Обзор законодательства Республики Кыргызстан в сфере информационной безопасности

Концепция информационной безопасности в Кыргызской Республике

1. Общий обзор

До 2001 года в законодательстве Кыргызской Республики не давалось определения понятию безопасность и только с принятием Концепции национальной безопасности Кыргызской Республики появилось нормативное определение этому понятию.

Действующая Концепция национальной безопасности Кыргызской Республики была утверждена указом Президента КР 12 июня 2012 года, в которой заложены и вопросы обеспечения информационной безопасности.

Концепция национальной безопасности КР (далее – Концепция) - официально принятая система взглядов, идей и принципов по защите личности, общества и государства от внешних и внутренних угроз безопасности во всех сферах жизнедеятельности на длительный период.

Интересы личности состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности граждан, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

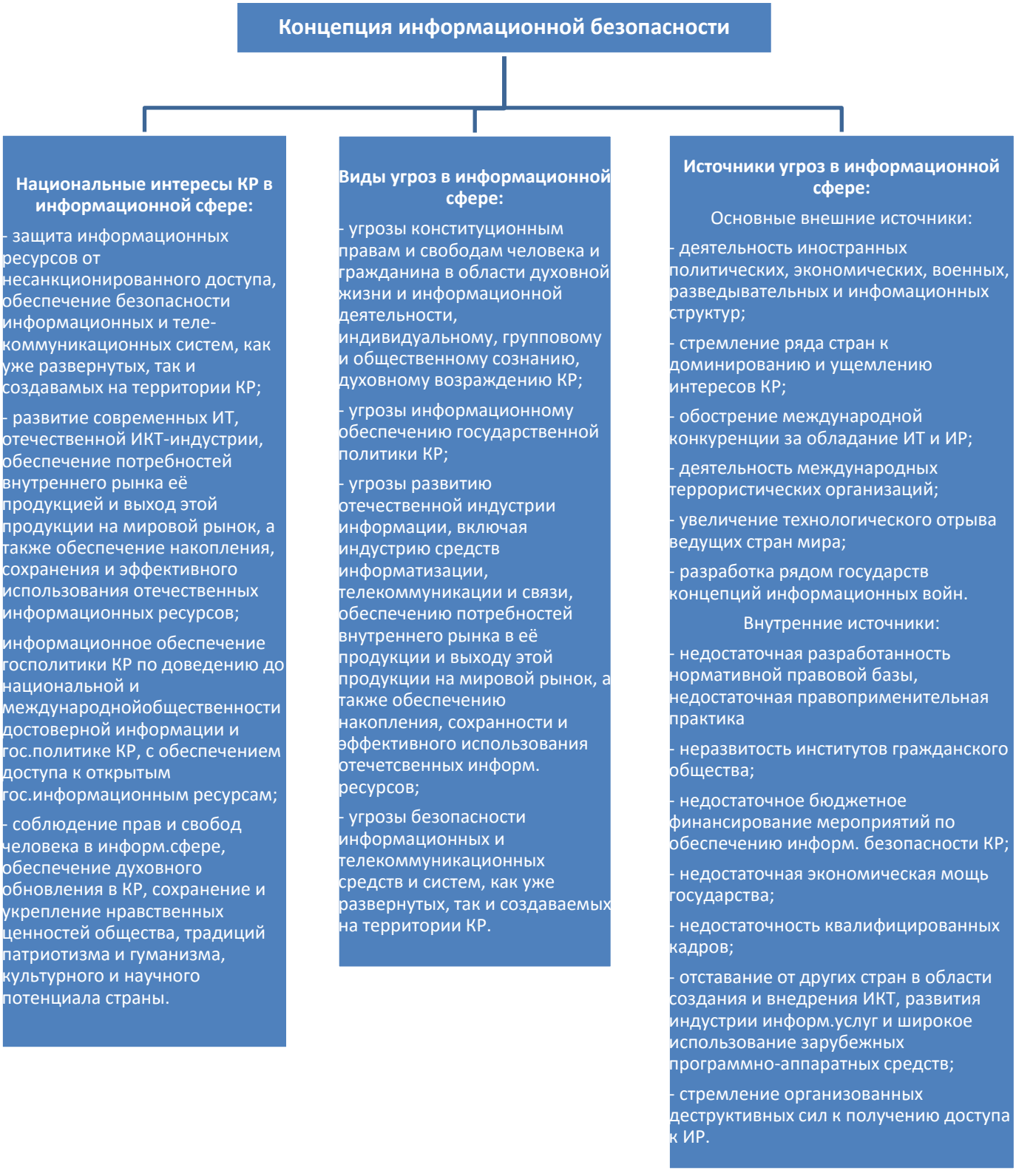
Интересы общества состоят в упрочении демократии, в создании правового государства, в достижении и поддержании общественного согласия, в духовно-нравственном обновлении Кыргызской Республики.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности Кыргызской Республики, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

В Концепции одной из внутренних угроз национальной безопасности страны определена **недостаточная развитость информационно-коммуникационных технологий и слабая защита информационного пространства страны.**

Принимая во внимание растущее использование сети Интернет с особой остротой встает вопрос защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с кибер-преступностью. Оперативное реагирование и эффективное противодействие противоправным действиям, требует развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с правоохранительными органами.

Недостаточное внимание уделяется вопросам формирования и реализации единой государственной политики по обеспечению информационной безопасности, координации деятельности органов власти и управления по ее укреплению. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.



В систему обеспечения безопасности личности, общества и государства включено, в первую очередь, совершенствование законодательства в названных направлениях.

К числу перспективных направлений развития законодательства в области национальной безопасности относится **сфера обеспечения информационной безопасности**: создание эффективных государственных механизмов по обеспечению информационной безопасности, а также участия в этой деятельности гражданского общества.

Направления регулирования в сфере информационной безопасности

Основными направлениями обеспечения информационной безопасности выступают:

- *правовое обеспечение* (применение правовых норм обеспечения безопасности);
- *организационное обеспечение* (регламентация деятельности, исключающее нанесение ущерба, наличие соответствующих служб);
- *инженерно-техническое обеспечение* (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

Нормативная правовая база обеспечения информационной безопасности формируется из:

- закона КР «О защите государственных секретов Кыргызской Республики»;

- закона КР «Об информатизации»;

- закона КР «О гарантиях и свободе доступа к информации»;

- закона КР «О Национальном архивном фонде»;

- закона КР «Об электрической и почтовой связи»;

- закона КР «Об электронной цифровой подписи»;

- закона КР «О средствах массовой информации»;

- закона КР «О правовой охране программ для ЭВМ и баз данных»;

- закона КР «Об основах технического регулирования в Кыргызской Республике»;

- закона КР «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» и другие;

- Гражданского, Семейного, Уголовного и др. кодексов;

- других подзаконных актов, регламентирующих общественные отношения в информационной сфере.

Анализ действующего законодательства в сфере информационной безопасности позволяет делать выводы о том, что оно:

- в определенной степени остается противоречивым, отражает ведомственные интересы и не подкреплено реальными ресурсами;

- не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений.

Ограничение доступа к информации, конфиденциальность и защита информации

Существует 4 вида информации:

1. информация с ограниченным доступом;
2. информация, доступ к которой не может быть ограничен никаким образом;

3. иная общедоступная информация;
4. информация, не подлежащая распространению как вредная.

В связи с отсутствием в Кыргызской Республике специального закона об информации и её защите, подобная градация находит своё отражение в нескольких нормативно-правовых актах страны.

Законом КР «О защите государственных секретов Кыргызской Республики» разграничены понятия и категории государственных и негосударственных секретов, а также определен правовой режим ограничений и допуска к данной категории информации.

Государственные секреты подразделены на следующие категории: государственная, военная и служебная тайны.

К **негосударственным секретам** относятся: коммерческая тайна, информация для служебного пользования, не для печати, тайна следствия, врачебная, личная и другие виды тайны. Сохранение негосударственных секретов осуществляется их собственником, а также лицами, которым они доверены по службе и роду деятельности.

В законе также определен перечень информации (сведений), которая не может быть засекречена и доступ к которой не может быть ограничен.

Отнесение информации к государственным секретам осуществляется в соответствии с Положением о порядке определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, на основании Перечня главнейших сведений, составляющих государственные секреты, и Перечня сведений, подлежащих засекречиванию, утверждаемых Правительством КР.

Закон КР «О коммерческой тайне» определяет правовые основы защиты коммерческой тайны на территории Кыргызской Республики и порядок доступа к ней.

Закон КР «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» регулирует отношения, связанные с доступом физических и юридических лиц к находящейся в ведении государственных органов и органов местного самоуправления информации.

Закон КР «Об информатизации» дает общее определение понятию **конфиденциальная информация** - это документированная информация, доступ к которой ограничен определенным кругом лиц.

Таким образом, правовой режим **конфиденциальности** устанавливается тем или иным законом, регулирующим определенную сферу использования различных категорий информации.

2. Персональные данные, личная и семейная тайна

2.1. Персональные данные и защита частной жизни в Кыргызской Республике.

В статье 16 Конституции Кыргызской Республики провозглашены основные права граждан в сфере информационной безопасности:

«Каждый имеет право на тайну переписки, телефонных переговоров, телеграфных, почтовых и иных сообщений.

Каждый имеет право на неприкосновенность его частной жизни, на уважение и защиту чести и достоинства.

Не допускается сбор, хранение, использование и распространение конфиденциальной информации о лице без его согласия, кроме случаев, установленных законом.

Каждому гарантируется судебная защита права опровергать недостоверную информацию о себе и членах своей семьи и права требовать изъятия любой информации, а также право на возмещение материального и морального ущерба, причиненного сбором, хранением и распространением недостоверной информации».

Конституция КР также декларирует, что каждый имеет право знакомиться в органах государственной власти, органах местного самоуправления, учреждениях и организациях со сведениями о себе, не являющимися государственной или иной защищенной законом тайной. Однако существующее законодательство КР не предусматривает механизм реализации этого положения.

В 2008 году был принят закон КР «Об информации персонального характера», направленный на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и законами КР в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

При этом данный закон не распространяется на хранение, обработку и использование персональных данных в связи с личными, семейными или хозяйственными делами физического лица.

2.2. Основные понятия

Информация персонального характера (персональные данные) - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

Обработка персональных данных - любая операция или набор операций, выполняемых независимо от способов держателем (обладателем) персональных данных либо по его поручению, автоматическими средствами или без таковых, в целях сбора, записи, хранения, актуализации, группировки, блокирования, стирания и разрушения персональных данных.

Субъект персональных данных (субъект) - физическое лицо, к которому относятся соответствующие персональные данные.

Держатель (обладатель) массива персональных данных - органы государственной власти, органы местного самоуправления и юридические лица, на которые возложены полномочия

определять цели, категории персональных данных и контролировать сбор, хранение, обработку и использование персональных данных в соответствии с настоящим Законом.

В законе также дается определение таким участникам отношений по обработке персональных данных, как обработчик и получатель персональных данных.

Обработчик - физическое или юридическое лицо, определяемое держателем (обладателем) персональных данных, которое осуществляет обработку персональных данных на основании заключенного с ним договора.

Получатель персональных данных - орган государственной власти или органы местного самоуправления, юридические и физические лица, а также субъект персональных данных (субъект), которым передаются и предоставляются персональные данные в соответствии с настоящим Законом.

Для проведения статистических, социологических, исторических, медицинских и других научных и практических исследований держатель (обладатель) массива персональных данных осуществляет **обезличивание** используемых данных, придавая им форму анонимных сведений. При этом режим конфиденциальности, установленный для персональных данных, снимается.
Обезличивание персональных данных - изъятие из персональных данных той их части, которая позволяет отождествить их с конкретным человеком.

2.3. Принципы и условия работы с персональными данными

Законом определены следующие **принципы** обработки персональных данных:

- Персональные данные должны быть получены и обработаны в порядке, предусмотренном законом «Об информации персонального характера».
- Персональные данные должны собираться для точно и заранее определенных, объявленных и законных целей, не использоваться в противоречии с этими целями и в дальнейшем не обрабатываться каким-либо образом, несовместимым с данными целями.
- Первоначальные данные должны быть точными и в случае необходимости обновляться.
- Персональные данные должны храниться не дольше, чем этого требуют цели, для которых они накапливались, и подлежат уничтожению по достижении целей или минованию надобности в них.
- Для персональных данных, сохраняемых более длительные сроки в исторических или иных целях, должны быть установлены необходимые гарантии обеспечения их защиты.
- Не допускается объединение массивов персональных данных, собранных держателями (обладателями) в разных целях, для автоматизированной обработки информации.
- Персональные данные должны храниться и защищаться держателями (обладателями) массивов персональных данных от незаконных доступов, внесений дополнений, изменений и уничтожений.

Основные принципы работы с персональными данными не носят исчерпывающий характер и могут дополняться в соответствии с законодательством КР.

Закон также определяет **случаи**, при которых держатель (обладатель) массива персональных данных может осуществлять работу с персональными данными:

1. если субъект персональных данных дал свое согласие на ее проведение;
2. если она необходима для выполнения органами государственной власти, органами местного самоуправления своей компетенции, установленной законодательством КР;

3. если она нужна для достижения законных интересов держателей (обладателей);
4. когда реализация этих интересов не препятствует осуществлению прав и свобод субъектов персональных данных применительно к обработке персональных данных;
5. когда она необходима для защиты интересов субъекта персональных данных;
6. если обработка персональных данных осуществляется исключительно в целях журналистики либо в целях художественного или литературного творчества при условии, что такие действия будут согласовываться с субъектом персональных данных с соблюдением права на неприкосновенность частной жизни и свободу слова.

В целях информационного обеспечения общества могут создаваться **общедоступные массивы персональных данных** (справочники, телефонные книги, адресные книги и т.п.).

По желанию субъекта для его персональных данных может быть установлен режим общедоступной информации (библиографические справочники, телефонные книги, адресные книги, частные объявления и т.д.). Исключения составляют случаи, когда информация должна носить публичный характер в соответствии с требованиями законодательства КР.

В общедоступные массивы персональных данных с письменного согласия субъекта могут включаться следующие персональные данные: фамилия, имя, отчество, год и место рождения, адрес местожительства, номер контактного телефона, сведения о профессии, иные сведения, предоставленные субъектом и/или полученные из открытых источников, других общедоступных массивов персональных данных, если эти источники сформированы **с согласия субъекта персональных данных.**

В случае если персональные данные получены держателем (обладателем) общедоступного массива персональных данных из открытых источников либо иных общедоступных массивов персональных данных, держатель (обладатель) общедоступного массива по запросу субъекта информирует в недельный срок о содержании его персональных данных, об источниках получения и цели использования.

Режим конфиденциальности для общедоступных массивов персональных данных не устанавливается.

Законом определены условия обработки **специальной категории персональных данных**.

Так сбор, накопление, хранение и использование персональных данных, раскрывающих расовое или этническое происхождение, национальную принадлежность, политические взгляды, религиозные или философские убеждения, а также касающихся состояния здоровья и сексуальных наклонностей, исключительно в целях выявления этих факторов, не допускаются.

Исключения составляют случаи:

а) если субъект персональных данных дал свое согласие на сообщение и обработку таких данных;

б) если обработка необходима для защиты здоровья и безопасности субъекта данных, иного лица или соответствующей группы лиц.

Принципы сбора, использования **биометрических данных** и порядок биометрической регистрации установлены в законе КР «О биометрической регистрации граждан КР».

К биометрическим данным отнесены:

- цифровое графическое изображение лица;

- графическое строение папиллярных узоров пальцев обеих рук;

- собственноручная подпись.

Сбор, обработка, хранение и использование биометрических данных осуществляются на принципах:

1) обязательной биометрической регистрации;

2) открытости (обеспечения доверия граждан к использованию государством биометрических данных);

3) гарантии законного использования биометрических и персональных данных органами государственной власти, местного самоуправления, наделенными специальными полномочиями в соответствии с законодательством КР;

4) защиты базы биометрических данных;

5) обеспечения безопасности биометрических данных при их сборе, обработке, хранении и использовании в информационных системах и соблюдения требований к материальным носителям.

Несмотря на **принцип обязательности** сдачи биометрических данных, данным законом установлено, что получение информации о биометрических данных осуществляется при наличии согласия в письменной форме субъекта биометрических данных в соответствии с законодательством КР, за исключением случаев, установленных тем же законом.

Получение информации о биометрических данных осуществляется **без согласия субъекта биометрических данных** только в случаях осуществления правосудия и исполнения судебного акта, а также в случаях, предусмотренных законодательством КР о национальной безопасности, о противодействии терроризму и коррупции, об оперативно-розыскной деятельности и иных случаях, определяемых законодательством КР.

При **трансграничной передаче персональных данных** держатель (обладатель) массива персональных данных, находящийся под юрисдикцией Кыргызской Республики, передающий данные, исходит из наличия международного договора между сторонами, согласно которому получающая сторона обеспечивает адекватный уровень защиты прав и свобод субъектов персональных данных и охраны персональных данных, установленный в Кыргызской Республике.

Кыргызская Республика обеспечивает законные меры охраны находящихся на ее территории или передаваемых через ее территорию персональных данных, исключающие их искажение и несанкционированное использование.

Передача персональных данных в страны, не обеспечивающие адекватный уровень защиты прав и свобод субъектов персональных данных, может иметь место при условии:

- согласия субъекта персональных данных на эту передачу;

- если передача необходима для защиты жизненно важных интересов субъекта персональных данных;

- если персональные данные содержатся в общедоступном массиве персональных данных.

При передаче персональных данных **по глобальной информационной сети (Интернет и т.п.)** держатель (обладатель) массива персональных данных, передающий такие данные, обязан обеспечить передачу необходимыми средствами защиты, соблюдая при этом конфиденциальность информации.

2.4. Права субъекта данных и обязанности держателя (обладателя) и обработчика массивов персональных данных. Ответственность

Субъект персональных данных самостоятельно решает вопрос о предоставлении кому-либо любых своих персональных данных, за исключением случаев, предусмотренных законом. Персональные данные предоставляются субъектом лично либо через доверенное лицо.

В целях реализации своих прав и свобод субъект предоставляет данные, а также сведения об их изменениях в соответствующие органы государственной власти, органы местного самоуправления, имеющие право на работу с персональными данными в пределах их компетенции.

Перед предоставлением своих персональных данных субъект должен быть ознакомлен держателем (обладателем) массива персональных данных с **перечнем собираемых данных**, основаниями и целями их сбора и использования, с возможной передачей персональных данных третьей стороне, а также информирован об ином возможном использовании персональных данных.

Субъект персональных данных при отказе в предоставлении своих данных имеет право не указывать причины своего отказа.

Субъект персональных данных имеет право знать о наличии у держателя (обладателя) относящихся к нему персональных данных и иметь к ним доступ. Право на доступ может быть ограничено только в случаях, предусмотренных законом.

Ограничение прав субъекта на предоставление и получение своих персональных данных возможно в отношении:

1) права предоставления субъектом своих персональных данных держателям (обладателям) массивов персональных данных - для субъектов персональных данных, допущенных к сведениям, составляющим государственную тайну, - в соответствии с законом КР "О защите государственных секретов Кыргызской Республики";

2) права доступа субъекта к своим персональным данным, внесения изменений в свои персональные данные, блокирования своих персональных данных:

а) для персональных данных, полученных в результате оперативно-розыскной деятельности, за исключением случаев, когда эта деятельность проводится с нарушением законодательства КР;

б) для персональных данных субъектов, задержанных по подозрению в совершении преступления либо которым предъявлено обвинение по уголовному делу, либо к которым применена мера пресечения до предъявления обвинения в органах, проводящих указанные действия.

Перечень ограничений прав доступа субъекта к своим персональным данным является **исчерпывающим**.

Держатель (обладатель) массива персональных данных обязан:

а) получать персональные данные непосредственно от субъекта персональных данных, его доверенных лиц;

б) обеспечивать режим конфиденциальности персональных данных в случаях, предусмотренных законодательством КР и законом «Об информации персонального характера»;

в) определить обработчика для обработки персональных данных, предоставляющего гарантии в отношении мер технической безопасности и организационных мер, регулирующих обработку персональных данных, за исключением случаев, когда держатель (обладатель) самостоятельно возлагает на себя функции и обязанности обработчика;

г) обеспечивать сохранность и достоверность персональных данных, а также установленный в нормативном порядке режим доступа к ним;

д) предоставлять персональные данные в недельный срок после поступления запроса от субъекта;

ж) в случае отказа в предоставлении субъекту по его требованию информации о наличии персональных данных о нем, а также самих персональных данных, выдавать письменный мотивированный ответ, в срок, не превышающий одной недели с момента обращения субъекта;

з) представлять по запросам уполномоченного государственного органа или Омбудсмена (Акыйкатчы) Кыргызской Республики в недельный срок информацию, необходимую для исполнения их полномочий;

и) в пределах компетенции разрабатывать в соответствии со спецификой своей деятельности перечни персональных данных и руководствоваться ими;

к) принять к производству заявление субъекта персональных данных (о выявленной недостоверности данных или неправомерности действий с ними держателя (обладателя) массивов) и заблокировать его персональные данные с момента его получения на период проверки заявления;

л) осуществлять действия по блокированию и снятию с блокирования, уничтожению данных в соответствии с требованиями закона «Об информации персонального характера»;

м) информировать субъекта персональных данных об осуществленной передаче его персональных данных третьей стороне в любой форме в недельный срок.

Обработчик персональных данных осуществляет обработку персональных данных на основании договора, заключенного с держателем (обладателем) персональных данных.

Обработчик должен выполнять сбор, запись, хранение, актуализацию, блокирование, уничтожение персональных данных, независимо от способа и средств обработки, по поручению держателя (обладателя) персональных данных.

Лица, которым персональные данные стали известны в силу их служебного положения, принимают на себя обязательства и **несут ответственность** по обеспечению конфиденциальности этих персональных данных. Такие обязательства остаются в силе и после окончания работы этих лиц с персональными данными в течение срока сохранения режима конфиденциальности, согласно закона.

Субъект персональных данных имеет право на возмещение причиненного ущерба и на компенсацию морального вреда в судебном порядке.

Ответственность за нарушение норм, установленных законом «Об информации персонального характера», наступает в соответствии с действующим законодательством КР.

2.5. Конфиденциальность и безопасность персональных данных

Персональные данные, находящиеся в ведении держателя (обладателя), относятся к **конфиденциальной информации**, кроме случаев, определенных законом.

Держатель (обладатель) персональных данных и обработчик обязаны обеспечивать охрану персональных данных во избежание несанкционированного доступа, блокирования, передачи, а равно их случайного или несанкционированного уничтожения, изменения или утраты.

Режим конфиденциальности персональных данных снимается в случаях:

- обезличивания персональных данных;

- по желанию субъекта персональных данных.

Держатель (обладатель) массива персональных данных и обработчик обязаны обеспечить гарантии в отношении **мер технической безопасности и организационных мер**, регулирующих обработку персональных данных.

При обработке персональных данных держатель (обладатель) массива персональных данных и обработчик обязаны:

- исключить доступ посторонних лиц к оборудованию, используемому для обработки персональных данных (контроль за доступом);

- препятствовать самовольному чтению, копированию, изменению или выносу носителей данных (контроль за пользованием носителями данных);

- препятствовать самовольной записи персональных данных и изменению или уничтожению записанных персональных данных (контроль за записью) и обеспечивать возможность установления задним числом когда, кем и какие персональные данные были изменены;

- обеспечить безопасность систем обработки данных, предназначенных для переноса персональных данных независимо от средств передачи данных (контроль за средствами передачи данных);

- обеспечить, чтобы каждый пользователь системы обработки данных имел доступ только к тем персональным данным, к обработке которых он имеет допуск (контроль за допуском);

- обеспечить возможность установления задним числом когда, кем и какие персональные данные вводились в систему обработки данных (контроль за вводом);

- не допускать несанкционированного чтения, копирования, изменения и уничтожения персональных данных при передаче и транспортировке персональных данных (транспортный контроль);

- обеспечить конфиденциальность информации, полученной при обработке персональных данных.

Требования к защите персональных данных и информационной безопасности при их обработке находятся на стадии разработки, которые планируется сформировать в виде подзаконного акта.

2.6. Уполномоченный орган

Законом КР «Об информации персонального характера» определено, что государство осуществляет регулирование работы с персональными данными в следующих формах:

- Правительством КР определяется уполномоченный государственный орган Кыргызской Республики;

- ведет учет и регистрацию массивов персональных данных и их держателей (обладателей);

- заключает международные договоры о трансграничной передаче персональных данных, за исключением случаев, противоречащих законодательству КР по защите государственных секретов.

Уполномоченный государственный орган - государственный орган, на который возложены функции по регистрации держателей (обладателей) массива персональных данных, ведению Реестра держателей массива персональных данных и другие задачи, предусмотренные законом.

Однако до настоящего времени данный уполномоченный орган так и не определен.

3. Государственные секреты

3.1. Сведения, составляющие государственные секреты

Правовые основы функционирования системы защиты государственных секретов во всех видах деятельности государственных органов, предприятий, объединений, организаций, независимо от форм собственности, воинских формирований и граждан Кыргызской Республики на всей территории республики и в ее учреждениях за границей регулируются законом КР «О защите государственных секретов КР».

Государственные секреты - информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными на основе и во исполнение Конституции КР.

Отнесение информации к государственным секретам основывается на **принципах**:

законности - осуществлении засекречивания информации в порядке, установленном действующим законодательством;

обоснованности - определения целесообразности засекречивания информации путем экспертной оценки в интересах государства и граждан;

своевременности - установлении ограничений на распространение сведений с момента их образования.

Государственные секреты КР подразделяются на три категории: государственная, военная и служебная тайны.

К государственной тайне относится информация, разглашение которой может повлечь тяжкие последствия для обороноспособности, безопасности, экономических и политических интересов Кыргызской Республики.

Информации, составляющей государственную тайну, присваиваются ограничительные грифы "особой важности" и "совершенно секретно".

Военную тайну образуют сведения военного характера, разглашение которых может нанести ущерб Вооруженным Силам и интересам КР.

Информации, составляющей военную тайну, присваиваются ограничительные грифы "совершенно секретно" и "секретно".

К **служебной тайне** относится информация, разглашение которой может оказать отрицательное воздействие на обороноспособность, безопасность, экономические и политические интересы КР. Такая информация имеет характер отдельных сведений, относящихся к государственной или военной тайне, и не раскрывает их полностью.

Информации, составляющей служебную тайну, присваивается ограничительный гриф "секретно".

Порядок установления ограничительных грифов секретности на информацию определяется Правительством КР.

Присвоение ограничительных грифов, не предусмотренных законом, не допускается.

Законом определены ограничения на засекречивание информации. **Не подлежат засекречиванию сведения:**

- о стихийных бедствиях и чрезвычайных происшествиях, угрожающих здоровью граждан;

- о катастрофах и их последствиях;

- о положении дел в экологии, использования природных ресурсов, здравоохранения, санитарии, культуре, сельском хозяйстве, образовании, торговли и обеспечения правопорядка;

- о фактах нарушения законности государственными органами и должностными лицами;

- о фактах, посягающих на права и законные интересы граждан, а также создающих угрозу их личной безопасности.

3.2. Режим государственной тайны

Основными элементами **системы защиты** государственных секретов являются:

- правила определения и установления степени секретности информации, содержащейся в работах, документах, изделиях и нетрадиционных носителях информации;

- порядок допуска к государственным секретам;

- ограничения для лиц, работающих с государственными секретами;

- порядок обращения с государственными секретами;

- контроль за обеспечением сохранности государственных секретов;

- органы обеспечения защиты государственных секретов;

- ответственность за невыполнение требований по защите государственных секретов.

Отнесение информации к государственным секретам осуществляется в соответствии с Положением о порядке определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, на основании Перечня главнейших сведений, составляющих государственные секреты, и Перечня сведений, подлежащих засекречиванию, утверждаемых Правительством КР.

Указанные Положение и Перечни являются документами для служебного пользования, доступ к которым ограничен.

Государственные органы, определяемые Правительством КР, вправе засекречивать и рассекречивать информацию, являющуюся собственностью юридических и физических лиц Кыргызской Республики и отвечающую требованиям закона, с компенсацией убытков собственникам.

Собственники информации вправе обжаловать в суде неправомерные действия по засекречиванию и рассекречиванию информации.

Порядок обращения с государственными секретами осуществляется в соответствии с законом КР «О защите государственных секретов КР» и Инструкцией по обеспечению режима секретности, утверждаемой Правительством КР.

Основанием для передачи секретной информации другому государству являются вступившие в установленном законом порядке в силу международные договоры, участницей которых является Кыргызская Республика, предусматривающие обязательства сторон по защите передаваемой секретной информации.

Секреты других государств и международных организаций, переданные в установленном порядке Кыргызской Республике, охраняются законом КР «О защите государственных секретов КР» на основе вступивших в установленном законом порядке в силу международных договоров, участницей которых является Кыргызская Республика.

Ответственность за обеспечение сохранности государственных секретов возлагается на руководителей государственных органов, предприятий, учреждений, организаций, объединений.

За разглашение секретных сведений, неправомерное завышение либо занижение степени их секретности, нарушение режима секретности, а также за нарушение требований настоящего Закона, виновные лица, в зависимости от тяжести нанесенного ущерба, привлекаются к уголовной, административной, дисциплинарной ответственности в соответствии с действующим законодательством Кыргызской Республики.

Порядок допуска к государственным секретам:

Гражданам Кыргызской Республики, которым для выполнения служебных обязанностей необходимо работать с государственными секретами, оформляется допуск к этим секретам. При этом, до заключения трудового договора (контракта), в отношении этих граждан, с их добровольного письменного согласия, осуществляются в установленном порядке проверочные мероприятия.

В трудовом договоре (контракте) отражаются: обязанность гражданина соблюдать требования по обеспечению защиты государственных секретов; обязательство о неразглашении этой информации, ограничения, связанные с работой с государственными секретами.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Устанавливаются три формы допуска граждан к государственным секретам, соответствующие трем степеням секретности сведений, составляющих государственные секреты: к сведениям особой важности, совершенно секретным или секретным. Наличие у граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Гражданам должна предоставляться только та информация, составляющая государственные секреты, которая необходима им для выполнения служебных обязанностей.

К государственным секретам без согласования с уполномоченным государственным органом, ведающим вопросами национальной безопасности, и **без оформления обязательств о неразглашении допускаются:**

- Президент Кыргызской Республики;
- Торага Жогорку Кенеша КР, его заместители;
- председатель и члены Комитета по обороне и безопасности Жогорку Кенеша КР;
- Премьер-министр, вице-премьер-министры, руководители государственных органов, ведающих вопросами обороны, безопасности, внутренних дел, охраны и защиты государственной границы, и их заместители. Другие члены Правительства, а также приравненные к ним должностные лица и их заместители, определяемые Премьер-министром КР по решению руководителя Аппарата Правительства КР;
- депутаты Жогорку Кенеша КР по решению Комитета по обороне и безопасности Жогорку Кенеша КР.

К государственным секретам не допускаются граждане Кыргызской Республики:

- постоянно проживающие за границей или обращающиеся в соответствующие государственные органы с просьбой о выходе из гражданства Кыргызской Республики, получении иностранного гражданства;

- признанные судом недееспособными, ограниченно дееспособными, привлеченные в качестве подозреваемого, обвиняемого, подсудимого за совершение умышленных преступлений, а также при наличии у них неснятой или непогашенной судимости за эти преступления в установленном законом порядке;

- имеющие медицинские противопоказания для работы с государственными секретами, перечень которых утверждается Правительством Кыргызской Республики;

- указавшие заведомо ложные сведения в анкетных данных, влияющие на принятие решения о допуске к государственным секретам;

- имеющие двойное гражданство.

Не допускаются к государственным секретам **иностранцы и лица без гражданства**.

Допуск граждан к секретной информации может быть прекращен по решению руководителя государственного органа, предприятия, учреждения, организации в случаях:

- расторжения трудового договора (контракта) в связи с организационно-штатными мероприятиями;

- грубого или систематического нарушения трудового договора (контракта), связанного с защитой секретной информации.

Прекращение допуска граждан к секретной информации является основанием для расторжения с гражданами трудового договора (контракта).

Прекращение допуска по указанным выше основаниям не освобождает гражданина КР от обязанностей неразглашения известных ему государственных секретов.

Сроки действия секретности информации

Рассекречивание информации производится в сроки, установленные при ее засекречивании, если не принято решение об их продлении в установленном порядке.

Сведения, составляющие государственные секреты, могут быть рассекречены досрочно или сроки их секретности продлены, если этого требуют политические, экономические интересы Кыргызской Республики, а также с появлением факторов, вызывающих необходимость их корректировки. Решение о рассекречивании и продлении сроков секретности принимается Правительством Кыргызской Республики по представлению заинтересованных министерств, государственных комитетов, административных ведомств, а также предприятий, учреждений, организаций.

4. Коммерческая тайна

4.1. Сведения, составляющие коммерческую тайну

Закон КР «О коммерческой тайне» определяет правовые основы защиты коммерческой тайны на территории Кыргызской Республики.

Под **коммерческой тайной** понимаются не являющиеся государственной тайной сведения, связанные с производством, технологией, управлением, финансовой и другой деятельностью хозяйствующего субъекта, разглашение которых может нанести ущерб его интересам.

Сведения, составляющие коммерческую тайну, являются собственностью субъекта предпринимательства либо находятся в его владении, пользовании, распоряжении в пределах, установленных им в соответствии с законодательством.

Гражданский кодекс КР дает следующее определение служебной и коммерческой тайне, включая её защиту:

«Гражданским законодательством защищается информация, составляющая служебную или коммерческую тайну, в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Лица, незаконными методами получившие такую информацию, а также служащие - вопреки трудовому договору или контрагенты - вопреки гражданско-правовому договору, разгласившие служебную или коммерческую тайну, обязаны возместить причиненный ущерб.»

Сведения, составляющие коммерческую тайну, должны соответствовать следующим требованиям:

а) иметь действительную или потенциальную ценность для субъекта предпринимательства;

б) не являться общеизвестными или общедоступными согласно законодательству;

в) обозначаться соответствующим образом с принятием субъектами предпринимательства надлежащих мер по сохранению их конфиденциальности через систему классификации названных сведений, разработку внутренних правил ограничения пользования, введение соответствующей маркировки документов и иных носителей информации, организации учета, хранения и применение.

К объектам коммерческой тайны не могут относиться:

а) учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности, подлежащей лицензированию (устав, решение о создании предприятия или договор учредителей, регистрационные удостоверения, лицензии, патенты);

б) сведения по утвержденным формам статистической отчетности, а также отчетности о финансово-экономической деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов, а также других обязательных платежей;

в) документы об уплате налогов и других обязательных платежей;

г) документы, удостоверяющие платежеспособность;

е) сведения о численности, составе работников, заработной плате руководителя организации и членов коллегиального исполнительного органа организации, системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и наличии свободных рабочих мест;

ж) сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении правил охраны труда, реализации продукции, причиняющей вред здоровью потребителей, а также о других нарушениях законодательства и размерах причиненного при этом ущерба;

з) сведения об участии должностных лиц государственных предприятий в организациях, занимающихся предпринимательской деятельностью.

4.2. Режим коммерческой тайны

Порядок защиты коммерческой тайны определяется субъектом предпринимательства или назначенным им руководителем, который доводит его до работников, имеющих доступ к сведениям, составляющим коммерческую тайну.

Субъектами коммерческой тайны разрабатываются **инструкции, положения по обеспечению сохранности коммерческой тайны**, в которых определяются:

а) состав и объем сведений, составляющих коммерческую тайну;

б) порядок присвоения грифа "Секрет предприятия" сведениям, работам и изделиям и его снятия;

в) процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

г) порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

д) организация контроля за порядком использования сведений, составляющих коммерческую тайну;

е) процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-либо совместных действий;

ж) порядок применения предусмотренных законодательством мер дисциплинарного, материального воздействия на работников, разгласивших коммерческую тайну;

з) возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

Работники хозяйствующего субъекта, имеющие доступ к сведениям, составляющим коммерческую тайну, обязаны:

- сохранять коммерческую тайну, которая станет им известна по работе, и не разглашать ее без разрешения, выданного в установленном порядке, при условии, что сведения, составляющие коммерческую тайну, не были известны им ранее либо не были получены ими от третьего лица без обязательства соблюдать в отношении их конфиденциальность;
- выполнять требования инструкций, положений, приказов по обеспечению сохранности коммерческой тайны;
- в случае попытки посторонних лиц получить от них сведения, составляющие коммерческую тайну, немедленно сообщить об этом соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта;
- сохранять коммерческую тайну хозяйствующих субъектов, с которыми имеются деловые отношения;
- не использовать знание коммерческой тайны для занятий деятельностью, которая в качестве конкурентного действия может нанести ущерб хозяйствующему субъекту;
- в случае увольнения передать все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, магнитные ленты, перфокарты, перфоленты, диски, дискеты, распечатки на принтерах, кино-, фотопленки, модели, материалы и др.), которые находились в их распоряжении, соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта.

Данные обязательства даются в письменной форме при заключении трудового или иного договора либо в процессе его исполнения.

Для обеспечения **защиты коммерческой тайны на хозяйствующих субъектах** могут создаваться специальные режимные подразделения, функции и полномочия которых отражаются в соответствующих инструкциях, положениях, приказах.

Правоохранительные и иные государственные органы оказывают содействие режимным подразделениям хозяйствующих субъектов в выполнении возложенных на них функций.

При осуществлении хозяйствующими субъектами торгово-экономических, научно-технических, валютно-финансовых и других деловых связей, в том числе с иностранными партнерами, договаривающиеся стороны специально оговаривают характер, состав сведений, составляющих коммерческую тайну, а также взаимные обязательства по обеспечению ее сохранности в соответствии с законодательством.

При заключении договора с иностранными партнерами условия конфиденциальности деятельности должны соответствовать законодательству страны, где заключается договор, если иное не предусмотрено межгосударственными соглашениями.

Доступ к коммерческой тайне имеют:

- работники, круг которых определен субъектом предпринимательства;

- государственные контролирующие и правоохранительные органы в соответствии с полномочиями, предоставленными им законодательством по контролю и надзору, имеющие право в пределах своей компетенции на основании письменного запроса знакомиться со сведениями, являющимися коммерческой тайной.

Физические и юридические лица, включая должностных лиц государственных органов контроля и надзора, а также уполномоченного органа по противодействию финансированию терроризма и легализации (отмыванию) доходов, полученных преступным путем, имеющие доступ к коммерческой тайне, обязаны строго соблюдать требования о ее неразглашении, не допускать утечки информации к конкурирующим хозяйствующим субъектам.

За несанкционированное разглашение коммерческой тайны физические и юридические лица привлекаются к **ответственности** в соответствии с законодательством КР.

Работники хозяйствующего субъекта, государственных органов, а также лица, незаконно получившие сведения, составляющие коммерческую тайну, или завладевшие ими, обязаны также возместить ущерб, причиненный хозяйствующему субъекту или субъекту предпринимательства.

Гражданским кодексом КР также регламентировано право на защиту нераскрытой коммерческой информации.

Лицо, правомерно обладающее технической, организационной или коммерческой информацией, в том числе секретами производства (ноу-хау), неизвестной третьим лицам (нераскрытая информация), имеет право на защиту этой информации от незаконного использования, если соблюдены условия, установленные законом для служебной и коммерческой тайны.

Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении этой информации каких-либо формальностей (ее регистрации, получения свидетельств и т.п.).

Лицо, обладающее нераскрытой информацией, может **передать** все или часть сведений, составляющих содержание этой информации, другому лицу по лицензионному договору.

Лицензиат обязан принимать надлежащие меры к охране конфиденциальности информации, полученной по договору, и имеет те же права на ее защиту от незаконного использования третьими лицами, что и лицензиар. Поскольку в договоре не предусмотрено иное, обязанность сохранять конфиденциальность информации лежит на лицензиате и после прекращения лицензионного договора, если соответствующие сведения продолжают оставаться нераскрытой информацией.

5. Иные виды тайн

Законодательством КР не предусмотрен конкретный перечень видов тайн. Например, законом «О защите государственных секретов КР» определено разделение на государственные и негосударственные секреты.

К негосударственным секретам законом отнесены, помимо коммерческой тайны, информация для служебного пользования, не для печати, тайна следствия, врачебная, личная и другие виды тайны. Таким образом, данный перечень является **неисчерпывающим.**

Перечень тайн, определенных законодательством КР.

Виды тайн	**Описание**
Банковская тайна	*Банковской тайной* считаются сведения о счетах (вкладах) клиента (корреспондента), ставшие известными банку в связи с его обслуживанием, сведения об операциях (сделках), совершенных по поручению клиента или в его пользу, а также сведения о самом клиенте, сведения о клиентах других банков, ставшие известными в результате обмена информацией между банками, и любые другие сведения, которые были доверены или стали известны банку в процессе отношений между банком и клиентом. Банку, его учредителям, акционерам, членам Совета директоров и правления, исполнительным должностным лицам, сотрудникам банка, а также лицам, которые работают на банк, запрещается раскрывать третьим лицам или использовать в каких-либо целях любую информацию, которая им была доверена или к которой они имели доступ в процессе отношений между банком и клиентами, иначе как по основаниям, предусмотренным законодательством. Данный запрет распространяется и на бывших клиентов банка и касается всей информации, полученной от таких клиентов. Кроме того, запрет касается всех лиц, которым банки оказывали услуги, независимо от того, имеют они счета в банке или нет.
Адвокатская тайна	Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Адвокат не вправе использовать в своих интересах или в интересах третьих лиц сведения, составляющие адвокатскую тайну.
Тайна совершения нотариальных действий	Нотариусы и другие должностные лица, уполномоченные совершать нотариальные действия, обязаны хранить в тайне сведения, которые стали им известны в связи с совершением нотариальных действий. Обязанность сохранения тайны совершаемых нотариальных действий распространяется также на лиц, которым о совершенных нотариальных действиях стало известно в связи с исполнением ими служебных обязанностей, в том числе и после прекращения трудового договора.
Врачебная тайна	Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных частями третьей и четвертой настоящей статьи.
Процессуальная тайна	Данные, полученные в ходе следствия по уголовному делу, не подлежат разглашению (тайна следствия).

	Следователь предупреждает свидетеля, потерпевшего, защитника, гражданского истца, гражданского ответчика или их представителей, эксперта, специалиста, переводчика, понятых и других лиц, присутствующих при производстве следственных действий, о недопустимости разглашения данных следствия и вправе отобрать у них подписку с предупреждением об ответственности. Тайна совещания присяжных заседателей - кроме присяжных заседателей присутствие иных лиц в совещательной комнате не допускается. Присяжные заседатели не вправе разглашать мнения, имевшие место при обсуждении и принятии вердикта, а также сведения, ставшие известными им во время закрытого судебного заседания.
Тайна информации, которая передается средствами связи	Тайна переписки, телефонных переговоров, телеграфных, а также других сообщений, которые передаются средствами связи, охраняется Конституцией и законом «Об электрической и почтовой связи». Предприятия связи всех форм собственности обязаны принимать необходимые организационно-технические меры по защите информации. Ограничение этого права допускается только с санкции прокурора.
Налоговая тайна	Налоговую тайну составляют любые полученные органом налоговой службы или его должностным лицом сведения о налогоплательщике, за исключением сведений: 1) о реквизитах налогоплательщика (наименование или фамилия, имя и отчество налогоплательщика, адрес), а также об идентификационном номере налогоплательщика; 2) о регистрации налогоплательщика в качестве плательщика налога на добавленную стоимость; 3) о счетах-фактурах по налогу на добавленную стоимость и марках акцизного сбора; 4) о сумме налоговой задолженности, признанной налогоплательщиком; 5) о нарушениях налогоплательщиком налогового законодательства КР и мерах ответственности за эти нарушения, установленные вступившим в силу решением суда либо признанные налогоплательщиком; 6) о фактических произведенных налоговых платежах в пользу государственного бюджета юридическими лицами. Налоговая тайна не подлежит разглашению органами налоговой службы, их должностными лицами, за исключением случаев, когда сведения передаются: 1) другим должностным лицам органов налоговой службы, таможенных органов, уполномоченного государственного органа в ходе или в целях исполнения ими своих обязанностей, предусмотренных настоящим Кодексом или законодательством КР в сфере таможенного дела; 2) правоохранительным органам, исключительно в отношении налогоплательщика, по которому возбуждено уголовное дело по факту налогового правонарушения; 3) суду в ходе судебного разбирательства по установлению налоговой задолженности налогоплательщика или его ответственности за налоговые правонарушения; 4) уполномоченному государственному органу по делам о банкротстве, администратору (временному администратору, специальному администратору, консерватору, внешнему управляющему) в целях осуществления ими полномочий, предусмотренных законодательством КР о банкротстве, по тем субъектам, в отношении которых возбужден

	процесс банкротства или в отношении которых вынесено решение об инициировании процесса банкротства; 5) уполномоченному государственному органу по делам государственной службы КР в отношении лиц, обязанных представлять декларацию об имуществе и доходах в соответствии с законодательством КР о государственной службе; 6) депутатам Жогорку Кенеша КР, аппарату Правительства КР, Службе финансовой разведки КР в случаях, установленных законодательством КР, регулирующим их деятельность; 7) налоговым или правоохранительным органам других государств в соответствии с международными договорами о взаимном сотрудничестве между налоговыми или правоохранительными органами, участником которых является Кыргызская Республика; 8) органам государственной статистики в целях осуществления статистической деятельности, предусмотренной законодательством КР.
Тайна страхования	Работники уполномоченного государственного органа в сфере регулирования и надзора за страховой деятельностью не вправе разглашать ставшие известными им в силу должностного положения сведения, составляющие коммерческую тайну страховщика, иную информацию, касающуюся страховщика и его клиентов, кроме случаев, предусмотренных законодательством КР в сфере противодействия финансированию терроризма и легализации (отмыванию) доходов, полученных преступным путем.
Тайна усыновления	Тайна усыновления ребенка охраняется законом. Должностные лица, вынесшие решение об усыновлении ребенка или осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка.

6. Криптография

В Кыргызской Республике деятельность в области криптографии (шифровании) регулируется незначительным количеством нормативно-правовых актов.

Существует «Национальный контрольный список Кыргызской Республики контролируемой продукции», утвержденный постановлением Правительства КР от 02.04.2014г. № 197, в который включены в том числе ЭВМ, сопутствующее оборудование и программное обеспечение, выполняющие функции **криптографии, криптоанализа**, сертифицируемой многоуровневой защиты информации или сертифицируемые функции изоляции пользователей либо ограничивающие электромагнитную совместимость (ЭМС).

Законом КР "Об органах национальной безопасности Кыргызской Республики" на **Государственный комитет национальной безопасности КР (ГКНБ КР)** возложены обязанности:

- осуществлять государственный контроль за исполнением требований при обеспечении криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи;

- осуществлять контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Кыргызской Республики и в ее учреждениях, находящихся за ее

пределами, а также контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

- осуществлять контроль и выдачу разрешений на ввоз в Кыргызскую Республику и вывоз за ее пределы, транзит, а также на разработку, производство, реализацию, приобретение на территории Кыргызской Республики в порядке, установленном Правительством Кыргызской Республики шифровальных средств и нормативно-технической документации к ним.

6.1. Ввоз и вывоз шифровальных средств

Законом КР «О лицензионной разрешительной системе в КР» закреплено, что для осуществления ввоза на территорию Кыргызской Республики и вывоза из Кыргызской Республики шифровальных средств (включая шифровальную технику, части для шифровальной техники и пакеты программ для шифрования), нормативно-технической документации к шифровальным средствам (включая конструкторскую и эксплуатационную) требуется получение **разрешения**.

Шифровальные (криптографические) средства внесены в перечень товаров, ввоз/вывоз которых на/с территории Кыргызской Республики **ограничен**.

Так как контроль и выдачу разрешений на ввоз и вывоз шифровальных средств осуществляет ГКНБ КР, имеющиеся подзаконные акты, регламентирующие требования к шифровальным средствам и порядку их ввоза/вывоза, существуют под грифом «для служебного пользования».

7. Техническая защита информации

Функции по технической защите информации, как и криптографической защите, отнесены к полномочиям органов национальной безопасности. Регулируемые данную область нормативные акты отнесены к документам для служебного пользования, доступ к которым ограничен.

8. Электронная разведка (прослушка)

8.1. Условия проведения оперативно-розыскных мероприятий

Законом КР «Об оперативно-розыскной деятельности» определен следующий перечень оперативно-розыскных мероприятий:

1) опрос граждан;

2) наведение справок;

3) сбор образцов для сравнительного исследования;

4) проверочные закупки;

5) исследование предметов и документов;

6) контролируемые поставки (проверочные поставки);

7) отождествление личности;

8) обследование помещений, зданий, сооружений, участков местности и транспортных средств;

9) контроль почтовых отправлений, телеграфных и иных сообщений;

10) прослушивание и запись переговоров, производящихся по телефону и другим переговорным устройствам;

11) снятие информации с технических каналов связи;

12) создание конспиративных предприятий и организаций;

13) оперативное внедрение;

14) оперативное наблюдение;

15) оперативный эксперимент;

16) оперативная установка;

17) применение технических средств для получения сведений, не затрагивающих охраняемые законом неприкосновенность частной жизни, жилища, личной и семейной тайны, а также тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

18) поиск технических средств незаконного снятия информации;

19) оперативный поиск в сетях и на каналах связи;

20) негласное прослушивание и запись разговоров (с использованием видео-, аудиотехники и (или) специальных технических средств);

21) получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Перечень этих действий является исчерпывающим и может быть изменен или дополнен только законом.

Ввоз в Кыргызскую Республику и вывоз за ее пределы, а также разработка, производство, сертификация, реализация, приобретение и использование специальных технических средств, предназначенных для негласного получения информации, осуществляются в порядке, устанавливаемом Правительством Кыргызской Республики. Перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством Кыргызской Республики.

Оперативно-розыскные мероприятия, связанные с использованием сети связи, в интересах решения задач органами, наделенными правом осуществления оперативно-розыскных мероприятий, технически осуществляются органами национальной безопасности в порядке, определяемом Правительством КР.

Проведение оперативно-розыскных мероприятий, затрагивающих охраняемые законом **тайну переписки, телефонных и иных переговоров, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи**, допускается лишь для сбора информации о лицах, подготавливающих или покушающихся на тяжкие и особо тяжкие преступления, совершающих либо совершивших тяжкие и особо тяжкие преступления, по мотивированному постановлению одного из руководителей соответствующего органа, осуществляющего оперативно-розыскную

деятельность, исключительно на основании судебного акта с последующим уведомлением надзирающего прокурора в течение 24 часов.

В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их письменного согласия разрешается **прослушивание переговоров, ведущихся с их телефонов или других переговорных устройств**, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) и надзирающего прокурора и последующим получением решения суда в течение 24 часов.

Рассмотрение материалов об ограничении конституционных прав граждан **на тайну переписки, телефонных разговоров, почтовых, телефонных и иных сообщений, передаваемых по сетям электрической и почтовой связи**, при проведении оперативно-розыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении. Указанные материалы рассматриваются судьей единолично и незамедлительно. Судья не вправе отказать в рассмотрении таких материалов в случае их представления.

Основанием для решения вопроса о проведении оперативно-розыскных мероприятий, ограничивающего конституционные права граждан, является мотивированное постановление одного из руководителей органа, осуществляющего оперативно-розыскную деятельность.

8.2. Требования к проведению оперативно-розыскных мероприятий на сетях электросвязи

Закон КР «Об электрической и почтовой связи» определяет круг обязанностей операторов связи при проведении оперативно-розыскных мероприятий на сетях связи.

Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность в сетях связи, информацию о пользователях услугами связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, обеспечивать им организационные и программно-технические возможности проведения оперативно-розыскных мероприятий во всех сетях и на каналах связи, доступ к базам данных, автоматизированным системам оператора связи в случаях, установленных законодательством Кыргызской Республики.

Операторы связи обязаны обеспечивать реализацию установленных Правительством КР **требований к сетям и средствам связи** для проведения оперативно-розыскных мероприятий, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Операторы сотовой связи обязаны вести **реестр идентификационных кодов абонентских устройств**, работающих в их сети, а также в порядке, определяемом Правительством КР, осуществлять сбор и хранение в течение 3 лет данных об абонентах.

Технические требования к сетям связи, специальным техническим средствам, предназначенным для контроля и фиксации получаемых законным путем сведений/информации, передаваемой по техническим каналам связи, порядку взаимодействия при реализации функций системы оперативно-розыскных мероприятий в сетях связи, включая проработку интерфейса (технического регламента), разработку необходимого программного обеспечения, решение вопроса о

соединении и каналах доступа, иные вопросы, связанные с обеспечением законности осуществления оперативно-розыскных мероприятий в сетях связи, комплексного решения всех вопросов и проблем, связанных с внедрением и функционированием системы оперативно-розыскных мероприятий в сетях связи, в соответствии с разработанными в этой сфере международными рекомендациями и техническими концепциями, а также требованиями действующего законодательства Кыргызской Республики устанавливаются Правительством Кыргызской Республики.

При проведении уполномоченными государственными органами следственных действий в сетях (на каналах) связи операторы связи оказывают этим органам содействие в соответствии с требованиями уголовно-процессуального законодательства КР.

Приостановление деятельности любых сетей и средств связи, а также оказания услуг связи юридическим и физическим лицам осуществляется операторами связи на основании мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, в случаях, установленных законами КР.

Операторы мобильной сотовой связи обязаны приостановить работу мобильного устройства, если его международный идентификатор включен в Реестр похищенных мобильных устройств, ведущийся органами внутренних дел КР в порядке, установленном Правительством КР.

Операторы связи обязаны возобновить оказание услуг связи на основании решения суда или мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, который принял решение о приостановлении оказания услуг связи.

Расходы операторов связи, связанные с обеспечением необходимыми программно-техническими и иными средствами для проведения оперативно-розыскных мероприятий в сетях и на каналах связи, обеспечиваются **за счет средств операторов связи**.

Порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, устанавливается «Инструкцией о порядке взаимодействия операторов электросвязи и операторов мобильной сотовой связи с государственными органами Кыргызской Республики, осуществляющими оперативно-розыскную деятельность», утвержденной постановлением Правительства КР.

9. Борьба с киберпреступностью

Уголовным кодексом КР предусмотрена ответственность за совершение преступлений, связанных с информационными технологиями. К ним относятся:

- Создание программ для ЭВМ или внесение изменение в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами;
- Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа и угроз в отношении лиц, владеющих коммерческой или банковской тайной, или их близких, перехвата информации в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных

технических средств, а равно иным незаконным способом с целью разглашения либо использования этих сведений;

- Несанкционированное изменение международного идентификатора мобильного устройства, установленного его производителем, а равно подделка международного идентификатора мобильного устройства, совершенные из корыстных побуждений;
- Изготовление с целью сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами;
- Нарушение тайны переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных или иных сообщений граждан , либо то же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.