The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several overlapping circular elements. A prominent one is a large circle with a scale around its perimeter, marked with numbers from 140 to 260 in increments of 10. Other circles are partially visible, some with dashed lines and arrows, suggesting a technical or scientific theme.

ОСОБЫЙ ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИИ

- **Правовой режим** – это сочетание в различных пропорциях способов, методов и типов регулирования, используемых для упорядочения общественных отношений в той или иной сфере.

- **Правовой режим информации** - это объектный режим, вводимый законодательным актом и позволяющий обеспечить комплексность воздействия в информационной сфере посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое сочетание дозволений, запретов и обязываний, а также гарантий по его соблюдению.

- **Специальные правовые режимы информации** направлены на охрану сведений, свободное распространение которых нарушает права и законные интересы общества, государства, личности. Специальный режим не просто ограничивает доступ к информации, ее использование и распространение, а определяет степень жесткости регулирования, возможные исключения, их основания, порядок введения и прекращения действия режима, сроки его действия.

ТАК «КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ» ОЗНАЧАЕТ СПЕЦИАЛЬНЫЙ ПРАВОВОЙ РЕЖИМ, УСТАНОВЛЕННЫЙ ЗАКОНОМ ИЛИ НА ОСНОВАНИИ ЗАКОНА, И ПРЕДУСМАТРИВАЮЩИЙ:

- ограничение доступа;запрет на передачу третьим лицам без согласия обладателя информации (за исключением случаев, установленных законом);
- запрет на распространение информации (вытекающий из первых двух позиций);
- возможность, по общему правилу, обладателя информации самостоятельно решать вопрос о сохранении конфиденциальности;производный характер обязанности по сохранению конфиденциальности информации одного субъекта от исполнения первичной обязанности другим субъектом – обладателем информации предоставить ее органу государственной власти или органу местного самоуправления, а также контрагенту по договору или иному лицу.

- Таким образом, можно заключить, что **правовой режим информации** определяется нормами, устанавливающими: порядок документирования информации; право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах; категорию информации по уровню доступа к ней; порядок правовой защиты информации.

КАКИЕ СВЕДЕНИЯ ОБРАЗУЮТ ЛИЧНУЮ ТАЙНУ

- Это сведения:- имеющие личный характер (об отношениях, причем не обязательно в интимной сфере, привычках, событиях в жизни, встречах, взглядах, пристрастиях, склонностях, физических недостатках, судимости, которая уже снята или погашена, психических и иных заболеваниях и др.);- разглашение которых лицо считает неприемлемым и предпринимает усилия (меры) для сохранения тайны. Тайна переписки и других сообщений может являться личной тайной тогда, когда само лицо считает определенную информацию тайной и заботится о сохранении конфиденциальности. Таким образом, можно сказать, что ведущей характеристикой понятия «личная тайна» является желание лица сохранить данные в секрете.

- Из чего можно заключить, что **личной тайной нельзя считать информацию**, если:- человек предпринял действия, чтобы сделать сведения общедоступными, и это было сделано по собственному желанию. Например, сведения ранее обнародованы самим гражданином в СМИ. В подобных случаях они уже не могут быть тайной;- лицо обнародует сведения, поскольку этого требует законодательство. Это, к примеру, сведения о доходе и имуществе лиц, претендующих на замещение государственных должностей, такая информация является открытой.

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 Кыргызской Республики.

- 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.

СЛУЖЕБНАЯ ТАЙНА

- — это информация, доступ к которой ограничен органами государственной власти и федеральными законами (сведения об усыновлении, вкладах граждан, характере заболевания пациента). Служебная тайна не подлежит разглашению, кроме случаев, когда 1С или иные сведения запрашиваются правоохранительными органами. Разница между служебной и коммерческой тайной состоит в том, что коммерческая тайна — это сведения, связанные с коммерческой деятельностью, и служебная тайна — это служебная информация, доступ к которой ограничен органами государственной власти.

- К служебной тайне не могут быть отнесены сведения:
- содержащиеся в актах законодательства, устанавливающих правовой статус государственных органов, организаций,
- общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- о чрезвычайных ситуациях, опасных природных явлениях, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенного пункта, граждан и населения в целом, а также производственных объектов: описание структуры органа власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностях населения;
- документы, накапливаемые в открытых фондах библиотек и архивах, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ)

- – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ ДОЛЖНА БЫТЬ:

- 1. Постоянной. Злоумышленник в любой момент может попытаться обойти модули защиты данных, которые его интересуют.
- 2. Целевой. Информация должна защищаться в рамках определенной цели, которую ставит организация или собственник данных.
- 3. Плановой. Все методы защиты должны соответствовать государственным стандартам, законам и подзаконным актам, которые регулируют вопросы защиты конфиденциальных данных.
- 4. Активной. Мероприятия для поддержки работы и совершенствования системы защиты должны проводиться регулярно, и другие.

ПРАВОВЫЕ ОСНОВАНИЯ ОСУЩЕСТВЛЕНИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Информация персонального 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.

Правовые основания осуществления работы с персональными данными

Работа с персональными данными может осуществляться держателем (обладателем) массива персональных данных только в случаях:

- если субъект персональных данных дал свое согласие на ее проведение;
- если она необходима для выполнения органами государственной власти, органами местного самоуправления своей компетенции, установленной законодательством Кыргызской Республики;
- если она нужна для достижения законных интересов держателей (обладателей);
- когда реализация этих интересов не препятствует осуществлению прав и свобод субъектов персональных данных применительно к обработке персональных данных;



- когда она необходима для защиты интересов субъекта персональных данных;
- 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.

- ных настоящим Законом.

- 2. 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.

- 3. Режим конфиденциальности персональных данных снимается в случаях:

- - обезличивания персональных данных;
- - по желанию субъекта персональных данных.

- 4. Правовой режим персональных данных, полученных в результате деятельности правоохранительных органов, устанавливается в соответствии с законодательством Кыргызской Республики.

- 5. 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 Кыргызской Республики.

- 6. С момента смерти субъекта персональных данных правовой режим персональных данных подлежит замене на режим архивного хранения или иной правовой режим, предусмотренный законодательством Кыргызской Республики.

- 7. Защита персональных данных умершего лица может осуществляться другими лицами, в том числе наследниками, в порядке, предусмотренном



Специальные категории персональных данных

- 1. 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.

- 2. Часть 1 настоящей статьи не применяется в случаях:

- 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

своего лица, если это возможно.



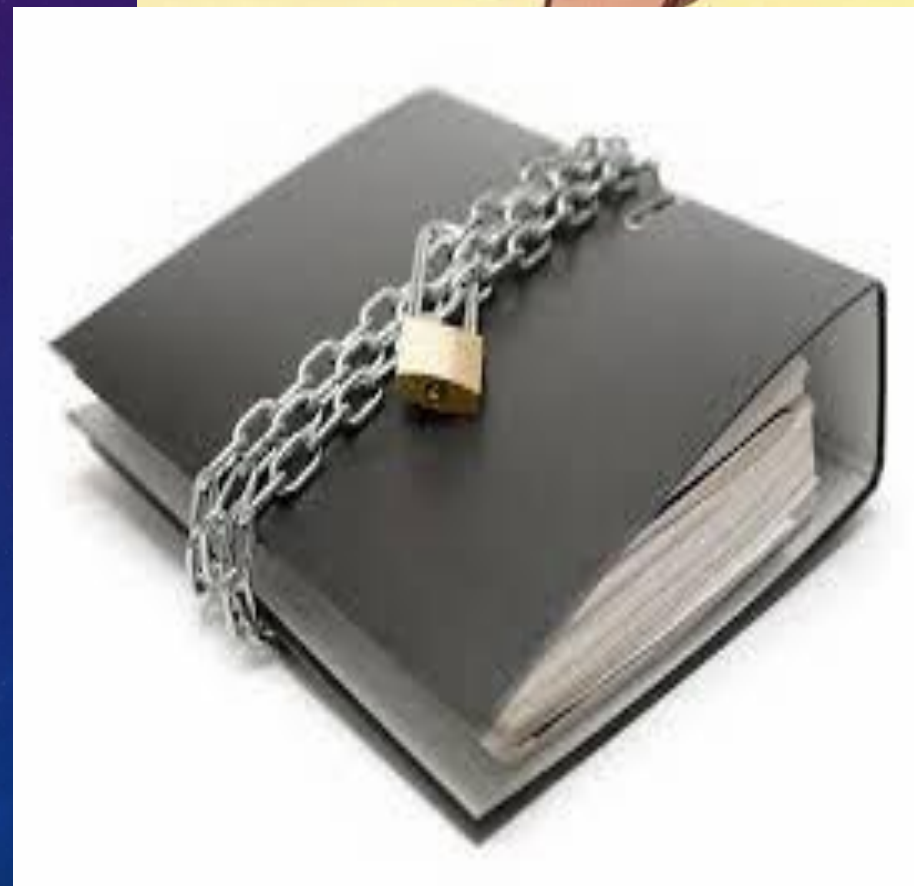
ЖИМ ГОСУДАРСТВЕННОЙ ТАЙНЫ

- **государственные секреты** - информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические, научно-технические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными в соответствии с настоящим Законом и другими нормативными правовыми актами Кыргызской Республики



- **Отнесение информации к государственным секретам и порядок ее засекречивания**

- 1. Отнесение сведений к государственным секретам осуществляется посредством определения сведений, которые подлежат защите в соответствии с настоящим Законом и другими нормативными правовыми актами Кыргызской Республики.
- 2. Отнесение информации к государственным секретам осуществляется согласно Перечню главнейших сведений, составляющих государственные секреты, утверждаемому Правительством Кыргызской Республики, а также ведомственным перечням сведений, подлежащих засекречиванию, утверждаемым руководителями государственных органов, органов местного самоуправления и организаций, наделенных полномочиями по отнесению сведений к государственным секретам.
- 3. Засекречивание информации осуществляется в соответствии с порядком определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, утверждаемым Правительством Кыргызской Республики.
- 4. Государственные органы, органы местного самоуправления и организации, определяемые Правительством Кыргызской Республики, вправе засекречивать и рассекречивать информацию, являющуюся собственностью юридических и физических лиц Кыргызской Республики



• Степени секретности сведений, составляющих государственные секреты, и грифы секретности носителей этих сведений

- 1. Государственные секреты Кыргызской Республики по степени важности составляющих их сведений подразделяются на две категории: государственную тайну (сведения, составляющие государственную тайну) и служебную тайну (сведения, составляющие служебную тайну).
- 2. Устанавливаются три степени секретности сведений, составляющих государственные секреты, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".



4. Сведениям, составляющим служебную тайну, присваивается гриф секретности "секретно". Служебная тайна имеет характер отдельных сведений, относящихся к государственной тайне, и не раскрывает их полностью.

- 5. Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственным секретам, а также присвоение указанным сведениям иных ограничительных грифов не допускаются.
- 6. Порядок установления ограничительных грифов на информацию определяется Правительством Кыргызской Республики.

РЕЖИМ КОММЕРЧЕСКОЙ ТАЙНЫ

- 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, 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.

РЕЖИМ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- **информационная безопасность Кыргызской** - состояние защищенности личности, общества и государства от информационных угроз;

КЛЮЧЕВЫМИ ПРОБЛЕМАМИ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЯВЛЯЮТСЯ:

- - незащищенность, неконтролируемость и недостаточность правового и технического регулирования информационного пространства;
- - распространение киберпреступности;
- - отсутствие эффективного противодействия трансграничной информационной преступности в современных условиях, сложность контроля за деятельностью интернет-ресурсов;
- - незащищенность индивидуального и массового сознания граждан от вредного и опасного контента в ходе информационного взаимодействия субъектов, манипуляция мнением пользователей сети Интернет представителями террористических и экстремистских организаций;
- - слаборазвитый отечественный контент средств массовой коммуникации;
- - недостаточное финансирование государственных инициатив в области обеспечения информационной безопасности Кыргызской Республики;
- - недостаточный уровень подготовки квалифицированных кадров в сфере информационной безопасности, информационной политики и защиты государственных секретов.

СПАСИБО ЗА ВНИМАНИЕ 🤔