незамедлительно по законному и обоснованному запросу правоохранительных органов информацию, необходимую для выявления, предупреждения, пресечения и расследования мошенничества, включая данные о соединениях, абонентских номерах, местоположении оборудования в момент совершения подозрительных действий, со строгим соблюдением законодательства Кыргызской Республики о защите персональных данных;

в) участвовать в автоматизированном обмене информацией с другими участниками взаимодействия о выявленных мошеннических номерах, вредоносных ссылках, признаках и схемах мошенничества в порядке и форматах, определенных Кабинетом Министров;

г) информировать пользователей о рисках мошенничества и мерах предосторожности.

4. Коммерческие банки, микрофинансовые организации и иные поставщики платежных услуг обязаны:

а) внедрять и использовать цифровую технологическую систему по противодействию мошенничеству для выявления подозрительных и несанкционированных операций клиентов, имеющих признаки связи с мошенничеством, совершенным с использованием телекоммуникаций;

б) предоставлять незамедлительно по законному и обоснованному запросу правоохранительных органов информацию о подозрительных операциях, счетах и электронных кошельках, предположительно используемых в мошеннических целях, со строгим соблюдением законодательства Кыргызской Республики о банках и банковской деятельности, коммерческой тайне и защите персональных данных;

в) участвовать в автоматизированном обмене информацией с другими участниками взаимодействия о выявленных мошеннических операциях, счетах, используемых методах и признаках мошенничества в порядке и форматах, определенных Кабинетом Министров по согласованию с Национальным банком Кыргызской Республики;

г) информировать клиентов о рисках мошенничества, мерах безопасного использования дистанционных финансовых услуг и действиях при подозрении на мошенничество;

д) применять меры по приостановлению или блокированию подозрительных операций в соответствии с законодательством Кыргызской Республики и нормативными актами Национального банка Кыргызской Республики.

5. Все действия по обмену и обработке информации в рамках настоящей статьи должны осуществляться с соблюдением требований законодательств Кыргызской Республики о защите персональных данных, банках и банковской деятельности, тайне телекоммуникаций и иной охраняемой законом тайне.

Статья 187. Взаимодействие с правоохранительными органами

Взаимодействие операторов телекоммуникаций и виртуальных операторов с уполномоченными государственными органами, осуществляющими оперативно-розыскную и контрразведывательную деятельность, устанавливается законодательством в сферах контрразведывательной и разведывательной деятельности, а также оперативно-розыскной деятельности.

Статья 188. Взаимодействие виртуальных операторов и операторов телекоммуникаций

1. Взаимодействие виртуальных операторов с операторами телекоммуникаций осуществляется на основании соглашения, предусматривающего:

1) право виртуального оператора на использование телекоммуникационной сети оператора телекоммуникаций;

2) порядок взаимодействия оператора телекоммуникаций с пользователями виртуального оператора;

3) требования к условиям пользовательского соглашения виртуального оператора;

4) порядок взаимодействия виртуального оператора с правоохранительными органами с использованием телекоммуникационной сети оператора телекоммуникаций;

5) порядок учета объема телекоммуникационных сервисов и расчетов за них;

6) распределение ответственности между сторонами в ходе взаимодействия;

7) основания и последствия прекращения соглашения.

2. После заключения соглашения в соответствии с настоящей статьей стороны передают его копию отраслевому регулятору телекоммуникаций не позднее 30 календарных дней со дня заключения такого соглашения.

Статья 189. Межсетевое соединение

1. Оператор телекоммуникаций имеет право на взаимодействие с другими операторами телекоммуникаций в Кыргызской Республике с использованием телекоммуникационных сетей.

2. Взаимодействие операторов телекоммуникаций с использованием телекоммуникационных сетей осуществляется на основании соглашения о межсетевом соединении, заключаемом в порядке, установленном настоящим Кодексом.

3. Оператор телекоммуникаций, получивший запрос о заключении соглашения о межсетевом соединении, обязан предоставить ответ с указанием условий взаимодействия, а именно:

1) технических условий, касающихся присоединения сети;

2) местонахождения точек присоединения сетей;

3) порядка пропуска трафика по телекоммуникационным сетям;

4) стоимости присоединения сетей, пропуска трафика и порядка расчетов за них;

5) порядка взаимодействия систем управления телекоммуникационными сетями.

4. Если операторы телекоммуникаций не смогли заключить соглашение о межсетевом соединении в течение 3 месяцев со дня направления первоначального запроса, каждый из операторов телекоммуникаций вправе обратиться к отраслевому регулятору телекоммуникаций для разрешения спора о взаимодействии в порядке, установленном настоящим Кодексом.

5. Операторы телекоммуникаций обязаны предоставлять подписанное соглашение о межсетевом соединении или внесенные изменения в него отраслевому регулятору телекоммуникаций в срок не более 1 месяца со дня подписания либо внесения соответствующих изменений.

6. Оператор телекоммуникаций, признанный хозяйствующим субъектом, занимающим доминирующее положение в соответствии с антимонопольным законодательством, обязан устанавливать равные условия межсетевого соединения с любым оператором телекоммуникаций, в том числе со своими аффилированными лицами. Для оператора телекоммуникаций, признанного хозяйствующим субъектом, занимающим доминирующее положение в соответствии с антимонопольным законодательством, заключение соглашения о межсетевом соединении является обязательным.

7. После подписания соглашения о межсетевом соединении операторы телекоммуникаций не могут в одностороннем порядке прервать взаимодействие полностью или частично, а также расторгнуть соглашение о взаимодействии, за исключением случаев, перечисленных в настоящей части статьи.

Межсетевое соединение может быть прервано частично:

а) на основании судебного акта, вступившего в законную силу;

б) в случае выявления факта модификации, подавления и (или) иного способа изменения данных о номере, передаваемых по сетям телекоммуникаций;

в) в случае выявления факта проведения лотерей, голосований, конкурсов, викторин, опросов, массовых вызовов или рассылок сообщений, распространения рекламной информации, не согласованных между операторами телекоммуникаций;

г) при недостижении в течение 2 месяцев договоренности по финансовым условиям пропуска трафика, если обе стороны обеспечивают соединение пользователям своих сетей через сети других операторов телекоммуникаций.

Межсетевое соединение может быть прервано полностью:

а) на основании судебного акта, вступившего в законную силу;

б) при наличии задолженности по соглашению о межсетевом соединении за период три месяца и более.

Соглашение о межсетевом соединении может быть расторгнуто в случаях:

а) прекращения или аннулирования лицензии на деятельность оператора телекоммуникаций;

б) прекращения деятельности оператора телекоммуникаций;

в) полного изъятия ресурса нумерации, используемого в рамках межсетевого соединения;

г) при непрерывном отсутствии пропуска пользовательского трафика в течение 60 (шестидесяти) последовательных календарных дней. При этом оператор телекоммуникаций, инициирующий расторжение соглашения о межсетевом соединении, должен иметь данные расчетной системы, сведения по загрузке межсетевых каналов, подтверждающие отсутствие пропуска пользовательского трафика в течение 60 (шестидесяти) последовательных календарных дней.

8. Оператор телекоммуникаций, прерывающий межсетевое соединение в одностороннем порядке, обязан уведомить отраслевого регулятора телекоммуникаций не позднее рабочего дня, следующего за днем прекращения взаимодействия.

9. Оператор телекоммуникаций обязан уведомить отраслевого регулятора телекоммуникаций обо всех фактах задолженности по соглашению о межсетевом соединении, превышающей двухмесячный период взаимодействия.

Статья 190. Рассмотрение споров

1. В случае возникновения споров по вопросам взаимодействия операторов телекоммуникаций любая из сторон в порядке досудебного рассмотрения обязана обратиться в отраслевой регулятор телекоммуникаций.

2. В целях достижения мирного разрешения спора стороны проводят предварительные переговоры и осуществляют переписку.

3. Отраслевой регулятор телекоммуникаций рассматривает обращение о досудебном рассмотрении спора в течение 2 месяцев с даты его получения.

4. В целях рассмотрения спора отраслевой регулятор телекоммуникаций имеет право запросить любые данные, в предоставлении которых не может быть отказано.

5. Отраслевой регулятор телекоммуникаций не рассматривает спор в следующих случаях:

1) если предметом спора не является взаимодействие с использованием цифровых технологических систем;

2) если предметом спора является заключение соглашения о взаимодействии, при этом с момента направления одним оператором телекоммуникаций запроса о заключении соглашения другому оператору прошло менее 3 месяцев;

3) если с даты последнего действия, совершенного в ходе переговорного процесса, прошло более одного года.

6. В случаях, предусмотренных пунктами 1 и 3 части 5 настоящей статьи, операторы телекоммуникаций вправе обратиться напрямую в суд.

7. Отраслевой регулятор телекоммуникаций в целях разрешения спора имеет право в своем решении установить технические и (или) финансовые условия взаимодействия, которые будут обязательными для сторон.

8. Отраслевой регулятор телекоммуникаций выносит решение по спору с учетом имеющихся и предоставленных данных, относящихся к предмету спора. Решение отраслевого регулятора телекоммуникаций выносится в виде административного акта и может быть обжаловано в судебном порядке.

9. В случае если отраслевой регулятор телекоммуникаций не вынес решения в срок, указанный в части 3 настоящей статьи, спор не считается решенным, а руководитель отраслевого регулятора телекоммуникаций подлежит привлечению к ответственности за бездействие в соответствии с законодательством о правонарушениях.

Глава 23. Системы искусственного интеллекта

Статья 191. Принципы проектирования, разработки и применения систем искусственного интеллекта

1. Системы искусственного интеллекта проектируются, разрабатываются и применяются в Кыргызской Республике без ограничений, за исключением случаев, установленных настоящим Кодексом.

2. Способы проектирования, разработки и применения систем искусственного интеллекта определяются их владельцами с учетом общепризнанной международной практики на основе следующих отраслевых принципов:

1) регулирование, разработка и использование систем искусственного интеллекта с учетом необходимости снижения рисков причинения вреда охраняемым благам (принцип снижения рисков);

2) понятность и предсказуемость характеристик системы искусственного интеллекта, доступность технической документации на нее (принцип открытости);

3) понятность оснований для решений или рекомендаций системы искусственного интеллекта, возможность перепроверки таких оснований (принцип объяснимости);

4) эффективный контроль человеком применения систем искусственного интеллекта (принцип подконтрольности);

5) достоверность результатов применения систем искусственного интеллекта, соответствующая целям их применения (принцип точности);

6) устойчивость систем искусственного интеллекта к случайным сбоям и неполадкам на основе принятия мер по предотвращению перебоев в работе системы и сохранности ее основных функций при сбоях или внеплановых внешних воздействиях (принцип надежности);

7) защищенность систем искусственного интеллекта от несанкционированного внешнего воздействия (принцип безопасности).

3. Принципы, определенные в настоящей статье, составляют основу правового регулирования отношений по проектированию, разработке, применению систем искусственного интеллекта, в том числе при определении требований к системам искусственного интеллекта. Выполнение установленных требований к системам искусственного интеллекта обеспечивает соблюдение принципов, предусмотренных настоящей статьей.

Статья 192. Ограничения и ответственность в связи с проектированием, разработкой и применением систем искусственного интеллекта

1. Обязательные требования либо иные ограничения в отношении систем искусственного интеллекта повышенной опасности могут устанавливаться настоящим Кодексом исключительно в целях минимизации риска причинения вреда следующим благам (охраняемые блага):

1) жизнь и здоровье людей;

2) права и свободы человека и гражданина;

3) окружающая среда;

4) обороноспособность государства;

5) национальная безопасность государства;

6) общественный порядок.

2. Запрещаются проектирование, разработка или применение систем искусственного интеллекта для целенаправленного и заведомо незаконного причинения вреда охраняемым благам.

3. Владельцы и пользователи систем искусственного интеллекта независимо от степени их опасности обязаны принимать все разумные и необходимые меры для минимизации рисков причинения вреда охраняемым благам при проектировании, разработке и применении таких систем и несут ответственность за причиненный вред в соответствии с законодательством Кыргызской Республики.

4. Правила и стандарты проектирования, разработки и применения систем искусственного интеллекта могут устанавливаться регламентом профессионального объединения владельцев систем искусственного интеллекта и должны включать в себя требования к профессиональной этике, оценке опасности систем искусственного интеллекта, управлению рисками, проектированию и разработке систем искусственного интеллекта, управлению цифровыми данными и системе менеджмента качества, а также иные требования, не противоречащие настоящему Кодексу и обязательные к исполнению.

Статья 193. Оценка опасности системы искусственного интеллекта

1. Все системы искусственного интеллекта, применяемые в Кыргызской Республике, подлежат оценке опасности, которую их применение может создать для охраняемых благ.

2. Оценка опасности осуществляется владельцем системы искусственного интеллекта:

1) на этапе проектирования системы искусственного интеллекта или планирования изменений в нее;

2) по завершении разработки и до начала применения системы искусственного интеллекта или внесенных в нее запланированных изменений;

3) при любом незапланированном изменении, произошедшем в системе искусственного интеллекта или в среде ее применения, о котором стало известно владельцу или пользователю системы, и которое может повлиять на результат оценки ее опасности.

3. Оценка опасности осуществляется владельцем системы искусственного интеллекта по методике, определенной им самостоятельно в соответствии с требованиями, установленными Кабинетом Министров, с учетом общепризнанной мировой практики.

4. Результаты оценки опасности системы искусственного интеллекта и методика оценки подлежат размещению на сайте владельца системы искусственного интеллекта в простой и понятной физическим лицам форме, а также в формате открытых данных, за исключением информации, относящейся к государственным секретам.

Статья 194. Системы искусственного интеллекта повышенной опасности

1. К системам искусственного интеллекта повышенной опасности относятся такие системы, применение которых, по сравнению с альтернативными способами, повышает риск (вероятность или размер) причинения вреда охраняемым благам до уровня, при котором требуется принятие мер по управлению такими рисками.

2. Система искусственного интеллекта, которая по итогам оценки опасности отнесена к системам искусственного интеллекта повышенной опасности, может проектироваться, разрабатываться и применяться при условии соблюдения требований, установленных настоящим Кодексом, на протяжении всего жизненного цикла такой системы.

3. Система искусственного интеллекта не может быть отнесена к системам повышенной опасности, если ее применение при принятии соответствующих решений или совершении действий носит исключительно вспомогательный характер и не приводит к повышению риска причинения вреда охраняемым благам.

4. Кабинет Министров устанавливает в отношении систем искусственного интеллекта повышенной опасности требования к:

1) управлению рисками;

2) характеристикам указанных систем, обеспечивающим открытость, объяснимость, подконтрольность, точность, надежность и цифровую устойчивость таких систем;

3) качеству цифровых данных для таких систем;

4) технической документации на такие системы.

5. Владелец системы искусственного интеллекта повышенной опасности обязан:

1) обеспечить соответствие такой системы обязательным требованиям;

2) внедрить и на протяжении всего жизненного цикла такой системы поддерживать систему управления рисками, соответствующую требованиям настоящего Кодекса;

3) разработать надлежащую техническую документацию такой системы;

4) обеспечивать сохранность журналов работы системы в период ее нахождения под его контролем;

5) подтвердить соответствие системы требованиям, установленным настоящим Кодексом, до начала ее применения;

6) принять меры по устранению выявленных несоответствий системы установленным обязательным требованиям;

7) по требованию соответствующего уполномоченного государственного органа приостановить, а на основании вступившего в законную силу судебного акта - прекратить проектирование и разработку системы, если такие действия осуществляются с нарушением требований настоящего Кодекса.

Статья 195. Подтверждение соответствия систем искусственного интеллекта повышенной опасности обязательным требованиям

1. До начала применения системы искусственного интеллекта повышенной опасности ее владелец обязан подтвердить ее соответствие требованиям, установленным настоящим Кодексом, путем принятия декларации. Форма указанной декларации, а также требования к ее содержанию утверждаются Кабинетом Министров.

2. Принятая декларация должна быть изложена в форме цифрового документа, подписана квалифицированной цифровой подписью и размещена на сайте владельца системы искусственного интеллекта. Указанная декларация относится к общедоступным цифровым записям.

Статья 196. Использование систем искусственного интеллекта повышенной опасности

1. Пользователь системы искусственного интеллекта повышенной опасности обязан:

1) использовать ее в соответствии с руководством по эксплуатации;

2) обеспечивать релевантность цифровых данных, обрабатываемых с использованием такой системы;

3) обеспечивать эффективный контроль работы системы в период ее использования, включая выделение для этого необходимых ресурсов и определение лиц, ответственных за такой контроль;

4) при наличии оснований полагать, что использование системы в соответствии с руководством по эксплуатации может привести к причинению вреда охраняемым благам, незамедлительно уведомить владельца системы и приостановить ее использование;

5) обеспечивать сохранность журналов работы системы в период ее нахождения под его контролем;

6) использовать информацию, предоставленную владельцем системы, для выполнения обязанностей, предусмотренных настоящим Кодексом;

7) по требованию уполномоченного государственного органа приостановить, а на основании вступившего в законную силу судебного акта - прекратить применение такой системы, если такие действия осуществляются с нарушением требований настоящего Кодекса.

2. При применении системы искусственного интеллекта повышенной опасности для получения результата, который используется для принятия решения, способного повлечь нарушение прав, свобод или законных интересов физических или юридических лиц, пользователь указанной системы обязан:

1) в случаях проектирования, разработки или применения системы для взаимодействия с физическими лицами - потребителями, размещать на своем сайте, а в остальных случаях - предоставлять в доступной и понятной форме общие сведения о характеристиках такой системы, принципах ее работы, а также о принципах получения и применения соответствующего результата;

2) по требованию лиц, интересы которых затрагиваются таким решением, безвозмездно предоставлять им информацию в доступной и понятной форме, позволяющей понять и проверить предпосылки и способы получения относящегося к ним результата, полученного с применением такой системы.

3. На пользователя системы искусственного интеллекта повышенной опасности либо на иное лицо возлагаются обязанности владельца такой системы, если:

1) система вводится в эксплуатацию от имени такого лица (под его наименованием, товарным знаком либо иным аналогичным обозначением);

2) такое лицо изменяет назначение системы после ее ввода в эксплуатацию, либо вносит в нее существенные изменения;

3) система вводится в эксплуатацию либо изменяется ее назначение таким образом, что она становится системой искусственного интеллекта повышенной опасности или частью такой системы.

4. В случаях, предусмотренных пунктами 2 и 3 части 3 настоящей статьи, первоначальный владелец системы искусственного интеллекта повышенной опасности освобождается от исполнения обязанностей, предусмотренных настоящей главой.

5. Если система искусственного интеллекта повышенной опасности применяется пользователем исключительно для личных или семейных нужд, такой пользователь освобождается от исполнения обязанностей, установленных пунктами 2-6 части 1 и частью 2 настоящей статьи. При этом в случаях, когда в результате такого применения нарушаются права, свободы или законные интересы третьих лиц, ответственность за исполнение указанных обязанностей несут солидарно данный пользователь и лицо, предоставившее ему доступ к соответствующей системе.

Статья 197. Раскрытие информации при применении отдельных видов систем искусственного интеллекта

1. Владельцы и пользователи систем искусственного интеллекта, проектирующие, разрабатывающие или применяющие такие системы в целях взаимодействия с физическими лицами - потребителями, обязаны информировать последних о факте взаимодействия с системами искусственного интеллекта, за исключением случаев, когда такое взаимодействие является очевидным из обстановки. Сведения о применении систем искусственного интеллекта в рамках правоотношений в цифровой среде являются общедоступной информацией. Данные сведения подлежат размещению в доступной и понятной форме на сайтах пользователей соответствующих систем и сайте отраслевого регулятора нацэкосистемы.

2. Пользователи систем искусственного интеллекта, предназначенных для распознавания эмоций или классификации физических лиц по биометрическим признакам, должны информировать физических лиц о применении в отношении них таких систем.

3. Обязанности, предусмотренные частями 1 и 2 настоящей статьи, не распространяются на проектирование, разработку и применение таких функций систем искусственного интеллекта, в отношении которых такое информирование препятствовало бы их законному использованию по назначению в целях обеспечения:

1) обороноспособности;

2) национальной безопасности;

3) общественного порядка в части обнаружения, предотвращения, расследования преступлений и осуществления уголовного преследования.

4. Пользователи систем искусственного интеллекта, которые используют такие системы для дипфейков, должны раскрыть информацию об искусственном происхождении или изменении материалов.

5. Обязанность, предусмотренная частью 4 настоящей статьи, не распространяется на случаи законного использования таких изображений или материалов в целях защиты охраняемых благ, предусмотренных частью 3 настоящей статьи, или в целях реализации права на свободу научного, технического, художественного и иных видов творчества, преподавания и обучения.

6. Применение исключений, предусмотренных частями 3 и 5 настоящей статьи, допускается лишь при условии принятия необходимых мер для защиты затрагиваемых прав и свобод человека и гражданина.

Глава 24. Обеспечение непрерывности отношений в цифровой среде

Статья 198. Действие ранее выданных документов

1. Лицензии на радиочастотный ресурс в соответствии с настоящим Кодексом признаются решениями о выделении радиочастот и действуют в течение всего указанного в них срока. Продление, переоформление, аннулирование лицензии на радиочастотный ресурс осуществляются согласно правилам, установленным настоящим Кодексом для продления, внесения изменений, прекращения права на использование радиочастотного спектра. Лицензии на радиочастотный ресурс не могут быть повторно выставлены на торги.

2. Разрешения на частотные присвоения в соответствии с настоящим Кодексом признаются решениями о присвоении радиочастот и действуют в течение всего указанного в них срока. Продление, переоформление, аннулирование частотных присвоений осуществляются по правилам, установленным настоящим Кодексом для продления, внесения изменений, прекращения решения о присвоении радиочастот. По желанию обладателя частотного присвоения и при наличии оснований, установленных настоящим Кодексом, отраслевой регулятор телекоммуникаций обязан вынести решение об общем присвоении.

3. Лицензии на деятельность в области электрической связи и в области передачи данных в соответствии с настоящим Кодексом признаются лицензиями на деятельность операторов телекоммуникаций и действуют бессрочно. Лицензии на деятельность в области электрической связи и в области передачи данных по желанию их обладателя могут быть переоформлены в лицензии оператора телекоммуникаций без взимания платы.

4. Записи в цифровые реестры вносятся в соответствии с настоящим Кодексом на основании выданных ранее документов без прерывания срока действия выданных ранее лицензий, разрешений, решений о выделении ресурса нумерации и сертификатов, при этом дополнительные разрешения и выплаты для внесения записей в цифровые реестры не требуются.

5. Сертификаты электронной подписи в соответствии с настоящим Кодексом признаются сертификатами цифровой подписи и действуют до окончания указанного в них срока.

6. К простым электронным подписям, созданным до момента вступления в силу настоящего Кодекса, применяются правила настоящего Кодекса, относящиеся к цифровым идентификаторам.

Статья 199. Регулирование отношений по обработке и передаче информации без использования цифровых технологий

1. Передача сообщений без использования цифровых технологий не регулируется настоящим Кодексом, за исключением случаев лицензирования соответствующей деятельности, и осуществляется на основании договоров, заключаемых в порядке, установленном гражданским законодательством.

2. Лица, предоставляющие услуги по передаче сообщений без использования цифровых технологий, обязаны соблюдать тайну переписки, почтовых, телеграфных и иных сообщений.

3. Если исполнение обязанности по уведомлению субъектов правоотношений, предусмотренной настоящим Кодексом, невозможно осуществить с использованием цифровых технологий по причине отсутствия соответствующей контактной информации, уведомление субъекта осуществляется при его личном обращении.

4. Информационные ресурсы государственных органов или органов местного самоуправления, представленные в виде нецифровых записей (государственные или муниципальные информационные ресурсы), подлежат преобразованию в государственные или муниципальные цифровые ресурсы соответственно. До завершения цифровизации государственных и муниципальных информационных ресурсов информация, содержащаяся в них, используется на тех же основаниях и с теми же ограничениями, что и информация, содержащаяся в государственных и муниципальных цифровых ресурсах.

Статья 200. Формирование нацэкосистемы

Владельцы (обработчики) государственных информационных систем и государственных информационных ресурсов обязаны обеспечить включение сведений о них в реестр нацэкосистемы в порядке, установленном настоящим Кодексом.

Президент Кыргызской Республики

С.Жапаров

Принят Жогорку Кенешем Кыргызской Республики

18 июня 2025 года

Проекты

Методика определения угроз

Публикации

Главная

Гражданам

Организациям

Нормативные правовые акты

Полезная информация

Часто задаваемые вопросы

Новости

Вакансии

Политика конфиденциальности

Контакты агентства

Адрес: Кыргызская Республика, г. Бишкек, пр. Чуй, 265а, здание Национальной Академии наук, 2 этаж, западное крыло.

Телефон: Общий отдел: +(996) 312 641 014, +(996) 990 950 850, По заполнению Реестра: WhatsApp: +(996) 998 950 350, WhatsApp: +(996) 709 950 750 , +(996) 997 950 850

E-mail: info@dpa.gov.kg

Почтовый адрес: 720071

Телеграм бот: t.me/@AgentstvoPDbot

Официальные ресурсы

Президент Кыргызской Республики

Кабинет Министров Кыргызской Республики

Жогорку Кенеш Кыргызской Республики

Мы в соцсетях:

Facebook

Instagram

Telegram

© 2026

Количество посещений сайта за сутки: 750

Количество посещений сайта за всё время: 15795