

Опорный конспект лекций

ТЕМА 1 ИНФОРМАЦИОННОЕ ПРАВО В СИСТЕМЕ ПРАВА

- 1. Понятие, юридические особенности и свойства информации.**
- 2. Понятие информационного права. История становления информационного права.**
- 3. Предмет, методы, принципы и система информационного права.**
- 4. Информационные правоотношения: понятие, виды, структура.**
- 5. Информационное общество и цифровая трансформация государства.**

1. Понятие, юридические особенности и свойства информации

Создание современных сложных информационных технологий нового поколения обусловило почти безграничные возможности общества и государства в получении и использовании информации. В результате информация превратилась в важнейший ресурс государства наряду с его другими основными ресурсами – природными, экономическими, трудовыми, материальными.

Стремительно растущие информационные потоки порождают риск того, что нужная пользователю информация может быть не найдена или потеряна. Поэтому сегодня граждане должны обладать навыком поиска, получения, обработки и непосредственной работы с информацией. Передача информации в рамках общественных отношений является необходимым условием прогрессивного и непрерывного развития общества.

Информация сегодня выступает не только в качестве предмета труда, но и объекта правоотношений, в которые вступают люди. Понятие информации является основополагающим в большинстве отраслей знаний, являясь при этом противоречивым, спорным и дискуссионным. У ученых на сегодняшний день нет единого мнения по поводу определения понятия «информация». Отметим, что рассматриваемый термин имеет разное значение в той или иной отрасли общественных отношений. Анализ приведенных ниже понятий в различных сферах, а также в действующем законодательстве позволит выделить основные свойства рассматриваемого понятия.

В литературе на сегодняшний день существуют различные подходы к определению понятия «информация», а также тесно связанного с ним понятия «право на информацию».

Термин «информация» имеет латинские корни и произошел от слова *information* – разъяснение, осведомление, изложение.

До середины 20-х годов XX века под информацией действительно понимались «сообщения и сведения», передаваемые людьми устным, письменным или другим способом. С середины XX века информация определяется как общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму (генетическая информация); как одно из основных понятий кибернетики.

Термин «информация» до 60-х годов XX века не применялся ни в отраслевой науке, ни в законодательстве. Ученые применяли иные термины, такие как «данные», «материалы», «сведения», «сообщения». Лишь в 90-е годы XX века понятие «информация» начало использоваться в общей теории права; также начали использоваться его производные: «информационные процессы», «информационные отношения», «информационные системы и ресурсы».

Одним из первых, кто начал использовать термин «информация», был американский ученый, математик, физик и философ Н. Винер. В одной из своих работ «Кибернетика, или Управление и связь в животном и машине» Н. Винер определил информацию следующим образом: «Информация есть информация, а не материя и не энергия».

Обращаясь к данному определению, можно отметить, что автор рассматривал «информацию» как противопоставление «материи» и «энергии». В своих работах автор начал изучение и рассмотрение обработки информации, управления и связи.

Среди ученых, которые изучали понятие «информация», можно выделить следующих: И.Л. Бачило, О.А. Городова, В.А. Копылова, В.Н. Лопатина, Л.Л. Попова, М.М. Рассолова, И.М. Рассолова, С.В. Тихомирова и других. Рассмотрим некоторые подходы к определению понятия «информация».

Российский ученый-юрист И.Л. Бачило рассматривает информацию как понятие, которое отражает представление о досубъектной (дочеловеческой) стадии развития материи, включающей такие разновидности, как структурная, потенциальная и относительная информационные составляющие информационного содержания объектов реального мира, существующие независимо от наличия в нем человека. Также автор определяет информацию как «воспринимаемую и понимаемую человеком характеристику окружающего мира во всем его многообразии, которое возникает в процессе познания последнего и позволяет на основе свойств предметов, процессов, фактов и отражения их в различных формах восприятия отличать их признаки, значения и устанавливать их связи и зависимости всего многообразия проявления материального, духовного, идеологического мира – формировать мировую систему знаний».

Российский ученый В.А. Копылов рассматривает информацию в качестве основного объекта информационной сферы и системы прав.

Л.Л. Попов представляет информацию как «снятую неопределенность» и рассматривает ее через призму структуры (сбор, передача, регистрация, хранение, обработка и использование информации). Также автор определяет, что под информацией необходимо понимать определенные известия, сведения, сообщения, которые адекватно отражают объективную действительность и позволяют узнать что-либо новое, то, что ранее не было известно, или подтвердить факт, чтобы принять верное решение.

Российский ученый С.Ф. Анисимов, полагает, что информация – это всякое сообщение или передача сведений о чем-либо, что заранее не было известно. Исходя из данного определения, предложенного автором, можно сделать вывод о том, что информация является информацией лишь при условии того, что о ней не было известно ранее. Следовательно, сведения, которые были известны ранее, нельзя рассматривать в качестве информации.

Известны следующие теоретические определения информации: информация – это отчужденное знание (сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления), которое может быть записано на материальный носитель для того, чтобы быть доступным кому-либо (А.А. Козырев). Как справедливо отмечает российский ученый, академик Н.Н. Моисеев, «универсального определения понятия информации не только нет, но и быть не может из-за широты этого понятия». Согласимся с мнением автора, поскольку понятие «информация» используется не только в отрасли информационного права. Рассматриваемое понятие используется во всех без исключения общественных отношениях и сферах жизнедеятельности человека. Для каждого общественного отношения можно сформулировать свое понятие, и в связи с этим затруднительно сформулировать единое (универсальное) понятие информации в широком смысле.

Как отмечает российский ученый В. Хургин, понятие «информация» начали изучать с появлением теории журналистики. В данной отрасли под ним понималось «описание каких-либо фактов». Также обсуждались не только новые факты, но и существующие. В связи с появлением журналистики также была выявлена такая взаимосвязь информации и публицистики, как объяснение и комментирование фактов. Были изучены источники информации, а также проведена их классификация, исследованы взаимоотношения потребителя информации и сама информация, свойства информации (новизна,

оригинальность, партийность, достоверность, важность, полнота, убедительность, агитационная действенность и так далее).

А.Д. Урсул понимает информацию как «разнообразие, которое один объект содержит о другом, отраженное разнообразие». Разнообразие здесь – «характеристика элементов множества, заключающаяся в их отличии, несовпадении». Передача разнообразия от одного объекта к другому представляет собой информационный процесс.

Белорусский ученый Д.В. Вершок полагает, что «информация – произведенные человеком, природой соответственно предметы, звуки, сигналы, знаки, символы, иные изображения и отражения, несущие передаваемые разными способами сведения о предметах, фактах, событиях, лицах, явлениях и процессах, по поводу которых между участниками информационной сферы возникают юридически значимые коммуникативные связи и отношения».

В «Словаре русского языка» доктора филологических наук С.И. Ожегова информация определена как сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством. Анализируя данное понятие, автор в качестве субъектов выделяет человека или специальное устройство.

Легальное определение информации содержится в ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»: **информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Для информации любого вида и назначения, создаваемой, применяемой или распространяемой в правовой системе, присущи некоторые свойства, которые влекут за собой определенные юридические последствия при ее обращении. Закрепляются же такие свойства и особенности в нормах права и реализуются в информационных правоотношениях в особенностях поведения субъектов, в их правах, обязанностях и ответственности по фактам поведения.

Совместное исследование информационных процессов в информационной сфере, правовых норм, регулирующих отношения, возникающие в этих процессах, с действиями над информацией, позволяет установить ее **особенности и свойства**. К основным из них можно отнести:

1. Свойство физической неотчуждаемости информации. Оно основано на том, что знания не отчуждаемы от человека, их носителя. Исходя из этого, при передаче информации от одного лица к другому и юридическому закреплению этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами.

2. Свойство обособляемости информации. Для включения в оборот информация всегда овеществляется в виде символов, знаков, волн, вследствие этого обособляется от ее производителя (создателя) и существует отдельно и независимо от него. Это подтверждает факт оборотоспособности информации как самостоятельного отдельного объекта правоотношений, в результате чего появляется возможность передачи информации в такой форме от одного субъекта к другому.

3. Свойство информационной вещи (информационного объекта). Это свойство возникает в силу того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплено. Это свойство позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие двух институтов — института авторского права и института вещной собственности.

4. Свойство тиражируемости (распространяемости) информации. Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания. Одна и та же информация (содержание) может принадлежать

одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации). Отсюда следует, что юридически необходимо закреплять объем прав по использованию информации (ее содержания) лицами, обладающими такой информацией (обладающими знаниями о содержании информации).

5. Свойство организационной формы. Информация, находящаяся в обороте, как правило, представляется в документированном виде, т.е. в форме документа. Это могут быть подлинник (оригинал) документа, его копия, массив документов на бумажном или электронном носителе (банк данных или база данных) тоже в виде оригинала или копии, библиотека, фонд документов, архив и т.п. Такое свойство дает возможность юридически закреплять факт «принадлежности» документа конкретному лицу, например, закрепив его соответствующей подписью в традиционном или в электронном виде (с помощью ЭЦП). Это свойство позволяет также относить к информационным вещам (информационным объектам) как отдельные документы, так и сложные организационные информационные структуры.

6. Свойство экзemplярности информации. Это свойство заключается в том, что информация распространяется, как правило, не сама по себе, а на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию. Понятие экзemplярности дает возможность учитывать документированную информацию и тем самым связывать содержательную сторону информации с ее «вещным» обрамлением, т.е. с отображением на носителе, вводить понятие учитываемой копии документа, а отсюда и механизма регистрации информации, в особенности учитывать обращение оригиналов (подлинников) документов. Экзemplярность информации уже сегодня активно реализуется при обращении информации ограниченного доступа.

Указанные юридические особенности и свойства должны учитываться при правовом регулировании информационных отношений.

Существует множество критериев **классификации информации**.

Так, например, Б. Евладов выделяет четыре основных вида информации:

1) Контрольно-измерительная информация – та, которая связана с постоянным техническим контролем на производстве, и та, которая добывается в естественнонаучных исследованиях. Она фиксируется приборами и первичными учетными документами (таблицами, перфокартами и т.п.) и используется в целях регуляции процессов.

2) Учетно-статистическая информация включает в себя данные, которые поступают главным образом в цифровом виде и отражают развитие экономики, культуры, здравоохранения, образования и т.д. Так, например, при решении комплексных задач государственного и хозяйственного управления в сфере природопользования находят широкое применение разного рода кадастры, реестры и регистры в области водного, лесного и рыбного хозяйства, геодезии и картографии, геологии и экологии, гидрометеорологии, землеустройства и землепользования, стройиндустрии, а также данные государственного учета ресурсов животного и растительного мира. Наиболее полное отражение статистическая информация находит в специфических отчетах, используемых в сфере управления.

3) Научно-техническая информация включает в себя разнообразные данные, характеризующие состояние тех или иных наук, технические достижения. Эта информация отражается обычно в массе специальной литературы по разным отраслям науки, промышленного и сельскохозяйственного производства и используется в основном узким кругом специалистов этих отраслей.

4) Общественно-политическая информация – сведения, рождаемые в повседневной экономической, политической и культурной жизни общества.

По степени организованности (упорядоченности) информацию можно разделить на документированную и не документированную.

В соответствии со ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» документированная информация – информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать. Информационные ресурсы составляют определенные документы или массивы документов, имеющие реквизиты. Недокументированная информация остается за пределами правового регулирования.

В зависимости от категории доступа информация делится на общедоступную информацию и информацию, распространение и (или) предоставление которой ограничено.

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены:

- о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;
- о деятельности государственных органов, общественных объединений;
- о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами;
- о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;
- о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
- о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;
- о состоянии преступности, а также о фактах нарушения законности;
- о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;
- о размерах золотого запаса;
- об обобщенных показателях по внешней задолженности;
- о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;
- накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

К информации, распространение и (или) предоставление которой ограничено, относится:

- информация о частной жизни физического лица и персональные данные;
- сведения, составляющие государственные секреты;
- служебная информация ограниченного распространения;
- информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;
- информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
- иная информация, доступ к которой ограничен законодательными актами.

Следует подчеркнуть, что исходя из подхода, предполагающего обязательное наличие субъекта, воспринимающего информацию, закрытой информации не бывает; так, это означало бы, что существует информация не известная никому, т.е. информация без субъекта, ее воспринимающего.

Информация делится по роли в системе права на правовую и неправовую.

Впервые термин «правовая информация» был закреплен в Положении о порядке распространения правовой информации, утвержденном Указом Президента Республики

Беларусь от 1 декабря 1998 г. № 565: правовая информация – это тексты правовых актов, составляющих законодательство Республики Беларусь. Из этого следует, полагаем, что законодатель понимает под правовой информацией только лишь законодательство Республики Беларусь, а не иные документы, которые содержат правовую информацию (к примеру, разъяснения, документы правоприменительного характера и иные, содержащие правовую информацию).

Рассматриваемое Положение утратило силу в связи с принятием Указа Президента Республики Беларусь от 30 декабря 2010 г. № 712 «О совершенствовании государственной системы правовой информации Республики Беларусь», которым утверждено Положение о деятельности по распространению (предоставлению) правовой информации в Республике Беларусь (далее – Положение № 712). Так, Положением № 712 понятие правовой информации было расширено и конкретизировано, но также приравнено к понятию законодательства. В соответствии с абз. 3 п. 2 Положения № 712 под правовой информацией понимаются «тексты и обязательные реквизиты правовых актов, составляющих законодательство Республики Беларусь, в том числе международных договоров Республики Беларусь».

В связи с принятием Указа Президента Республики Беларусь от 11 июля 2016 г. № 261 «О внесении изменений и дополнений в указы Президента Республики Беларусь» понятие «правовая информация» было изложено в новой редакции и теперь в действующей редакции Положения № 712 (Указ Президента Республики Беларусь № 415 от 17 ноября 2020 г.) закреплено следующее определение: «правовая информация – правовые акты, составляющие законодательство Республики Беларусь, в том числе международные договоры Республики Беларусь».

Неправовая информация создается не как результат правотворческой деятельности, обращается в обществе в соответствии с предписанием правовых норм.

2. Понятие информационного права. История становления информационного права.

Термин «информационное право» обычно понимается в 3-х значениях:

- как наука;
- как учебная дисциплина;
- как отрасль права.

Информационное право как наука представляет собой систему научных знаний об информационном праве как отрасли права, его предмете и методе правового регулирования, истории развития, содержании правовых институтов и т.д.

Как учебная дисциплина информационное право – это система знаний об информационном праве, обязательных для изучения в учебных заведениях (главным образом, юридических) на основании и в соответствии с государственными образовательными стандартами и учебными программами.

Что касается информационного права как отрасли права, то правоприменительная практика показывает, что предписания, правовые конструкции и механизмы регулирования традиционных отраслей права в принципе не могут быть применены к общественным отношениям, складывающимся в информационной сфере. Это обстоятельство явилось предпосылкой формирования новой комплексной отрасли права, а именно информационного права. Многие специалисты относят комплексность информационного права к явлению временному, которое свойственно периоду становления и накопления нормативной базы.

Кроме того, информационное право на сегодняшний день – одна из наиболее спорных областей юриспруденции. Это подтверждается и неопределенностью даже в самом наименовании отрасли, что проявляется в научных диспутах и литературе. Имеют место такие дефиниции, как: «правовая кибернетика», «правовая информатика»,

«практическая информатика», «компьютерное право», «электронное право», «электронно-компьютерное право», «информационно-компьютерное право» и т.д.

Согласимся с тем, что информационное право – это совокупность правовых норм, регулирующих общественные отношения, связанные с информацией (вполне классическое нормативистское определение).

Практически все отношения в социуме имеют информационную составляющую. Поэтому об информационном праве можно говорить как в широком, так и в узком смысле слова. В первом случае нормами информационного права пронизано все законодательство (например, информационно-правовой характер носят нормы Уголовно-процессуального кодекса Республики Беларусь о процессуальных действиях со свидетелями и прочими лицами, налогового законодательства о декларировании и отчетности и т.д.). Однако в этих случаях информационная деятельность играет хотя и важную, но вспомогательную роль, то есть является средством для достижения цели, лежащей за пределами информационной сферы (раскрытие преступления и наказание виновных, взимание налогов и т.д.). К информационному праву в узком или собственном смысле слова могут быть отнесены лишь такие нормы, которые регулируют информационные процессы, являются самоцелью, то есть когда информация есть не только средство достижения чего-либо иного, но и конечный итог. Можем ли мы говорить принципиально о самодостаточности информационной деятельности, или она всегда направлена на получение какого-либо материального результата?

Как известно, отрасли права можно разделить на две большие группы – классические, или «гомогенные» (это, например, уголовное, гражданское, конституционное право), и комплексные, или интегральные. По сути, речь идет о двух, одновременно существующих, способах классификации всего нормативного поля. Информационное право носит интегральный характер, так как состоит из норм, относящихся к классическим отраслям, объединенных спецификой объекта своего воздействия – информационных отношений.

Информационное право в обобщенной форме может быть определено, как самостоятельная отрасль права, представляющая собой совокупность правовых норм, закрепляющих и регулирующих общественные отношения, возникающие в процессе создания, преобразования, хранения, распространения и потребления информации.

Информационное право является самостоятельной отраслью национальной системы права в силу следующих обстоятельств:

- наличия у него своего предмета правового регулирования и особых методов регулирующего воздействия;
- наличия значительного объема достаточно развитого информационного законодательства;
- наличия системы специальных принципов правового регулирования.

Развитие **доктрины информационного права** и законодательства прошли несколько этапов.

Первая волна публикаций приходится на 60-е – первую половину 70-х годов XX века. В данный период интерес ученых сосредоточен на исследовании информационного обеспечения механизма государственного управления, развитии автоматизированных систем управления, использовании кибернетического моделирования и вычислительной техники в сфере юридической деятельности и отдельных видов последней. Это направление позже получило определение «правовая кибернетика».

Одной из первых работ, посвященной данному направлению, была статья Д.А. Керимова, в которой автор отметил, что изучение опыта по использованию методов и средств кибернетики в различных областях теории и практики дает основание утверждать, что они могут быть эффективно использованы и при решении ряда государственно-правовых проблем в целях получения определенных результатов с минимальной затратой времени, труда и энергии. Вызывает интерес позиция ученого относительно возможностей

использования кибернетической техники при решении правовых проблем, к числу которых он относит справочно-информационную службу в области права, некоторые задачи правотворчества, кодификации законодательства, помощь в обобщении судебной практики, проведении различного рода криминалистических экспертиз и т.д.

Дальше всех из исследователей, изучая правовую кибернетику, зашел Н.В. Витрук, рассматривая в своих трудах правовую кибернетику как науку, научный метод и учебную дисциплину.

Таким образом, на данном этапе юридическая наука приступила к разработке правовых аспектов применения автоматизированных систем и вычислительной техники в государственном управлении, а также в отдельных видах юридической деятельности.

Второй этап научных исследований приходится на вторую половину 70-х – начало 90-х годов XX века. Особенностью данного периода является то, что ученые впервые заговорили о самостоятельности информационных отношений. Так, формируется подход, определяющий информационные отношения как объект правового регулирования. Однако на данном этапе информационные отношения рассматриваются только в рамках автоматизации государственного управления или в связи с созданием и использованием объектов компьютерной техники и технологии. Данный подход отражен в работах В.А. Рассудовского, А.Б. Венгерова, Ю.М. Батурина и др. Значительное влияние на исследование данной проблемы оказали работы А.Б. Венгерова, в которых, во-первых, положено начало рассмотрению информации как объекта правового регулирования; во-вторых, заявлено о самостоятельности информационных правоотношений; в-третьих, предпринята попытка определить юридическую ответственность в сфере использования автоматизированных систем в управлении; в-четвертых, затронуты проблемные стороны систематизации и кодификации законодательства об автоматизации и прочее.

Позже, в 1984 году, вопрос о самостоятельности информационных отношений исследуется В.А. Рассудовским. Автор отмечает, что информационные отношения существуют в основном либо в гражданско-правовой, либо в административно-правовой формах. Он один из первых определяет правовой режим научно-технических знаний (идей), исследует право на них, а также отмечает, что стремительное развитие информационных отношений на этапе научно-технической революции приводит к возникновению концепции информационного права, предметом которого являются общественные отношения в области организации и использования систем информации. В.А. Рассудовский полагает, что современный этап научно-технической революции воплощается в электронно-вычислительной технике, «машинной информатике». Исследователь связывает прогнозы на будущее с развитием «информатизированного» общества.

По сравнению с первым периодом уделяется больше внимания проблемам создания системы правовой информации, формируется информационный подход к праву, исследуются информационное содержание и функции правовых норм в качестве разновидности социальной управляющей информации, служащей средством управления поведением людей.

М.М. Рассолов, в своих работах рассматривает значительный круг теоретических проблем управления, информатизации и компьютеризации в сфере права, создание автоматизированных информационно-поисковых систем. Несомненным достоинством его трудов является то, что автором выработано обобщающее определение правовой кибернетики как самостоятельной юридической науки и учебной дисциплины, имеющей свой объект, предмет, методы исследования, а также строго очерченный круг задач.

Значительное влияние на исследования в области информационного права и законодательства оказала работа Ю.М. Батурина, посвященная правовым проблемам, рожденным компьютеризацией общественной жизни. Предметом исследования стали теоретические проблемы компьютеризации общественной жизни, которые стали рассматриваться под углом зрения теории права и теории государства. В работе

обособливаются информационные общественные отношения по поводу создания, использования объектов компьютерной техники и технологии и определяется их правовое регулирование. Исследователь обращает внимание на то, что эти отношения частично уже регулируются нормами административного, гражданского, трудового, уголовного и других отраслей права, но вся проблематика «разбрасывается» по уже существующим отраслям без остатка. Автор предпринял попытку выделить предмет и метод компьютерного права, сформулировал предложения по изменению законодательства об административных правонарушениях, уголовного законодательства, законодательства о защите интеллектуальной собственности, предложил проект закона о защите гражданских прав и свобод в связи с компьютерной обработкой информации, а также проект международного договора о взаимной компьютерной безопасности.

Таким образом, Ю.М. Батуриным ввел в научный оборот словоформу «компьютерное право», которая далее использовалась наравне с «правовой кибернетикой» и «правовой информатикой». В то же время данная словоформа отличалась от «правовой кибернетики» и «правовой информатики» и их отдельных направлений, которые были до этого момента основным предметом исследования ученых.

Таким образом, основными результатами исследований на данном этапе являются:

1) выделение информационных отношений в качестве самостоятельной группы социальных отношений, которые становятся предметом исследования не только в рамках гражданского и административного права, но и в иных отраслях права;

2) появление идеи о формировании информационного права (компьютерного права), требующей более глубокой и всесторонней теоретической обоснованности.

Третий этап научных исследований приходится на начало 90-х годов XX века – начало XXI века. На данном этапе информационные отношения начинают развиваться в различных направлениях в рамках процесса информатизации общества, поэтому предметом исследования ряда ученых становится разработка направлений информатизации общества и ее правового регулирования. Вместе с тем в указанном периоде еще не было выработано единого определения понятия «информатизация», и очень часто данный термин отождествлялся с «компьютеризацией».

Новым направлением исследований, которое возникает на данном этапе, являются правовое регулирование отношений в глобальной сети Интернет и разработка теоретических и практических основ правового регулирования данных отношений, которые нашли отражение в работах российских ученых М.В. Якушева, М.А. Федотова, Л.К. Терещенко и др.

Формируется научная доктрина о праве граждан на информацию и ответственность в случае его ограничения. Благодаря этому в доктрине начинают укрепляться позиции авторов об институте собственности на информацию, о доступе к информации, реализации механизма ее защиты, а также видах информации и об ограниченном доступе к ней.

На данном этапе впервые появляются работы, в которых ученые рассматривают проблему определения места информационного права в системе права, а также особенности взаимодействия информационного права с другими отраслями права. Исследователями делается акцент на развитие информационного права как самостоятельной отрасли права. Данные разработки нашли отражение в работах российских авторов И.Л. Бачило, О.Е. Кутафина, Ю.И. Попугаева и др. Происходит осмысление необходимости формирования информационного права как самостоятельной отрасли права, изучения его с точки зрения теории права, что позволило разработать методологические основы данной отрасли.

В этот период появляется одна из первых работ, посвященных комплексному исследованию структуры и состава информационного законодательства, – монография российского ученого А.Б. Агапова «Информационное законодательство России». Автором предпринята попытка исследовать информационное законодательство в рамках

регламентации информационных отношений, возникающих в процессе сбора, аналитической обработки и распространения информации на основе новых электронных средств.

Таким образом, на данном этапе закладываются теоретические основы правового регулирования новых видов информационных отношений и информатизации общества. Начинают формироваться методологические основы информационного права, предпринимаются попытки определения его места среди других отраслей права. Положено начало исследованиям формирования информационного законодательства.

Четвертый этап развития научных взглядов приходится на начало XXI века – конец первого десятилетия XXI века. Данный период научных исследований закладывает теоретическую и правовую основу развития доктрины о формировании общества нового типа – «информационного». К работам комплексного характера по данной тематике необходимо отнести труды российских ученых И.Л. Бачило, М.В. Якушева и др. Стоит отметить, что на протяжении первых трех этапов научных исследований ученые говорили о «компьютеризации общества» или об «информатизированном обществе», однако данные понятия определяли отдельные стороны информационного общества.

Начало формирования информационного общества оказало значительное влияние на научно-исследовательскую работу ученых указанного периода, занимающихся изучением проблемных вопросов государственной информационной политики государства, – авторами впервые была выделена информационная функция государства. Кроме этого, возрос интерес в исследовании вопросов правового обеспечения информационной безопасности, что во многом было определено уровнем развития государства и его вхождением в мировое информационное пространство. Данные аспекты нашли отражение в работах белорусских, российских и украинских авторов А.Н. Васенина, В.Б. Долголева, Ю.И. Кашиńskiego, П.У. Кузнецова, Б.А.Кормича, А.П. Леонова, М.В. Мясниковича, Ю.Г. Просвирнина, А.А. Стрельцова и др.

В связи с появлением концепции информационного общества резко возрастает интерес ученых к юридическим аспектам общественных отношений, возникающих в информационной сфере. К комплексным работам по рассматриваемой тематике можно отнести труд российского ученого Д.В. Огородова, который является одним из первых исследователей информационных отношений с точки зрения теории права. Ученый полагает, что данные правовые отношения представляют собой правоотношения в полном смысле, поскольку возникают как результат правового регулирования соответствующих общественных отношений, не являясь результатом лишь информационного действия права, а также включают в себя все элементы, присущие правоотношению (субъекты, объект, содержание). Автор обращает внимание на двойственное понимание информационных правоотношений: во-первых, отображающих информационное действие права, во-вторых, – правоотношений в определенной сфере с выделением всех элементов.

В данный период российскими учеными были выделены новые направления юридической науки в информационной сфере. Так, И.М. Рассолов в своем труде выделяет новый институт права – интернет-право, который представляет собой отдельное направление юридической науки. Л.В. Голоскоков и А.В. Малько формируют концепцию сетевого права, исследуют принципы его построения, сферы сопряжения информационно-коммуникационных технологий, права и экономики.

В то же время Ю.М. Батурин в труде «Телекоммуникации и право: вопросы стратегии» отмечает, что, несмотря на все условности теоретической проблемы определения самостоятельных отраслей права в системе российского права, телекоммуникационное право, право Интернета и другие подобные обозначения самостоятельных правовых отраслей пока не имеют «права на существование».

Ю.В. Волков в диссертации «Субъекты телекоммуникационного права», затрагивая проблемы правового регулирования телекоммуникационной деятельности, не выделяет

отдельный институт «телекоммуникационное право», а правовое регулирование телекоммуникационной сферы рассматривает как предмет науки информационного права.

На данном этапе возрастает количество работ методологического характера. Устанавливается концептуальное видение специфики правового регулирования информационной сферы, исследуются вопросы выделения предмета, метода, основных институтов, источников и прочих критериев формирующейся «отрасли информационного права». Информационное право начинает рассматриваться как самостоятельная наука и учебная дисциплина. Данные вопросы исследуются в работах как белорусских, так и российских и украинских ученых И.Л. Бачило, А.Ю. Головиной, Д.В. Вершка, П.У. Кузнецова, Л.Н. Мороза, С.Г. Чубукова, М.Я. Швеца и др.

На данном этапе издаются учебные пособия, которые преимущественно направлены на исследование теоретических характеристик информационного права, его основных институтов. Авторами учебных пособий подробно рассматривается правовое регулирование основных видов информационных отношений (И.Л. Бачило, М.В. Боер, О.А. Городова, М.А. Лапина, В.А. Копылов, М.М. Рассолов и др.).

В работах названных ученых объект правового регулирования исследуется в рамках анализа отдельных видов информации в различных отраслях права. Что же касается комплексных исследований информации как объекта, лежащего в основе правового регулирования информационных отношений, то здесь необходимо обратить внимание на работу российского ученого А.В. Минбалева, который проанализировал общественные отношения, складывающиеся по поводу информации и отдельных ее видов, а также правовой режим информации. В связи с этим особую актуальность и значимость приобрели правовые исследования информации как объекта, лежащего в основе всех информационных отношений.

В Республике Беларусь на данном этапе вопросами формирования и развития информационного права занимались Д.В. Вершок, Л.Н. Мороз.

Одной из первых работ в данном направлении является монография белорусского ученого Д.В. Вершка «Информационное право: правовой режим радиоэлектронной информации», в которой обосновывается и исследуется правовой режим радиоэлектронной теле-, радио-, телефонно-телеграфной и компьютерной информации. Правовые нормы, регламентирующие использование и применение данного вида информации, должны составлять один из основных институтов формирующейся правовой отрасли, предметов юридической науки и учебной дисциплины «Информационное право».

В 2007 году выходит работа белорусского ученого Л.Н. Мороза «Информационное право: общая часть», ставшая одной из первых работ, в которой в сравнительно-правовом аспекте комплексно исследуются теоретические и прикладные правовые проблемы: информации и информационных ресурсов; информационной сферы; информационных пространств и обществ; становления, развития и совершенствования информационного права и информационного законодательства; сущность и структура информационных правоотношений, информационного правосознания; общие вопросы управления и юридической ответственности в информационной сфере.

Обобщающей работой, комплексно исследующей информационное законодательство, можно назвать труд российского ученого В.И. Кутузова «Основы информационного законодательства». В монографии прокомментированы основополагающие законодательные акты как общего информационного законодательства, так и регулирующего отдельные виды информационной деятельности в сфере информационных и коммуникационных технологий, а также в сфере интеллектуальной собственности.

Таким образом, на данном этапе происходит формирование доктрины становления информационного общества, что качественно повлияло на изменение информационной

сферы и ее правового регулирования. Кроме этого, завершается разработка основных методологическо-теоретических вопросов информационного права и законодательства.

Пятый этап научных исследований приходится на конец первого десятилетия XXI века – по настоящее время. Данный период можно охарактеризовать как «этап реализации теоретических разработок на практике». Резко возрастает количество публикаций по различным направлениям реформирования информационного законодательства в условиях формирования информационного общества. Авторы приходят к выводу о том, что правовое регулирование информационных отношений отстает от потребностей общества и препятствует формированию информационного общества. Учеными предлагаются отдельные варианты систематизации информационного законодательства, которое рассматривается ими как форма внутреннего упорядочения действующей правовой системы, приведения в определенную единую систему.

Проблемные стороны информационного законодательства и его систематизация исследуются в Республике Беларусь, Украине и Российской Федерации. Наиболее значимый вклад в изучение проблем информационного законодательства в Республике Беларусь внесли такие ученые, как М.С. Абламейко, Г.А. Василевич, В.И. Шабайлов и др.

Отдельного рассмотрения требует комплексная работа М.С. Абламейко, которая посвящена правовым проблемам построения информационного общества в Республике Беларусь и направлена на дальнейшее развитие новой отрасли права – информационного права. Автором выявлены основные аспекты правового регулирования отношений на современном этапе развития информационного общества, проанализирована роль государства в данном процессе и его взаимодействие с частным ИТ-сектором, разработаны практические предложения и рекомендации по правовому обеспечению оказания электронных услуг гражданам и организациям в Республике Беларусь, выявлены особенности правовой защиты информационных систем в Республике Беларусь, сформулированы предложения, связанные с уголовно-правовой оценкой нарушений авторских прав в данной сфере, определены основные направления дальнейшего развития и совершенствования законодательства Республики Беларусь в области информационной безопасности и защиты от кибератак информационного пространства Республики Беларусь, конкретизированы пути унификации законодательства с другими странами, в первую очередь Россией и Казахстаном, и дальнейшей интеграции Республики Беларусь в глобальное информационное общество.

В Российской Федерации исследованием совершенствования информационного законодательства в этот период занимаются А.Н. Алферов, И.Л. Бачило, Л.А. Коврижных, Е.А. Кусова, Ю.Г. Просвинин, Т.А. Полякова и др.

Фундаментальным трудом российских авторов стала работа «Концепция Информационного кодекса Российской Федерации» (2014 год), в которой на основе действующего законодательства Российской Федерации обосновывается подход к разработке Информационного кодекса, предлагается концепция Кодекса, основанная на взаимосвязи суперинститутов, институтов и субинститутов, формирующих механизмы взаимодействия материальных и процессуальных правовых норм.

Изучением проблем совершенствования информационного законодательства активно занимаются украинские исследователи М.И. Димчогло, В.А. Зализняк, В.А. Липкан, А.И. Марущак, Е.Д. Скулиш, А.Л. Петрицкий, И.Б. Тацишин, К. Татарникова, К.П. Череповский, В.С. Цимбалюк и др.

Среди комплексных работ необходимо отметить монографию В.А. Липкана и М.И. Димчогло, в которой проводится комплексный анализ консолидации как многоаспектной составляющей систематизации информационного законодательства, а также разработаны предложения и рекомендации по осуществлению данной деятельности. Кроме этого, в целях дальнейшего совершенствования национального информационного законодательства и практики его применения изложены предложения по структуре

Информационного кодекса Украины и этапов проведения систематизации отечественного информационного законодательства.

Таким образом, наибольших результатов в исследованиях информационного права и информационного законодательства достигли ученые Российской Федерации, усилиями которых были сформулированы теоретико-методологические основы информационного права и законодательства, а также изучены структура, система, состав информационного законодательства, его соотношение с информационным правом. Ученые Украины концентрировали свое внимание преимущественно на прикладных аспектах совершенствования информационного законодательства. На сегодняшний день в Республике Беларусь по сравнению с Украиной и Российской Федерацией имеются отдельные теоретико-правовые исследования в сфере информационного права и законодательства, посвященные совершенствованию отдельных структурных частей информационного законодательства.

Формирование в Республике Беларусь информационного общества настоятельно требует системного анализа информационного права и информационного законодательства, разработки перспектив совершенствования информационного законодательства, его систематизации и последующей кодификации, механизма совершенствования информационного законодательства. В данном вопросе следует опираться на достижения доктрины информационного права и законодательства Российской Федерации и Украины, учитывать при этом положительный опыт и имеющиеся недостатки.

3. Предмет, методы, принципы и система информационного права.

Отрасли права отличаются друг от друга, прежде всего, предметом своего регулирования. У каждой отрасли права есть свой, только ей присущий предмет. В теории права **предметом правового регулирования** признается совокупность общественных отношений, на регулирование которых непосредственно направлены соответствующие нормы права.

Четкое определение предмета информационного права имеет немаловажное значение, так как позволяет избежать дублирования с другими отраслями права, появления коллизий и пробелов. Отграничение одной отрасли права от другой способствует выявлению наиболее эффективных инструментов правового регулирования определенной группы общественных отношений.

В настоящее время вопрос о предмете информационного права не решен однозначно. Однако попытки сформулировать предмет информационного права предпринимались ведущими учеными в данной области.

Так, коллектив авторов И.Л. Бачило, В.Н. Топорин, М.А. Федотов полагают, что предмет информационного права составляют общественные отношения, связанные с правовым регулированием оборота информации, формированием и использованием информационных ресурсов, созданием и использованием информационных систем, обеспечивающих процессы информатизации, удовлетворение потребностей пользователей, а также обеспечения информационной безопасности всех участников информационных отношений.

В.А. Копылов отмечает, что предметом информационного права являются общественные отношения, возникающие, изменяющиеся и прекращающиеся при обращении информации в информационной сфере в результате осуществления информационных процессов.

П.У. Кузнецов под предметом информационного права понимает область общественных отношений, связанных с формированием и использованием информационных ресурсов, информатизацией, информационными системами и телекоммуникационной деятельностью, а также обеспечением информационной безопасности.

Коллектив белорусских исследователей (Г.А. Василевич, Д.А. Плетнев, Т.З. Шалаева, М.С. Абламейко, Е.В. Семашко, Д.Е. Тагунов) рассматривают предмет правового регулирования информационного права как общественные информационные отношения, связанные с созданием, преобразованием, хранением, передачей, распространением, потреблением информации. Авторы называют весьма условным выделение названных групп отношений, составляющих предмет информационного права, и отмечают в большей степени его теоретически ориентированный характер.

Таким образом, поскольку информационное право по своей сути является правом об информации, предмет его регулирования составляют те общественные отношения, которые связаны с информацией (возникают по поводу данного объекта, опосредуются процессами обращения информации).

Специфика **методов информационного права** – сочетание конституционного регулирования, административных способов обеспечения особенностей информационной деятельности и привлечение контрольных, принудительных и карательных мер в процессе обеспечения соблюдения информационного законодательства.

Основными методами правового регулирования в информационном праве являются следующие:

1. Диспозитивный (разрешительный) метод правового регулирования информационных отношений (предполагает такой характер информационной деятельности соответствующих субъектов правоотношений, при котором им предлагается свобода в реализации своих прав). Данный метод применяется, в частности, при регулировании отношений информационной собственности, при создании и использовании информационных технологий и средств их обеспечения и т.д.

2. Ограничительно-запретительный (императивный) метод правового регулирования информационных отношений состоит в установлении запретов и определении правового статуса субъектов информационных отношений.

Императивный метод правового регулирования информационных отношений используется в процессе регламентации деятельности государственных органов в информационной сфере, например, формирования и реализации государственной политики по развитию информационного общества; при определении компетенции государственных органов в сфере предоставления информации, затрагивающей интересы человека; при регулировании информационных отношений в области обеспечения информационной безопасности и т.д.

Правовое регулирование информационных отношений основывается на **принципах информационного права**, под которыми понимаются основные исходные положения, юридически закрепляющие объективные закономерности общественных отношений, проявляющихся в информационной сфере. Исходя из особенностей информации как объекта правового регулирования, можно назвать следующие принципы правового регулирования общественных отношений в информационной сфере:

1) принцип законности в информационных отношениях и строгого соблюдения прав и интересов человека в информационной сфере;

2) принцип правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;

3) принцип свободы информации, который включает в себя свободу создания, распространения, поиска, передачи и получения информации;

4) принцип ограничения или запрещения производства и распространения отдельных видов информации. Необходимость введения данного принципа определяется тем, что отдельные виды информации при неконтролируемом распространении могут представлять опасность как для отдельных людей, так и для общества и государства в целом;

5) принцип собственности на информацию. Данный принцип основывается на положениях гражданского законодательства о том, что информация является объектом гражданских прав, в силу чего может находиться в собственности физических и юридических лиц, государства и т.д.;

6) принцип овеществления информации, который предполагает, что объектом правоотношений может быть только овеществленная информация, закрепленная на определенном носителе;

7) принцип полноты обработки и оперативности предоставления информации, который означает обязанность любого государственного органа собирать, накапливать и хранить информацию в полном объеме в соответствии со своей компетенцией, а также предоставлять потребителям запрашиваемую информацию в установленные законодательством сроки;

8) принцип ответственности, который применительно к информационно-правовому регулированию означает неотвратимое наступление юридической ответственности за нарушение требований и положений информационно-правовых норм;

9) принцип обеспечения информационной безопасности, который предполагает обеспечение всесторонней и полной защиты человека, общества и государства от недоброкачественной информации, а также защиту информации и информационных продуктов от несанкционированного использования.

Как правило, структурно система отрасли права включает общую и особенную части.

Общая часть информационного права может включать общие понятия и определения (в том числе теоретические основы информационной безопасности и использования национального сегмента сети Интернет), принципы, предмет и метод информационного права, задачи и характеристику сферы применения информационного законодательства; понятие и структуру информационного правоотношения, объекты, субъекты и их права и обязанности, компетенцию должностных лиц государственных органов и организаций в области их регулирования информационных правоотношений, информационные и цифровые права и свободы.

Особенная часть информационного права включает институты информационного права: правовой режим информации и информационных ресурсов, институт информатизации и защиты информации, массовой информации, рекламы, правовой охраны коммерческой тайны, государственных секретов и персональных данных, электронного товарооборота, обеспечения информационной безопасности, использования национального сегмента сети Интернет; ответственности за нарушения информационного законодательства.

4. Информационные правоотношения: понятие, виды, структура.

Информационное право как отрасль права регулирует особую группу общественных отношений – информационные отношения (отношения в информационной среде).

Вопрос о выделении информационных отношений в отдельную группу общественных отношений и признании их как объекта права был поставлен А.Б. Венгеровым еще в 1978 г. Сегодня термин «информационные отношения» укоренился в терминологическом аппарате юридической науки.

Согласно ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» **информационные отношения** – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Особенность информационных отношений заключается в том, что они возникают, развиваются и прекращаются в информационной сфере при обращении информации в

результате осуществления информационных процессов с учетом особенностей и свойств информации, проявляющихся в системе права.

Правовые отношения определяются как юридическая форма общественных отношений, представляющая собой возникающие на основе правовых норм и определенных жизненных обстоятельств связи конкретных субъектов права, обладающих взаимными субъективными правами и обязанностями, гарантированными государством.

Информационные правоотношения можно рассматривать как юридическую форму общественных отношений, возникающих на основе информационно-правовых норм и юридических фактов между субъектами, обладающими взаимными субъективными правами и обязанностями, гарантированными государством.

А.В. Капылов рассматривает информационное правоотношение как урегулированное информационно-правовой нормой информационное отношение, стороны которого выступают в качестве носителей взаимных прав и обязанностей, установленных и гарантированных информационно-правовой нормой.

Информационные правоотношения – это юридическая форма общественных отношений в информационной сфере, урегулированных нормами информационного права, в которых стороны выступают носителями взаимных субъективных прав и обязанностей, соответствующих конкретным юридическим фактам и реализация которых гарантируется государством.

Юридическая наука использует достаточно широкий спектр общепризнанных критериев и оснований для классификации правоотношений.

Информационные правоотношения можно классифицировать следующим образом по критерию связи с конкретным информационным процессом: связанные с созданием информации; связанные с обработкой информации; связанные с хранением информации; связанные с распространением информации; связанные с потреблением информации.

По функциональному критерию информационные правоотношения делятся на регулятивные и охранительные.

Кроме того, по степени конкретизации и субъектному составу можно выделить следующие информационные правоотношения: абсолютные, относительные и общерегулятивные. В абсолютных точно определена лишь одна сторона (например, собственник информационных ресурсов, информационных систем, технологий и средств обеспечения, которому противостоят все те, кто с ним соприкасается или может соприкоснуться, и которые обязаны уважать это его право). В относительных строго определены обе стороны. Общерегулятивные правоотношения выражают юридические связи более высокого уровня между государством и гражданами, а также последних между собой по поводу гарантирования и осуществления основных прав и свобод личности, а равно обязанностей. Они возникают, таким образом, на основе норм Конституции, других основополагающих актов и являются базовыми, исходными для отраслевых правоотношений.

Под **структурой информационного правоотношения** следует понимать совокупность обязательных элементов, составляющих его, к которым относятся субъекты информационных правоотношений, субъективные права и обязанности сторон информационного правоотношения, объекты информационных правоотношений.

В соответствии со ст. 5 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» **субъектами информационных отношений** могут являться:

- Республика Беларусь, административно-территориальные единицы Республики Беларусь;
- государственные органы, другие государственные организации;
- иные юридические лица, организации, не являющиеся юридическими лицами;
- физические лица, в том числе индивидуальные предприниматели;

– иностранные государства, международные организации.

Указанных субъектов информационных отношений можно отнести к категории общих субъектов. Наряду с общими субъектами информационных правоотношений целесообразно выделять специальные субъекты. Термины «общий субъект» и «специальный субъект» в законодательстве не употребляются, однако применяются исследователями для обозначения определенной группы субъектов правоотношений. Наряду с общими признаками, специальный субъект обладает дополнительными.

Так, субъекты информационных отношений могут выступать в качестве:

– обладателя информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства, или по договору;

– пользователя информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею,

– пользователя информационных систем и (или) информационных сетей – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими;

– собственника программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями;

– владельца программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями в пределах и порядке, определенных их собственником в соответствии с законодательством;

– информационного посредника – субъект информационных отношений, предоставляющий информационные услуги обладателям и (или) пользователям информации;

– оператора информационных систем – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги.

Субъективные права и обязанности сторон информационного правоотношения можно определить как возникающие в пределах, предусмотренных информационно-правовой нормой, и вследствие юридических фактов рамки поведения участников данных правоотношений. Говоря о субъективных правах, имеем в виду рамки возможного поведения субъектов информационных правоотношений, о субъективных обязанностях – рамки должного поведения субъектов информационных правоотношений. Субъективные права и обязанности предполагают возможность или необходимость определенного поведения.

В информационных правоотношениях субъективные права и обязанности участников взаимосвязаны и корреспондируют, т.е. осуществление субъективных прав одной стороной обеспечивается выполнением субъективных обязанностей другой стороной.

Субъективные права и обязанности составляют юридическую форму информационного правоотношения (внешнее выражение), а реальное поведение сторон – его содержание. Между формой и содержанием любого явления могут возникнуть противоречия: возможны такие противоречия между субъективными правами и обязанностями участников информационных правоотношений и их фактическим поведением.

Объект информационного права образуют материальные и нематериальные процессы, блага побуждающие субъектов информационного права вступать в определённые отношения. Объектом информационного права выступает информация: информационные ресурсы, базы данных, различные печатные материалы, аудиоматериалы, видеоматериалы и многое другое. Стоит отметить, что независимо от принимаемой формы, информация – это всегда сведения о событиях, лицах, процессах. Человек извлекает её из внешней среды и отображает в своем сознании.

5. Информационное общество и цифровая трансформация государства.

Информация в истории развития цивилизации всегда играла определяющую роль и служила основой для принятия решений на всех уровнях и этапах развития общества и государства. В истории общественного развития можно выделить несколько информационных революций, связанных с кардинальными изменениями в сфере производства, обработки и обращения информации, приведших к радикальным преобразованиям общественных отношений. В результате таких преобразований общество приобретало в определенном смысле новое качество.

Первая информационная революция связана с изобретением письменности, что привело к гигантскому качественному и количественному скачку в информационном развитии общества. Появилась возможность фиксировать знания на материальном носителе, тем самым отчуждать их от производителя и передавать от поколения к поколению.

Вторая информационная революция (середина XVI в.) вызвана изобретением книгопечатания (первопечатники Гуттенберг и Иван Федоров). Появилась возможность тиражирования и активного распространения информации, возросла доступность людей к источникам знаний. Эта революция радикально изменила общество, создала дополнительные возможности приобщения к культурным ценностям сразу больших слоев населения.

Третья информационная революция (конец XIX в.) обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, позволяющие оперативно передавать и накапливать информацию в значительных объемах. Следствие этой революции – повышение степени распространяемости информации, повышение информационного «охвата» населения средствами вещания. Повысилась роль средств массовой информации как механизмов распространения сообщений и знаний на больших территориях и обеспечения ими проживающих на них граждан, повысилась доступность членов общества к сообщениям и знаниям. Существенно возросла роль информации как средства воздействия на развитие общества и государства, появилась возможность оперативного общения людей между собой.

Четвертая информационная революция (середина XX в.) связана с изобретением вычислительной техники и появлением персонального компьютера, созданием сетей связи и телекоммуникаций. Стало возможным накапливать, хранить, обрабатывать и передавать информацию в электронной форме. Возросли оперативность и скорость создания и обработки информации, в памяти компьютера стали накапливаться практически неограниченные объемы информации, увеличилась скорость передачи, поиска и получения информации.

Сегодня мы переживаем пятую информационную революцию, связанную с формированием и развитием трансграничных глобальных информационно-телекоммуникационных сетей, охватывающих все страны и континенты, проникающих в каждый дом и воздействующих одновременно и на каждого человека в отдельности, и на огромные массы людей. Наиболее яркий пример такого явления и результат пятой революции – Интернет. Суть этой революции заключается в интеграции в едином информационном пространстве по всему миру программно-технических средств, средств связи и телекоммуникаций, информационных запасов или запасов знаний как единой

информационной телекоммуникационной инфраструктуры, в которой активно действуют юридические и физические лица, органы государственной власти и местного самоуправления. В итоге неимоверно возрастают скорости и объемы обрабатываемой информации, появляются новые уникальные возможности производства, передачи и распространения информации, поиска и получения информации, новые виды традиционной деятельности в этих сетях.

Мы являемся свидетелями существенного повышения роли и места информации в жизни личности, общества, государства, воздействия информации на развитие личности, общества, государства. Информация сегодня превратилась в мощный реально ощутимый ресурс, имеющий даже большую ценность, чем природные финансовые, трудовые и иные ресурсы. Информация стала товаром, который продается и покупается. Информация превратилась в оружие, возникают и прекращаются информационные войны. Активнейшим образом развивается и входит в нашу жизнь трансграничная информационная сеть Интернет.

Все это серьезно трансформирует жизнь личности, общества, государства. Цивилизация в целом и каждый из нас, в частности, находимся в стадии формирования общества нового типа – информационного общества. Это общество все еще непонятно для многих. Социальная система и право как один из основных регуляторов этой системы существенно отстают от темпов развития информационного общества, от непостижимых скоростей наступления на нас новых информационных технологий и всемирной паутины Интернет – «строительного материала» информационного общества.

Среди глобальных трендов, существенно повлиявших на развитие всех систем и институтов современного социума и вызвавших его глубокие трансформации в экономической, политической, социальной и культурных сферах, особая роль принадлежит процессу информатизации. Информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений.

Введение понятия информационного общества в широкий научный оборот произошло практически одновременно в таких странах, как США и Япония, благодаря работам Ф. Махлупа и Т. Умесао. Ф. Махлуп изучал информационную составляющую экономики в США, а Т. Умесао исследовал данный сектор в своей стране. Независимо друг от друга ученые указали не только на значимость компьютеризации и автоматизации производства, но и сделали вывод о ключевом статусе информации в данном процессе. Тем не менее, в исследованиях информатизации Ф. Махлупа и Т. Умесао еще отсутствовала интенция к распространению полученных выводов на весь социальный порядок.

Свое более широкое употребление понятие «информационное общество» обрело лишь в 70-80-х гг. XX в., благодаря работам Д. Белла, Е. Масуды, О. Тоффлера, М. Кастельса. Значимый вклад в развитие теории информационного общества внесли М. Порат, Т. Стоуньер, Р. Катц, У. Мартин, Р. Брэйтенштейн, Т. Бэккер, В. Дайзард, Г. Краух, Д. Мур, М. Понятовски, Дж. Пэлтон и др. Проведенные ими исследования продемонстрировали, что с началом развития компьютерных технологий и совершенствования механизмов функционирования информации и социальной коммуникации стало возможным с принципиально новых позиций оценить целостность и единство человеческой цивилизации, переопределить принципы и практики самоорганизации людей на основе открывшегося широкого доступа к информационным ресурсам, а также произошедшей на этой основе трансформации системы власти, которая стала более ориентированной на профессиональные и интеллектуальные ценности. В результате развития представлений об информационном обществе как новой ступени развития человеческого сообщества были кардинально пересмотрены взгляды на экономику, образование и культуру. Также претерпели изменения и сама социальная

стратификация, социально-психологические и коммуникационные основы общественных взаимодействий.

Следует отметить, что информационное общество рассматривается с разных точек зрения, в зависимости от области применения.

С экономической точки зрения, информационное общество можно определить, как особую форму организации общества, в которой создание информации, ее обработка и передача становятся фундаментальными источниками производительности труда.

С юридической точки зрения информационное общество – это общество, в котором на основании развитой законодательной базы обработка и использование знаний и информации становится основной производительной силой, а развитые социально-политические электронные механизмы позволяют населению активно и беспрепятственно участвовать в жизни общества.

Характерным признаком такого общества является главенствующая роль информации и информационных технологий в жизни людей, что в свою очередь приводит к возрастанию количества занятых в информационной сфере людей.

Одной из главных задач построения информационного общества является цифровизация всех процессов, происходящих в государстве. В связи с этим в последние годы все более широко применяется термин «цифровая трансформация общества».

Цифровизация (внедрение современных цифровых технологий в различные сферы жизни и производства) становится основой функционирования различных субъектов общественных отношений в большинстве сфер их деятельности. И государственные органы, учреждения, частные компании сегодня ставят цифровизацию для себя в ряд своих основных и стратегических приоритетов.

Цифровизация общественных отношений выражается в применении современных цифровых технологий в самых различных сферах деятельности человека. Современные цифровые технологии формируют новый способ производства, создают предпосылки для перехода к новой общественно-экономической формации, к цифровизации самого права, регулирующего такие отношения. Становятся они и фактором динамичного развития социума.

Цифровая трансформация оказывает самое непосредственное влияние на реализацию конституционных прав и свобод человека и гражданина, способствует появлению новых. Сегодня сеть, являясь средством общения, превратилась в инструмент для заработка, финансовые потоки которого также нуждаются в регулировании. Так, формируется целая культура, находящаяся в настоящее время за пределами правового регулирования и вне зоны государственного влияния. И чтобы устранить этот пробел, необходимы разработка и принятие соответствующего законодательства.

На уровне Конституции Республики Беларусь вопросы правового регулирования цифровизации пока не отражены, но не остаются без внимания. Беларусь начала свое продвижение в информационное пространство, приняв в декабре 2002 г. комплексную Государственную программу «Электронная Беларусь». На ее основе в стране уже сделано многое по внедрению информационных технологий, а особое внимание уделено именно правовому регулированию общественных отношений в информационной сфере. Так, правовые нормы об электронной цифровой подписи содержатся в Налоговом кодексе Республики Беларусь, Хозяйственном процессуальном кодексе Республики Беларусь, Гражданском кодексе Республики Беларусь и иных законодательных актах.

В 2016 году Республика Беларусь взяла курс на «цифровизацию». Утверждение Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы (постановление Совета Министров Республики Беларусь от 23 марта 2016 г. № 235) способствовало активному внедрению и развитию цифровых технологий, что привело к качественной трансформации общественных отношений.

Следует также обратить внимание и на Концепцию информационной безопасности Республики Беларусь, утвержденную постановлением Совета безопасности Республики

Беларусь от 18 марта 2019 г. № 1. В п. 9 отмечается, что основополагающим национальным интересом Республики Беларусь в информационной сфере, с точки зрения гуманитарного аспекта, является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

Постановлением Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66 утверждена Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы. Государственная программа разработана в соответствии с приоритетными направлениями социально-экономического развития республики до 2025 года и направлена на внедрение информационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества.

В рамках Государственной программы предусматривается выполнение мероприятий по созданию (развитию) современной информационно-коммуникационной инфраструктуры, внедрению цифровых инноваций в отраслях экономики и технологий «умных городов», а также обеспечению информационной безопасности таких решений.

ТЕМА 2

ПРАВО НА ИНФОРМАЦИЮ, ЕГО ОХРАНА И ЗАЩИТА

1. Конституционная основа осуществления права на поиск, получение и передачу информации.

2. Правовые гарантии поиска и получения информации. Свобода доступа к информации. Правовой режим доступа к открытой информации. Ограничение доступа к информации на основе законодательства Республики Беларусь.

3. Право граждан на обращение в государственные органы и получение информационных государственных услуг. Единый портал электронных услуг ОАИС.

1. Конституционная основа осуществления права на поиск, получение и передачу информации.

Информационные права и свободы являются фундаментом развития информационного общества и связаны со всем комплексом прав человека.

Мировое сообщество еще в середине XX ст. ввело правовые механизмы, обеспечивающие гарантии прав и свобод человека и гражданина, значительную роль в которых играют информационные права и свободы.

Информационные права и свободы впервые были закреплены во Всеобщей декларации прав человека, утвержденной и провозглашенной Генеральной Ассамблеей Организации Объединенных Наций (ООН) 10 декабря 1948 г. Например, ст. 19 декларации закрепила свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

Конвенция Совета Европы о защите прав человека и основных свобод от 4 ноября 1950 г. развивает положения, закрепляющие информационные права и свободы. В частности, в ст. 10 содержится норма о свободе получать и распространять информацию и идеи без какого-либо вмешательства со стороны государственных органов и независимо от государственных границ.

Международный пакт о гражданских и политических правах от 16 декабря 1966 г. также включает статьи, закрепляющие информационные права и свободы (статьи 17-19).

Согласно п. 1 ст. 13 Конвенции о правах ребенка, принятой резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 г. ребенок имеет право свободно

выражать свое мнение; это право включает свободу искать, получать и передавать информацию и идеи любого рода, независимо от границ, в устной, письменной или печатной форме, в форме произведений искусства или с помощью других средств по выбору ребенка.

Информационные права и свободы закреплены в действующей Конституции Республики Беларусь. Свобода информации в конституционном праве представляет собой группу прав и свобод, включающую в себя:

- свободу слова;
- свободу печати и иных средств массовой информации;
- право на получение информации, имеющей общественное значение;
- свободу распространения информации любым законным способом.

Конституционной основой поиска, получения и распространения информации являются следующие положения Конституции Республики Беларусь:

1) Статья 34: «Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, о политической, экономической, культурной и международной жизни, состоянии окружающей среды. Государственные органы, должностные лица обязаны предоставить гражданину Республики Беларусь возможность ознакомиться с материалами, затрагивающими его права и законные интересы. Пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, частной и семейной жизни граждан и полного осуществления ими своих прав».

2) Часть 1 статьи 51: «Каждый имеет право на участие в культурной жизни. Это право обеспечивается общедоступностью ценностей отечественной и мировой культуры».

3) Статья 28: «Каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. Государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании».

4) Статья 33: «Каждому гарантируется свобода мнений, убеждений и их свободное выражение. Никто не может быть принужден к выражению своих убеждений или отказу от них. Монополизация средств массовой информации государством, организациями или отдельными гражданами, а также цензура не допускаются».

2. Правовые гарантии поиска и получения информации. Свобода доступа к информации. Правовой режим доступа к открытой информации. Ограничение доступа к информации на основе законодательства Республики Беларусь.

Конституционные нормы, содержащие в себе информационные права, реализуются в различных нормативных правовых актах.

Так, положения статьи 34 Конституции Республики Беларусь реализуются в статье 6 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», в соответствии с которой право на информацию включает:

- право государственных органов, физических и юридических лиц осуществлять поиск, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации, пользование информацией в соответствии с Законом об информации и иными актами законодательства;

- право граждан на ознакомление с информацией, затрагивающей их права и законные интересы, в порядке, установленном Законом об информации и иными актами законодательства;

- право граждан на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни,

состоянии окружающей среды в порядке, установленном Законом об информации и иными актами законодательства.

Что касается норм статьи 28 Конституции Республики Беларусь понятие права на неприкосновенность частной жизни не закреплено в законодательстве Республики Беларусь. В юридической практике к информации о частной жизни относят те сведения, которые человек сам желает оставить в тайне.

Указанная конституционная норма реализуется в статье 18 Закона об информации. Так право на неприкосновенность частной жизни и персональных данных включает:

- право на личную и семейную тайну,
- право на тайну телефонных переговоров, почтовых и иных сообщений,
- право на врачебную тайну.

В соответствии со статьей 1 Закона об информации персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

В соответствии со ст. 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с письменного согласия данного физического лица, если иное не установлено законодательными актами.

Порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления информации о частной жизни физического лица и персональных данных, а также пользования ими устанавливается законодательными актами.

Как уже отмечалось выше, право на свободу выражения мнений, убеждений и их свободное выражение содержится в статье 33 Конституции Республики Беларусь. Никто не может быть принужден к выражению своих убеждений или отказу от них. Монополизация средств массовой информации государством, организациями или отдельными гражданами, а также цензура не допускаются. Указанные положения также закреплены в статьях 5 и 6 Закона Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации»: в Республике Беларусь каждому гарантируются свобода мнений, убеждений и их свободное выражение. Монополизация средств массовой информации государственными органами, политическими партиями, другими общественными объединениями, иными юридическими или физическими лицами не допускается.

В соответствии с белорусским законодательством дети также обладают информационными правами. В соответствии со ст. 11 Закона Республики Беларусь от 19 ноября 1993 г. № 2570-ХІІ «О правах ребенка» каждый ребенок имеет право на получение, хранение и распространение информации в соответствии с Законом о правах ребенка и иными законодательными актами, свободу мнений, убеждений и их свободное выражение.

Каждый ребенок, способный формулировать свои взгляды, имеет право свободно их выражать по всем вопросам, которые его затрагивают, причем взглядам ребенка уделяется должное внимание в соответствии с его возрастом. В частности, ребенку предоставляется возможность непосредственно либо через представителя или соответствующий орган быть заслушанным в ходе любого затрагивающего его судебного или административного разбирательства в порядке, предусмотренном законодательством.

В статье 28 Закона о правах ребенка закреплено право ребенка на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений.

В 2016 г. в рассматриваемом законе появилась статья 37¹, закрепившая нормы о праве детей на защиту от информации, причиняющей вред их здоровью и развитию.

К информации, причиняющей вред здоровью и развитию детей, относится следующая способная оказать негативное влияние на здоровье, физическое, нравственное и духовное развитие детей определенной возрастной категории информация:

- вызывающая желание употреблять алкогольные, слабоалкогольные напитки, пиво, потреблять наркотические средства, психотропные вещества, их аналоги, токсические или другие одурманивающие вещества, табачные изделия;

- побуждающая к совершению преступления или иного общественно опасного деяния, в том числе к занятию проституцией, попрошайничеством, бродяжничеством, участию в азартных играх, совершению действий, связанных с изготовлением, распространением порнографических материалов или предметов порнографического характера;

- положительно оценивающая преступление или идеализирующая преступников, поощряющая поведение, ущемляющее человеческое достоинство, в том числе совершение насильственных действий по отношению к людям или животным;

- отображающая издевательства над человеком или группой людей либо их унижения в связи с этническим происхождением, национальной, расовой, религиозной, языковой, половой принадлежностью, убеждениями или взглядами, социальным положением, заболеванием;

- поощряющая или положительно оценивающая жестокость, физическое, психическое, сексуальное насилие, сексуальную эксплуатацию, сексуальные отношения с участием детей;

- побуждающая к нанесению телесных повреждений или самоубийству, описывающая средства или обстоятельства самоубийства;

- содержащая методики либо иные материалы о способах изготовления опасных для жизни и здоровья людей предметов и их использования;

- поощряющая привычки, противоречащие формированию здорового образа жизни;

- содержащая нецензурные слова и выражения;

- дискредитирующая институт семьи и брачно-семейные отношения;

- устрашающего характера, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме смерти, несчастного случая, аварии, катастрофы, заболевания и (или) их последствий;

- содержащая порнографические материалы и (или) эротику.

В целом, право свободного поиска и получения информации означает:

- право каждого обращаться в органы государственной власти, общественные объединения, организации, другие структуры за получением необходимой информации;

- право обращаться в учреждения культуры, иные структуры, к хранителям культурных ценностей с целью получения у них запрашиваемой информации;

- право свободно получать сообщения, подготавливаемые и распространяемые средствами массовой информации;

- право получать информацию, содержащуюся в научных трудах и литературных произведениях, а также другую информацию.

В соответствии со статьей 15 Закона об информации в зависимости от категории доступа информация делится на общедоступную информацию и информацию, распространение и (или) предоставление которой ограничено.

Согласно статье 16 Закона об информации к общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

- о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;
- о деятельности государственных органов, общественных объединений;
- о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами;
- о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;
- о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
- о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;
- о состоянии преступности, а также о фактах нарушения законности;
- о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;
- о размерах золотого запаса;
- об обобщенных показателях по внешней задолженности;
- о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;
- накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

Статья 21 Закона об информации регламентирует порядок предоставления общедоступной информации на основании обращения.

Предоставление общедоступной информации может осуществляться на основании обращения заинтересованного государственного органа, физического или юридического лица к обладателю такой информации. Обращение за получением общедоступной информации может быть изложено в письменной, электронной или устной форме.

Предоставление заинтересованному государственному органу, физическому или юридическому лицу общедоступной информации на основании обращения может осуществляться посредством:

- устного изложения содержания запрашиваемой информации;
- ознакомления с документами, содержащими запрашиваемую информацию;
- предоставления копии документа, содержащего запрашиваемую информацию, или выписок из него;
- предоставления письменного или электронного ответа (справки), содержащего (содержащей) запрашиваемую информацию.

Общедоступная информация может не предоставляться на основании обращения в случае, если:

- для получения запрашиваемой информации требуется проведение аналитической работы, непосредственно не связанной с защитой прав и законных интересов обратившегося лица;
- запрашиваемая информация опубликована в официальных периодических печатных изданиях, средствах массовой информации либо размещена в открытом доступе на официальных сайтах государственных органов в глобальной компьютерной сети Интернет или на других государственных информационных ресурсах глобальной компьютерной сети Интернет;
- запрашиваемая информация ранее предоставлялась обратившемуся лицу;
- запрашивается информация, содержащаяся в докладных записках, поручениях должностных лиц и другой внутренней переписке государственного органа, иного

юридического лица, если такая информация непосредственно не связана с защитой прав и законных интересов лица, обратившегося за получением общедоступной информации;

– запрашиваются копии имеющихся в государственном органе, у юридического лица документов других государственных органов, юридических лиц, за исключением случая, когда указанные государственные органы, юридические лица ликвидированы и отсутствуют их правопреемники, а также в иных случаях, когда от указанных государственных органов, юридических лиц получить такие копии документов в установленном порядке невозможно;

– в иных случаях, установленных законодательными актами.

Порядок подачи обращений за получением общедоступной информации, а также порядок их рассмотрения определяются законодательными актами.

В международном и национальном праве в целях обеспечения информационных интересов личности, общества и государства, в интересах национальной безопасности и защиты нравственности, разработана система ограничения информационных прав и свобод.

В статье 29 Всеобщей декларации прав человека указано, что при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе.

Международный пакт о гражданских и политических правах в статье 19 гласит, что каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения или иными способами по своему выбору.

Пользование предусмотренными выше правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

а) для уважения прав и репутации других лиц;

б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Законодательство Республики Беларусь также содержит нормы об ограничении информационных прав и свобод. Согласно статье 23 Конституции Республики Беларусь ограничение прав и свобод личности допускается только в случаях, предусмотренных законом, в интересах национальной безопасности, общественного порядка, защиты нравственности, здоровья населения, прав и свобод других лиц.

Статья 34 Конституции Республики Беларусь, закрепляющая право на информацию, содержит основания для ограничения указанного права: пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, частной и семейной жизни граждан и полного осуществления ими своих прав.

В статье 6 Закона об информации указывается, что право на информацию не может быть использовано для пропаганды войны или экстремистской деятельности, а также для совершения иных противоправных деяний.

Право на неприкосновенность частной жизни может быть ограничено, например, нормами Закона Республики Беларусь от 15 июля 2015 г. № 307-3 «Об оперативно-розыскной деятельности»: ограничение прав, свобод и законных интересов граждан, прав и законных интересов организаций при осуществлении оперативно-розыскной деятельности допускается в интересах национальной безопасности Республики Беларусь, общественного порядка, защиты нравственности, здоровья населения, прав и свобод других граждан в соответствии с настоящим Законом и иными законодательными актами (статья 7).

Рассматриваемое право может быть ограничено в процессе осуществления оперативного опроса; наведения справок; сбора образцов; исследования предметов и документов, компьютерной информации; оперативного отождествления; оперативного осмотра; наблюдения; проверочной закупки; контролируемой поставки; слухового контроля; контроля в сетях электросвязи; контроля почтовых отправлений; оперативного внедрения; оперативного эксперимента.

3. Право граждан на обращение в государственные органы и получение информационных государственных услуг. Единый портал электронных услуг ОАИС.

Расширение технических возможностей человека обмениваться информацией с неизбежностью отражается на характере складывающихся в государстве общественных отношений, в связи с этим возникает необходимость в пересмотре подходов к их правовому регулированию.

Принимая во внимание возможности государства по сбору и распространению информации, а также обязанность по обеспечению основных прав и свобод человека, полагаем, что правовое регулирование внедрения технологий для распространения информации, находящейся во владении органов государственного управления, позволит повысить эффективность информирования граждан и субъектов хозяйствования о деятельности государства.

В Республике Беларусь, согласно Конституции Республики Беларусь, гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов (ч. 1 ст. 34 Конституции Республики Беларусь). При этом учитывая, что к стратегическим целям внутренней политики нашей страны относится обеспечение прав и свобод человека и гарантии их реализации, совершенствование правового регулирования удаленного доступа к информации о деятельности органов государственного управления направлено на достижение стратегических целей внутренней политики Республики Беларусь по обеспечению права на эту информацию и укрепление гарантий его реализации.

Согласно ст. 21 Закона об информации предоставление общедоступной информации может осуществляться на основании обращения заинтересованного государственного органа, физического или юридического лица к обладателю такой информации. Обращение за получением данной информации может быть изложено в электронной форме, а ее предоставление заинтересованному лицу – посредством электронного ответа или справки. Соответственно, обработка индивидуальных запросов на доступ заявителя к имеющимся в органе государственного управления документам и сведениям вправе осуществляться удаленно.

В соответствии со ст. 3 Закона Республики Беларусь от 18 июля 2011 г. № 300-З «Об обращениях граждан и юридических лиц» граждане Республики Беларусь имеют право на обращение в организации путем подачи письменных, электронных или устных обращений, а также к индивидуальным предпринимателям путем внесения замечаний и (или) предложений в книгу замечаний и предложений. Юридические лица Республики Беларусь, индивидуальные предприниматели имеют право на обращение в организации путем подачи письменных (за исключением замечаний и (или) предложений, вносимых в книгу замечаний и предложений), электронных или устных обращений. Находящиеся на территории Республики Беларусь иностранные граждане и лица без гражданства, представительства иностранных организаций пользуются правом на обращение наравне с гражданами Республики Беларусь и юридическими лицами Республики Беларусь, если иное не определено Конституцией Республики Беларусь, законами и международными договорами Республики Беларусь.

Порядок рассмотрения электронных обращений регулируется Законом Республики Беларусь от 18 июля 2011 г. № 300-З «Об обращениях граждан и юридических лиц» с учетом особенностей, отраженных в ст. 25 данного Закона.

Значительным направлением развития распространения сведений, содержащихся в государственных информационных системах в области государственного управления, является их размещение на интернет-сайтах не просто в виде сканированных электронных копий бумажных документов, а в составе «экосистем» государства как «платформы».

Вместе с тем подчеркнем, что Законом об информации определен особый правовой режим для «государственного информационного ресурса» и «государственной информационной системы»:

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;

государственный информационный ресурс – информационный ресурс, формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Так, в соответствии с абз. 2 ст. 23 Закона об информации состав государственных информационных ресурсов, порядок их формирования, а также пользования документированной информацией из них определяются законодательными актами Республики Беларусь и (или) постановлениями Совета Министров Республики Беларусь.

Постановлением Совета Министров Республики Беларусь от 26 мая 2009 г. № 673 «О некоторых мерах по реализации Закона Республики Беларусь «Об информации, информатизации и защите информации» утверждены:

Положение о составе государственных информационных ресурсов, порядке их формирования и пользования документированной информацией из государственных информационных ресурсов;

Положение о порядке государственной регистрации информационных ресурсов и ведения Государственного регистра информационных ресурсов;

Положение о порядке государственной регистрации информационных систем, использования государственных информационных систем и ведения Государственного регистра информационных систем.

В соответствии с пунктом 20 Положения о составе государственных информационных ресурсов если иное не установлено законодательными актами, доступ пользователей в автоматическом и (или) автоматизированном режимах к информации, содержащейся в государственных информационных ресурсах, организуется посредством ОАИС либо обеспечивается их владельцами на период проведения технических и организационных мероприятий по интеграции государственных информационных ресурсов (систем) с ОАИС.

Государственные информационные системы создаются в целях предоставления общедоступной информации, обеспечения ее объективности, полноты и достоверности, оказания информационных услуг, оптимизации деятельности государственных органов и обеспечения информационного обмена между ними.

ОАИС (общегосударственная автоматизированная информационная система) – государственная информационная система, предназначенная для интеграции государственных информационных ресурсов, осуществления административных процедур в электронном виде и иных электронных услуг посредством Единого портала электронных услуг. ОАИС реализована не как законченная система, а как

интеграционный инструмент по наращиванию функционала и электронных сервисов под текущие нужды для пользователей внутри страны и за рубежом.

Общегосударственная автоматизированная информационная система обеспечивает предоставление электронных услуг из государственных информационных ресурсов, интегрированных с ОАИС, на едином портале электронных услуг portal.gov.by.

ОАИС предназначена для интеграции государственных информационных ресурсов и автоматизации деятельности органов государственного управления по предоставлению информационных услуг другим государственным органам, организациям и гражданам.

При этом целью создания ОАИС является повышение эффективности и качества функционирования государственных органов и, как следствие, качества оказываемых услуг.

Благодаря налаживанию механизмов межведомственного взаимодействия государственные структуры смогут быстрее и эффективнее осуществлять свои функции, выполнять административные процедуры. Для рядовых граждан это означает простоту, удобство и скорость в удовлетворении их запросов.

В современной версии Портала реализованы электронные услуги в сфере налогообложения, учета и обращения недвижимого имущества, труда и социальной защиты на основе информации из ГИР – государственных информационных ресурсов – информационных систем, баз данных, которые наполняет и ведет то или иное ведомство (всего 37 ГИР).

Одни услуги на портале доступны широкому кругу пользователей, бесплатны и не требуют регистрации на портале, другие открыты лишь после проверки идентификационных данных Оператором ОАИС. Последним выступает республиканское унитарное предприятие «Национальный центр электронных услуг», на его серверах и находится аппаратно-программная часть ОАИС, обеспечивается безопасность и защищенность передаваемых сведений.

Таким образом, реализация доктрины «прозрачного правительства» посредством интернета в Республике Беларусь регулируется положениями об удаленном предоставлении общедоступной информации при помощи норм права о порядке рассмотрения электронных обращений, пользовании документированной информацией из государственных информационных ресурсов и пользовании государственной информационной системой.

При этом если необходимая информация отсутствует в государственном информационном ресурсе или государственной информационной системе, то гражданин вправе направить электронное обращение о предоставлении электронного ответа (справки), содержащего (содержащей) запрашиваемую информацию.

Здесь следует акцентировать внимание на том, что общедоступная информация согласно абз. 3 ч. 4 ст. 21 Закона об информации может не предоставляться на основании обращения в случае, если «запрашиваемая информация... размещена в открытом доступе на официальных сайтах государственных органов в глобальной компьютерной сети Интернет...». Из этого следует, что эффективность предоставления общедоступной информации может быть повышена посредством ее размещения в открытом доступе на интернет-сайтах органов государственного управления в связи с наличием юридической возможности отказывать в рассмотрении индивидуальных запросов, что позволяет сократить время, затрачиваемое государственными служащими на рассмотрение электронных обращений.

ПРАВОВЫЕ РЕЖИМЫ ИНФОРМАЦИИ

1. Понятие правового режима информации и его разновидности.
2. Режим свободного доступа. Режим ограниченного доступа.
3. Служебная информация ограниченного распространения. Информация, запрещенная к обороту.

1. Понятие правового режима информации и его разновидности.

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.

Виды правового режима информации:

1. Общий правовой режим, который выражает общие, исходные способы правового регулирования.

2. Специальные правовые режимы.

Общий правовой режим информации характеризуется открытостью, доступностью информации как для физических, так и для юридических лиц. Исключения из общего режима информации могут устанавливаться только законом.

Общий правовой режим информации складывается из: права свободно получать информацию; права свободно передавать информацию; права свободно распространять информацию.

Режим общедоступной информации представляет собой максимально возможную свободу не только доступа, но и использования информации, что можно охарактеризовать следующим образом:

1. Круг лиц, имеющих право получить общедоступную информацию, неограничен.
2. Форма предоставления информации зависит от конкретной ситуации.
3. Цель предоставления информации не имеет значения.
4. Доступ к информации открыт.
5. Объем предоставляемой информации неограничен.

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.

2. Режим свободного доступа. Режим ограниченного доступа.

Режим информации свободного доступа можно разделить на несколько режимов:

1. Режим исключительных прав. В отношении информации, существующей в форме охраняемых результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации участников гражданского оборота и производимой ими продукции, специальным законодательством определен адекватный их правовой природе режим правовой охраны. Главнейшей функцией института исключительных прав является наделение их обладателя определенным объемом правомочий, отражающих меру его юридических возможностей по контролю над тем или иным результатом интеллектуальной деятельности. Содержание прав на охраняемый результат варьируется в зависимости от разновидности последнего. Практически для каждого из охраняемых продуктов интеллектуальной деятельности законодательством сделаны изъятия в форме указания на случай их свободного использования или формулирования.

2. Режим общественного достояния. Данный правовой режим информации является модифицированным вариантом режима свободного доступа к информации. Установление режима общественного достояния в отношении информации обусловлено необходимостью придания отдельным разновидностям сведений качеств, общественно необходимых и полезных всем членам общества. В таком режиме может находиться не любая общедоступная информация, а лишь та, которая незаменима и по своей природе уникальна (например, сведения о научных открытиях, уникальные рукописи, документы, архивы, произведения устного народного творчества и т. п.).

Принципы, на которых основывается режим общественного достояния, сводятся к следующему:

- общедоступность;
- равенство возможностей на доступ;
- обеспеченность информации особой охраной государства.

Принцип общедоступности реализуется посредством создания условий для беспрепятственного ознакомления и (или) использования соответствующих сведений. Принцип равенства возможностей на доступ реализуется путем предоставления всем членам общества при наличии оправданного к тому интереса единообразных условий для ознакомления с информацией, отнесенной к общественному достоянию, и ее получения. Принцип обеспеченности информации особой государственной охраной реализуется через комплекс организационно-обеспечительных мер, направленных на сохранность наиболее ценных и необходимых обществу информационных ресурсов.

3. Режим массовой информации. Правовой режим массовой информации обусловлен ролью института массовой информации, которую последний призван играть в общественной жизни. Состояние свободы массовой информации является доминирующим среди иных состояний открытой информации. В отличие от режима исключительных прав и режима общественного достояния режим массовой информации характеризуется меньшей степенью формализации информационных отношений применительно к ее потребителям. В целом потребитель массовой информации в отличие от потребителя информации, существующей в форме охраняемых результатов интеллектуальной деятельности или информации, отнесенной к общественному достоянию, не ограничен какими-либо запретами, помимо социальных ограничений возможности выбора или языковых барьеров, которые не относятся к сфере правовой регламентации. Действующие нормативные запреты в основном касаются лиц, производящих для неограниченного круга потребителей печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Наиболее общим запретом в отношении массовой информации является недопущение пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду.

Понятие «информация, распространение и (или) предоставление которой ограничено» применяется в ст. 15 Закона Республики Беларусь «Об информации, информатизации и защите информации». К информации, распространение и (или) предоставление которой ограничено, относится:

- информация о частной жизни физического лица и персональные данные;
- сведения, составляющие государственные секреты;
- служебная информация ограниченного распространения;
- информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;
- информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
- иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

3. Служебная информация ограниченного распространения. Информация, запрещенная к обороту.

К **служебной информации ограниченного распространения** относятся сведения, касающиеся деятельности государственного органа, юридического лица, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые не отнесены к государственным секретам.

Сведения относятся к служебной информации ограниченного распространения в соответствии с перечнем сведений, относящихся к служебной информации ограниченного распространения, определяемым Советом Министров Республики Беларусь, а также в случаях, предусмотренных законами Республики Беларусь и решениями Президента Республики Беларусь. Решение об отнесении сведений к служебной информации ограниченного распространения принимается руководителем государственного органа, юридического лица или уполномоченным им лицом. Постановлением Совета Министров от 12 августа 2014 г. № 783 утверждено Положение о порядке проставления ограничительного грифа «Для служебного пользования», грифа «Коммерческая тайна» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения и информацию, составляющую коммерческую тайну.

На документах, содержащих служебную информацию ограниченного распространения, проставляется ограничительный гриф «Для служебного пользования». Порядок проставления ограничительного грифа «Для служебного пользования» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения, определяется Советом Министров Республики Беларусь. В случае ликвидации государственного органа, юридического лица решение о дальнейшем использовании служебной информации ограниченного распространения принимается ликвидационной комиссией.

В Законе «Об информации, информатизации и защите информации» указано, что право на информацию не может быть использовано для пропаганды войны или экстремистской деятельности, а также для совершения иных противоправных деяний.

Полный перечень **информации, запрещенной к распространению**, отсутствует в каком-либо правовом акте. Основными нормативно-правовыми актами в этой сфере являются Уголовный Кодекс Республики Беларусь, Закон «О противодействии

экстремизму», Закон «О борьбе с терроризмом», Закон «О недопущении реабилитации нацизма», Кодекс об административных правонарушениях.

В перечень информации, запрещенной к распространению относятся:

1. Пропаганда войны, под которой понимается распространение в любой форме взглядов, идей или призывов с целью вызвать агрессию одной страны против другой.
2. Информация, пропагандирующая экстремистскую деятельность или содержащая призывы к такой деятельности.
3. Экстремистские материалы.
4. Произведения, пропагандирующие культ насилия и жестокости.
5. Пропаганда или оправдание терроризма.
6. Информация, направленная на разжигание расовой, национальной, религиозной либо иной социальной вражды или розни.
7. Пропаганда исключительности, превосходства либо неполноценности граждан по признаку их социальной, расовой, национальной, религиозной или языковой принадлежности.
8. Пропаганда и публичное демонстрирование, изготовление и распространение нацистской символики или атрибутики.
9. Сведения, пропагандирующих потребление наркотических средств, психотропных веществ, их аналогов, токсических и других одурманивающих веществ, а также сведений о способах и методах разработки, изготовления, использования и местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов.
10. Порнографические материалы или предметы порнографического характера.
11. Порнографические материалы или предметы порнографического характера с изображением несовершеннолетнего.
12. Сведения о частной жизни лица, составляющие его личную или семейную тайну, полученные и распространяемые без его согласия.
13. Клевета, то есть заведомо ложные сведения, порочащие честь и достоинство другого лица или подрывающие его репутацию.
14. Клевета в отношении Президента Республики Беларусь (является уголовным преступлением в соответствии со ст. 367 Уголовного кодекса).

В средствах массовой информации, на Интернет-ресурсах запрещено распространение:

- 1) информации от имени организаций, не прошедших в установленном порядке государственную регистрацию (перерегистрацию) в случаях, когда такая процедура является обязательной в соответствии с законодательными актами, а также организаций, в отношении которых имеется вступившее в законную силу решение уполномоченного государственного органа об их ликвидации;
- 2) сведений, пропагандирующих потребление наркотических средств, психотропных веществ, их аналогов, токсических и других одурманивающих веществ, а также сведений о способах и методах разработки, изготовления, использования и местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов;
- 3) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилию, собственное имя, отчество (если имеется), фото- и видеоизображения этого несовершеннолетнего, его родителей или иных законных представителей, дату его рождения, аудиозапись его голоса, место его жительства, учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность этого несовершеннолетнего, без согласия его законного представителя;
- 4) информации о способах изготовления взрывных устройств и взрывчатых веществ, а также предметов, поражающее действие которых основано на использовании горючих веществ;
- 5) ненадлежащей рекламы;

б) информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к такой деятельности, порнографии, насилия и жестокости, в том числе пропагандирующей или побуждающей к самоубийству, другой информации, распространение которой способно нанести вред национальным интересам Республики Беларусь или запрещено законодательными актами;

7) результатов опросов общественного мнения, относящихся к общественно-политической ситуации в стране, республиканским референдумам, выборам Президента Республики Беларусь, депутатов Палаты представителей, членов Совета Республики Национального собрания Республики Беларусь, проведенных без получения аккредитации;

8) гиперссылки на информационные сообщения и (или) материалы, содержащие информацию, распространение которой в средствах массовой информации, на Интернет-ресурсах запрещено.

В радио-, теле-, видео-, кинохроникальных программах, на Интернет-ресурсах запрещается использование скрытых вставок, воздействующих на подсознание людей или оказывающих вредное влияние на их здоровье.

ТЕМА 4

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ОРГАНИЗАЦИИ И ДЕЯТЕЛЬНОСТИ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ

1. Понятие средств массовой информации.
2. Порядок учреждения и государственной регистрации (перерегистрации) средств массовой информации.
3. Распространение продукции средств массовой информации.
4. Порядок распространения рекламы в средствах массовой информации.
5. Отношения средств массовой информации с государственными органами, иными юридическими и физическими лицами.
6. Правовой статус журналиста.

1. Понятие средств массовой информации.

Государство рассматривает систему средств массовой информации как основу реализации конституционного права граждан на свободу слова, как важную составляющую часть национальной культуры и определяет меры, направленные на обеспечение экономической поддержки массовой информации.

Одним из способов реализации свободы мнений, убеждений и их свободного выражения является использование средств массовой информации.

Согласно ст. 1 Закона о СМИ **средство массовой информации** – форма периодического распространения массовой информации с использованием печати, вещания теле- или радиопрограммы, глобальной компьютерной сети Интернет, а также сетевое издание как форма распространения массовой информации с использованием глобальной компьютерной сети Интернет.

Иностранное средство массовой информации – средство массовой информации, созданное за пределами Республики Беларусь в соответствии с законодательством иностранного государства иностранным физическим лицом и (или) иностранной организацией, местом нахождения которой не является Республика Беларусь.

Массовая информация – предназначенные для неопределенного круга лиц печатные, аудио-, аудиовизуальные и другие информационные сообщения и (или) материалы, опубликованные в печати, сообщенные посредством вещания теле- или радиопрограммы, интернет-ресурса или в иной форме распространения.

Основными принципами деятельности СМИ являются:

достоверность информации – средства массовой информации должны распространять информацию, соответствующую действительности;

законность – информация не должна противоречить требованиям законодательства;

равенство – средства массовой информации исходят из равенства прав всех физических лиц, государственных органов, политических партий, других общественных объединений, иных юридических лиц на распространение и получение массовой информации;

уважение прав и свобод человека – средства массовой информации обеспечивают соблюдение прав и свобод человека, гарантированных Конституцией Республики Беларусь и иными актами законодательства;

многообразие мнений – средства массовой информации обеспечивают свободное выражение и распространение различных мнений и взглядов в обществе;

развитие национальной культуры – средства массовой информации содействуют распространению и популяризации национальных культурных ценностей;

защита нравственности – средства массовой информации не должны допускать распространения информации, посягающей на нормы общественной нравственности;

соблюдение норм профессиональной этики журналистов и общепринятых норм морали – журналисты средств массовой информации в своей деятельности должны неукоснительно соблюдать нормы профессиональной этики и общепринятые нормы морали.

Виды СМИ:

– газета;

– журнал;

– бюллетень;

– радио-, теле-, видео-, кинохроникальная программа – совокупность аудио-, аудиовизуальных сообщений и (или) материалов (передач), аудиовизуальных произведений, радио-, телепередач, имеющая постоянное название и носящая периодический характер;

– сетевое издание – интернет-ресурс, прошедший государственную регистрацию в порядке, установленном Законом о СМИ В свою очередь интернет-ресурс – интернет-сайт, страница интернет-сайта, форум, блог, приложение для мобильного устройства, иной информационный ресурс (его составная часть), размещенный в глобальной компьютерной сети Интернет, посредством которых распространяется массовая информация;

иная совокупность информационных сообщений и (или) материалов (передач), носящая периодический характер и предназначенная для неопределенного круга лиц.

К печатным СМИ относятся газета, журнал, бюллетень, другое издание, имеющие постоянное название, порядковый номер, сквозную нумерацию страниц и выходящие в свет не реже одного раза в шесть месяцев.

Радиовещательное СМИ – радиопрограмма, распространяемая с использованием сетей электросвязи не реже одного раза в шесть месяцев.

Телевизионное СМИ – телепрограмма, распространяемая с использованием сетей электросвязи не реже одного раза в шесть месяцев

2. Порядок учреждения и государственной регистрации (перерегистрации) средств массовой информации.

Порядок учреждения и государственной регистрации СМИ регламентирован главой 2 (статьи 10–16) Закона о СМИ.

В соответствии со ст. 10 Закона о СМИ учреждать СМИ могут физические лица, политические партии, другие общественные объединения, иные юридические лица, а также государственные органы в порядке и на условиях, определенных актами законодательства.

Не могут выступать в качестве учредителя средства массовой информации:

1) физическое лицо, не достигшее восемнадцатилетнего возраста, за исключением случаев, когда в соответствии с гражданским законодательством несовершеннолетний приобретает дееспособность в полном объеме до достижения восемнадцатилетнего возраста;

2) физическое лицо, отбывающее наказание по приговору суда или признанное решением суда недееспособным;

3) физическое лицо, юридическое лицо, ранее выступавшие в качестве учредителя средства массовой информации, выпуск которого прекращен по основаниям, предусмотренным пунктом 2 статьи 51 (однократное нарушение положений Закона о СМИ, устанавливающих порядок распространения продукции иностранными средствами массовой информации, официальных информационных сообщений и (или) материалов, продукции эротического характера, а также порядок осуществления вещания теле- или радиопрограммы; получение свидетельства о государственной регистрации средства массовой информации с нарушением законодательства путем внесения заведомо ложных сведений в документы, представленные для государственной регистрации средства массовой информации) Закона о СМИ, – в течение пяти лет со дня вступления в законную силу решения суда о прекращении выпуска средства массовой информации;

4) физическое лицо, лишенное в установленном порядке права заниматься деятельностью, связанной с производством и выпуском средства массовой информации;

5) физическое лицо, юридическое лицо, являющиеся владельцем интернет-ресурса, владельцем сетевого издания, в отношении которых принято решение об ограничении доступа, – в течение трех лет со дня принятия решения об ограничении доступа к соответствующему интернет-ресурсу;

6) физическое лицо, юридическое лицо, ранее выступавшие в качестве участника (собственника имущества) организации, признанной экстремистской, – в течение пяти лет со дня вступления в законную силу решения суда о ликвидации организации, признанной экстремистской;

7) иностранное юридическое лицо, а также иностранный гражданин и лицо без гражданства;

8) юридическое лицо, акциями, долей (долями) в уставном фонде которого в размере 20 и более процентов прямо или косвенно (через другие организации и (или) физических лиц) владеют каждый в отдельности или в совокупности иностранное государство, иностранное и (или) международное юридическое лицо (организация, не являющаяся юридическим лицом), иностранный гражданин, лицо без гражданства, за исключением случаев, когда учредителями такого юридического лица являются иностранные государства совместно с Республикой Беларусь.

При учреждении средства массовой информации двумя и более учредителями между ними должен быть заключен договор, содержащий их права, обязанности, ответственность, порядок, условия и последствия изменения состава учредителей, а также процедуру разрешения споров между ними.

В договоре о редакции средства массовой информации определяются имущественные, в том числе финансовые, отношения между учредителем (учредителями) средства массовой информации и юридическим лицом, на которое возложены функции редакции средства массовой информации, включая порядок выделения и использования средств на содержание юридического лица, на которое возложены функции редакции средства массовой информации, распределения прибыли, их обязанности.

Средства массовой информации подлежат государственной регистрации в республиканском органе государственного управления в сфере массовой информации (Министерство информации Республики Беларусь).

При государственной регистрации средства массовой информации в республиканский орган государственного управления в сфере массовой информации

учредителем (учредителями) либо уполномоченным им (ими) лицом подается заявление по форме, установленной республиканским органом государственного управления в сфере массовой информации, с указанием следующих сведений: учредитель (учредители) СМИ (включая сведения о том, является ли он учредителем, главным редактором или журналистом других СМИ (для учредителя СМИ – физического лица), распространителем продукции СМИ); название и вид СМИ; язык СМИ; юридическое лицо, на которое возложены функции редакции СМИ; адрес юридического лица, на которое возложены функции редакции СМИ; предполагаемая территория распространения СМИ (за исключением сетевого издания); специализация (тематика) СМИ; источники финансирования СМИ; периодичность СМИ (за исключением сетевого издания); предполагаемый тираж СМИ (для печатного СМИ); главный редактор СМИ; владелец сетевого издания; доменное имя сетевого издания; объем телепередач, аудиовизуальных произведений, иных сообщений и (или) материалов белорусского (национального) производства в ежемесячном объеме вещания телевизионных СМИ (для телевизионного СМИ).

К заявлению прилагаются следующие документы:

1) копия устава (учредительного договора – для коммерческой организации, действующей только на основании учредительного договора) со штампом, свидетельствующим о проведении государственной регистрации (для учредителя СМИ – юридического лица Республики Беларусь);

2) копия документа, удостоверяющего личность физического лица (для учредителя СМИ – физического лица);

3) копия устава (учредительного договора – для коммерческой организации, действующей только на основании учредительного договора) со штампом, свидетельствующим о проведении государственной регистрации (для юридического лица, на которое возложены функции редакции СМИ, не являющегося учредителем СМИ);

4) копия решения о редакции СМИ либо договора о редакции СМИ;

5) документ, подтверждающий уплату государственной пошлины за государственную регистрацию СМИ;

6) развернутая концепция вещания теле- или радиопрограммы по форме, установленной республиканским органом государственного управления в сфере массовой информации.

Решение о государственной регистрации средства массовой информации и его включении в Государственный реестр средств массовой информации принимается республиканским органом государственного управления в сфере массовой информации в **двухмесячный срок** со дня получения заявления и документов. Республиканский орган государственного управления в сфере массовой информации в пределах указанного срока, принимает решение о государственной регистрации СМИ либо об отказе в государственной регистрации СМИ.

Средство массовой информации считается зарегистрированным и вправе осуществлять свою деятельность со дня включения его в Государственный реестр средств массовой информации, ведение которого осуществляется республиканским органом государственного управления в сфере массовой информации, за исключением телевизионных и радиовещательных средств массовой информации, которые имеют право осуществлять свою деятельность со дня получения специального разрешения (лицензии) на осуществление деятельности в области вещания. Деятельность СМИ, не прошедшего государственную регистрацию, за исключением случаев, когда его государственная регистрация не требуется, запрещена.

После включения СМИ в Государственный реестр средств массовой информации его учредителю (учредителям) выдается свидетельство о государственной регистрации средства массовой информации.

Не требуется государственной регистрации:

- СМИ, специально учрежденных государственными органами и иными государственными организациями только для распространения их официальных заявлений, а также для официального опубликования правовых актов;
- радио- и телепрограмм, распространяемых по сетям, ограниченными помещениями и территорией одной организации или имеющим не более десяти абонентов;
- аудио- и видеопрограмм, распространяемых в записи тиражом не более десяти экземпляров;
- печатных средств массовой информации, выходящих в свет тиражом, не превышающим 299 экземпляров.

Интернет-ресурс, посредством которого распространяется массовая информация, может быть зарегистрирован как сетевое издание в порядке, установленном Законом о СМИ. Интернет-ресурс, не зарегистрированный в качестве сетевого издания, средством массовой информации не является.

Иностранские СМИ, распространяющие на территории Республики Беларусь свою продукцию с изменением ее формы или содержания, подлежат государственной регистрации в республиканском органе государственного управления в сфере массовой информации в порядке, установленном Законом о СМИ.

3. Распространение продукции средств массовой информации.

Распространение продукции средства массовой информации – продажа, подписка, доставка печатного средства массовой информации, аудио- либо видеозаписей программ, трансляция и ретрансляция радио-, телепрограмм, демонстрация кинохроникальных программ, иная форма доведения массовой информации до всеобщего сведения, в том числе посредством интернет-ресурса, сетевого издания.

Распространитель продукции средства массовой информации – юридическое лицо, индивидуальный предприниматель, осуществляющие распространение продукции средства массовой информации в порядке, установленном законодательством, а также юридическое или физическое лицо, в том числе индивидуальный предприниматель, являющееся владельцем интернет-ресурса, владельцем сетевого издания, в случае распространения продукции средства массовой информации посредством интернет-ресурса, сетевого издания.

Распространение продукции СМИ регулируется главой 3 Закона о СМИ.

Распространение продукции средства массовой информации осуществляется в соответствии с законодательством:

- юридическим лицом, на которое возложены функции редакции СМИ, либо на основании договора, заключенного юридическим лицом, на которое возложены функции редакции СМИ, иным правообладателем продукции средства массовой информации в установленном порядке с распространителем продукции СМИ;
- владельцем интернет-ресурса, владельцем сетевого издания в случае распространения продукции средства массовой информации посредством интернет-ресурса, сетевого издания.

Если СМИ, информационное агентство, интернет-ресурс распространяют информационные сообщения и (или) материалы, ранее распространенные другими СМИ, информационным агентством, интернет-ресурсом, то при этом должна быть сделана ссылка на средство массовой информации, информационное агентство, интернет-ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе.

Распространение информационных сообщений и (или) материалов в глобальной компьютерной сети Интернет, ранее распространенных другими средством массовой информации, информационным агентством, интернет-ресурсом в глобальной компьютерной сети Интернет, осуществляется при наличии гиперссылки на средство

массовой информации, информационное агентство, интернет-ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе.

Продукция иностранного средства массовой информации, распространяемая на территории Республики Беларусь без изменения формы или содержания, может быть распространена в Республике Беларусь после получения иностранным средством массовой информации разрешения на распространение продукции иностранного средства массовой информации на территории Республики Беларусь без изменения формы или содержания в республиканском органе государственного управления в сфере массовой информации.

До начала распространения продукции средства массовой информации юридическое лицо, на которое возложены функции редакции средства массовой информации, обязано в порядке и в соответствии с критериями, установленными Советом Министров Республики Беларусь, присвоить продукции средства массовой информации знак возрастной категории, за исключением случаев, когда наличие такого знака является необязательным, в частности без знака возрастной категории распространяются:

- теле- и радиопередачи, транслируемые в прямом эфире;
- теле- и радиопередачи информационно-аналитического, информационного, культурно-просветительного, спортивного и духовно-просветительного характера;
- иностранные теле- и радиoproграммы, распространяемые на территории Республики Беларусь без изменения формы или содержания;
- печатные средства массовой информации, специализирующиеся на распространении информации общеполитического, научного, производственно-практического, нормативного производственно-практического, массово-политического, официального, духовно-просветительного, справочного, культурно-просветительного, реферативного и статистического характера;
- информационные сообщения и (или) материалы, распространяемые через глобальную компьютерную сеть Интернет (кроме сетевых изданий).

Распространители продукции печатных средств массовой информации, а также продукции телевизионных, радиовещательных средств массовой информации подлежат включению в Государственный реестр распространителей продукции печатных средств массовой информации и Государственный реестр распространителей продукции телевизионных и радиовещательных средств массовой информации соответственно.

Деятельность по распространению продукции печатных средств массовой информации, а также продукции телевизионных и радиовещательных средств массовой информации без включения в соответствующий Государственный реестр является незаконной и влечет ответственность в соответствии с законодательными актами.

Указанные правила не применяются к распространителям – юридическим лицам, на которые возложены функции редакций средств массовой информации, при распространении выпускаемых ими средств массовой информации.

Включение распространителей в соответствующий Государственный реестр осуществляется республиканским органом государственного управления в сфере массовой информации не позднее пятнадцати рабочих дней со дня подачи ими заявления с приложением документов, перечень, порядок подачи и рассмотрения которых определяются республиканским органом государственного управления в сфере массовой информации.

Распространители продукции телевизионных, радиовещательных средств массовой информации до начала (прекращения) распространения радио-, телепрограммы уведомляют республиканский орган государственного управления в сфере массовой информации о начале (прекращении) распространения радио-, телепрограммы.

Распространение продукции печатного средства массовой информации считается коммерческим, если за нее взимается плата.

Юридическое лицо, на которое возложены функции редакции средства массовой информации, владелец интернет-ресурса обязаны распространить бесплатно и в определенный срок:

– вступившее в законную силу решение суда, в котором содержится требование о сообщении для всеобщего сведения такого решения через данное средство массовой информации, интернет-ресурс;

– поступившие из государственных органов информационные сообщения и (или) материалы, касающиеся деятельности юридического лица, на которое возложены функции редакции данного средства массовой информации, владельца данного интернет-ресурса.

Учредитель (учредители) средства массовой информации вправе обязать юридическое лицо, на которое возложены функции редакции средства массовой информации, поместить в средстве массовой информации бесплатно и в определенный им (ими) срок официальное информационное сообщение и (или) материал от его (их) имени (заявление учредителя (учредителей)). Максимальный объем заявления учредителя (учредителей) определяется в решении о редакции средства массовой информации либо договоре о редакции средства массовой информации.

Юридическое лицо, на которое возложены функции редакции средства массовой информации, обязано сохранять оригиналы распространенных им информационных сообщений и (или) материалов в течение шести месяцев после их распространения.

Юридическое лицо, на которое возложены функции редакции телевизионного или радиовещательного средства массовой информации, обязано сохранять в записи не менее шести месяцев со дня выпуска информационные сообщения и (или) материалы собственных радио-, телепередач.

4. Порядок распространения рекламы в средствах массовой информации.

Порядок распространения рекламы в СМИ определен ст. 11 Закона о рекламе.

Реклама в средствах массовой информации, не зарегистрированных в качестве специализированных для размещения (распространения) рекламы, не должна превышать:

– 25 % объема одного номера государственных периодических печатных изданий;

– 30 % объема одного номера иных периодических печатных изданий;

– 20 % объема вещания для радио- и телепрограмм в течение суток. При этом в период с 18.00 до 22.00 реклама не должна превышать 16 минут в течение каждого часа.

При трансляции радио- и телепрограмм не допускаются прерывание рекламой или совмещение с рекламой, включая рекламу в виде наложений, в том числе способом «бегущей строки»:

– выступлений Президента Республики Беларусь, Премьер-министра Республики Беларусь, Председателя Совета Республики Национального собрания Республики Беларусь, Председателя Палаты представителей Национального собрания Республики Беларусь, трансляций сессий Палаты представителей и Совета Республики Национального собрания Республики Беларусь, государственных мероприятий, траурных и других официальных церемоний;

– религиозных передач;

– передач продолжительностью менее 15 минут;

– передач, в том числе радиопостановок и художественных фильмов, без согласия правообладателей.

Детские передачи, включая детские художественные фильмы, и образовательные передачи продолжительностью:

– от 15 до 30 минут включительно могут прерываться рекламой непосредственно в начале и перед окончанием передачи на периоды, не превышающие 60 секунд;

– более 30 минут могут прерываться рекламой непосредственно в начале и перед окончанием передачи на периоды, не превышающие 60 секунд, а также дополнительно один раз каждые 30 минут передачи на период, не превышающий 60 секунд.

В остальное время размещение (распространение) рекламы в таких передачах не допускается.

Объект рекламирования и содержание рекламы в детских передачах, включая детские художественные фильмы, должны соответствовать особенностям детской и подростковой зрительской аудитории. В таких передачах запрещается размещение (распространение) рекламы лекарственных препаратов, методов оказания медицинской помощи, работ и (или) услуг, составляющих медицинскую деятельность, изделий медицинского назначения, медицинской техники, биологически активных добавок к пище, лотерей, рекламных игр, иных рекламных мероприятий, услуг, связанных с привлечением, использованием денежных средств граждан.

Трансляция в прямом эфире или в записи спортивного соревнования может прерываться рекламой только в перерывах в ходе спортивных соревнований или во время их остановок. Трансляция в прямом эфире или в записи спортивного соревнования, в котором не предусмотрены перерывы или остановки, может прерываться рекламой таким образом, чтобы прерывание трансляции не привело к потере части существенной информации о спортивном соревновании.

Продолжительность каждого прерывания передачи рекламой, в том числе художественного фильма, не должна превышать шести минут, за исключением периода с 18.00 до 22.00. Допускается прерывание передач рекламой, в том числе художественных фильмов, не более четырех раз в течение часа эфирного времени.

Реклама в виде наложений, в том числе способом «бегущей строки», должна размещаться по краям или в углу кадра и не должна:

- превышать семи процентов площади кадра;
- накладываться на субтитры, а также надписи разъясняющего характера.

Размещение (распространение) рекламы эротической продукции, продукции, содержащей элементы эротики, а также услуг, связанных с распространением такой продукции, на телевидении и радио допускается с 24.00 до 4.00.

Реклама пива и слабоалкогольных напитков, производимых за пределами Республики Беларусь, разрешенного к обороту на территории Республики Беларусь гражданского оружия более чем два раза в течение каждого прерывания передачи рекламой не допускается.

Ограничения, установленные ст. 11 Закона о рекламе, не распространяются на рекламу, размещаемую (распространяемую) в месте события, транслируемого в прямом эфире или в записи, за исключением специально созданных для трансляции постановок.

5. Отношения средств массовой информации с государственными органами, иными юридическими и физическими лицами.

Правовой статус субъектов информационных отношений в сфере массовой информации определен в главе 6 Закона о СМИ.

Республиканским органом государственного управления в сфере массовой информации является Министерство информации, которое в пределах своей компетенции:

- проводит государственную политику в сфере массовой информации;
- осуществляет регулирование, управление и координацию деятельности других республиканских органов государственного управления в сфере массовой информации;
- осуществляет государственную регистрацию средств массовой информации;
- осуществляет мониторинг массовой информации;
- выполняет иные функции, определенные Законом о СМИ, иными актами законодательства.

Республиканским органом государственного управления в сфере массовой информации создается общественный координационный совет в сфере массовой информации, состоящий из представителей государственных органов, общественных объединений, средств массовой информации, других организаций и иных лиц.

Общественный координационный совет в сфере массовой информации является общественным консультационным и координационным органом и создается в целях реализации и защиты конституционных прав граждан на свободу получения и распространения информации.

Основными задачами общественного совета являются:

- координация взаимодействия органов государственного управления, общественных объединений и иных организаций, осуществляющих свою деятельность в сфере массовой информации;
- обеспечение правильного применения норм Закона о СМИ и иного законодательства в сфере массовой информации;
- рассмотрение спорных вопросов, возникающих при применении Закона о СМИ и иного законодательства в сфере массовой информации.

В соответствии с возложенными на него задачами общественный совет имеет право:

- давать оценку о наличии (отсутствии) в продукции вышедших в свет средств массовой информации нарушений требований Закона о СМИ;
- давать разъяснения по вопросам, возникающим в процессе выпуска средств массовой информации;
- вносить предложения в Министерство информации о совершенствовании законодательства о средствах массовой информации;
- запрашивать у государственных органов, общественных объединений, иных организаций необходимые документы, касающиеся выносимых на рассмотрение общественного совета вопросов;
- приглашать на заседания общественного совета руководителей юридических лиц, на которые возложены функции редакции средства массовой информации, учредителей средств массовой информации, журналистов средств массовой информации и заслушивать их сообщения по вопросам, входящим в компетенцию этого совета.

Заседания общественного совета проводятся по мере необходимости, но не реже одного раза в квартал. Ведет заседания председатель общественного совета или по его поручению один из членов этого совета. Заседания общественного совета считаются правомочными, если на нем присутствует не менее половины его членов. Решения принимаются путем открытого голосования большинством голосов и носят рекомендательный характер. В случае равенства голосов решающим является голос председательствующего.

Учредитель (учредители) средства массовой информации – физическое или юридическое лицо, государственный орган, самостоятельно либо совместно с другими физическими или юридическими лицами принявшие решение о создании средства массовой информации и обратившиеся за его государственной регистрацией.

Учредитель (учредители) средства массовой информации вправе:

- выступать в качестве юридического лица, на которое возложены функции редакции средства массовой информации (если учредителем средства массовой информации является юридическое лицо), распространителя продукции средства массовой информации;
- передавать свои права и обязанности третьему лицу, в том числе другому учредителю (учредителям) средства массовой информации, на основании договора в соответствии с законодательством;
- в случаях, предусмотренных в решении о редакции средства массовой информации либо в договоре о редакции средства массовой информации, прекратить выпуск средства массовой информации. Решение учредителя (учредителей) о прекращении выпуска

средства массовой информации в трехдневный срок со дня его принятия направляется в республиканский орган государственного управления в сфере массовой информации;

– осуществлять иные права в соответствии с Законом о СМИ.

Учредитель (учредители) средства массовой информации не имеет права вмешиваться в деятельность средства массовой информации, за исключением случаев, предусмотренных Законом о СМИ, решением о редакции средства массовой информации либо договором о редакции средства массовой информации.

Учредитель (учредители) СМИ несет ответственность за выполнение требований, заявленных им при учреждении и государственной регистрации средства массовой информации, установленных Законом о СМИ и другими актами законодательства, а также за содержание информации, распространяемой учрежденным им средством массовой информации.

Юридическое лицо, на которое возложены функции редакции средства массовой информации, – юридическое лицо Республики Беларусь, осуществляющее производство и выпуск средства массовой информации на основании решения учредителя (учредителей) средства массовой информации либо, если указанное юридическое лицо не является учредителем средства массовой информации или является одним из соучредителей, на основании договора этого юридического лица с учредителем (учредителями) средства массовой информации.

Юридическое лицо, на которое возложены функции редакции средства массовой информации, осуществляет производство и выпуск средства массовой информации на основе Закона о СМИ, иных актов законодательства, решения о редакции средства массовой информации либо договора о редакции средства массовой информации.

Юридическое лицо, на которое возложены функции редакции средства массовой информации, обязано:

– соблюдать основные принципы деятельности средств массовой информации;

– не допускать распространение информации, распространение которой запрещено Законом о СМИ и иными законодательными актами, а также материалов, содержащих нецензурные слова и выражения;

– не допускать распространение недостоверной информации, которая может причинить вред государственным или общественным интересам;

– не допускать распространение сведений, не соответствующих действительности и порочащих честь, достоинство или деловую репутацию физических лиц либо деловую репутацию юридических лиц;

– не допускать использование средства массовой информации для осуществления запрещенной в соответствии с законодательными актами деятельности;

– распространять информационные сообщения и (или) материалы, ранее распространенные в глобальной компьютерной сети Интернет другими средством массовой информации, информационным агентством, интернет-ресурсом, при наличии гиперссылки на средство массовой информации, информационное агентство, интернет-ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе;

– распространять информационные сообщения и (или) материалы, ранее распространенные другими средством массовой информации, информационным агентством, интернет-ресурсом, при наличии ссылки на средство массовой информации, информационное агентство, интернет-ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе;

– выполнять иные требования законодательства в сфере массовой информации.

Интернет-ресурс – интернет-сайт, страница интернет-сайта, форум, блог, приложение для мобильного устройства, иной информационный ресурс (его составная часть), размещенный в глобальной компьютерной сети Интернет, посредством которых распространяется массовая информация.

Владелец интернет-ресурса – юридическое или физическое лицо, в том числе индивидуальный предприниматель, реализующее права владения, пользования и (или) распоряжения интернет-ресурсом.

Сетевое издание – интернет-ресурс, прошедший государственную регистрацию в порядке, установленном Законом о СМИ.

Владелец сетевого издания – владелец интернет-ресурса, прошедшего государственную регистрацию в порядке, установленном Законом о СМИ.

Владелец интернет-ресурса, владелец сетевого издания имеют право:

- собирать, получать, передавать и распространять информацию любым способом в соответствии с законодательством;

- излагать на интернет-ресурсе, в сетевом издании личные суждения и оценки с указанием собственного имени или псевдонима;

- при проведении предварительной идентификации пользователя собирать, обрабатывать, хранить и предоставлять с соблюдением требований, определенных законодательными актами, следующие персональные данные такого лица: фамилию, собственное имя, отчество (если имеется), пол, число, месяц, год рождения, место рождения, а также номер мобильного телефона и (или) адрес электронной почты;

- совершать иные действия в соответствии с законодательством.

Владелец интернет-ресурса, владелец сетевого издания обязаны:

- анализировать содержание интернет-ресурса, сетевого издания;

- соблюдать основные принципы деятельности средств массовой информации;

- не допускать распространение посредством интернет-ресурса, сетевого издания информации, распространение которой запрещено Законом о СМИ и иными законодательными актами, а также материалов, содержащих нецензурные слова и выражения;

- не допускать распространение посредством интернет-ресурса, сетевого издания недостоверной информации, которая может причинить вред государственным или общественным интересам;

- соблюдать требования законодательства, регулирующие порядок распространения продукции средств массовой информации;

- не допускать распространение на интернет-ресурсе, в сетевом издании сведений, не соответствующих действительности и порочащих честь, достоинство или деловую репутацию физических лиц либо деловую репутацию юридических лиц;

- незамедлительно удалять по требованию республиканского органа государственного управления в сфере массовой информации информацию, размещенную на интернет-ресурсе, не зарегистрированном в качестве сетевого издания, содержание которой противоречит требованиям Закона о СМИ;

- хранить массовую информацию, распространенную посредством сетевого издания, а также сведения об источнике ее получения, о сроках ее распространения в течение шести месяцев;

- не допускать размещение на интернет-ресурсе, в сетевом издании информационных сообщений и (или) материалов (в том числе комментирование) другими пользователями без их предварительной идентификации, порядок которой устанавливается Советом Министров Республики Беларусь;

- распространять информационные сообщения и (или) материалы, ранее распространенные в глобальной компьютерной сети Интернет другими средствами массовой информации, информационным агентством, интернет-ресурсом, при наличии гиперссылки на средство массовой информации, информационное агентство, интернет-

ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе;

- распространять информационные сообщения и (или) материалы, ранее распространенные другими средством массовой информации, информационным агентством, интернет-ресурсом, при наличии ссылки на средство массовой информации, информационное агентство, интернет-ресурс, ранее распространившие эти информационные сообщения и (или) материалы, если правообладателем таких сообщений и (или) материалов не определены иные условия их распространения, размещенные в открытом доступе;

- не допускать использование интернет-ресурса, сетевого издания для осуществления запрещенной в соответствии с законодательными актами деятельности;

- выполнять иные требования законодательства в сфере массовой информации.

Владелец сетевого издания обязан разместить в сетевом издании:

- наименование юридического лица, на которое возложены функции редакции сетевого издания, его юридический адрес, адрес электронной почты и номера телефонов;

- сведения о главном редакторе (фамилия, собственное имя, отчество (если имеется), номер служебного телефона);

- знак возрастной категории, присвоенный в порядке и в соответствии с критериями, установленными Советом Министров Республики Беларусь.

Владелец интернет-ресурса обязан разместить на интернет-ресурсе адрес своей электронной почты.

Республиканский орган государственного управления в сфере массовой информации вправе запрашивать:

- у государственного органа (организации), поставщика интернет-услуг и иных лиц, обеспечивающих размещение интернет-ресурса, сведения, позволяющие идентифицировать владельца интернет-ресурса, владельца сетевого издания;

- у владельца интернет-ресурса, владельца сетевого издания, поставщика интернет-услуг и иных лиц, обеспечивающих размещение интернет-ресурса, сведения, необходимые для анализа информации, размещенной на интернет-ресурсе, в сетевом издании, в целях оценки ее соответствия законодательству.

Запрашиваемая информация предоставляется в течение пяти рабочих дней со дня получения запроса.

В случае неисполнения владельцем интернет-ресурса (его составной части) обязанностей, установленных Законом о СМИ, республиканский орган государственного управления в сфере массовой информации направляет владельцу данного интернет-ресурса (его составной части) требование об устранении (недопущении) нарушений.

В случае невозможности установления владельца составной части интернет-ресурса требование об устранении (недопущении) нарушений направляется владельцу интернет-ресурса.

Требование об устранении (недопущении) нарушений не позднее трех рабочих дней после его вынесения направляется по почте и (или) электронной почте владельцу интернет-ресурса (его составной части) с указанием допущенных нарушений и срока их устранения.

Владелец интернет-ресурса (его составной части) обязан письменно сообщить в республиканский орган государственного управления в сфере массовой информации об устранении нарушений, послуживших основанием для направления требования, и представить подтверждающие документы не позднее трех рабочих дней по истечении срока устранения нарушений, установленного в требовании.

Главным редактором средства массовой информации может быть руководитель юридического лица, на которое возложены функции редакции средства массовой информации, либо уполномоченное им лицо, осуществляющие свою профессиональную

деятельность в соответствии с Конституцией Республики Беларусь, Законом о СМИ и иными актами законодательства. Главный редактор средства массовой информации принимает окончательное решение в отношении производства и выпуска средства массовой информации.

Информационное агентство – юридическое лицо, осуществляющее сбор, создание (подготовку), хранение информационных сообщений и (или) материалов и их распространение в средствах массовой информации и имеющее одновременно статус юридического лица, на которое возложены функции редакции средства массовой информации, и распространителя продукции средства массовой информации.

Корреспондентский пункт – обособленное подразделение юридического лица, на которое возложены функции редакции средства массовой информации и которое осуществляет сбор, хранение и создание (подготовку) информационных сообщений и (или) материалов для данного средства массовой информации, а также распространение его продукции. Открытие корреспондентского пункта регулируется Постановлением Совета Министров Республики Беларусь от 25 декабря 2008 г. № 2015 «О некоторых вопросах регулирования деятельности средств массовой информации».

6. Правовой статус журналиста.

Журналист средства массовой информации – физическое лицо, занимающееся сбором, редактированием и созданием (подготовкой) информационных сообщений и (или) материалов для юридического лица, на которое возложены функции редакции средства массовой информации, связанное с этим юридическим лицом трудовыми либо другими договорными отношениями.

В связи с осуществлением профессиональных обязанностей журналист средства массовой информации имеет право:

- собирать, запрашивать и получать информацию из государственных органов, от политических партий, других общественных объединений, иных юридических лиц, а также хранить и распространять информацию, необходимую для осуществления его профессиональной деятельности;

- присутствовать в порядке, определенном законодательством, в районах вооруженных конфликтов или чрезвычайных ситуаций, на массовых мероприятиях, в местах других общественно важных событий и передавать оттуда информацию;

- производить при наличии аккредитации или по согласованию с физическими или юридическими лицами в отношении этих лиц записи, в том числе с использованием средств аудиовизуальной техники, кино- и фотосъемок, если иное не предусмотрено законодательством;

- обращаться к специалистам при проверке фактов и обстоятельств в связи с поступившими информационными сообщениями и (или) материалами;

- высказывать свое личное мнение по информационным сообщениям и (или) материалам, предназначенным для распространения, за своей подписью;

- распространять подготовленные им информационные сообщения и (или) материалы за своей подписью, под псевдонимом либо без подписи, оговаривать в случае необходимости сохранение тайны авторства.

Журналист средства массовой информации имеет также иные права в соответствии с законодательством.

Журналист средства массовой информации **обязан**:

- уважать права, свободы и законные интересы физических лиц, права и законные интересы юридических лиц;

- проверять достоверность полученных им сведений;

- предоставлять для распространения достоверную информацию;

- указывать по желанию лиц, предоставляющих информацию, их авторство;

– сохранять конфиденциальность информации и источники ее получения, за исключением случаев, предусмотренных Законом о СМИ;

– получать согласие на распространение в средстве массовой информации сведений о личной жизни физического лица от самого физического лица либо его законного представителя, за исключением случаев, установленных законодательными актами;

– получать согласие физических лиц на проведение аудио- и видеозаписи, кино- и фотосъемок, за исключением их проведения в местах, открытых для массового посещения, на массовых мероприятиях, а также случая, предусмотренного статьей 40 Закона о СМИ (распространение в средствах массовой информации информационных сообщений и (или) материалов, подготовленных с использованием аудио- и видеозаписи, кино- и фотосъемки физического лица без его согласия, допускается только при принятии мер против возможной идентификации данного лица посторонними лицами, а также при условии, что распространение этих информационных сообщений и (или) материалов не нарушает конституционных прав и свобод личности и необходимо для защиты общественных интересов, за исключением случаев распространения таких информационных сообщений и (или) материалов по требованию органа уголовного преследования, суда в связи с производством предварительного расследования, судебным разбирательством.);

– отказаться от данного ему учредителем (учредителями), главным редактором средства массовой информации задания, если это задание либо его выполнение связаны с нарушением законодательства;

– при осуществлении профессиональной деятельности предъявлять по требованию служебное удостоверение;

– соблюдать ограничения при проведении предвыборной агитации, агитации по референдуму, отзыву депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, установленные избирательным законодательством;

– не допускать нарушение норм профессиональной этики журналистов;

– выполнять иные требования и обязанности, установленные законодательными актами для журналистов средств массовой информации.

Журналист средства массовой информации исполняет также иные обязанности в соответствии с законодательством.

Не допускается использование установленных Законом о СМИ прав журналиста средства массовой информации в целях:

– фальсификации информации, умышленного распространения недостоверной информации под видом достоверных сообщений, сбора информации в пользу третьего лица, в том числе юридического лица, не являющегося редакцией средства массовой информации;

– опорочить посредством распространения недостоверной информации гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и (или) работы, в связи с их политическими убеждениями, а также деловую репутацию юридического лица.

Журналисты средств массовой информации имеют право на аккредитацию при государственных органах, политических партиях, других общественных объединениях, иных юридических лицах для освещения организуемых ими заседаний, совещаний и других мероприятий в порядке, установленном этими государственными органами, политическими партиями, другими общественными объединениями, иными юридическими лицами.

Не допускается необоснованный отказ в аккредитации журналистов средств массовой информации.

Журналист средства массовой информации может быть лишен аккредитации в случае, если им:

- нарушены требования и (или) не исполнены обязанности, установленные статьей 34 и пунктом 2 статьи 52 (субъекты правоотношений в сфере массовой информации, перед распространением сведений, которые могут дискредитировать Республику Беларусь, а также порочить честь, достоинство или деловую репутацию физических лиц либо деловую репутацию юридических лиц, полученных от политических партий, других общественных объединений, иных юридических лиц, а также содержатся в официальных информационных сообщениях и (или) материалах пресс-служб политических партий, других общественных объединений и иных юридических лиц, обязаны проверить достоверность указанных сведений и предоставить возможность распространения одновременного комментария физических и (или) юридических лиц, в том числе государственных органов и иных государственных организаций (их пресс-служб), в отношении которых могут быть распространены данные сведения либо в компетенцию которых входит подготовка разъяснений в отношении распространяемой информации) Закона о СМИ;
- совершено умышленное противоправное деяние при осуществлении профессиональной деятельности;
- нарушен установленный порядок аккредитации.

ТЕМА 5

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ И В ОБЛАСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

- 1. Государственное регулирование и управление в сфере государственных секретов.**
- 2. Субъекты информационных правоотношений в сфере государственных секретов.**
- 3. Отнесение сведений к государственным секретам. Категории государственных секретов.**
- 4. Степени секретности. Грифы секретности. Засекречивание. Рассекречивание.**
- 5. Защита государственных секретов. Допуск и доступ к государственным секретам.**
- 6. Надзор, контроль и ответственность в сфере государственных секретов.**
- 7. Режим коммерческой тайны. Права владельца коммерческой тайны. Доступ к коммерческой тайне.**
- 8. Правовые средства охраны коммерческой тайны в отношениях с контрагентами и работниками. Ответственность за нарушение законодательства о коммерческой тайне.**

1. Государственное регулирование и управление в сфере государственных секретов.

Правовой режим государственных секретов определяется Законом Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах».

В соответствии со ст. 1 Закона о государственных секретах **государственные секреты** (сведения, составляющие государственные секреты) – сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с настоящим Законом и другими актами законодательства.

Для государственных секретов установлен особый правовой режим, суть которого заключается в жестком ограничении доступа к такой информации, защите ее от несанкционированного использования и четком определении круга лиц, которым предоставляется доступ к такой информации.

Государственное регулирование и управление в сфере государственных секретов осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, а также Межведомственной комиссией по защите государственных секретов при Совете Безопасности Республики Беларусь, уполномоченным государственным органом по защите государственных секретов, органами государственной безопасности, Оперативно-аналитическим центром при Президенте Республики Беларусь.

Президент Республики Беларусь в сфере государственных секретов:

- определяет государственную политику;
- утверждает государственные программы;
- утверждает Положение о Межведомственной комиссии по защите государственных секретов при Совете Безопасности Республики Беларусь и ее состав;
- создает, реорганизует и упраздняет уполномоченный государственный орган по защите государственных секретов;
- утверждает перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечень сведений, подлежащих отнесению к государственным секретам;
- ведет переговоры и подписывает межгосударственные договоры Республики Беларусь о защите государственных секретов;
- принимает решения о передаче государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, если иное не установлено настоящим Законом;
- устанавливает порядок предоставления допуска к государственным секретам иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь;
- осуществляет иные полномочия в соответствии с Законом о государственных секретах и другими законодательными актами.

Совет Министров Республики Беларусь в сфере государственных секретов:

- организует разработку проектов государственных программ, перечня государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечня сведений, подлежащих отнесению к государственным секретам, и представляет их на утверждение Президенту Республики Беларусь, принимает меры по выполнению государственных программ;
- организует разработку проектов актов законодательства, международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства;
- заключает межправительственные договоры Республики Беларусь о защите государственных секретов, принимает меры по реализации международных договоров Республики Беларусь о защите государственных секретов;
- утверждает положение об экспертных комиссиях в сфере государственных секретов, перечень особо режимных и режимных объектов, положение об особо режимных и режимных объектах, порядок создания и деятельности подразделений по защите государственных секретов;
- принимает решения о создании межведомственных экспертных комиссий в сфере государственных секретов;
- устанавливает порядок определения тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате разглашения или утраты государственных секретов;

- устанавливает порядок предоставления гражданам допуска к государственным секретам, если иное не установлено Законом о государственных секретах;
- устанавливает с учетом положений Закона о государственных секретах порядок осуществления гражданами доступа к государственным секретам;
- устанавливает с учетом положений о государственных секретах порядок отнесения сведений к государственным секретам, засекречивания, рассекречивания, а также защиты государственных секретов, за исключением технической защиты государственных секретов;
- устанавливает с учетом положений Закона о государственных секретах порядок передачи государственных секретов государственным органам и иным организациям;
- устанавливает с учетом положений Закона о государственных секретах порядок передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;
- устанавливает размеры компенсационных выплат гражданам на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне, надбавок работникам на период доступа к государственным секретам в зависимости от степени секретности и работникам подразделений по защите государственных секретов за работу в этих подразделениях, а также порядок их выплат;
- определяет порядок материально-технического и финансового обеспечения деятельности в сфере государственных секретов;
- осуществляет иные полномочия в соответствии с Законом о государственных секретах и другими законодательными актами.

Межведомственная комиссия по защите государственных секретов при Совете Безопасности Республики Беларусь в сфере государственных секретов:

- координирует деятельность государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;
- осуществляет подготовку предложений Президенту Республики Беларусь и Совету Безопасности Республики Беларусь о формировании государственной политики и совершенствовании защиты государственных секретов;
- рассматривает проекты государственных программ, актов законодательства, международных договоров Республики Беларусь о защите государственных секретов;
- осуществляет иные полномочия в соответствии с законодательными актами.

Уполномоченный государственный орган по защите государственных секретов (Комитет государственной безопасности) в сфере государственных секретов:

- координирует деятельность государственных органов и иных организаций по защите государственных секретов;
- разрабатывает предложения о формировании государственной политики и совершенствовании защиты государственных секретов;
- осуществляет государственный контроль;
- разрабатывает проекты государственных программ, актов законодательства, международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства;
- проводит проверочные мероприятия в государственных органах и иных организациях в связи с предоставлением им допуска к государственным секретам;
- устанавливает порядок выдачи разрешений на осуществление деятельности с использованием государственных секретов, выдает, приостанавливает, возобновляет и аннулирует разрешения на осуществление деятельности с использованием государственных секретов государственным органам и иным организациям, за исключением государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;

- согласовывает перечни сведений, подлежащих засекречиванию, номенклатуры должностей работников, подлежащих допуску к государственным секретам;

- согласовывает предоставление гражданам допуска к государственным секретам, а также осуществление доступа к государственным секретам граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований;

- создает экспертные комиссии в сфере государственных секретов для рассмотрения материалов о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, выносит заключения о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;

- осуществляет государственную регистрацию информационных систем, содержащих государственные секреты;

- организует повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов;

- оказывает методическую и практическую помощь государственным органам и иным организациям, осуществляющим деятельность с использованием государственных секретов, по вопросам защиты государственных секретов;

- определяет порядок аттестации руководителей, ответственных за обеспечение защиты государственных секретов, если иное не установлено Законом о государственных секретах;

- делегирует органам государственной безопасности в пределах их компетенции полномочия на проведение проверочных мероприятий в государственных органах и иных организациях, за исключением государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, в связи с предоставлением им допуска к государственным секретам, на выдачу, приостановление, возобновление и аннулирование разрешений на осуществление деятельности с использованием государственных секретов государственным органам и иным организациям, на согласование номенклатур должностей работников, подлежащих допуску к государственным секретам, на согласование предоставления гражданам допуска к государственным секретам;

- осуществляет иные полномочия в соответствии с Законом о государственных секретах и другими актами законодательства.

Органы государственной безопасности в сфере государственных секретов:

- координируют применение государственными органами и иными организациями средств шифрованной, других видов специальной связи, осуществляют контроль за их использованием;

- координируют применение государственными органами и иными организациями криптографических средств защиты государственных секретов, осуществляют контроль за их использованием;

- осуществляют в пределах своих полномочий контроль за защитой государственных секретов, в том числе контроль при использовании криптографических средств защиты государственных секретов;

- осуществляют подтверждение соответствия средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов требованиям технических нормативных правовых актов в области технического нормирования и стандартизации и выдают сертификаты соответствия;

- определяют порядок технической защиты государственных секретов в своей деятельности, организуют такую техническую защиту и осуществляют за ней контроль;

– определяют порядок применения технических мер защиты государственных секретов в системах шифрованной, других видов специальной связи, осуществляют контроль за применением таких мер;

– разрабатывают проекты актов законодательства, в том числе технических нормативных правовых актов, принимают в пределах своей компетенции акты законодательства;

– согласовывают создание, реорганизацию и ликвидацию государственными органами и иными организациями подразделений по защите государственных секретов, а также назначение на должности и освобождение от должностей руководителей этих подразделений;

– проводят в пределах своей компетенции проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам, осуществлением ими деятельности в сфере государственных секретов;

– вносят предложения в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о временном ограничении права граждан, осведомленных о государственной тайне, на выезд из Республики Беларусь;

– вносят предписания в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о прекращении допуска к государственным секретам граждан;

– осуществляют иные полномочия в соответствии с Законом о государственных секретах и другими актами законодательства.

Оперативно-аналитический центр при Президенте Республики Беларусь в сфере государственных секретов:

– определяет порядок технической защиты государственных секретов, если иное не определено Законом о государственных секретах;

– координирует техническую защиту государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов;

– осуществляет контроль за технической защитой государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, в порядке, установленном этим центром, если иное не определено Президентом Республики Беларусь и Законом о государственных секретах;

– разрабатывает проекты актов законодательства, в том числе технических нормативных правовых актов, принимает (издает) в пределах своей компетенции акты законодательства по вопросам технической защиты государственных секретов;

– осуществляет подтверждение соответствия средств защиты государственных секретов требованиям технических нормативных правовых актов в области технического нормирования и стандартизации, за исключением средств шифрованной, других видов специальной связи, криптографических средств защиты государственных секретов;

– осуществляет методическое руководство повышением квалификации, подготовкой и переподготовкой руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, по вопросам технической защиты государственных секретов, определяет порядок их аттестации;

– осуществляет иные полномочия в соответствии с актами законодательства.

2. Субъекты информационных правоотношений в сфере государственных секретов.

Государственное регулирование и управление в сфере государственных секретов осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, а также Межведомственной комиссией по защите государственных секретов при Совете Безопасности Республики Беларусь, уполномоченным государственным органом по защите государственных секретов, органами государственной безопасности, Оперативно-аналитическим центром при Президенте Республики Беларусь.

Деятельность с использованием государственных секретов осуществляют государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, другие государственные органы, иные организации и граждане.

Условием осуществления деятельности с использованием государственных секретов является наличие у государственных органов, иных организаций и граждан допуска к государственным секретам, предоставленного в соответствии с Законом о государственных секретах и другими актами законодательства.

Перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам утвержден Указом Президента Республики Беларусь от 25 февраля 2011 г. № 68 «О некоторых вопросах в сфере государственных секретов».

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере государственных секретов:

- относят в сфере своей деятельности сведения к государственным секретам, разрабатывают и утверждают перечни сведений, подлежащих засекречиванию;

- организуют и осуществляют в сфере своей деятельности защиту государственных секретов;

- вносят в Совет Министров Республики Беларусь предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечня особо режимных и режимных объектов, а также предложения о создании межведомственных экспертных комиссий в сфере государственных секретов;

- передают государственные секреты другим государственным органам и иным организациям;

- принимают решения о передаче служебной тайны иностранным государствам, международным организациям, межгосударственным образованиям при наличии международного договора Республики Беларусь о защите государственных секретов;

- осуществляют контроль за защитой государственных секретов в подчиненных организациях, а также в государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

- согласовывают создание, реорганизацию и ликвидацию подразделений по защите государственных секретов в подчиненных организациях, а также в других государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

- создают, реорганизуют и ликвидируют подразделения по защите государственных секретов, обеспечивают их функционирование;

- определяют руководителей, ответственных за обеспечение защиты государственных секретов;

- создают условия для осуществления деятельности с использованием государственных секретов;

- разрабатывают и утверждают номенклатуры должностей работников, подлежащих допуску к государственным секретам;

- принимают в пределах своей компетенции решения о создании экспертных комиссий в сфере государственных секретов;

– обеспечивают повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников, осуществляющих деятельность с использованием государственных секретов;

– осуществляют иные полномочия в соответствии с Законом о государственных секретах и другими актами законодательства.

Другие государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, в сфере государственных секретов:

– организуют и осуществляют защиту государственных секретов, находящихся в их пользовании;

– осуществляют полномочия, предусмотренные абзацами седьмым–четырнадцатым статьи 11 Закона о государственных секретах;

– вносят в государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечней сведений, подлежащих засекречиванию, перечня особо режимных и режимных объектов, а также предложения о создании экспертных комиссий в сфере государственных секретов;

– осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства.

Граждане в сфере государственных секретов имеют право:

– на осуществление деятельности с использованием государственных секретов с соблюдением требований, предусмотренных Законом о государственных секретах и другими актами законодательства о государственных секретах;

– на получение компенсационных выплат на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне;

– ознакомиться с законодательством о государственных секретах в необходимом объеме;

– осуществлять иные права, предусмотренные Законом о государственных секретах и другими актами законодательства.

Граждане обязаны выполнять требования, предусмотренные Законом о государственных секретах и другими актами законодательства о государственных секретах.

3. Отнесение сведений к государственным секретам. Категории государственных секретов.

Отнесение сведений к государственным секретам осуществляется посредством определения сведений, которые подлежат защите в соответствии с Законом о государственных секретах и другими актами законодательства.

Отнесение сведений к государственным секретам осуществляется государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, с учетом перечня сведений, подлежащих отнесению к государственным секретам.

В соответствии со ст. 14 Закона о государственных секретах к **государственным секретам могут быть отнесены:**

1) сведения в области политики:

– о стратегии и тактике внешней политики, а также внешнеэкономической деятельности;

– о подготовке, заключении, содержании, выполнении, приостановлении или прекращении действия международных договоров Республики Беларусь;

– об экспорте и импорте вооружения и военной техники;

о содержании или объемах экономического сотрудничества с иностранными государствами в военное время;

2) сведения в области экономики и финансов:

– о содержании планов подготовки экономики к отражению возможной военной агрессии;

– о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники;

– о планах (заданиях) государственного оборонного заказа, об объемах выпуска и поставках вооружения и военной техники, военно-технического имущества;

– об объемах финансирования из республиканского бюджета Вооруженных Сил Республики Беларусь, других войск и воинских формирований, правоохранительных и иных государственных органов, обеспечивающих национальную безопасность Республики Беларусь;

– о технологии изготовления системы защиты, применяемой при производстве денежных знаков, бланков ценных бумаг и других документов с определенной степенью защиты, обеспечиваемых государством;

3) сведения в области науки и техники:

– о содержании государственных и других программ, концепций по направлениям, определяющим национальную безопасность Республики Беларусь;

– о проведении научно-исследовательских, опытно-технологических и опытно-конструкторских работ в интересах национальной безопасности Республики Беларусь;

4) сведения в военной области:

– о планах строительства Вооруженных Сил Республики Беларусь, содержании основных направлений (программ) развития вооружения и военной техники;

– о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;

– о системе управления Вооруженными Силами Республики Беларусь;

– о содержании стратегических или оперативных планов, планов территориальной обороны, документов боевого управления по подготовке и проведению операций, стратегическому развертыванию Вооруженных Сил Республики Беларусь, других войск и воинских формирований, их боевой, мобилизационной готовности и мобилизационных ресурсах;

– о назначении, местонахождении, степени защищенности, системе охраны особо режимных и режимных объектов, пунктов управления государством в военное время или их проектировании, строительстве, эксплуатации, степени готовности;

5) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

– об организации, тактике, силах, средствах, объектах, методах, планах разведывательной, контрразведывательной и оперативно-розыскной деятельности, в том числе по обеспечению собственной безопасности в органах, осуществляющих такую деятельность;

– о финансировании мероприятий, проводимых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– о гражданах, оказывающих (оказывавших) на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также о штатных негласных сотрудниках и сотрудниках этих органов, в том числе внедренных в организованные группы, выполняющих (выполнявших) специальные задания;

6) сведения в информационной и иных областях национальной безопасности Республики Беларусь:

– о содержании, организации или результатах основных видов деятельности Совета Безопасности Республики Беларусь, государственных органов, обеспечивающих национальную безопасность Республики Беларусь;

– об организации, силах, средствах и методах обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;

– о финансировании мероприятий, проводимых в целях обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;

– о системе, методах и средствах защиты государственных секретов, состоянии защиты государственных секретов;

– о шифрах, системах шифрованной, других видов специальной связи;

7) иные сведения в области политики, экономики, финансов, науки, техники, в военной области, области разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационной и иных областях национальной безопасности Республики Беларусь, которые включаются в перечень сведений, подлежащих отнесению к государственным секретам.

Сведения, полученные государственными органами и иными организациями, а также гражданами при осуществлении деятельности, не связанной с использованием государственных секретов, собственниками которых они являются, могут быть отнесены к государственным секретам после передачи их этими государственными органами и иными организациями, а также гражданами по договору государственному органу и иной организации, наделенным полномочием по отнесению сведений к государственным секретам. Договор о передаче таких сведений заключается в соответствии с Гражданским кодексом Республики Беларусь и должен содержать указание на условия передачи этих сведений. До принятия решения об отнесении к государственным секретам указанных сведений государственными органами и иными организациями, а также гражданами осуществляется их защита.

К государственным секретам не могут быть отнесены сведения:

– являющиеся общедоступной информацией, доступ к которой, распространение и (или) предоставление которой не могут быть ограничены в соответствии с законодательными актами;

– находящиеся в собственности иностранных государств, международных организаций, межгосударственных образований и переданные Республике Беларусь (ст. 15 Закона о государственных секретах).

Сведения признаются государственными секретами, если:

– имеют действительную или потенциальную ценность;

– свободное распространение таких сведений способно повлечь за собой причинение вреда национальной безопасности Республики Беларусь, правам и законным интересам ее граждан;

– соответствуют требованиям законодательства Республики Беларусь;

– к ним нет свободного доступа на законном основании;

– обладатель таких сведений принимает меры к охране их конфиденциальности.

Государственные секреты подразделяются на две категории:

– государственная тайна – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

– служебная тайна – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь. Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

4. Степени секретности. Грифы секретности. Засекречивание. Рассекречивание.

Степень секретности – показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие степени секретности:

- для государственной тайны – «Особой важности», «Совершенно секретно»;
- для служебной тайны – «Секретно».

Гриф секретности – реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов.

На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются следующие грифы секретности:

- на носителях государственной тайны и (или) сопроводительной документации к ним – «Особой важности», «Совершенно секретно»;
- на носителях служебной тайны и (или) сопроводительной документации к ним – «Секретно».

Определение и изменение степени секретности осуществляются государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности.

Засекречивание осуществляется на основании перечня сведений, подлежащих засекречиванию, посредством установления ограничений на распространение и (или) предоставление сведений и применения иных мер защиты в соответствии с Законом о государственных секретах и другими актами законодательства.

При засекречивании на носителе государственных секретов и (или) сопроводительной документации к нему проставляется гриф секретности.

Для государственных секретов, как правило, устанавливаются следующие сроки засекречивания:

- для государственной тайны – до тридцати лет;
- для служебной тайны – до десяти лет.

Срок засекречивания исчисляется с даты засекречивания. Изменение срока засекречивания осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

Рассекречивание осуществляется посредством снятия ограничений на распространение и (или) предоставление государственных секретов и прекращения иных мер защиты.

Рассекречивание осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

При рассекречивании на носителях государственных секретов и (или) сопроводительной документации к ним аннулируется гриф секретности.

5. Защита государственных секретов. Допуск и доступ к государственным секретам.

Организация защиты государственных секретов в государственных органах и иных организациях возлагается на их руководителей.

Защита государственных секретов осуществляется посредством применения правовых, организационных, технических мер, в том числе посредством использования сертифицированных средств защиты государственных секретов, средств шифрованной, других видов специальной связи, и иных мер в соответствии с законодательством в целях

предотвращения наступления тяжких последствий или причинения существенного вреда национальной безопасности Республики Беларусь.

Средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов.

Техническая защита государственных секретов – деятельность, направленная на обеспечение защиты государственных секретов техническими мерами, за исключением технических мер защиты государственных секретов, применяемых в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов.

Средства шифрованной, других видов специальной связи – средства защиты государственных секретов и средства электросвязи, в которых они реализованы, используемые в системах шифрованной, других видов специальной связи.

В государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, должны быть созданы подразделения по защите государственных секретов.

Другие государственные органы и иные организации по решению их руководителей создают подразделения по защите государственных секретов или заключают договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов, по согласованию с государственным органом и иной организацией, которые передают им государственные секреты.

Государственные органы и иные организации в случае их реорганизации или ликвидации, а также прекращения деятельности с использованием государственных секретов обязаны в соответствии с Законом о государственных секретах и другими актами законодательства принять меры по защите находящихся у них государственных секретов.

Допуск к государственным секретам – право гражданина Республики Беларусь, иностранного гражданина, лица без гражданства (далее, если не указано иное, – гражданин) или государственного органа, иной организации на осуществление деятельности с использованием государственных секретов.

Допуск к государственным секретам государственным органам и иным организациям предоставляется при соблюдении ими законодательства о государственных секретах, а также если:

- в их структуре имеется подразделение по защите государственных секретов, состоящее из работников, количество и уровень квалификации которых достаточны для защиты государственных секретов, или ими заключен договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов;

- разработана и утверждена номенклатура должностей работников, подлежащих допуску к государственным секретам;

- их руководители, ответственные за обеспечение защиты государственных секретов, имеют допуск к государственным секретам;

- приняты иные меры защиты государственных секретов, предусмотренные законодательством о государственных секретах (ст. 30 Закона о государственных секретах).

Допуск к государственным секретам государственным органам и иным организациям, наделенным полномочием по отнесению сведений к государственным секретам, предоставляется на основании включения их в перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, утвержденный Президентом Республики Беларусь.

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, осуществляют деятельность с

использованием государственных секретов при наличии в их структуре подразделения по защите государственных секретов и выполнении условий, предусмотренных абзацами первым, третьим–пятым статьи 30 Закона о государственных секретах (см. выше). Информация о состоянии защиты государственных секретов в государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, учитывается при проведении в соответствии с актами законодательства аттестации их руководителей.

Допуск к государственным секретам другим государственным органам и иным организациям предоставляется на основании разрешения на осуществление деятельности с использованием государственных секретов, выданного уполномоченным государственным органом по защите государственных секретов либо органом государственной безопасности в случае, предусмотренном абз. 15 ст. 7 Закона о государственных секретах (при делегировании ему полномочий комитетом гос. безопасности), по результатам проверочных мероприятий.

Разрешение на осуществление деятельности с использованием государственных секретов выдается после выполнения другими государственными органами и иными организациями условий, предусмотренных статьей 30 Закона о государственной тайне, и аттестации их руководителей, ответственных за обеспечение защиты государственных секретов.

Допуск к государственным секретам предоставляется:

- гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций, принимаемых ими с учетом обязанностей, исполняемых работниками по месту работы (службы);

- гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, не являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций о привлечении их к проведению работ с использованием государственных секретов;

- гражданам Республики Беларусь, указанным в статье 35 Закона о государственных секретах (Президенту Республики Беларусь, Премьер-министру Республики Беларусь, должностным лицам, избранным (назначенным) на высшие государственные должности, и их заместителям, руководителям государственных органов и иных государственных организаций, подчиненных Президенту Республики Беларусь, руководителям республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь, председателям областных и Минского городского исполнительных комитетов, Руководителю Аппарата Совета Министров Республики Беларусь, помощникам Президента Республики Беларусь, депутатам Палаты представителей, членам Совета Республики Национального собрания Республики Беларусь, депутатам местных Советов депутатов, судьям), – на основании решений об избрании (назначении) их на соответствующие должности;

- участникам уголовного, гражданского, хозяйственного, административного процесса, не имеющим допуска к государственным секретам, – на основании решений органов, ведущих соответственно уголовный, гражданский, хозяйственный или административный процесс;

- иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), –

на основании решений об использовании в интересах Республики Беларусь их профессиональных навыков и квалификации, принимаемых с учетом заключения уполномоченного государственного органа по защите государственных секретов о предоставлении им допуска к государственным секретам;

– гражданам, оказывающим на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, гражданам Республики Беларусь, являющимся штатными негласными сотрудниками этих органов, а также гражданам, привлекаемым указанными органами к участию в оперативно-розыскном мероприятии, – на основании решений, принимаемых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность.

Допуск к государственным секретам гражданам предоставляется, если:

– граждане ознакомлены с законодательными актами, устанавливающими ответственность за нарушение законодательства о государственных секретах, а также с временным ограничением прав граждан, предусмотренным статьей 41 Закона о государственных секретах;

– имеется письменное согласие граждан на проведение в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам;

– гражданами представлены их персональные данные;

– имеется согласование уполномоченным государственным органом по защите государственных секретов либо органом государственной безопасности в случае, предусмотренном абзацем пятнадцатым статьи 7 Закона о государственных секретах, предоставления гражданам допуска к государственным секретам;

– проведены проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам;

– граждане, получившие от иностранных государств документы, предоставляющие права на льготы и преимущества в связи с политическими, религиозными взглядами или национальной принадлежностью, передали их на время работы (службы) в кадровую службу соответствующего государственного органа или иной организации.

Обязанность граждан, которым для исполнения их обязанностей по месту работы (службы) необходим допуск к государственным секретам, соблюдать требования законодательства о государственных секретах указывается в трудовом договоре (контракте).

Доступ к государственным секретам – ознакомление гражданина с государственными секретами или осуществление им иной деятельности с использованием государственных секретов.

Доступ к государственным секретам осуществляется гражданами на основании предоставленного им допуска к государственным секретам после их ознакомления в необходимом объеме с законодательством о государственных секретах.

Руководители государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, создают условия для осуществления гражданами доступа к государственным секретам, при которых граждане будут иметь доступ только к тем государственным секретам и в таком объеме, которые необходимы им для исполнения их обязанностей.

Доступ к государственным секретам осуществляется:

– гражданами Республики Беларусь, постоянно проживающими в Республике Беларусь, – в период исполнения ими обязанностей по месту работы (службы) либо в связи с привлечением их к проведению работ с использованием государственных секретов;

– гражданами Республики Беларусь, указанными в статье 35 Закона о государственных секретах, – в период осуществления ими полномочий в связи с избранием (назначением) их на соответствующие должности;

– участниками уголовного, гражданского, хозяйственного или административного процесса (их представителями) – в период их участия в процессе в соответствии с процессуальным законодательством;

– иностранными гражданами и лицами без гражданства, а также гражданами Республики Беларусь, постоянно проживающими за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), – в период использования в интересах Республики Беларусь их профессиональных навыков и квалификации;

– гражданами, являющимися представителями иностранных государств, международных организаций, межгосударственных образований, участвующими в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов, при наличии международных договоров Республики Беларусь о защите государственных секретов и по согласованию с уполномоченным государственным органом по защите государственных секретов – в период их участия в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов;

– гражданами, оказывающими на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, гражданами Республики Беларусь, являющимися штатными негласными сотрудниками этих органов, а также гражданами, привлекаемыми указанными органами к участию в оперативно-розыскном мероприятии, – в период оказания ими содействия на конфиденциальной основе этим органам или исполнения обязанностей штатных негласных сотрудников этих органов либо привлечения их указанными органами к участию в оперативно-розыскном мероприятии.

Орган, ведущий уголовный, гражданский, хозяйственный или административный процесс, в тридцатидневный срок со дня вынесения соответствующего постановления, решения, приговора, определения по делу, в материалах которого содержатся сведения, составляющие государственные секреты, письменно уведомляет государственный орган, иную организацию, предоставившие государственные секреты, о гражданах, ознакомившихся с государственными секретами, в том числе об их процессуальном положении, фамилии, собственном имени, отчестве (если таковое имеется), дате и месте рождения, гражданстве, месте жительства, работы (службы, учебы), а также о наименовании, грифе секретности, датах регистрации и регистрационных индексах носителей государственных секретов, с которыми ознакомились эти граждане.

В случае применения к участнику уголовного процесса меры по обеспечению безопасности в виде неразглашения сведений о личности в уведомлении указываются измененные анкетные данные. В отношении присутствующих в зале судебного заседания судьи, народных заседателей, секретаря судебного заседания, прокурора, защитника, эксперта, сотрудников органов внутренних дел, входящих в состав конвоя, в уведомлении указываются фамилия, собственное имя, отчество (если таковое имеется), место работы (службы) и занимаемая должность.

6. Надзор, контроль и ответственность в сфере государственных секретов.

Надзор за точным и единообразным исполнением законодательства о государственных секретах осуществляют Генеральный прокурор и подчиненные ему прокуроры в пределах предоставленных им полномочий.

Государственный контроль в сфере государственных секретов осуществляется уполномоченным государственным органом по защите государственных секретов в порядке, установленном Президентом Республики Беларусь.

Контроль за защитой государственных секретов в пределах полномочий осуществляется органами государственной безопасности, государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, другими государственными органами и иными организациями, осуществляющими деятельность с использованием государственных секретов, в порядке, установленном Советом Министров Республики Беларусь, если иное не определено Президентом Республики Беларусь.

Нарушение законодательства о государственных секретах влечет ответственность, установленную законодательными актами.

Уголовная ответственность:

Статья 356 УК. Измена государству;

Статья 358 УК. Шпионаж;

Статья 358¹. Агентурная деятельность;

Статья 373. Умышленное разглашение государственной тайны;

Статья 374. Разглашение государственной тайны по неосторожности;

Статья 375. Умышленное разглашение служебной тайны;

Статья 375¹. Незаконное собирание либо получение сведений, составляющих государственные секреты;

Административная ответственность:

Статья 23.8. Разглашение служебной тайны по неосторожности.

Ответственность за организацию защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, возлагается на их руководителей.

7. Режим коммерческой тайны. Права владельца коммерческой тайны. Доступ к коммерческой тайне.

Коммерческая тайна – сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям Закона о коммерческой тайне, в отношении которых установлен режим коммерческой тайны.

Из указанного определения следует, что перечень видов сведений, которые могут составлять коммерческую тайну, является открытым, при этом это могут быть сведения любого характера, в том числе прямо названные в Законе о коммерческой тайне сведения технического, производственного, организационного, коммерческого и финансового характера. Тем самым законодатель не устанавливает ограничений, относящихся к существу и назначению информации, которая может охраняться в качестве коммерческой тайны. При этом круг сведений, которые могут составлять коммерческую тайну, определяется с учетом ограничений, предусмотренных ст. 6 Закона о коммерческой тайне «Сведения, которые не могут составлять коммерческую тайну».

Режим коммерческой тайны – правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

В ст. 5 Закона о коммерческой тайне определены условия охраноспособности сведений в режиме коммерческой тайны. При этом перечисленные в части первой требования к сведениям, которые предполагается охранять в режиме коммерческой тайны, неоднородны по своей природе, поскольку касаются как свойств самих сведений, так и формальных препятствий к установлению в отношении определенных сведений режима коммерческой тайны. Так, режим коммерческой тайны может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям:

– не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобными сведениями. Под такими лицами следует понимать тех, для кого эти сведения представляют коммерческий интерес; к их числу, в

первую очередь, необходимо относить конкурентов потенциального владельца коммерческой тайны. Известность сведений должностным лицам и иным работникам органов и организаций, которым эти сведения стали известны в связи с выполнением ими служебных обязанностей и на которых лежит обязанность по сохранению их в тайне, не препятствует признанию информации коммерческой тайной.

Общеизвестная информация не может признаваться коммерческой тайной постольку, поскольку доступна любому участнику рынка и обладание ею не дает каких-либо конкурентных преимуществ и, как следствие, не требует ограничения доступа к такой информации, имеющейся у кого-либо из участников рынка;

– имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам. Ценность информации – комплексный показатель ее качества, мера пригодности для принятия решений в конкретной сфере. Соответственно, коммерческая ценность информации – это показатель ее пригодности (полезности) для принятия решений в коммерческой деятельности. Как отмечается в литературе, данный показатель с учетом сложившейся деловой практики имеет три составляющие: 1) достоверность информации; 2) актуальность информации; 3) полнота информации.

Для целей Закона о коммерческой тайне понятие «коммерческая ценность сведений» раскрывается в ч. 2 ст. 5: сведения оцениваются как имеющие коммерческую ценность в том случае, если обладание ими позволяет лицу при существующих или возможных обстоятельствах увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду. Из данного определения следует, что коммерчески ценными являются любые сведения, полезные для осуществления предпринимательской или иной хозяйственной деятельности.

Законодатель уточняет определение коммерческой ценности сведений, указывая на то, что такая ценность должна быть следствием их неизвестности третьим лицам. Широко применяемая в гражданском праве категория «третьи лица» обозначает субъектов, не являющихся непосредственными участниками отношений, связанных с охраной коммерческой тайны (работниками владельца коммерческой тайны или его контрагентами). Предполагается, что третьи лица могут получить указанную информацию только незаконным путем либо в результате небрежности ее обладателя.

В литературе также высказывается мнение о том, что поскольку на практике определить, обладает ли информация коммерческой ценностью, бывает достаточно сложно, следует говорить о возможности разглашения данной информации нанести ущерб интересам ее владельца.

Обобщая приведенные мнения, можно говорить о том, что коммерческая ценность предполагаемых к охране сведений определяется самим лицом, устанавливающим в их отношении режим коммерческой тайны;

– не являются объектами исключительных прав на результаты интеллектуальной деятельности. Указание на то, что в режиме коммерческой тайны не могут охраняться сведения, являющиеся объектами исключительных прав на результаты интеллектуальной деятельности, необходимо для того, чтобы разграничить сферы действия законодательства о коммерческой тайне и законодательства об интеллектуальной собственности; в режиме коммерческой тайны не может охраняться информация, которая выражена в охраняемых объектах авторского или патентного права. Система объектов права интеллектуальной собственности, в отношении которых действует исключительное право, определена в ст. 980 ГК; исключения составляют секреты производства (ноу-хау), охраняемые в режиме коммерческой тайны;

– не отнесены в установленном порядке к государственным секретам.

В ст. 6 Закона о коммерческой тайне определены сведения, которые не могут составлять коммерческую тайну. К ним относятся:

содержащиеся в учредительных документах юридического лица, а также внесенные в Единый государственный регистр юридических лиц и индивидуальных предпринимателей;

содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

являющиеся врачебной, адвокатской, банковской, налоговой или иной охраняемой законом тайной;

о недвижимом имуществе, правах и ограничениях (обременениях) прав на недвижимое имущество, содержащиеся в едином государственном регистре недвижимого имущества, прав на него и сделок с ним;

о составе имущества государственных юридических лиц и юридических лиц, акции (доли в уставных фондах) которых принадлежат государству;

об использовании средств республиканского и (или) местных бюджетов;

о состоянии окружающей среды, противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих или способных оказать негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и населения в целом;

о подлежащих уплате суммах налогов, сборов (пошлин) и других обязательных платежей;

о численности и составе работников, об условиях и охране труда, о показателях производственного травматизма и профессиональной заболеваемости, а также о наличии свободных рабочих мест (вакансий);

о задолженности нанимателей по выплате заработной платы и по социальным выплатам;

о нарушениях законодательства и фактах привлечения к ответственности за совершение этих нарушений;

об условиях аукционов (конкурсов) по продаже объектов приватизации и конкурсов по передаче принадлежащих Республике Беларусь или ее административно-территориальной единице акций открытых акционерных обществ в доверительное управление, в том числе с правом выкупа части этих акций по результатам доверительного управления, а также о проданных объектах приватизации, об условиях их продажи и о покупателях;

о финансовом состоянии лица, предоставляемые в соответствии с требованиями законодательства об экономической несостоятельности (банкротстве);

иные сведения, определенные законодательными актами.

Право на установление в отношении сведений режима коммерческой тайны принадлежит лицу, правомерно обладающему такими сведениями.

Режим коммерческой тайны считается установленным после определения состава сведений, подлежащих охране в режиме коммерческой тайны, и принятия лицом, правомерно обладающим такими сведениями, совокупности мер, необходимых для обеспечения их конфиденциальности.

Режим коммерческой тайны включает в себя следующие меры:

– ограничение доступа к коммерческой тайне путем установления порядка обращения с носителями коммерческой тайны, а также контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к коммерческой тайне;

– регулирование отношений, связанных с доступом работников к коммерческой тайне, на основании трудового договора (контракта), а также на основании обязательства о неразглашении коммерческой тайны, дополнительно заключаемого по требованию нанимателя с работником, получающим доступ к коммерческой тайне;

- регулирование отношений, связанных с доступом контрагентов к коммерческой тайне, на основании гражданско-правового договора;
- определение работников, ответственных за принятие мер по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Наряду с мерами, указанными выше, владелец коммерческой тайны вправе применять не запрещенные законодательством технические средства и методы защиты информации, а также другие меры, не противоречащие законодательству.

Владелец коммерческой тайны – юридическое или физическое лицо, в том числе индивидуальный предприниматель, а также государственный орган, иностранная организация, не являющаяся юридическим лицом, правомерно обладающие сведениями, в отношении которых такими лицами в соответствии с Законом о коммерческой тайне установлен режим коммерческой тайны, за исключением случаев, когда эти сведения составляют коммерческую тайну других лиц.

Закон не ограничивает круг владельцев коммерческой тайны только субъектами предпринимательской деятельности. Владельцами коммерческой тайны могут быть и иные хозяйствующие субъекты (некоммерческие организации, ремесленники, лица, оказывающие услуги в сфере агроэкотуризма, и др.), чья деятельность не признается предпринимательской, но которые также могут находиться в конкурентных отношениях и в связи с этим заинтересованы в использовании правового механизма охраны конфиденциальности информации, которая может быть использована в целях осуществления их хозяйственной и профессиональной деятельности.

Закон также не исключает возможности для государственных органов выступать в качестве владельцев коммерческой тайны и в этих целях устанавливать соответствующий режим охраны определенных экономически значимых сведений в режиме коммерческой тайны.

Указание в числе возможных владельцев коммерческой тайны иностранных организаций, не являющихся юридическими лицами, необходимо для того, чтобы предоставить возможность охраны коммерческой тайны иностранным компаниям, не признаваемым юридическими лицами по законодательству Республики Беларусь. Согласно норме ст. 1110 ГК гражданская правоспособность иностранных организаций, не являющихся юридическими лицами по иностранному праву, определяется по праву страны, где организация учреждена.

Для признания за лицом статуса владельца коммерческой тайны необходимо соблюдение двух основных условий: 1) правомерное обладание сведениями и 2) установление в отношении этих сведений режима коммерческой тайны.

Владелец коммерческой тайны вправе:

- изменять или отменять режим коммерческой тайны;
- изменять состав сведений, составляющих коммерческую тайну;
- использовать сведения, составляющие коммерческую тайну;
- разрешать или запрещать доступ других лиц к коммерческой тайне, изменять порядок и условия доступа к ней, если иное не установлено законодательством;
- распоряжаться сведениями, составляющими коммерческую тайну;
- применять предусмотренные гражданским законодательством способы защиты от действий (бездействия) лиц, нарушающих режим коммерческой тайны или создающих угрозу такого нарушения.

Владелец коммерческой тайны может передать все или часть сведений, составляющих коммерческую тайну, другому лицу по договору, обязательным условием которого является обеспечение конфиденциальности передаваемых сведений.

Владелец коммерческой тайны обязан поддерживать установленный им режим коммерческой тайны, принимать меры, необходимые и достаточные для обеспечения конфиденциальности сведений, составляющих коммерческую тайну. Для выполнения этих обязанностей владелец коммерческой тайны вправе:

– требовать от лиц, в том числе от государственных органов, получивших доступ к коммерческой тайне, исполнения предусмотренных Законом о коммерческой тайне и (или) договором обязательств по соблюдению конфиденциальности сведений, составляющих коммерческую тайну;

– требовать от лиц, получивших возможность ознакомления со сведениями, составляющими коммерческую тайну, в результате случайности либо действий других лиц, которые не имели права предоставлять доступ к коммерческой тайне, соблюдения конфиденциальности этих сведений;

– совершать иные действия для обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

Владелец коммерческой тайны может на носителях коммерческой тайны применять гриф «Коммерческая тайна» с указанием владельца коммерческой тайны (для юридических лиц – полное наименование и место нахождения, для физических лиц – фамилия, собственное имя, отчество (если таковое имеется) гражданина и место его жительства).

Доступ к коммерческой тайне – возможность ознакомления с согласия владельца коммерческой тайны или на ином законном основании определенного круга лиц со сведениями, составляющими коммерческую тайну.

Сущностной характеристикой понятия «доступ к коммерческой тайне» является правомерность ознакомления с составляющими эту тайну сведениями. Если ознакомление с охраняемыми сведениями было незаконным, такое действие должно квалифицироваться как действие, влекущее ответственность.

В качестве общего правила устанавливается, что доступ к коммерческой тайне может быть предоставлен только ее владельцем. Такой доступ предоставляется контрагентам и работникам. В качестве исключения из общего правила предусматривается возможность предоставления доступа к коммерческой тайне по требованию перечисленных в ч. 2 ст. 11 Закона о коммерческой тайне государственных органов. В случаях, порядке и пределах, предусмотренных законодательством, доступ к коммерческой тайне предоставляется по требованию:

суда общей юрисдикции – по находящимся в его производстве уголовным, гражданским, экономическим делам и делам об административных правонарушениях;

прокурора или его заместителя;

органов дознания и предварительного следствия – по находящимся в их производстве материалам и уголовным делам;

органов, осуществляющих оперативно-розыскную деятельность;

органов Комитета государственного контроля Республики Беларусь;

налоговых и таможенных органов;

антимонопольных органов;

других государственных органов и иных лиц, определенных законодательными актами.

Требование о предоставлении доступа к коммерческой тайне должно быть оформлено в письменной форме, подписано уполномоченным лицом и должно содержать цель, правовое основание для ознакомления со сведениями, составляющими коммерческую тайну, и срок их предоставления, если иное не установлено законодательными актами.

При предъявлении требования о предоставлении доступа к коммерческой тайне к лицу, не являющемуся ее владельцем, такое лицо, если иное не предусмотрено законодательными актами, отказывает в предоставлении сведений, составляющих коммерческую тайну, ограничившись предоставлением информации о владельце этой коммерческой тайны.

Государственные органы и иные лица, получившие в соответствии с их требованием доступ к коммерческой тайне, обязаны создать условия, обеспечивающие соблюдение конфиденциальности сведений, составляющих коммерческую тайну.

Носители коммерческой тайны, предоставляемые по требованию государственных органов и иных лиц, должны быть идентифицированы владельцем коммерческой тайны путем нанесения грифа «Коммерческая тайна» с указанием ее владельца (для юридических лиц – полное наименование и место нахождения, для физических лиц – фамилия, собственное имя, отчество (если таковое имеется) гражданина и место его жительства).

Должностные лица государственных органов, а также работники иных лиц не вправе разглашать сведения, составляющие коммерческую тайну, или предоставлять доступ третьим лицам к сведениям, ставшим известными им в силу выполнения трудовых (служебных) обязанностей и составляющим коммерческую тайну, за исключением случаев, предусмотренных законодательными актами, а также не вправе использовать эти сведения в целях, непосредственно не связанных с выполнением трудовых (служебных) обязанностей.

В целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну, государственные органы и иные лица могут использовать любые не противоречащие законодательству способы ограничения доступа к таким сведениям.

8. Правовые средства охраны коммерческой тайны в отношениях с контрагентами и работниками. Ответственность за нарушение законодательства о коммерческой тайне.

Контрагент – сторона гражданско-правового договора (за исключением лиц, состоящих в трудовых отношениях с владельцем коммерческой тайны), которой владелец коммерческой тайны предоставляет доступ к сведениям, составляющим коммерческую тайну.

До заключения с контрагентом гражданско-правового договора независимо от его вида в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну и относящихся к предмету заключаемого договора, обязательства по обеспечению конфиденциальности этих сведений могут быть закреплены в самостоятельном соглашении о конфиденциальности. Обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, могут быть также предусмотрены самим договором с контрагентом.

Соглашение о конфиденциальности – гражданско-правовой договор, заключаемый владельцем коммерческой тайны с контрагентом, предметом которого являются обязательства сторон по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Обязательство о неразглашении коммерческой тайны – гражданско-правовой договор, заключаемый владельцем коммерческой тайны или лицом, получившим к ней доступ, с лицом, состоящим в трудовых отношениях с владельцем коммерческой тайны или лицом, получившим к ней доступ, и определяющий обязательства сторон, связанные с соблюдением конфиденциальности сведений, составляющих коммерческую тайну.

Наниматель, являющийся владельцем коммерческой тайны и (или) получивший доступ к коммерческой тайне третьих лиц, в связи с установлением режима коммерческой тайны вправе определить работников, с которыми необходимо заключить обязательство о неразглашении коммерческой тайны.

Обязательство о неразглашении коммерческой тайны определяет права и обязанности сторон, связанные с соблюдением конфиденциальности сведений, составляющих коммерческую тайну, порядок доступа работника к сведениям, составляющим коммерческую тайну нанимателя, и (или) сведениям, составляющим

коммерческую тайну третьих лиц, к которым наниматель получил доступ, а также срок действия обязательства.

Обязательство о неразглашении коммерческой тайны может содержать условие о выплате работнику вознаграждения за выполнение обязательств, связанных с соблюдением режима коммерческой тайны, а также условие об ответственности работника за его нарушение.

Обязательство о неразглашении коммерческой тайны должно содержать условие об ответственности нанимателя за ненадлежащее выполнение обязанности, предусмотренной ч. 2 ст. 9 Закона о коммерческой тайне.

Работники, получившие доступ к сведениям, составляющим коммерческую тайну, и подписавшие обязательство о неразглашении коммерческой тайны, после прекращения трудового договора (контракта) с нанимателем обязаны соблюдать конфиденциальность таких сведений в течение срока действия обязательства о неразглашении коммерческой тайны либо до момента отмены режима коммерческой тайны в отношении сведений, составляющих коммерческую тайну, к которым работник имел доступ, если этот момент наступит ранее окончания срока действия обязательства о неразглашении коммерческой тайны.

Соглашение о конфиденциальности, а также любой иной гражданско-правовой договор с контрагентом, закрепляющий обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, должны быть оформлены в письменной форме и должны содержать перечень сведений, составляющих коммерческую тайну, или порядок их определения, пределы использования этих сведений, а также указание о сроке, в течение которого контрагент обязан обеспечивать их конфиденциальность, в том числе в случае расторжения или отказа от исполнения договора.

Недействительность гражданско-правового договора с контрагентом не влечет за собой недействительности его части, содержащей обязательства по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Если иное не установлено соглашением сторон, контрагент самостоятельно определяет необходимые способы обеспечения конфиденциальности сведений, составляющих коммерческую тайну, к которым он получил доступ. При этом в отношении третьих лиц контрагент имеет те же права на защиту коммерческой тайны, что и ее владелец, если иное не определено заключенным между ними договором.

Контрагент обязан незамедлительно сообщить владельцу коммерческой тайны о допущенных им либо ставших известными ему факте незаконного ознакомления со сведениями, составляющими коммерческую тайну, факте незаконного использования этих сведений, факте разглашения коммерческой тайны или угрозы разглашения коммерческой тайны третьими лицами, а также о требованиях доступа к коммерческой тайне со стороны государственных органов и иных лиц.

Наниматель, являющийся владельцем коммерческой тайны и (или) получивший доступ к коммерческой тайне третьих лиц, обязан:

- ознакомить работников, которым доступ к коммерческой тайне необходим для выполнения трудовых (служебных) обязанностей, с категориями сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ (без раскрытия содержания этих сведений);

- ознакомить работников, получающих доступ к коммерческой тайне, с установленным им режимом коммерческой тайны и мерами ответственности за его нарушение, а также за разглашение сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ;

- создать работникам необходимые условия для соблюдения установленного им режима коммерческой тайны;
- осуществлять иные действия, предусмотренные законодательством.

В целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну, работники обязаны:

- соблюдать установленный нанимателем режим коммерческой тайны, не разглашать сведения, составляющие коммерческую тайну нанимателя, и (или) сведения, составляющие коммерческую тайну третьих лиц, к которым наниматель получил доступ, и не использовать сведения, составляющие коммерческую тайну, в целях, не связанных с выполнением трудовых (служебных) обязанностей;

- незамедлительно сообщать нанимателю о допущенных ими либо ставших известными им фактах незаконного ознакомления со сведениями, составляющими коммерческую тайну нанимателя, и (или) сведениями, составляющими коммерческую тайну третьих лиц, к которым наниматель получил доступ, фактах незаконного использования этих сведений, фактах разглашения или угрозы разглашения сведений, составляющих коммерческую тайну нанимателя, и (или) сведений, составляющих коммерческую тайну третьих лиц, к которым наниматель получил доступ, а также о требованиях доступа к коммерческой тайне со стороны государственных органов и иных лиц;

- подписать по требованию нанимателя обязательство о неразглашении коммерческой тайны;

- передать нанимателю при прекращении трудового договора (контракта) находящиеся у них носители коммерческой тайны.

За действия (бездействие), повлекшие незаконное ознакомление со сведениями, составляющими коммерческую тайну, или за незаконное использование этих сведений, а также за разглашение коммерческой тайны физические и юридические лица, государственные органы и их должностные лица несут ответственность, предусмотренную законодательными актами (дисциплинарную, гражданско-правовую, административную, уголовную).

В случае незаконного ознакомления со сведениями, составляющими коммерческую тайну, или незаконного использования этих сведений, а также разглашения коммерческой тайны физические и юридические лица, государственные органы и их должностные лица обязаны:

- прекратить действия, связанные с незаконным ознакомлением со сведениями, составляющими коммерческую тайну, или с незаконным использованием этих сведений, а также с разглашением коммерческой тайны;

- возместить убытки (включая упущенную выгоду), причиненные владельцу коммерческой тайны в результате незаконного ознакомления со сведениями, составляющими коммерческую тайну, или незаконного использования этих сведений, а также разглашения коммерческой тайны.

Государственные органы и иные лица, получившие в соответствии с их требованием доступ к коммерческой тайне, несут перед владельцем коммерческой тайны ответственность за ее разглашение, а также за незаконное использование сведений, составляющих коммерческую тайну, лицами, которым они стали известны в связи с выполнением трудовых (служебных) обязанностей.

Контрагент, не обеспечивший в соответствии с условиями гражданско-правового договора конфиденциальность сведений, составляющих коммерческую тайну, обязан возместить владельцу коммерческой тайны убытки (включая упущенную выгоду), если иное не предусмотрено этим договором.

Уголовная ответственность: ст. 254 УК Коммерческий шпионаж и ст. 255 УК Разглашение коммерческой тайны.

Административная ответственность: ст. 23.6 КоАП Разглашение коммерческой или иной охраняемой законом тайны.

ТЕМА 6 ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Правовой режим персональных данных. Особенности информационных правоотношений в области персональных данных.
2. Субъекты информационных правоотношений в области персональных данных.
3. Государственное регулирование работы с персональными данными.
4. Защита персональных данных.
5. Международные правовые акты в сфере защиты персональных данных.

1. Правовой режим персональных данных. Особенности информационных правоотношений в области персональных данных.

Основополагающим документом Республики Беларусь, гарантирующим право граждан на доступ к информации, является Конституция Республики Беларусь. В статье 28 Конституции Республики Беларусь гарантируется неприкосновенность личной жизни. Каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

В соответствии с Законом об информации никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь. Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с согласия данного физического лица, если иное не установлено законодательством Республики Беларусь.

В Республике Беларусь принят Закон от 7 мая 2021 г. № 99-З «О защите персональных данных», направленный на обеспечение защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных.

В соответствии со статьей 1 указанного Закона **персональные данные** – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Физическое лицо, которое может быть идентифицировано – физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Законом определены следующие виды персональных данных:

общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов;

специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности,

биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое);

генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца.

2. Субъекты информационных правоотношений в области персональных данных.

Субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом о защите персональных данных и иными законодательными актами.

Согласие субъекта персональных данных представляет собой свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных.

Согласие субъекта персональных данных может быть получено в письменной форме, в виде электронного документа или в иной электронной форме.

Субъект персональных данных имеет следующие права:

– право на отзыв согласия субъекта персональных данных. Субъект персональных данных вправе в любое время без объяснения причин отозвать свое согласие посредством подачи оператору заявления в порядке, установленном ст. 14 Закона о защите персональных данных, либо в форме, посредством которой получено его согласие;

– право на получение информации, касающейся обработки персональных данных, и изменение персональных данных;

– право на получение информации о предоставлении персональных данных третьим лицам. Субъект персональных данных вправе получать от оператора информацию о предоставлении своих персональных данных третьим лицам один раз в календарный год бесплатно, если иное не предусмотрено Законом и иными законодательными актами;

– право требовать прекращения обработки персональных данных и (или) их удаления. Субъект персональных данных вправе требовать от оператора бесплатного прекращения обработки своих персональных данных, включая их удаление, при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами;

– право на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных.

Также выделены следующие субъекты:

Оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие или осуществляющие обработку персональных данных.

Оператор обязан:

– разъяснять субъекту персональных данных его права, связанные с обработкой персональных данных;

– получать согласие субъекта персональных данных, за исключением случаев, предусмотренных Законом о защите персональных данных и иными законодательными актами;

– обеспечивать защиту персональных данных в процессе их обработки;

– предоставлять субъекту персональных данных информацию о его персональных данных, а также о предоставлении его персональных данных третьим лицам, за исключением случаев, предусмотренных настоящим Законом и иными законодательными актами;

– вносить изменения в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных;

– прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных настоящим Законом и иными законодательными актами;

– уведомлять уполномоченный орган по защите прав субъектов персональных данных о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, за исключением случаев, предусмотренных уполномоченным органом по защите прав субъектов персональных данных;

– осуществлять изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных субъекта персональных данных по требованию уполномоченного органа по защите прав субъектов персональных данных, если иной порядок внесения изменений в персональные данные, их блокирования или удаления не установлен законодательными актами;

– исполнять иные требования уполномоченного органа по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных;

– выполнять иные обязанности, предусмотренные Законом о защите персональных данных и иными законодательными актами.

Оператор, являющийся республиканским органом государственного управления, размещает на своем официальном сайте в глобальной компьютерной сети Интернет информацию об информационных ресурсах (системах), содержащих персональные данные, владельцем которых он является, за исключением информации об информационных ресурсах (системах), содержащих:

– персональные данные, обработка которых осуществляется в случаях, предусмотренных абзацами четвертым – седьмым пункта 3 статьи 11 Закона о защите персональных данных;

– персональные данные его работников в процессе осуществления трудовой (служебной) деятельности;

– служебную информацию ограниченного распространения.

Уполномоченное лицо – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

3. Государственное регулирование работы с персональными данными.

Порядок обработки персональных данных определен Законом о защите персональных данных и иными актами законодательства.

Обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами.

В случае обработки персональных данных без согласия субъекта персональных данных цели обработки персональных данных устанавливаются настоящим Законом и иными законодательными актами.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее заявленных законных целей. Не допускается обработка персональных данных, не совместимая с первоначально заявленными целями их обработки.

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

Обработка персональных данных должна носить прозрачный характер. В этих целях субъекту персональных данных в случаях, предусмотренных настоящим Законом, предоставляется соответствующая информация, касающаяся обработки его персональных данных.

Оператор обязан принимать меры по обеспечению достоверности обрабатываемых им персональных данных, при необходимости обновлять их.

Хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных.

Согласие субъекта персональных данных на обработку персональных данных, за исключением специальных персональных данных, порядок обработки которых установлен ст. 8 Закона, не требуется:

- для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности;
- для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов;
- в целях осуществления контроля (надзора) в соответствии с законодательными актами;
- при реализации норм законодательства в области национальной безопасности, о борьбе с коррупцией, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;
- при реализации норм законодательства о выборах, референдуме, об отзыве депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, депутата местного Совета депутатов;
- для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в том числе профессионального пенсионного страхования;
- при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством;
- для осуществления нотариальной деятельности;

- при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь;
- в целях назначения и выплаты пенсий, ежемесячного денежного содержания отдельным категориям государственных служащих, пособий;
- для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;
- в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- при осуществлении учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением и возмещения расходов на электроэнергию, платы за другие услуги и возмещения налогов, а также при предоставлении льгот и взыскании задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением и возмещению расходов на электроэнергию;
- при получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;
- при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа;
- в целях осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации, организации, осуществляющей издательскую деятельность, направленных на защиту общественного интереса, представляющего собой потребность общества в обнаружении и раскрытии информации об угрозах национальной безопасности, общественному порядку, здоровью населения и окружающей среде, информации, влияющей на выполнение своих обязанностей государственными должностными лицами, занимающими ответственное положение, общественными деятелями, за исключением случаев, предусмотренных гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса;
- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;
- в отношении распространенных ранее персональных данных до момента заявления субъектом персональных данных требований о прекращении обработки распространенных персональных данных, а также об их удалении при отсутствии иных оснований для обработки персональных данных, предусмотренных настоящим Законом и иными законодательными актами;
- в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;
- в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

4. Защита персональных данных.

Оператор (уполномоченное лицо) обязан принимать правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Оператор (уполномоченное лицо) определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты персональных данных, с учетом требований Закона и иных актов законодательства.

Обязательными мерами по обеспечению защиты персональных данных являются:

- назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных;

- издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных;

- ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством;

- установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);

- осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Оператор (уполномоченное лицо), являющийся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, обязан обеспечить неограниченный доступ, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику оператора (уполномоченного лица) в отношении обработки персональных данных, до начала такой обработки.

Классификация информационных ресурсов (систем), содержащих персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных устанавливается уполномоченным органом по защите прав субъектов персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных принимает меры по защите прав субъектов персональных данных при обработке персональных данных.

В соответствии с Указом № 422 уполномоченным органом по защите прав субъектов персональных данных является Национальный центр защиты персональных данных Республики Беларусь. Учредителем Национального центра защиты персональных данных и государственным органом, осуществляющим от имени Республики Беларусь права собственника имущества этого учреждения, является Оперативно-аналитический центр при Президенте Республики Беларусь.

Уполномоченный орган по защите прав субъектов персональных данных:

- осуществляет контроль за обработкой персональных данных операторами (уполномоченными лицами) в соответствии с законодательными актами;

- рассматривает жалобы субъектов персональных данных по вопросам обработки персональных данных;

- требует от операторов (уполномоченных лиц) изменения, блокирования или удаления недостоверных или полученных незаконным путем персональных данных, устранения иных нарушений Закона;

- определяет перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

- выдает разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных;
- участвует в подготовке проектов актов законодательства о персональных данных;
- дает разъяснения по вопросам применения законодательства о персональных данных, проводит иную разъяснительную работу о законодательстве о персональных данных;
- участвует в работе международных организаций по вопросам защиты персональных данных;
- ежегодно не позднее 15 марта публикует в средствах массовой информации отчет о своей деятельности за предыдущий год;
- осуществляет иные полномочия, предусмотренные Законом и иными законодательными актами.

5. Международные правовые акты в сфере защиты персональных данных.

Во Всеобщей декларации прав человека 1948 года определено, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» (статья 12).

28 января 1981 года в Страсбурге был открыт для подписания первый имеющий обязательную силу международный договор, удовлетворяющий потребность в защите персональных данных – Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, также известная как «Конвенция 108». Она определяет порядок сбора, хранения, способы защиты персональных данных физических лиц, а также возможность получения доступа к ним. Положения Конвенции являются обязательными и распространяются на обработку персональных данных в рамках национальных юрисдикций для всех физических лиц вне зависимости от их гражданства и места жительства.

Договор был модернизирован в 2018 году путем принятия Протокола о внесении изменений. Протокол направлен на обеспечение того, чтобы принципы защиты персональных данных были адаптированы к новым технологиям, а также на укрепление предусмотренного конвенцией контрольного механизма.

«Конвенция 108», открытая для всех стран и обладающая уникальным потенциалом стать глобальным стандартом, закрепила основополагающие принципы и правила защиты данных, которые применяются и сегодня. Конвенция, составленная в нейтральном стиле с точки зрения технологий, полностью сохраняла свою актуальность на протяжении четырех десятилетий. На сегодняшний день она насчитывает 55 стран-участников на четырех континентах, еще 20 государств принимают участие в ее работе.

Во многих государствах по всему миру «Конвенция 108» стала основой соответствующего национального законодательства. Кроме того, она послужила основой для первой директивы Европейского союза по защите данных, принятой в 1995 году, за которой в 2018 году последовало принятие Общего регламента по защите персональных данных лиц Европейского союза General Data Protection Regulation (GDPR), который вступил в силу 25 мая 2018 года.

GDPR представляет собой совокупность двух документов: Регламент 2016/679 Европейского Парламента и Совета Европы «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ ЕС (общие правила защиты данных)», а также Директива 2016/680 Европейского Парламента и Совета Европы «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения расследования уголовных преступлений, ведения розыскных или судебных действий или

исполнения уголовных наказаний, а также за свободное перемещение таких данных». Регламент не требует от правительств стран - участниц ЕС никаких изменений в локальных законодательствах и, таким образом, является непосредственно обязательным к исполнению. Это применимо не только к странам - участницам ЕС, но также к любому юридическому лицу, обрабатывающему персональные данные лиц ЕС. Регламент имеет, таким образом, трансграничное действие.

Обеспечение соблюдения Регламента обязательно для всех, кто осуществляет следующую деятельность:

1. Компания находится на территории ЕС и собирает персональные данные.
2. Компания находится за пределами ЕС, но деятельность направлена на территорию ЕС.
3. Компания сотрудничает с европейскими партнерами и получает от них персональные данные пользователей.
4. Компания собирает и анализирует информацию с территории ЕС.
5. Компания реализует товары и услуги для граждан ЕС (открыто или скрыто).
6. Компания обрабатывает персональные данные по поручению оператора, который подпадает под требования регламента GDPR.

GDPR усиливает и унифицирует защиту персональных данных всех лиц в Европейском Союзе, а также отличается применением штрафных санкций за нарушение требований закона.

ТЕМА 7

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1. **Понятие электронного документа.**
2. **Понятие электронной цифровой подписи. Правовое регулирование применения электронной цифровой подписи.**
3. **Система межведомственного документооборота.**
4. **Правовое регулирование и юридические риски электронного документооборота.**
5. **Проблемы применения электронной цифровой подписи в условиях глобализации информационного общества.**

1. Понятие электронного документа.

В контексте современных научных исследований понятие «электронного документа» хотя и используется как устоявшееся, но по сей день исследуется на предмет неоднозначности его содержания.

И.Ю. Востриков предлагает следующее: «под электронным документом следует понимать документ, созданный при помощи электронных аппаратно-технических и программных средств, фиксируемых в цифровом коде в форме идентифицируемого именованного файла (файлов) или записи в файле (файлах) базы данных, доступный для последующей обработки в электронных системах, использования, воспроизведения, отображения и виртуального восприятия, а также для передачи и получения по телекоммуникационным линиям связи».

А.П. Вершинин (следует обратить внимание, что он внимательно относится к теории вопроса, памятуя о том, что есть информация как содержание доказательства, а есть ее носитель как средство доказывания) определяет электронный документ, как информацию, зафиксированную на электронных носителях и позволяющую ее идентифицировать. Иногда к возможности идентификации названный автор добавляет и требование аутентификации, т.е. возможность проверки целостности и неизменности содержания электронного документа.

А.В. Рыбин предлагает понимать под электронным документом сведения об обстоятельствах, подлежащих установлению по делу, записанных на перфокарту, магнитный, оптический, магнитооптический накопитель, карту флэшпамяти или иной подобный носитель, полученный с соблюдением процессуального порядка его собирания.

С точки зрения Т.Э. Кукарниковой, электронный документ – это объект, несущий информацию, имеющую смысловое значение и существующий только в электронной среде, где под электронной средой понимается система объектов (компьютерных средств и систем), взаимодействующих на основе формальных правил обработки, хранения и передачи информации, представленной в цифровой форме.

И.Н. Подволоцкий, рассматривая в своей монографии «Осмотр и предварительное исследование документов» электронный документ в процессе доказывания, определяет его как любые сведения, хранимые, обрабатываемые и передаваемые с помощью информационных и телекоммуникационных систем, полученные или представленные с соблюдением процессуального порядка их собирания, на основе которых суд, прокурор, следователь, дознаватель устанавливают наличие или отсутствие обстоятельств, имеющих значение для уголовного дела. К ним допустимо отнести документы, выполненные в виде текста, рисунка, фотографии, карты, плана, схемы, графика, фильма, звуковой дорожки или иной записи, которую возможно воспроизвести.

Электронный документ – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность, которые подтверждаются путем применения сертифицированных средств электронной цифровой подписи с использованием при проверке электронной цифровой подписи открытых ключей организации или физического лица, подписавших этот электронный документ (статья 1 Закона Республики Беларусь от 28.12.2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»).

Электронные документы могут применяться во всех сферах деятельности, где используются технические, программные и программно-аппаратные средства, необходимые для создания, обработки, хранения, передачи и приема информации в электронном виде.

Электронный документ должен соответствовать следующим требованиям:

создаваться, обрабатываться, храниться, передаваться и приниматься с помощью технических, программных и программно-аппаратных средств;

иметь структуру, установленную законодательством;

быть представляемым в форме, доступной и понятной для восприятия человеком.

Структура электронного документа включает два обязательных элемента – общую и особенную части. Общая часть электронного документа состоит из информации, составляющей содержание документа. Особенная часть электронного документа состоит из одной или нескольких электронных цифровых подписей, может содержать штамп времени (штамп времени – реквизит электронного документа, удостоверяющий дату и время создания электронного документа), а также дополнительные данные, необходимые для проверки электронных цифровых подписей и идентификации электронного документа, которые устанавливаются техническими нормативными правовыми актами.

Электронный документ имеет формы внутреннего и внешнего представления. Формой внутреннего представления электронного документа является запись информации, составляющей электронный документ, на электронном носителе информации. Формой внешнего представления электронного документа является воспроизведение электронного документа на электронном средстве отображения информации, на бумажном носителе в форме, доступной и понятной для восприятия человеком.

Оригинал электронного документа существует только в электронном виде. Все идентичные экземпляры электронного документа являются оригиналами и имеют одинаковую юридическую силу. Документы, созданные организацией или физическим

лицом на бумажном носителе и в электронном виде, идентичные по содержанию, имеют одинаковую юридическую силу. В этом случае документ на бумажном носителе не является копией электронного документа.

Подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу.

Обязательным реквизитом электронного документа является электронная цифровая подпись, которая представляет собой последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности, а также для иных целей, предусмотренных законодательством.

2. Понятие электронной цифровой подписи. Правовое регулирование применения электронной цифровой подписи.

Электронная цифровая подпись – это последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности, а также для иных целей, предусмотренных законодательством.

Электронная цифровая подпись предназначена для:

удостоверения информации, составляющей общую часть электронного документа, осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием личных ключей организации или физических лиц, подписывающих этот электронный документ;

подтверждения целостности и подлинности электронного документа осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием при проверке электронной цифровой подписи открытых ключей организации или физических лиц, подписавших этот электронный документ;

подписания электронной копии документа на бумажном носителе.

Электронная цифровая подпись, владельцем личного ключа которой является физическое лицо, является аналогом собственноручной подписи.

Электронная цифровая подпись, владельцем личного ключа которой является организация, может применяться:

в качестве аналога оттиска печати организации; совместно с электронной цифровой подписью, владельцем личного ключа которой является физическое лицо, если информация о полномочиях этого физического лица, предоставленных ему от имени этой организации, не содержится в атрибутивном сертификате;

для создания и подписания электронных документов посредством автоматизированных информационных систем без участия физического лица;

в иных случаях, предусмотренных законодательством Республики Беларусь.

Электронная цифровая подпись имеет личный (личный ключ – последовательность символов, принадлежащая определенному организации или физическому лицу и используемая при выработке электронной цифровой подписи) и открытый (открытый ключ – последовательность символов, соответствующая определенному личному ключу, доступная для всех заинтересованных организаций или физических лиц и применяемая при проверке электронной цифровой подписи) ключи.

Владельцем личного ключа являются организация или физическое лицо, осуществившие выработку личного ключа с использованием сертифицированного средства электронной цифровой подписи.

Владелец личного ключа обязан:

хранить в тайне личный ключ;

обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);

не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия этого открытого ключа истек;

отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена.

Открытый ключ вырабатывается на базе личного ключа с использованием сертифицированного средства электронной цифровой подписи. Владельцем открытого ключа являются организация или физическое лицо, являющиеся владельцем личного ключа, на базе которого выработан этот открытый ключ. Распространение открытого ключа осуществляется в целях обеспечения получения всеми заинтересованными организациями и физическими лицами открытого ключа, который требуется для проверки электронной цифровой подписи.

Атрибутный сертификат подтверждает связь физического лица, являющегося владельцем личного ключа, с организацией или физическим лицом, от имени которых этому физическому лицу предоставлены полномочия и которые являются владельцем атрибутного сертификата. Атрибутный сертификат применяется в информационных системах совместно с сертификатом открытого ключа.

Цифровую подпись представляют в виде:

флеш-карты, которую вставляют в персональный компьютер при необходимости проверить правильность и реальность отчета или другой документации;

сим-карты, на которой имеется приложение, включающее личный электронный ключ. Это удобно для работающих на смартфонах или планшетах;

подписи в облаке, находящейся на сервере ответственного за это центра. Такая ЭЦП не обладает реальным воплощением и считается самой неподдельной.

3. Система межведомственного документооборота.

Непосредственно сам электронный документооборот представляет собой движение документов в организации с момента их создания или получения до завершения исполнения или отправления; комплекс работ с документами: прием, регистрация, рассылка, контроль исполнения, формирование дел, хранение и повторное использование документации, справочная работа.

Для автоматизации внутреннего и внешнего документооборота предприятия или организации сейчас применяют различные системы. Они созданы конкретно для управления электронным документооборотом. В результате этого предприятие может полностью работать без использования бумажных носителей. Вся его деятельность связана с документами, представленными в электронном виде. Таким образом, под электронным документооборотом понимается обмен электронными документами в локальной сети или в интернете.

В настоящее время электронный документооборот представляют собой важную составную часть ИТ-инфраструктуры. Их использование позволяет повысить эффективность работы многих предприятий в промышленности и коммерческих организаций. Кроме того, технологии электронного документооборота в государственных учреждениях создают условия для того, чтобы максимально оперативно решать задачи по управлению. Они необходимы для организации эффективного взаимодействия государственных органов с населением и различными ведомствами.

Система электронного документооборота – это специальное программное обеспечение, которое помогает организовать работу и навести порядок в электронных документах, а также осуществлять взаимодействие между сотрудниками.

Система автоматизации электронного документооборота позволяет: организовать электронное хранилище документов с возможностью контекстного поиска; повысить качество обработки электронных документов; ускорить процессы рассмотрения и согласования; автоматизировать делопроизводство; обеспечить работу с документами по тонким каналам связи через Вебинтерфейс; повысить уровень информационной

безопасности; минимизировать риски потери информации; анализировать качество процессов обработки документов.

Система межведомственного электронного документооборота (СМДО) государственных органов Республики Беларусь – государственная межведомственная информационная система, обеспечивающая межведомственное взаимодействие государственных органов и иных организаций посредством обмена электронными документами. СМДО была разработана в рамках Государственной программы информатизации Республики Беларусь на 2003-2005 годы и на перспективу до 2010 года «Электронная Беларусь», утвержденной постановлением Совета Министров Республики Беларусь от 27.12.2002 № 1819 (проект 49 «Создание первой очереди системы межведомственного электронного документооборота государственных органов Республики Беларусь»).

Цели проекта СМДО:

переход от бумажного документооборота к электронному документообороту;
обеспечение организации информационного взаимодействия республиканских органов государственного управления и организаций;
повышение оперативности принятия управленческих решений;
дебюрократизация государственного аппарата.

Все имущественные права на использование системы были переданы Национальному центру электронных услуг. НЦЭУ является единственным правообладателем СМДО.

В Республике Беларусь всем государственным органам, иным государственным организациям, а также хозяйственным обществам, в отношении которых государство может определять принимаемые ими решения, было поручено обеспечить приобретение (разработку, модернизацию) ведомственных систем электронного документооборота, которые должны обеспечивать возможность взаимодействия с СМДО.

4. Правовое регулирование и юридические риски электронного документооборота.

Недооценка рисков на одном этапе может привести к нарушениям работы системы на другом. Чем раньше возник риск, тем более разрушительны в дальнейшем будут его последствия.

Риски можно разделить на группы: административные, субъективные, технологические. Данное деление условно, так как риски зачастую тесно связаны и взаимно обуславливают друг друга.

Административные риски:

1. Отсутствие или некорректная постановка целей и задач проекта – один из весьма распространенных рисков. К сожалению, руководители и собственники компаний не всегда осознают возможности и преимущества электронных систем. Следствием этого риска является отсутствие понимания, каких результатов ожидать от проекта, какие показатели его считать успешными.

2. Недостаточное внимание руководства к проекту. Если руководство компаний не может сформулировать, что они хотят получить от системы электронного документооборота (СЭД), то, конечно, невозможно будет и четко спланировать проект: его этапы, необходимые ресурсы, показатели качества, ожидаемый результат.

3. Слабая вовлеченность в проект сотрудников. Чем выше активность персонала в проекте, тем выше вероятность, что нововведения будут отвечать ожиданиям коллектива и вызовут положительную реакцию.

4. Недооценка важности отдельных этапов проекта (например, информационное обследование, обучение пользователей, опытная эксплуатация). Часто недооценивается такой этап, как обследование. А ведь именно информационное обследование помогает выявить наиболее проблемные зоны и ключевые точки, определить участников и

потребителей результатов процессов, собрать материал для оценки трудоемкости доработок и перспектив внедрения системы.

Субъективные риски. Такие риски являются наиболее сложно управляемыми и прогнозируемыми.

1. Отсутствие навыков работы с компьютером. Несмотря на значительное развитие информационных технологий в компаниях за последнее десятилетие, отсутствие навыков использования ПК, низкая культура работы с информацией в электронном виде по-прежнему остаются существенным препятствием на пути внедрения автоматизированных систем. В результате персонал приходится обучать работе с компьютером, прежде чем внедрять СЭД.

2. Недостаточный опыт работы с информацией в электронном виде. Нередко проект по внедрению встречает довольно резкое сопротивление со стороны работников компании как среди простых служащих, так и среди руководителей высшего звена. Это обусловлено рядом причин:

нежелание обучаться новым методам работы; нежелание менять привычный порядок работы и взаимоотношений;

опасения того, что станут видны недостатки в работе, необоснованные временные потери, так как в процессе обследования и оптимизации процессов деятельность сотрудников становится прозрачной и контролируемой;

боязнь штрафных санкций, штатных изменений в связи с обнаружением зон с низкой эффективностью труда;

страх перед неумением работать в системе, боязнь того, что ошибки дискредитируют работника в глазах руководства или подчиненных.

3. Отсутствие доверия к внешним консультантам – еще одно препятствие на пути успешного проекта. Часто это можно наблюдать, когда на автоматизируемом предприятии слишком много ответственности возлагают на внешних специалистов, не поддерживая их авторитетом местного руководства, особенно, если в компании уже были неудачные попытки внедрить какую-либо систему или методику.

Технологические риски. Технологические риски могут существенно замедлить реализацию проекта, а также серьезно повлиять на ожидаемый результат. Более того, проект может быть остановлен.

1. Неготовность имеющейся в организации ИТ-инфраструктуры. Внедрение СЭД повлечет за собой увеличение количества пользователей ПК, переход к безбумажной обработке документов приведет к существенному увеличению нагрузки на серверы, необходимости хранить на них больший объем информации. В результате имеющаяся ИТ-инфраструктура может оказаться неготовой к новым методам работы, что приведет к низкой работоспособности системы, зависанию, сбоям и пр., длительная работа с документами за устаревшими мониторами будет утомительной и даже вредной для сотрудников.

2. Недостаточное исследование потребностей компании. При этом на стадии внедрения или эксплуатации может выясниться, что работа системы не соответствует ожиданиям: не поддерживаются необходимые сценарии работы, не выполняются нужные функции. Или, наоборот, система слишком сложна, но в реальной работе используется минимум возможностей.

3. Отсутствие нормативной базы. Неформализованные бизнес-процессы существенно затрудняют внедрение СЭД, так как при отсутствии четких правил работы и единых регламентов документооборота невозможна эффективная эксплуатация системы.

5. Проблемы применения электронной цифровой подписи в условиях глобализации информационного общества.

Проблемы применения электронной цифровой подписи можно выделить следующие:

1. Распространяемость технологии. Так, в Европе цифровые подписи начали работать еще в 1999 году, когда приняли Декларацию об электронных подписях. Технологию быстро внедрили в систему образования, здравоохранения, торговли и другие сферы. С 2016 года любое физическое или юридическое лицо получило разрешение на пользование электронной подписи по всему Евросоюзу. У нас в стране физические лица практически не пользуются подписями в обычной жизни. Но при дальнейшем развитии подобных технологий у каждого человека получится оформлять электронные документы для ребенка в школе или детском саду, или заключать согласие на предоставление услуг в различных организациях по электронной почте или другим способом, находясь дома и экономя время на поездки по городу.

2. Дороговизна технологии. Так, для получения и дальнейшего продления срока действия ЭЦП необходимо платить. В связи с этим, физические лица менее активно, чем юридические присоединяются к использованию технологии.

3. Надежность технологии. В связи с тем, что ЭЦП является аналогом собственноручной подписи необходимо обеспечивать и постоянно совершенствовать уровень ее защиты.

ТЕМА 8

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ БИБЛИОТЕЧНОГО ДЕЛА

1. Особенности информационных правоотношений, возникающих в области библиотечного дела. Законодательство в области библиотечного дела.

2. Субъекты в области библиотечного дела. Права и обязанности граждан и иных субъектов в области библиотечного дела.

3. Обязанности государства в области библиотечного дела.

4. Правовое регулирование взаимодействия библиотек.

5. Защита авторских прав при поиске и получении информации.

1. Особенности информационных правоотношений, возникающих в области библиотечного дела. Законодательство в области библиотечного дела.

Институт библиотечного дела представляет собой одно из направлений правового регулирования отношений информационной сферы в области обеспечения реализации права каждого на поиск, получение и передачу библиотечной информации (право на доступ к информации или право знать), которое является важнейшим правом человека и гражданина.

Библиотечное дело – направление культурной деятельности по созданию и развитию библиотек, формированию и обработке библиотечных фондов, организации библиотечного, информационного и справочно-библиографического обслуживания пользователей библиотек, научно-методического обеспечения деятельности библиотек (ст. 131 Кодекса о культуре).

Основными принципами организации работы библиотеки являются:

1) рациональное и оптимальное размещение библиотек в соответствии с демографическим составом населения и с учетом специфики развития отдельных регионов и отраслей;

2) взаимодействие библиотек и взаимное использование их информационных ресурсов, а также библиотечных каталогов, карточек, баз данных, справочно-библиографических изданий, предназначенных для поиска библиографической и иной информации;

3) государственно-общественный характер библиотечного управления.

Нормативная правовая база является информационным источником правовых знаний в любой области, включая библиотечное дело. Активное участие библиотек в построении информационного общества влечет за собой развитие профильного законодательства в рассматриваемой области.

Основные НПА, регулирующие библиотечное дело:

1. Конституция Республики Беларусь.

Часть 1 статьи 51: «Каждый имеет право на участие в культурной жизни. Это право обеспечивается общедоступностью ценностей отечественной и мировой культуры».

2. Модельный Библиотечный кодекс для государств – участников СНГ (1 часть – 1996 г., 2 часть – 1998 г.)

Библиотечное дело – отрасль информационной, культурно-просветительской и образовательной деятельности граждан и их объединений, включающая создание и развитие сети библиотек, формирование и обработку их фондов, организацию библиотечного, информационного и справочно-библиографического обслуживания пользователей, подготовку библиотечных кадров, научное и методическое обеспечение развития библиотек.

3. Кодекс о культуре (глава 18) – основной НПА, регулирующий библиотечное дело.

4. Постановление Совета Министров Республики Беларусь 29 января 2021 г. № 53 «О Государственной программе «Культура Беларуси» на 2021–2025 годы».

Подпрограмма 1 «Культурное наследие» направлена на решение следующих задач:

- сохранение культурного наследия;
- обеспечение доступности, качества и разнообразия услуг, предоставляемых библиотеками и музеями, выставочными организациями, парками культуры и отдыха, зоопарками;

- поддержка развития культур национальных меньшинств.

К наиболее динамичному направлению библиотечной деятельности следует отнести работу по обеспечению доступа все большего количества виртуальных пользователей к библиотечным ресурсам. В республике для нужд сельских жителей активно осуществляется нестационарное информационно-библиотечное обслуживание посредством более 100 библиобусов (передвижные библиотеки).

В библиотеках Беларуси создаются условия для работы людей с ограниченными возможностями. В регионах функционируют специализированные библиотеки для обслуживания людей с нарушением зрения. Для комфортного передвижения инвалидов-колясочников здание Национальной библиотеки Беларуси оборудовано специальными подъемными устройствами, есть лифт, созданы специализированные рабочие места для незрячих и слабовидящих посетителей.

5. Постановление Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66 «О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы».

Государственная программа развития цифровой экономики и информационного общества на 2016–2020 гг. предусматривала увеличение количества в местах общественного пользования точек доступа по технологии Wi-Fi для предоставления широкополосного доступа к государственным информационным ресурсам, а также создание республиканской платформы, действующей на основе технологий облачных вычислений.

Данная платформа создана в соответствии с Указом Президента Республики Беларусь «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» в целях дальнейшего развития в республике информационного общества, совершенствования инфраструктуры сети передачи данных, а также повышение уровня обслуживания. Предполагается поэтапный переход ведущих библиотек на использование ресурсов республиканской платформы.

Национальная библиотека Беларуси данный переход начала в 2018 г. заключив договор с ООО «Белорусские облачные технологии». В 2019 г. был осуществлен перенос

ИТ-инфраструктуры резервного центра обработки данных в основной центр обработки данных.

В 2020 г. на облачную платформу перенесены системы, обеспечивающие функционирование 6-ти региональных сводных каталогов (далее – РСЭК), генерируемых областными библиотеками республики совместно с другими библиотеками своих регионов. На 01.01.2021 участниками РСЭК были 44 библиотеки регионов с общим объемом 3,6 млн. записей.

2. Субъекты в области библиотечного дела. Права и обязанности граждан и иных субъектов в области библиотечного дела.

Субъектами библиотечного дела являются библиотеки и пользователи библиотек.

В соответствии со ст. 133 Кодекса о культуре **библиотека** – культурная организация или подразделение юридического лица, осуществляющее сбор и обеспечение сохранности документов для общего пользования.

Документ – носитель информации, в том числе электронный, на котором содержится информация в виде текста, аудио или изображения и который предназначен для передачи информации во времени и пространстве.

По форме собственности библиотеки делятся на государственные и частные.

По назначению библиотеки делятся на публичные и специальные.

Публичная библиотека – это библиотека, которая удовлетворяет универсальные информационные потребности пользователей библиотек.

Специальная библиотека – это библиотека, обеспечивающая информационные потребности пользователей библиотек, связанные с профессиональной деятельностью (производственные библиотеки), образовательной деятельностью (библиотеки образовательных учреждений), научной деятельностью (научные библиотеки) или иной специальной деятельностью.

В зависимости от территории деятельности библиотеки делятся на сельские, поселковые городского типа, городские, районные, областные, республиканские.

Основными задачами библиотек являются:

- наполнение библиотечных фондов документами и обеспечение их сохранности;
- осуществление обработки документов, создание справочно-библиографического аппарата;
- оказание библиотечных, информационных и справочно-библиографических услуг пользователям библиотек в соответствии с их потребностями и интересами;
- проведение культурно-просветительской работы, направленной на содействие культурному развитию пользователей библиотек.

Библиотеки имеют право:

- 1) самостоятельно определять содержание, формы и методы своей деятельности в соответствии с целями и функциями, установленными в уставе (положении);
- 2) определить источники библиотечного фонда;
- 3) осуществлять приносящую доход деятельность, в том числе оказывать платные услуги;
- 4) формировать обменные библиотечные фонды;
- 5) исключать и продавать документы из библиотечных коллекций;
- 6) устанавливать по согласованию с учредителем библиотеки, являющейся юридическим лицом, или юридическим лицом, подразделением которого является библиотека, правила пользования библиотекой, порядок регистрации пользователей библиотеки;
- 7) определять залоговую стоимость наиболее ценных изданий при их выпуске, а также в иных случаях, установленных правилами пользования библиотекой;
- 8) принимать меры по возмещению вреда, причиненного пользователями библиотеки, в соответствии с гражданским законодательством;

9) определять условия использования библиотечных фондов на основании договоров с юридическими лицами, гражданами, в том числе с индивидуальными предпринимателями;

10) участвовать в реализации государственных и иных программ, направленных на сохранение, развитие, распространение и (или) популяризацию культуры;

11) сотрудничать с зарубежными библиотеками, иностранными и международными юридическими лицами, в том числе осуществлять международный документооборот, вступать в установленном порядке в международные организации, участвовать в реализации международных программ;

12) вступать в библиотечные ассоциации (союзы);

13) приобретать, создавать, формировать и использовать информационные ресурсы;

14) собирать документы в электронном виде, при необходимости создавать копии документов в электронном виде с соблюдением требований законодательства об авторском праве и смежных правах.

2. Библиотеки обязаны:

1) способствовать обеспечению прав пользователей библиотек, предусмотренных Кодексом о культуре;

2) обслуживать пользователей библиотеки в соответствии с ее уставом (положением) и правилами пользования библиотекой;

3) не использовать информацию о пользователях библиотеки и их запросах в целях, отличных от научных и библиотечных;

4) облегчить доступ пользователей библиотек к национальным и глобальным базам данных;

5) обеспечивать сохранность библиотечных фондов;

6) при наличии в фондах библиотеки книжных памятников обеспечить их сохранность и включение в Государственный реестр книжных памятников Республики Беларусь, другие сводные каталоги, базы данных;

7) при обеспечении пользователей библиотеки актуальной правовой информацией Республики Беларусь обеспечить доступ к справочной правовой информации.

Юридические лица, граждане, в том числе индивидуальные предприниматели, которым предоставляются библиотечные услуги, являются их пользователями.

Пользователи библиотеки имеют право на библиотечное, информационное и справочно-библиографическое обслуживание в соответствии со своими потребностями и интересами.

Право на библиотечное, информационное и справочно-библиографическое обслуживание обеспечивается путем:

– создания различных типов библиотек;

– содействием доступу к национальным и глобальным базам данных;

– организации межбиблиотечного абонементов;

– электронной доставки документов;

– организации библиотечного, информационного и справочно-библиографического обслуживания пользователей библиотек по месту жительства (местонахождения), работы (службы), учебы, отдыха;

– использованием нестационарных форм обслуживания;

– созданием и функционированием на базе государственных публичных библиотек центров публичной правовой информации.

Пользователи государственных библиотек имеют право:

– бесплатно получать полную информацию о составе и содержании библиотечных фондов;

– получать бесплатную консультационную помощь в поиске источников информации;

- бесплатно получать во временное пользование документы из библиотечных фондов;
- получать доступ к информационным ресурсам библиотек;
- получать документы или их копии по межбиблиотечному абонементу;
- принимать участие в культурных мероприятиях, проводимых библиотеками;
- использовать технические средства с автономным питанием без звуковой сигнализации в зонах обслуживания пользователей библиотек, за исключением копировальных устройств (сканеры, аудио-, фото- и видеотехника), мобильных телефонов и других технических средств в целях фото- и видеосъемки документов из библиотечных фондов;
- пользоваться библиотечными услугами, в том числе платными;
- иные права в соответствии с законодательными актами.

Лица с нарушением зрения и лица, лишенные зрения, имеют право на получение документов на специальных материальных носителях информации.

Инвалиды и иные лица с физическими недостатками имеют преимущественное право на получение документов из библиотечных фондов публичных библиотек через нестационарные формы обслуживания.

Пользователи библиотек имеют право участвовать в деятельности попечительских советов, объединений пользователей библиотек.

Пользователи библиотеки обязаны:

- соблюдать правила пользования библиотекой;
- бережно относиться к библиотечным фондам;
- возвращать документы, полученные из фондов библиотеки, в сроки, установленные библиотекой;
- своевременно и в соответствии с порядком регистрации пользователей библиотеки проходить перерегистрацию пользователей библиотеки;
- при получении документов с дефектами сообщить об этом библиотекарю;
- выполнять иные обязанности в соответствии с законодательными актами.

Регистрация граждан в качестве пользователей библиотеки осуществляется непосредственно в библиотеке или на официальном сайте библиотеки в глобальной компьютерной сети Интернет.

Регистрация юридических лиц и индивидуальных предпринимателей в качестве пользователей библиотек осуществляется на основании договора на библиотечное, информационное и справочно-библиографическое обслуживание.

Порядок регистрации пользователей библиотеки утверждается заведующим библиотекой, являющейся юридическим лицом, по согласованию с учредителем библиотеки или руководителем юридического лица, подразделением которого является библиотека.

3. Обязанности государства в области библиотечного дела.

В основе государственной политики в области библиотечного дела лежит принцип создания условий для всеобщей доступности информации и культурных ценностей, собираемых и предоставляемых в пользование библиотеками.

Государственные органы, органы местного самоуправления выступают гарантами прав пользователей библиотек и не вмешиваются в профессионально-творческую деятельность библиотек, за исключением случаев, когда такая деятельность ведет к пропаганде войны, насилия и жестокости, расовой, национальной, религиозной, классовой и иной исключительности или нетерпимости, а также порнографии.

Государство поддерживает развитие библиотечного дела путем его финансирования, проведения протекционистской налоговой, кредитной и ценовой политики, разрабатывает и финансирует целевые программы развития библиотечного дела. Органы государственной власти организуют координацию межрегиональных и

межведомственных связей по библиотечному обслуживанию населения, в том числе в целях информатизации общества.

Государство поддерживает развитие библиотечного обслуживания наименее социально и экономически защищенных слоев и групп населения (детей, юношества, инвалидов, пенсионеров, беженцев, безработных, жителей сельской местности, труднодоступных районов).

Органы государственной власти стимулируют путем материальной поддержки библиотеки негосударственных форм собственности, организующие бесплатное общедоступное обслуживание населения.

Органы государственной власти обеспечивают:

1) регистрацию и контроль за соблюдением особого режима хранения и использования библиотечных фондов, отнесенных к национальному культурному достоянию;

2) создание и финансирование национальных библиотек, управление этими библиотеками;

3) государственную политику в области подготовки и переподготовки библиотечных кадров, занятости, оплаты труда, установления социальных гарантий и льгот для работников библиотек;

4) создание и финансирование образовательных учреждений, осуществляющих подготовку и переподготовку библиотечных кадров, управление этими образовательными учреждениями;

5) содействие научным исследованиям и методическому обеспечению в области библиотечного дела, а также их финансированию;

6) установление государственных библиотечных стандартов и нормативов, организацию системы информационного обеспечения библиотечного дела;

7) организацию государственного статистического учета библиотечной деятельности.

Органы местного самоуправления обеспечивают:

1) гарантированное финансирование комплектования и сохранности библиотечных фондов государственных и муниципальных библиотек;

2) реализацию прав граждан на библиотечное обслуживание.

Органы государственной власти и органы местного самоуправления не вправе принимать решения и осуществлять действия, которые влекут ухудшение материально-технического обеспечения действующих библиотек, находящихся на бюджетном финансировании, их перевод в помещения, не соответствующие требованиям охраны труда, хранения библиотечных фондов и библиотечного обслуживания.

Решения указанных органов, а также действия их должностных лиц, ущемляющие интересы библиотек и их пользователей, могут быть обжалованы в судебном порядке.

Для разработки предложений по вопросам библиотечного дела, совершенствования деятельности и взаимодействия библиотек, а также оказания им методической помощи при Министерстве культуры создается Республиканский библиотечный совет.

Республиканский библиотечный совет:

– осуществляет подготовку предложений по развитию библиотечного дела;

– способствует усовершенствованию координации и кооперации библиотечного дела;

– выявляет и исследует актуальные проблемы и определяет перспективы развития библиотечного дела в соответствии с современными научными разработками и практикой деятельности библиотек;

– готовит предложения по решению текущих проблем библиотечного дела и вносит их на рассмотрение государственных органов;

– изучает и обобщает положительный опыт библиотек, разрабатывает предложения по его использованию и развитию;

– содействует активной реализации культурных проектов, государственных и иных программ, направленных на сохранение, развитие, распространение и (или) популяризацию культуры;

– осуществляет подготовку предложений по совершенствованию законодательства о культуре в части регулирования библиотечного дела, укрепления связей с отечественными и зарубежными библиотеками;

– принимает решения по жалобам на заключения комиссий государственных библиотек по оценке стоимости культурных ценностей, составляющих Библиотечный фонд Республики Беларусь.

4. Правовое регулирование взаимодействия библиотек.

Сеть библиотек – это совокупность библиотек, объединенных по своему назначению, территориальной принадлежности и (или) учредителю и имеющих координационно-методический центр.

Совокупная сеть библиотек состоит из сетей общедоступных и сетей специальных библиотек.

Государственное учреждение «Национальная библиотека Беларуси» является координационным и методическим центром совокупной сети библиотек. Отнесение библиотек к определенным библиотечным сетям осуществляется их учредителями. Среди координационно-методических центров библиотечных сетей выделяют координационно-методические центры республиканского, областного, районного и городского уровней.

Координационно-методическими центрами республиканского уровня являются:

1) в сетях общедоступных библиотек – государственное учреждение «Национальная библиотека Беларуси»;

2) в сети специальных библиотек – государственные учреждения «Президентская библиотека Республики Беларусь», «Республиканская научно-техническая библиотека», «Республиканская научная медицинская библиотека», «Центральная научная библиотека имени Якуба Коласа Национальной академии наук Беларуси», «Белорусская сельскохозяйственная библиотека им. И.С. Лупиновича НАН Беларуси», Научно-педагогическая библиотека учреждения «Главный информационно-аналитический центр Министерства образования Республики Беларусь» и Фундаментальная библиотека Белорусского государственного университета.

Взаимодействие библиотек осуществляется в соответствии с основными принципами деятельности библиотек, включая обмен и перераспределение документами, организацию и функционирование национальной системы межбиблиотечного абонементов.

Обмен документами и перераспределение документов – безвозмездная передача из одной библиотеки излишне тиражированных (дубликатных) и непрофильных для этой библиотеки документов в другую библиотеку для пополнения ее фонда.

Передача документов, составляющих библиотечный фонд Республики Беларусь и находящихся на постоянном хранении в государственных библиотеках, допускается только в государственные библиотеки.

В целях обмена документами и распространения документов библиотеки создают обменные фонды.

Обменные фонды формируются из чрезмерно дублирующихся (повторяющихся) непрофильных для данной библиотеки документов, которые:

– исключен из основного фонда;

– полученные в качестве безвозмездной (спонсорской) помощи, пожертвований.

Для взаимного информирования о составе обменных фондов библиотеки регулярно формируют и распространяют (в том числе по электронным каналам) списки (указатели, списки) документов, предназначенных для обмена и перераспределения документов.

Межбиблиотечный абонемент – форма библиотечного обслуживания пользователей библиотек, основанная на взаимном использовании информационных ресурсов и

справочно-библиографического аппарата библиотек путем предоставления пользователям библиотек оригиналов документов или их копий, полученных из другой библиотеки.

Услуги межбиблиотечного абонемента оказываются на основании договоров (соглашений) между библиотеками, являющимися юридическими лицами, и (или) юридическими лицами, подразделением которых библиотека является, или грамот.

Пользователи библиотеки не ограничены в выборе библиотеки для отправки заказов на доставку документов. Доставка документов осуществляется в соответствии с правилами пользования библиотекой, в которой находится документ.

Заказ на межбиблиотечный абонемент оформляется на бланке заказа, который рассылается по любым каналам связи (почта, электронная почта и т.п.). Бланк заказа заполняется разборчиво на каждый отдельный документ, без произвольных сокращений, с указанием всех реквизитов, предусмотренных в бланке заказа.

Форма бланка приказа устанавливается Министерством культуры.

Корпоративное взаимодействие библиотек осуществляется в соответствии с основными принципами библиотечной деятельности путем формирования и использования информационных ресурсов.

Информационные ресурсы государственных библиотек являются неотъемлемой частью информационных ресурсов Республики Беларусь.

Библиотеки участвуют в формировании сводного электронного каталога библиотек Беларуси и других корпоративных информационных ресурсов.

Сводный электронный каталог библиотек Беларуси является информационным ресурсом, отражающим состав, содержание и структуру Библиотечного фонда Республики Беларусь.

В целях повышения качества информационно-библиотечных услуг и эффективного использования глобальных информационных ресурсов библиотеки на корпоративной основе приобретают эти ресурсы и предоставляют к ним доступ. Порядок корпоративного взаимодействия определяется договорами между библиотеками, являющимися юридическими лицами, и (или) юридическими лицами, подразделением которых является библиотека.

Координацию корпоративного взаимодействия библиотек осуществляет государственное учреждение «Национальная библиотека Беларуси».

5. Защита авторских прав при поиске и получении информации.

Статья 37 Закона Республики Беларусь от 17 мая 2011 г. № 262-З «Об авторском праве и смежных правах» регламентирует свободное использование произведений библиотеками.

Допускается без согласия автора или иного правообладателя и без выплаты авторского вознаграждения, но с обязательным указанием автора произведения предоставление библиотеками экземпляров правомерно опубликованных произведений во временное безвозмездное пользование. При этом выраженные в электронной форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, в том числе в порядке взаимного использования библиотечных ресурсов, могут предоставляться только в помещениях библиотек, в том числе с использованием локальных компьютерных сетей, а также удаленного доступа, при условии использования технических средств защиты авторского права или смежных прав, исключающих для пользователей возможность создания полных копий этих произведений на бумажном носителе или в электронной форме.

Библиотеки могут осуществлять репродуцирование и иное воспроизведение без цели извлечения прибыли правомерно опубликованных произведений для комплектования библиотечных фондов, замены утраченных, уничтоженных или ставших непригодными для использования экземпляров произведений.

Статьи и иные малообъемные произведения, правомерно опубликованные в сборниках, а также газетах, журналах и других печатных средствах массовой информации, отрывки из правомерно опубликованных литературных и иных произведений могут быть воспроизведены путем репродуцирования и иного воспроизведения без цели извлечения прибыли библиотеками по запросам физических и юридических лиц в образовательных и исследовательских целях.

ТЕМА 9

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ АРХИВНОГО ДЕЛА И АРХИВОВ

- 1. Особенности информационных правоотношений, возникающих в области архивного дела и архивов. Законодательство в области архивного дела и архивов.**
- 2. Субъекты информационных правоотношений в области архивного дела и архивов. Права и обязанности граждан в области архивного дела и архивов.**
- 3. Объекты информационных правоотношений в области архивного дела и архивов. Правовой режим архивов.**
- 4. Государственное управление архивным делом.**
- 5. Правовые основы комплектования, хранения, учета и использования архивных фондов. Порядок доступа к архивным фондам и использования архивных документов.**

1. Особенности информационных правоотношений, возникающих в области архивного дела и архивов. Законодательство в области архивного дела и архивов.

Архивное дело – деятельность по созданию и комплектованию архивов, организации хранения, учета и использования архивных документов.

Документы, хранящиеся в государственных архивах, территориальных (городских или районных) архивах (за исключением документов, переданных в эти архивы на основании договора хранения), государственных музеях и библиотеках, находятся только в собственности государства.

Документы, образовавшиеся в процессе деятельности государственных органов, иных государственных организаций и деятельности подчиненных им (входящих в состав, систему) органов и (или) организаций, расположенных на территории Республики Беларусь, находятся только в собственности государства.

В целях удовлетворения нужд граждан, общества и государства в использовании информации, содержащейся в архивных документах, архивы осуществляют:

- информационное обеспечение пользователей в соответствии с их запросами;
- предоставление архивных документов пользователям с учетом требований, предусмотренных статьей 28 Закона об архивном деле;
- публикацию архивных документов;
- популяризацию архивных документов в средствах массовой информации;
- организацию выставок архивных документов.

2. Субъекты информационных правоотношений в области архивного дела и архивов. Права и обязанности граждан в области архивного дела и архивов.

Государственные органы, иные организации и индивидуальные предприниматели обязаны обеспечивать в течение установленных сроков накопление, хранение, учет и использование образующихся в процессе их деятельности документов.

Государственные органы, иные организации, в процессе деятельности которых образуются документы государственной части Национального архивного фонда, обязаны

обеспечивать их передачу в государственные архивы по истечении сроков, установленных частями второй и третьей статьи 20 Закона об архивном деле.

Представительства иностранных организаций обязаны обеспечивать в течение установленных сроков накопление, хранение, учет и использование образующихся в процессе их деятельности документов по личному составу работников этих представительств и передачу их в территориальные (городские или районные) архивы в случае, предусмотренном частью восьмой статьи 19 Закона об архивном деле.

Негосударственные организации и граждане также имеют право на участие в комплектовании государственных архивов и включение своих документов в состав государственной части Национального архивного фонда.

Республиканский орган государственного управления в сфере архивного дела и делопроизводства устанавливает перечень типовых документов с указанием сроков хранения.

Государственные органы, иные государственные организации по согласованию с республиканским органом государственного управления в сфере архивного дела и делопроизводства устанавливают перечни документов, образующихся в процессе их деятельности и деятельности подчиненных им (входящих в состав, систему) органов и (или) организаций, с указанием сроков хранения.

Негосударственные организации могут устанавливать перечни документов, образующихся в процессе их деятельности и деятельности подчиненных им (входящих в состав, систему) организаций, с указанием сроков хранения. Негосударственные организации, являющиеся источниками комплектования государственных архивов, устанавливают перечни документов, образующихся в процессе их деятельности и деятельности подчиненных им (входящих в состав, систему) организаций, с указанием сроков хранения по согласованию с государственными архивами.

3. Объекты информационных правоотношений в области архивного дела и архивов. Правовой режим архивов.

Архив – организация или структурное подразделение организации, если иное не предусмотрено частью четвертой статьи 13 Закона об архивном деле, осуществляющие прием, хранение, учет и использование архивных документов.

Архивы в Республике Беларусь создаются в виде государственных архивов, территориальных (городских или районных) архивов, архивов государственных органов, иных организаций. Государственные органы, иные организации имеют право на создание объединенных архивов.

Государственными архивами в Республике Беларусь являются республиканские, областные (г. Минска) и зональные архивы.

Государственные архивы являются научно-исследовательскими и методическими центрами по работе с документами Национального архивного фонда.

Государственные архивы осуществляют прием, постоянное хранение, учет и использование документов государственной части Национального архивного фонда, а в случаях, предусмотренных частью второй статьи 16 Закона об архивном деле, – иных документов Национального архивного фонда.

Территориальные (городские или районные) архивы осуществляют прием, хранение, учет и использование документов реорганизованных, ликвидированных организаций, прекративших деятельность индивидуальных предпринимателей и представительств иностранных организаций, за исключением документов, подлежащих передаче на постоянное хранение в государственные архивы.

Архивы государственных органов, иных организаций осуществляют прием, хранение, учет и использование документов, образующихся в процессе деятельности этих государственных органов, иных организаций, а в случаях, предусмотренных частями

четвертой–шестой статьи 19 Закона об архивном деле, – документов подчиненных им (входящих в состав, систему) органов и (или) организаций.

Республиканские архивы создаются по решению республиканского органа государственного управления в сфере архивного дела и делопроизводства, а областные (г. Минска) и зональные архивы – по решению соответствующих областных (Минского городского) исполнительных комитетов согласно системе государственных архивных учреждений, утвержденной Советом Министров Республики Беларусь.

Территориальные (городские или районные) архивы создаются соответствующими местными исполнительными и распорядительными органами по согласованию с республиканским органом государственного управления в сфере архивного дела и делопроизводства.

Архивы государственных органов, иных организаций создаются по решению руководителей этих государственных органов, иных организаций.

В организациях, в которых установление штатных должностей работников архива не предусмотрено, выполнение функций по осуществлению приема, хранения, учета и использования архивных документов возлагается на назначаемое руководителем организации лицо.

Государственные органы, иные организации, индивидуальные предприниматели, представительства иностранных организаций могут передавать образовавшиеся в процессе их деятельности документы в государственные архивы, территориальные (городские или районные) архивы, иные организации на основании договора хранения.

Запрещается передача документов Национального архивного фонда государственных органами, иными организациями, являющимися источниками комплектования государственных архивов, на основании договора хранения без согласования с соответствующими государственными архивами.

Права владения, пользования и (или) распоряжения передаваемыми на основании договора хранения документами сохраняются за государственными органами, иными организациями, индивидуальными предпринимателями, представительствами иностранных организаций, в процессе деятельности которых эти документы образовались.

4. Государственное управление архивным делом.

Государственное регулирование и управление в сфере архивного дела и делопроизводства осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, республиканским органом государственного управления в сфере архивного дела и делопроизводства, местными исполнительными и распорядительными органами в пределах их компетенции.

Государственное регулирование и управление в сфере архивного дела и делопроизводства включают:

- разработку и реализацию единой государственной политики в сфере архивного дела и делопроизводства;

- единых принципов организации архивного дела и делопроизводства, порядка накопления, хранения, учета и использования архивных документов, создания и деятельности архивов и осуществление контроля за соблюдением этих принципов и порядка;

- комплектование государственных архивов, территориальных (городских или районных) архивов, архивов государственных органов и иных государственных организаций, обеспечение постоянного хранения документов государственной части Национального архивного фонда, их учета и использования;

- решение вопросов о вывозе архивных документов из Республики Беларусь.

Республиканский орган государственного управления в сфере архивного дела и делопроизводства осуществляет управление деятельностью подчиненных ему

государственных организаций с анализом эффективности работы этих организаций и выработкой предложений по ее повышению.

Основными направлениями деятельности в сфере архивного дела и делопроизводства являются:

- формирование Национального архивного фонда;
- постоянное хранение документов государственной части Национального архивного фонда, их учет и использование;
- установление общих требований к документированию и организации работы с документами;
- осуществление контроля за соблюдением законодательства в сфере архивного дела и делопроизводства в государственных органах, иных организациях, оказание им методической помощи;
- подготовка и повышение квалификации кадров.

Контроль за соблюдением законодательства в сфере архивного дела и делопроизводства осуществляется в соответствии с законодательством о контрольной (надзорной) деятельности Департаментом по архивам и делопроизводству Министерства юстиции.

5. Правовые основы комплектования, хранения, учета и использования архивных фондов. Порядок доступа к архивным фондам и использования архивных документов.

Хранение документов Национального архивного фонда осуществляется на возмездной и безвозмездной основе.

Постоянное хранение документов государственной части Национального архивного фонда осуществляют государственные архивы на безвозмездной основе.

Документы негосударственной части Национального архивного фонда могут храниться их собственниками самостоятельно или на возмездной основе в государственных архивах, территориальных (городских или районных) архивах и иных организациях на основании договора хранения, а также передаваться на безвозмездной основе в государственные архивы на основании договора, предусматривающего передачу права собственности на документы государству.

Документы негосударственной части Национального архивного фонда, предусмотренные частью третьей настоящей статьи, собственники которых без уважительных причин не продлили договор хранения и не востребовали указанные документы в течение сроков, установленных этим договором, переходят по судебному постановлению в собственность государства.

В случае невозмещения собственником расходов на хранение документов негосударственной части Национального архивного фонда в государственном архиве, территориальном (городском или районном) архиве и иной организации указанные архивы и иная организация имеют право вернуть собственнику эти документы и потребовать возмещения расходов в порядке, установленном договором хранения.

Хранение, учет и использование научно-технической документации, кино-, фото-, фоно- и видеодокументов, а также особо ценных и уникальных документов осуществляются в порядке, установленном для этих видов документов республиканским органом государственного управления в сфере архивного дела и делопроизводства.

Собственники особо ценных и уникальных документов обязаны создавать за свой счет их страховые копии и фонды пользования. Порядок создания и хранения страховых копий устанавливается республиканским органом государственного управления в сфере архивного дела и делопроизводства.

Документы в электронном виде, в том числе электронные документы, образовавшиеся в информационной системе государственного органа, иной организации, хранятся в этой информационной системе до их передачи на хранение в архив

государственного органа, иной организации, а не подлежащие передаче на хранение в архив – до их уничтожения.

Документы в электронном виде, в том числе электронные документы, установленный нормативными правовыми актами срок хранения которых превышает 10 лет, включая документы постоянного хранения, передаются из информационной системы государственного органа, иной организации на временное хранение в информационную систему архива государственного органа, иной организации.

Документы в электронном виде, в том числе электронные документы, государственной части Национального архивного фонда по истечении срока временного хранения, установленного частью третьей статьи 20 Закона, передаются из информационной системы архива государственного органа, иной организации на постоянное хранение в государственный архив посредством информационной системы архива электронных документов Национального архивного фонда Республики Беларусь.

Порядок функционирования информационной системы архива электронных документов Национального архивного фонда Республики Беларусь определяется Советом Министров Республики Беларусь.

Информационная система, в которой осуществляется электронное информационное взаимодействие государственных органов, иных организаций, должна обеспечивать передачу государственными органами, иными организациями образовавшихся в ней документов в электронном виде, в том числе электронных документов, постоянного хранения в государственный архив посредством информационной системы архива электронных документов Национального архивного фонда Республики Беларусь.

Требования к информационной системе, в которой осуществляется электронное информационное взаимодействие государственных органов, иных организаций, в части передачи документов в электронном виде, в том числе электронных документов, в архив государственного органа, иной организации при создании и (или) модернизации этой информационной системы согласовываются заказчиком информационной системы с республиканским органом государственного управления в сфере архивного дела и делопроизводства.

Порядок передачи документов в электронном виде, в том числе электронных документов, в архив государственного органа, иной организации, государственный архив, их хранения и учета определяется республиканским органом государственного управления в сфере архивного дела и делопроизводства.

При реорганизации организаций их документы передаются правопреемникам, если иное не установлено частью четвертой настоящей статьи.

В случае реорганизации организаций в форме разделения, выделения, слияния, присоединения их архивные фонды, сформированные до реорганизации, не разделяются и не объединяются.

В случае реорганизации организаций, являющихся источниками комплектования государственных архивов, в форме разделения, выделения, слияния, присоединения их документы Национального архивного фонда по согласованию с государственными архивами, источниками комплектования которых они являются, могут быть переданы на постоянное хранение в государственные архивы до истечения сроков временного хранения, установленных частями второй и третьей статьи 20 Закона.

При преобразовании государственных организаций, являющихся источниками комплектования государственных архивов, в организации иной формы собственности их документы Национального архивного фонда передаются в соответствующие государственные архивы, а документы с неистекшими сроками временного хранения, в том числе по личному составу, – в территориальные (городские или районные) архивы или архивы вышестоящих организаций (архивы учредителей (участников)).

При ликвидации организаций, являющихся источниками комплектования государственных архивов, их документы Национального архивного фонда передаются в

соответствующие государственные архивы, а документы с истекшими сроками временного хранения, в том числе по личному составу, – в территориальные (городские или районные) архивы или архивы вышестоящих организаций (архивы учредителей (участников)).

При ликвидации организаций, не являющихся источниками комплектования государственных архивов, прекращении деятельности индивидуальных предпринимателей их документы передаются в территориальные (городские или районные) архивы или архивы вышестоящих организаций (архивы учредителей (участников)).

При передаче документов ликвидируемой организацией в архив ее вышестоящей организации (архив учредителя (участника)) в случаях, предусмотренных частями пятой и шестой настоящей статьи, вышестоящая организация (учредитель (участник)) в течение трех рабочих дней после передачи документов представляет в территориальный (городской или районный) архив сведения о видах принятых документов, в том числе по личному составу, и сроках их хранения.

При прекращении деятельности представительств иностранных организаций документы по личному составу работников этих представительств передаются в территориальные (городские или районные) архивы.

При передаче ликвидируемой организацией в государственный архив документов Национального архивного фонда в случае, предусмотренном частью пятой настоящей статьи, ликвидируемая организация в течение трех рабочих дней после передачи документов представляет в территориальный (городской или районный) архив сведения о переданных документах.

В случае смерти гражданина, являющегося источником комплектования государственного архива, и при отсутствии у него наследников документы этого гражданина передаются в государственный архив.

Архивы обеспечивают пользователям доступ к архивным документам. При использовании архивных документов указание пользователями ссылки на место их хранения является обязательным.

Порядок пользования документами, хранящимися в государственных архивах, территориальных (городских или районных) архивах, устанавливается республиканским органом государственного управления в сфере архивного дела и делопроизводства, а документами, хранящимися в архивах государственных органов, иных организаций, – их руководителями в соответствии с законодательством.

Доступ к документам негосударственной части Национального архивного фонда осуществляется в порядке, установленном собственником этих документов в соответствии с законодательством.

Порядок пользования документами Национального архивного фонда, переданными негосударственными организациями и гражданами в государственные архивы, определяется договорами, предусмотренными частью третьей статьи 18 Закона.

Порядок пользования архивными документами, содержащими государственные секреты, коммерческую и иную охраняемую законом тайну, особо ценными и уникальными документами, а также архивными документами, физическое состояние которых является неудовлетворительным, устанавливается Законом и иными законодательными актами.

Доступ к архивным документам, на которые распространяется действие законодательства об авторском праве и смежных правах, и их использование осуществляются в соответствии с требованиями законодательства об авторском праве и смежных правах.

В случае изъятия (выемки) документов, находящихся на постоянном хранении, а также документов по личному составу их возврат является обязательным.

Доступ к архивным документам ограничивается, если есть основания считать, что это:

повлечет разглашение государственных секретов, коммерческой и иной охраняемой законом тайны;

может нанести вред сохранности архивных документов;

нарушает права и законные интересы граждан;

повлечет иное нарушение законодательства.

Вывоз из Республики Беларусь на постоянное хранение оригиналов архивных документов запрещается.

Порядок временного вывоза оригиналов архивных документов из Республики Беларусь, а также порядок ввоза в Республику Беларусь либо транзита через ее территорию архивных документов других государств устанавливаются законодательством о внешнеэкономической деятельности, законодательством о таможенном регулировании, а также международными договорами Республики Беларусь и международно-правовыми актами, составляющими право Евразийского экономического союза.

ТЕМА 10 ИНТЕРНЕТ И ЕГО ПРАВОВОЕ РЕГУЛИРОВАНИЕ

1. Государственное регулирование национального сегмента сети Интернет.

2. Особенности правового регулирования отношений при реализации права на поиск, получение и потребление информации в глобальной компьютерной сети Интернет.

3. Вопросы правового обеспечения информационной безопасности в глобальной компьютерной сети Интернет.

4. Зарубежный опыт правового регулирования отношений в глобальной компьютерной сети Интернет.

5. Правовая основа электронной торговли, электронного бизнеса.

1. Государственное регулирование национального сегмента сети Интернет.

В Республике Беларусь нормативно не закреплено понятие «Интернет», хотя сам термин используется довольно часто в актах законодательства.

Сеть Интернет – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи, при доступе к которой возникают (изменяются, прекращаются) информационные отношения между физическими и юридическими лицами, государственными органами и организациями, иными лицами, использующими информационные технологии.

В целях обеспечения защиты интересов личности, общества и государства в информационной сфере, создания условий для дальнейшего развития национального сегмента глобальной компьютерной сети Интернет, повышения качества и доступности предоставляемой гражданам и юридическим лицам информации о деятельности государственных органов, иных организаций и интернет-услуг принят Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет».

Под **национальным сегментом сети Интернет** понимается совокупность информационных сетей, систем и ресурсов, имеющих подключение к сети Интернет, размещенных на территории Республики Беларусь и (или) использующих доменные имена в национальной доменной зоне, которую образуют доменные зоны «.by» и «.бел».

Информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 18 июня 2010 г. № 47 «О регистрации доменных имен в национальной доменной зоне» утверждена Инструкция о регистрации доменных имен в национальной доменной зоне.

Доменная зона – область иерархического пространства доменных имен глобальной компьютерной сети Интернет, которая обозначается уникальным доменным именем.

Доменное имя (домен) – символьное (буквенно-цифровое) обозначение, сформированное в соответствии с международными правилами адресации сети Интернет, предназначенное для поименованного обращения к интернет-ресурсу и связанное при его делегировании с определенным сетевым адресом.

Интернет-ресурс – интернет-сайт, страница интернет-сайта, веб-портал, форум, блог, чат, приложение для мобильного устройства и другие ресурсы, имеющие подключение к сети Интернет.

Доменные имена могут быть первого, второго, третьего и последующих уровней. Второй и последующие уровни доменного имени определяются порядковым номером расположенной слева от доменного имени первого уровня «.by» или «.бел» последовательности символов, разделенных точкой.

Доменное имя в доменной зоне «.by» должно содержать не менее двух и не более шестидесяти трех букв латинского алфавита, цифр, символов «дефис» («-»), не должно начинаться, заканчиваться символом «дефис» («-»), а также содержать символ «дефис» («-») в третьей и четвертой позициях одновременно.

Доменное имя в доменной зоне «.бел» формулируется с использованием букв белорусского или русского алфавита, цифр, символов «дефис» («-») и «апостроф» («'»), которые при их переводе в латинскую транслитерацию составляют в совокупности не менее двух и не более шестидесяти трех букв, цифр, символов, не должно начинаться и заканчиваться символами «дефис» («-») и (или) «апостроф» («'»).

При выборе доменного имени, в том числе в случае его регистрации по результатам проведения аукциона, заявителю следует избегать названий, тождественных или сходных до степени смешения с наименованиями зарегистрированных средств индивидуализации участников гражданского оборота, товаров (работ, услуг), если заявитель не является обладателем права на фирменное наименование, владельцем товарного знака и знака обслуживания, лицом, обладающим правом пользования географическим указанием.

Заявитель несет ответственность за выбор доменного имени, а также за возможные нарушения прав третьих лиц, связанные с выбором и регистрацией домена, несет риск убытков, обусловленных такими нарушениями.

Администратор национальной доменной зоны – Оперативно-аналитический центр при Президенте Республики Беларусь.

Регистратор – юридическое лицо Республики Беларусь, осуществляющее регистрацию доменных имен в национальной доменной зоне и участвующее в формировании базы данных;

Регистрация доменного имени – внесение в базу данных сведений о домене, его владельце и иной информации, предусмотренной Инструкцией.

Функции регистратора может выполнять юридическое лицо Республики Беларусь, с которым администратором национальной доменной зоны заключено соглашение о взаимодействии и которое должно обеспечивать наличие:

– чистых активов стоимостью в эквиваленте не менее 2600 базовых величин на основании данных бухгалтерского баланса и расчета стоимости чистых активов (для юридических лиц, применяющих упрощенную систему налогообложения и ведущих учет в книге учета доходов и расходов, – на основании данных такой книги) на первое число первого месяца квартала, в котором заключается соглашение о взаимодействии, а также в течение всего периода осуществления деятельности по регистрации доменных имен;

– информационной системы регистрации доменных имен, соответствующей требованиям законодательства (на дату заключения соглашения о взаимодействии, а также в течение всего периода осуществления деятельности по регистрации доменов).

Срок действия регистрации доменного имени составляет по выбору заявителя один или два года и указывается в заявке на регистрацию домена.

Окончание срока действия договора на регистрацию определяется окончанием срока действия регистрации доменного имени.

Срок действия регистрации домена может быть продлен неограниченное число раз посредством продления договора на регистрацию каждый раз на один или два года по выбору владельца домена.

Регистратор не позднее чем за один месяц до истечения срока действия договора на регистрацию направляет владельцу домена напоминание об окончании срока действия договора на регистрацию и возможности его продления.

Владелец домена имеет право направить заявку на продление договора на регистрацию и оплатить продление срока действия регистрации домена не ранее чем за два месяца до окончания срока действия текущей регистрации.

Договор на регистрацию считается продленным после получения регистратором от владельца домена заявки на продление и оплаты за продление срока действия регистрации домена.

Сведения о продлении срока действия регистрации доменного имени вносятся регистратором в базу данных.

Деятельность по реализации товаров, выполнению работ, оказанию услуг на территории Республики Беларусь с использованием информационных сетей, систем и ресурсов, имеющих подключение к сети Интернет, осуществляется юридическими лицами, их филиалами и представительствами, созданными в соответствии с законодательством Республики Беларусь, с местонахождением в Республике Беларусь, а также индивидуальными предпринимателями, зарегистрированными в Республике Беларусь, с использованием информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь и зарегистрированных в установленном порядке.

Государственная регистрация информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь осуществляется по заявительному принципу Министерством связи и информатизации либо уполномоченной им организацией на основании соответствующего обращения поставщиков интернет-услуг.

Постановлением Министерства связи и информатизации Республики Беларусь от 19 марта 2010 г. № 4 «О делегировании отдельных полномочий министерства связи и информатизации» определено, что Республиканское унитарное предприятие по надзору за электросвязью «БелГИЭ» осуществляет государственную регистрацию информационных сетей, систем и ресурсов национального сегмента глобальной компьютерной сети Интернет, размещенных на территории Республики Беларусь.

Перечень и формы документов, представляемых поставщиками интернет-услуг для государственной регистрации информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь, порядок их государственной регистрации определяются Советом Министров Республики Беларусь по

согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь.

Постановлением Совета Министров Республики Беларусь от 29.04.2010 г. № 644 «О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет» утверждено Положение о порядке государственной регистрации информационных сетей, систем и ресурсов национального сегмента глобальной компьютерной сети Интернет, размещенных на территории Республики Беларусь.

Сведения о зарегистрированных информационных сетях, системах и ресурсах национального сегмента сети Интернет предоставляются на безвозмездной основе уполномоченной Министерством связи и информатизации организацией Министерству информации, органам, осуществляющим оперативно-розыскную деятельность, органам прокуратуры и предварительного следствия, органам Комитета государственного контроля, налоговым органам, судам, органам принудительного исполнения для выполнения возложенных на них задач и функций.

Республиканские органы государственного управления, местные исполнительные и распорядительные органы, иные государственные органы и государственные организации, а также хозяйственные общества, в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами, обязаны размещать информацию о своей деятельности в глобальной компьютерной сети Интернет на официальных сайтах этих государственных органов и организаций либо на соответствующих страницах официальных сайтов вышестоящих государственных органов и организаций.

Государственные органы и организации обеспечивают создание, функционирование и систематическое обновление интернет-сайтов с использованием информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь.

Интернет-сайты государственных органов и организаций формируются на русском и (или) белорусском языках, а при необходимости также на одном или нескольких иностранных языках. Государственные организации, осуществляющие экспорт продукции за пределы Республики Беларусь, дополнительно обеспечивают формирование языковой версии своих интернет-сайтов на одном или нескольких иностранных языках.

Главные страницы интернет-сайтов государственных органов и организаций должны непосредственно либо в виде отдельных рубрик содержать общую информацию о государственном органе и организации (о руководстве, структуре, режиме работы, задачах и функциях, почтовом адресе, адресе электронной почты, номерах телефонов справочных служб этого органа (организации), территориальных подразделений и др.), о работе с обращениями граждан и юридических лиц, об осуществлении административных процедур в отношении граждан, юридических лиц и индивидуальных предпринимателей, о товарах (работах, услугах), производимых (выполняемых, оказываемых) государственной организацией, а также иную информацию, определяемую Президентом Республики Беларусь либо Советом Министров Республики Беларусь или размещаемую по решению руководителя государственного органа и организации.

Доступ к информации, размещенной на интернет-сайтах государственных органов и организаций, является свободным. Государственные органы и организации не вправе взимать плату за доступ к данной информации.

Государственные органы и организации обязаны регулярно проводить анализ посещаемости их интернет-сайтов и принимать меры по реализации предложений граждан, направленных на совершенствование функционирования этих сайтов.

Требования к содержанию интернет-сайтов государственных органов и организаций, а также порядок их функционирования определяются Советом Министров Республики Беларусь по согласованию с Администрацией Президента Республики Беларусь.

Постановлением Совета Министров Республики Беларусь от 29.04.2010 г. № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192» утверждено Положение о порядке функционирования интернет-сайтов государственных органов и организаций.

Целями создания и функционирования интернет-сайтов государственных органов и организаций являются:

- предоставление официальной информации о деятельности государственных органов и организаций;
- своевременное обеспечение граждан и юридических лиц полной и достоверной информацией;
- осуществление взаимосвязи между информационными ресурсами государственных органов и организаций;
- содействие гражданам Республики Беларусь в реализации их прав и законных интересов.

Информация на интернет-сайтах государственных органов и организаций размещается с учетом следующих требований:

- актуальность, оперативность, достоверность и целостность;
- четкость структуризации, распределение данных по тематическим рубрикам (разделам, подразделам);
- многовариантность представления информации с использованием различных телекоммуникационных средств, технопрограммных решений и различного уровня доступа к ней;
- представление информации на русском и (или) белорусском языках, а при необходимости также на одном или нескольких иностранных языках;
- доступность для инвалидов по зрению в соответствии с требованиями, определенными в технических нормативных правовых актах.

Доступ к информации, размещенной на интернет-сайтах государственных органов и организаций, является свободным и бесплатным.

Состав размещаемой на интернет-сайте информации должен отражать специфику деятельности государственного органа и организации. Информация должна обладать необходимой глубиной содержания и регулярно обновляться (не реже одного раза в неделю), а информация о новостях – также датироваться. Информация в виде текста размещается на интернет-сайте в формате, обеспечивающем возможность поиска и копирования фрагментов текста.

Структура интернет-сайта включает в себя главную страницу, страницы нижнего уровня, а также рубрики (разделы, подразделы).

Структура интернет-сайта должна обеспечивать оптимальное размещение различных видов информации, простоту навигации и доступа пользователей с различным уровнем образования и технической подготовки к содержанию рубрик (разделов, подразделов) интернет-сайта, а также единство дизайна всех страниц.

Для сложных по структуре интернет-сайтов, содержащих значительный объем разнородной информации, на главной странице обеспечивается возможность осуществления поиска информации на интернет-сайте с помощью средств навигации (путем последовательного перехода по ссылкам, начиная с главной страницы интернет-сайта).

Интернет-сайт должен предусматривать версию (поддерживать специальные технологии) для инвалидов по зрению и быть совместимым с различными веб-браузерами.

Поставщик интернет-услуг – юридическое лицо или индивидуальный предприниматель, оказывающие интернет-услуги на территории Республики Беларусь.

Интернет-услуги – услуги по обеспечению доступа юридических лиц и физических лиц, в том числе индивидуальных предпринимателей, к сети Интернет и (или) размещению в данной сети информации, ее передаче, хранению, модификации.

Поставщики интернет-услуг обязаны:

- осуществлять идентификацию абонентских устройств при оказании интернет-услуг, учет и хранение сведений об абонентских устройствах, оказанных интернет-услугах;

- устранять различные виды неправомерных воздействий, о наличии которых поставщику интернет-услуг стало известно, заведомо приводящих к нарушению конфиденциальности, целостности, подлинности, доступности, сохранности информации, направленных на пользователей интернет-услуг и (или) исходящих от них;

- осуществлять при оказании услуг по размещению в сети Интернет информационных систем и (или) информационных ресурсов адресацию по технологии, предусматривающей полную поддержку интернет-протоколов версий 4 и 6 сетевыми устройствами;

- обеспечивать оказание интернет-услуг по технологии, предусматривающей полную поддержку интернет-протокола версии 6 сетевыми устройствами, на основании обращения пользователя интернет-услуг;

- выполнять иные требования законодательства.

Идентификация пользователя интернет-ресурса – совокупность мероприятий по установлению сведений о пользователе интернет-ресурса.

Собственники пунктов коллективного пользования интернет-услугами либо уполномоченные ими лица осуществляют идентификацию пользователей интернет-услуг в пунктах коллективного пользования интернет-услугами, учет и хранение персональных данных пользователей интернет-услуг, а также сведений об интернет-услугах, оказанных пунктами коллективного пользования интернет-услугами, и посещаемых пользователями интернет-услуг информационных ресурсах (их составных частях).

Хранение сведений, указанных выше, осуществляется в течение одного года со дня оказания интернет-услуг.

Сведения об абонентских устройствах, персональные данные пользователей интернет-услуг в пунктах коллективного пользования интернет-услугами, а также сведения об оказанных интернет-услугах и посещаемых пользователями интернет-услуг информационных ресурсах (их составных частях) представляются поставщиками интернет-услуг, собственниками пунктов коллективного пользования интернет-услугами либо уполномоченными ими лицами по требованию органов, осуществляющих оперативно-розыскную деятельность, органов прокуратуры и предварительного следствия, органов Комитета государственного контроля, налоговых органов, судов в порядке, установленном законодательными актами.

Пункт коллективного пользования интернет-услугами – компьютерные клубы, интернет-кафе, домашние сети, иные места, в которых обеспечивается коллективный доступ пользователей интернет-услуг к сети Интернет.

Постановление Совета Министров Республики Беларусь от 10.02.2007 № 175 «Об утверждении Положения о порядке работы компьютерных клубов и Интернет-кафе» регулирует отношения в сфере осуществления деятельности компьютерных клубов и Интернет-кафе, порядок оказания информационных услуг пользователям на основе предоставления по месту фактического нахождения компьютерного клуба или Интернет-кафе во временное пользование вычислительной техники, программного обеспечения, предоставления информации, размещенной на компьютерных носителях информации, возмездного оказания услуг электросвязи, а также услуг общественного питания.

Постановлением Совета Министров Республики Беларусь от 23.11.2018 г. № 850 «Об утверждении Положения о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания» определяется порядок предварительной идентификации владельцем интернет-ресурса, сетевого издания пользователей, размещающих информационные сообщения и (или) материалы на интернет-ресурсе, в том числе осуществляющих комментирование. Предварительная идентификация пользователя осуществляется при регистрации им учетной записи на интернет-ресурсе путем заключения пользовательского соглашения (договора между владельцем интернет-ресурса и пользователем, в котором определены условия использования интернет-ресурса, а также взаимные права и обязанности сторон).

Владелец интернет-ресурса осуществляет активацию учетной записи пользователя путем отправки кода активации в СМС-сообщении на указанный при заполнении пользовательского соглашения номер мобильного телефона пользователя или с использованием иных идентификационных данных и технических средств, позволяющих идентифицировать личность пользователя. При этом один номер мобильного телефона и (или) один комплект иных идентификационных данных могут быть использованы для регистрации не более одной учетной записи пользователя на каждом конкретном интернет-ресурсе.

После активации своей учетной записи пользователь вправе размещать на интернет-ресурсе информационные сообщения и (или) материалы, включая комментарии к информационным сообщениям и (или) материалам иных пользователей данного интернет-ресурса, при условии авторизации на интернет-ресурсе (введения при входе на интернет-ресурс своего логина и пароля, указанных при регистрации).

2. Особенности правового регулирования отношений при реализации права на поиск, получение и потребление информации в глобальной компьютерной сети Интернет.

Интернет на данном этапе стал одним из важнейших источников познаний. Интернет представляет собой распределенную всемирную базу знаний, включающую в себя множество различных информационных массивов (информационных ресурсов, баз, знаний). В состав Интернета входят и обеспечивают его функционирование множество провайдеров (т.е. субъектов, предоставляющих информационные услуги пользователя Интернета).

В сети Интернет можно выделить 3 группы субъектов:

1) субъекты, которые создают программно-техническую часть информационной структуры Интернет, включая средства связи и телекоммуникаций, обеспечивают ее эксплуатацию, расширение и развитие. Основными субъектами выступают разработчики трансграничных информационных сетей, в том числе технических средств, средств связи и телекоммуникаций, программных средств разного уровня и назначения;

2) субъекты, которые производят и распространяют информацию в сети Интернет, предоставляют услуги к подключению к Интернету. К ним можно отнести специалистов, которые производят исходную информацию, формируют информационные ресурсы, осуществляют раскрутку сайтов и предоставляют информацию из этих ресурсов потребителям, пользователям Интернета.

3) потребители информации и услуг в Интернете. Выделяют:

- потребители информации, осуществляющие поиск и получение информации в Интернете;

- потребители услуг по хостингу. Хостинг – услуга по предоставлению ресурсов для размещения информации на сервере, постоянно имеющем доступ к сети (обычно Интернет);

- потребители услуг информационной почты.

Основные объекты, по поводу которых возникают информационные отношения в сети Интернет:

1) программно-технические комплексы, информационные системы, информационно-телекоммуникационные технологии, средства связи и телекоммуникации, обеспечивающие осуществление информационных процессов;

2) информация, информационные услуги, информационные продукты и информационные ресурсы;

3) доменные имена;

4) информационные права и свободы;

5) интересы личности, общества и государства в информационной сфере;

6) информационная целостность и информационный суверенитет государства;

7) информационная безопасность.

Применение Интернета позволяет осуществить следующие формы и виды деятельности:

1) подготовка членов общества к работе на ПК и в трансграничных информационно-телекоммуникационных сетях;

2) купля-продажа товаров и услуг в сети, связь и коммуникация, отдых и развлечение;

3) возможность каждому получать полную и достоверную информацию;

4) мгновенная телекоммуникация.

3. Вопросы правового обеспечения информационной безопасности в глобальной компьютерной сети Интернет.

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

В соответствии с Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь» необходимым условием реализации прав граждан в информационной сфере, поддержания высокого уровня информационного обмена, оказания информационных услуг является устойчивое функционирование и управляемость национального сегмента сети Интернет.

В Республике Беларусь кибербезопасность национального сегмента сети Интернет обеспечивается главным образом за счет отражения основного объема кибератак на информационные системы и сети передачи данных путем блокирования вредоносных коммуникаций между субъектами и объектами воздействий.

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Государством поддерживается и стимулируется применение лучших практик обеспечения кибербезопасности. Наиболее перспективной задачей рассматривается создание единой государственной системы мониторинга национального сегмента сети Интернет с одновременным формированием облачной платформы предоставления комплексных сервисов информационной безопасности государственному сектору и бизнес-сообществу в интересах автоматизированного учета киберинцидентов и

оперативного обмена информацией о них между уполномоченными государственными органами, операторами электросвязи и командами быстрого реагирования на компьютерные инциденты (CERT/CSIRT). В перспективе также необходимо формирование экосистемы для создания и функционирования национального удостоверяющего центра, корневой сертификат которого будет являться доверенным для основных операционных систем и веб-браузеров.

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.

Наряду с этим требуется организовать функционирование службы оценки репутации IP-адресов для предоставления в режиме реального времени поставщикам интернет-услуг сведений об адресах, используемых для кибератак.

Необходимо обеспечить достижение и сохранение баланса между надежной идентификацией пользователей, регистрацией их действий и созданием условий для безопасного сбора, обработки, предоставления, хранения и распространения персональных данных в национальном сегменте сети Интернет, а также формирование и развитие национальных рынков страхования киберрисков и услуг тестирования на проникновение.

Специально уполномоченным государственным органом в сфере безопасности использования национального сегмента сети Интернет является Оперативно-аналитический центр при Президенте Республики Беларусь, который:

- координирует деятельность государственных органов, поставщиков интернет-услуг по обеспечению безопасности информации при использовании информационных сетей, систем и ресурсов национального сегмента сети Интернет;
- определяет по согласованию с Президентом Республики Беларусь перечень операторов электросвязи, имеющих право на пропуск международного трафика и присоединение к сетям электросвязи иностранных государств;
- определяет порядок регистрации доменных имен в национальной доменной зоне, в том числе требования к юридическим лицам, планирующим осуществлять регистрацию доменных имен, учитывающие финансово-экономическое положение и технические возможности данных юридических лиц, и меры реагирования на нарушения такого порядка;
- организует и осуществляет международное сотрудничество по вопросам обеспечения безопасности информации при использовании информационных сетей, систем и ресурсов национального сегмента сети Интернет, в том числе с международными организациями, включая форум команд реагирования на компьютерные инциденты в качестве национального центра реагирования на компьютерные инциденты;
- осуществляет иные полномочия в соответствии с законодательными актами.

4. Зарубежный опыт правового регулирования отношений в глобальной компьютерной сети Интернет.

К настоящему времени сложилось несколько уровней правового регулирования отношений, складывающихся в сети Интернет:

- международный;
- региональный (в рамках межгосударственных объединений);
- национальный.

На надгосударственном уровне ведется активная работа по формированию нормативных актов, различных конвенций, резолюций рекомендаций, которые закрепляют основные принципы регулирования правоотношений в сети Интернет. Ответственность по разработке более детального законодательства в отношении Всемирной паутины лежит на плечах каждого отдельного государства. С одной стороны,

ситуация, когда государство самостоятельно разрабатывает собственные методы правового регулирования тех или иных отношений, является обычной практикой и не создает каких-то особых трудностей. С другой стороны, сеть Интернет не имеет территориальных границ, и каждое государство не может затрагивать только свою частичку Интернета.

На сегодняшний момент конкретные нормы, касающиеся правоотношений в Интернете, государства устанавливают сами и вырабатывают основные направления регулирования этой сферы. Поэтому политика в отношении Интернета в разных странах может коренным образом отличаться. Государственная политика может быть направлена на ограничение доступа к определенной информации для взрослых. Этот подход используется в австралийском федеральном законе, в Китае, Саудовской Аравии, Сингапуре, Объединенных Арабских Эмиратах, Вьетнаме. Некоторые страны требуют от Интернет-провайдеров блокировать подобную информацию, в то время как 66 другие страны допускают ограниченный доступ в Интернет, контролируемый государственными органами.

Государство может запрещать открытый доступ к Интернету. Отдельные страны требуют от пользователя зарегистрироваться или получить лицензию для того, чтобы получить доступ с ограничениями, перечисленными выше. Например, на Кубе пользование Интернетом ограничено и контролируется правительством.

В настоящее время одним из самых либеральных подходов к регулированию Интернета считается подход, реализуемый в США. Благодаря первой поправке к Конституции США, в стране не могут приниматься законы, ограничивающие свободу слова. Поэтому регулирование Интернета ограничивается защитой личной информации, авторских прав и обеспечения честной конкуренции. Несмотря на это, вопросы регулирования доступа к информации и контроля трафика в Сети спецслужбами решаются в интересах руководства страны за счет наличия законов о противодействии террористической деятельности.

Страны ЕС также можно отнести к либеральной группе, стремящейся минимизировать участие государства в регулировании доступа к информации. В этих странах стремятся сохранить баланс между конституционным правом доступа к информации и защитой национальной безопасности. Регулирование доступа (блокирование и фильтрация контента) осуществляется, как правило, в двух областях: негативное воздействие на подрастающее поколение и защита авторских прав. Правда, в последнее время в некоторых странах Европы (например, в Германии) наметилась тенденция на принятие более жестких законов по контролю за информацией в Сети в рамках противодействия террористической деятельности.

Великобритания и Франция в 2018 году утвердили совместный план действий по повышению эффективности выявления и удаления контента, который квалифицируют как террористический, радикальный или ненавистнический.

Китайская система контроля Интернета являет собой сложный, комплексный и очень эффективный механизм. Фильтрация контента осуществляется как программными, так и аппаратными средствами. Интернет с самого начала своего появления в Китае находится под пристальным контролем со стороны властей. Периодически в черный список попадают и некоторые иностранные электронные СМИ, в основном тайваньские и американские. В разное время запрещались такие ресурсы как Википедия, Gmail, Twitter и др. В КНР вместо запрещенных ресурсов создаются локальные аналоги. Так, вместо Википедии была создана Байдупедия – аналог Википедии.

5. Правовая основа электронной торговли, электронного бизнеса.

Современные технологии получают все большее распространение в сфере ведения бизнеса. В условиях скоростного Интернета и передовых IT-технологий многие традиционные гражданско-правовые отношения, в т.ч. договорные, приобретают новые

механизмы реализации, которые должны получать соответствующее отражение в законодательстве. Процессы неоиндустриализации, захватившие экономическую сферу жизнедеятельности общества, не могут не оказывать серьезное влияние на область правового регулирования, в т.ч. в сфере осуществления торговли.

Одним из способов использования цифровых технологий в гражданском обороте можно признать электронную коммерцию и как ее вариант – электронную торговлю.

Электронная коммерция является неотъемлемым элементом сетевой экономики, поскольку она способствует проведению сделок с использованием возможностей сети Интернет.

Традиционно в электронной коммерции выделяют шесть составляющих элементов, каждый из которых в той или иной степени обеспечивает проведение бизнес-операций:

1. Электронный обмен данными (Electronic Data Interchange, EDI) – обмен информацией с использованием цифровых средств коммуникации, главным образом, между сторонами коммерческих сделок. Основу электронного обмена данными составляют стандарты форматирования и передачи информации, разрабатываемые Международной организацией по стандартизации (ISO).

В качестве примеров стандартов по обмену данными можно указать на: стандарт EDIFACT (ISO 9735) – «Электронный обмен данными в управлении, торговле и на транспорте», региональные стандарты, например ГОСТ 6.20.1–90 (Россия), ANSI X.12 (США).

2. Электронное движение капитала (Electronic Funds Transfer, EFS) – электронный обмен или перевод денег с одного счета на другой. В электронной коммерции EFS связано с проведением электронных денежных транзакций. EFS предполагает обмен данными между серверами, обрабатывающими денежные транзакции и связанную с ними информацию.

В качестве примера такого обмена данными можно привести систему международных межбанковских расчетов SWIFT (Society for Worldwide Interbank Financial Telecommunications). В электронной коммерции такие системы используются достаточно широко, в т.ч. для осуществления как межбанковских, так и любых иных видов платежей. Операторами транзакций могут выступать и «виртуальные организации» (например, сервисы для обмена виртуальных денег).

3. Электронная торговля (e-trade) представляет собой совершение сделок купли-продажи товаров посредством ИКТ. В экономической теории распространено широкое понимание электронной торговли, в т.ч. в него включаются: выбор товара, подтверждение заказа, прием платежей и обеспечение доставки. При этом оплата и доставка могут не иметь электронную форму (например, осуществляться по почте или с использованием услуг транспортных компаний). Хотя тенденция развития электронных продаж свидетельствует о постепенном переходе к использованию возможностей Интернета на всех этапах цикла реализации товаров.

4. Электронные деньги (e-cash) – денежные обязательства эмитента перед доверителем в электронном виде. Электронные деньги одновременно являются средством платежа и обязательством эмитента. Электронные деньги обеспечивают высокую скорость осуществления безналичных расчетов, но имеют ограниченное применение, поскольку конвертировать электронные деньги в обычные возможно только в рамках взаимоотношений между их владельцем и эмитентом. Инструментом оборота электронных денег являются электронные кошельки, которые представляют собой сервис онлайн-транзакций, сохраняющий платежную информацию пользователей. Разновидностью электронных денег являются prepaid пластиковые карты, которые обладают всеми характеристиками пластиковых карт, но не предполагают возможности пополнения.

5. Электронный маркетинг (e-marketing) – комплекс маркетинговых мероприятий, связанный с анализом рынка и продвижением товаров в сети Интернет. Электронный

маркетинг может состоять в размещении в сети маркетинговой информации (сайты, блоги, реклама и т.д.), а также в управлении размещенным контентом (веб-проектирование, веб-дизайн, веб-программирование и веб-администрирование).

6. Электронный банкинг (e-banking) – технология дистанционного банковского обслуживания, при которой доступ к счетам и операциям клиента осуществляется посредством сети Интернет. В Республике Беларусь эта технология называется «интернет-банкинг», она включает в себя: денежные переводы, оплату товаров и услуг, проверку остатков на банковских счетах и пластиковых картах и др. В настоящее время системы дистанционного банковского обслуживания стали распространенным инструментом для заключения большинства банковских сделок, которые могут подтверждаться выдачей соответствующего бумажного аналога только по специальному запросу клиента.

Приведенный краткий обзор вариантов электронной коммерции наглядно свидетельствует, что указанная сфера чрезвычайно широка и нет необходимости в ее едином правовом регулировании.

Электронная торговля – это собирательное наименование коммерческих операций, совершаемых с использованием Интернета. С каждым годом электронные формы торговли занимают все большую часть рынка. Увеличиваются объемы реализуемых в Интернете товаров, расширяются области применения. К электронной торговле относится не только торговля товарами, но и бронирование и реализация различных заказов (гостиничный сервис, билеты и др.), а также транзакции через банковские сервисы и системы электронных денег.

Вместе с тем законодательное регулирование этой новой сферы экономических отношений в значительной мере отстает от развития информационно-коммуникационных технологий. Не будет преувеличением сказать, что электронная торговля в Беларуси остается пока в серой зоне регулирования: многие актуальные вопросы остаются нерешенными.

Понятия «электронная торговля», «электронная коммерция» в законодательстве Беларуси не закреплены. Закон «О государственном регулировании торговли и общественного питания в Республике Беларусь» определил лишь самые общие требования к осуществлению «торговли с использованием сети Интернет» (ст. 16). По смыслу Закона торговля может осуществляться не только в обычном формате контактов продавца и покупателя, но и посредством использования информационно-коммуникационных технологий; при этом законодательное регулирование торговли полностью распространяется и на торговлю с использованием сети Интернет. Сами по себе тезисы о возможности таких форм торговых отношений и о распространении на них всех законодательных требований и ограничений, включая защиту прав потребителя, не вызывают возражений. Однако очевидно, что распространение общего законодательства о торговле на рассматриваемую сферу не решает проблем их урегулирования, поскольку специфика электронных форм торговли требует особых норм, специально предназначенных для бесконтактных, опосредованных сетью Интернет правовых отношений.

Прежде всего, электронная торговля не исчерпывается формами, приведенными в Законе о государственном регулировании торговли и общественного питания. Закон не распространяется на довольно обширную группу торговых отношений, включая внешнюю торговлю, куплю-продажу валюты, ценных бумаг, тепловой и электрической энергии, куплю-продажу объектов интеллектуальной собственности и др. Законодательство же в перечисленных областях не содержит специальных норм о «торговле с использованием сети Интернет», даже в таком виде, как это имеет место в рассматриваемом Законе о государственном регулировании торговли и общественного питания.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Государственная политика в области информационной безопасности. Угрозы безопасности в информационной сфере.

2. Правовая защита от угроз воздействия информации на личность, общество, государство.

3. Правовая защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц.

1. Государственная политика в области информационной безопасности. Угрозы безопасности в информационной сфере.

Прогресс ИКТ, повлекший многообразие информационных процессов и развитие информационных отношений, обусловил потребность введения в юридический оборот понятия «информационная безопасность».

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Сущность информационной безопасности позволяет сформировать следующие признаки:

- информационная безопасность характеризует защищенность определенной совокупности прав и интересов субъектов отношений;
- субъектами отношений выступают личность, общество и государство;
- объектами защиты являются права и интересы субъектов, возникающие по поводу информации;
- средой возникновения и реализации отношений выступает информационная среда;
- технологической основой информационной безопасности являются процессы развития ИТ, сетевых коммуникаций (информатизация, цифровизация);
- защищаемые права и интересы представляют собой динамично развивающуюся систему;
- последствия реализации отношений по поводу информационной безопасности проявляются в других сферах национальной безопасности (политической, экономической, военной);
- информационная безопасность представляет собой состояние, которое проявляется только при одновременном обеспечении заданного уровня безопасности всех реализуемых субъектов прав и интересов;
- информационная безопасность не является самоцелью, а лишь обеспечивает устойчивое развитие информационных отношений.

Государственная политика обеспечения информационной безопасности – основные направления деятельности республиканских и местных органов власти и управления в данной области, порядок закрепления их обязанностей по защите интересов Республики Беларусь в информационной сфере.

Целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

Обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы главным образом обеспечивается и ее безопасность.

На государственном уровне осуществляются мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз информационной безопасности, минимизации их деструктивного воздействия и локализации последствий. Разрабатывается и реализуется комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз.

Постановлением Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств № 41-15 «О модельном законе «Об информации, информатизации и обеспечении информационной безопасности» принятым в г. Санкт-Петербурге 28.11.2014 определены основные принципы государственной политики в области информации, информатизации и обеспечения информационной безопасности:

- обеспечение прав и законных интересов граждан, институтов общества и государства в информационной среде и пространстве информационного взаимодействия национальных и межгосударственных информационных систем;
- социальная направленность стратегических целей, основных задач и мероприятий, проводимых в сфере информатизации;
- ликвидация информационного неравенства в обществе, реализация условий для развития информационного общества;
- обеспечение доступа широких слоев граждан к информационно-коммуникационным сетям, информационным системам и технологиям, к системам открытого доступа к информации;
- открытость политики информатизации и активное привлечение к этой деятельности представителей науки, высшей школы и предпринимателей, работающих в информационной сфере;
- безопасность создаваемых и используемых информационно-коммуникационных сетей, информационных технологий и систем;
- правовая, научная, техническая и экономическая обоснованность разрабатываемых и принимаемых решений;
- комплексность и системность подхода к разработке, созданию и использованию информационно-коммуникационных сетей, информационных технологий и систем;
- системный подход к организационно-правовому обеспечению использования информационных технологий в государственном управлении, перевод реализации функций административных структур на цифровые технологии;
- развитие международного сотрудничества и использование зарубежного опыта в сфере информатизации в целях обеспечения конкурентоспособности создаваемых товаров и услуг на отечественном и мировом рынках;
- развитие законодательства в сфере информации, информатизации и обеспечения информационной безопасности.

С позиций теории национальной безопасности **угроза** – это фактически любые внутренние и внешние условия и факторы, оказывающие негативное воздействие на процесс развития и требующие для повышения уровня социального развития снижения своих количественных характеристик. В соответствии с Концепцией национальной безопасности Республики Беларусь существует градация названных негативных факторов:

1) источник угрозы национальной безопасности – фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;

2) угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь.

Угроза не является самостоятельным феноменом, а представляет собой категорию, корреспондирующую с такой позитивной конструкцией, как интересы субъектов отношений.

Угрозы информационной безопасности могут иметь объективный и субъективный характер, способны выражаться в явлениях, процессах и действиях (или их совокупности), исходить от внешних и внутренних источников.

Анализ теоретических подходов исследователей информационного права позволяет выделить комплекс актуальных для Республики Беларусь основных угроз информационной безопасности:

- посягательства на информационный суверенитет, право субъектов отношений самостоятельно владеть, пользоваться и распоряжаться своими информационными ресурсами;

- использование ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии, противоречащих международному праву;

- деструктивное информационное воздействие на личность, общество, государственные институты и их информационную инфраструктуру, наносящее ущерб национальным интересам, в том числе посредством вмешательства во внутренние дела государства, нарушения общественного порядка, разжигания межнациональной, межрасовой, сословной и межконфессиональной вражды, пропаганды расистских и ксенофобских идей, порождающих ненависть и дискриминацию, подстрекающих к насилию;

- нарушение безопасного, стабильного функционирования объектов критически важной информационной инфраструктуры;

- рост киберпреступности, в том числе кибертерроризма.

В информационной сфере внутренними источниками угроз национальной безопасности являются:

- распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

- несоответствие качества национального контента мировому уровню;

- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

- рост преступности с использованием информационно-коммуникационных технологий;

- недостаточная эффективность информационного обеспечения государственной политики;

- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В информационной сфере внешними источниками угроз национальной безопасности являются:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

- развитие технологий манипулирования информацией;
- препятствование распространению национального контента Республики Беларусь за рубежом;

- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

Существует градация источников угроз по признаку объекта.

Основные угрозы воздействия информации на личность (угрозы конституционным правам и свободам человека и гражданина в информационной сфере):

- принятие нормативно-правовых актов, ущемляющих конституционные права и свободы граждан;

- неправомерное ограничение доступа к открытым информационным ресурсам;

- нарушение конституционных прав и свобод граждан в области массовой информации;

- противоправное применение специальных средств воздействия на сознание;

- манипулирование информацией.

Основные угрозы воздействия информации на общество (угрозы интересам общества в информационной сфере):

- неисполнение требований законодательства в области информационной сферы;

- создание монополии на формирование, получение и распространение информации;

- активизация различного рода религиозных сект;

- нарушение правил в области функционирования информационных систем (например, разработка и распространение программ, нарушающих нормальное функционирование информационных систем, внедрение электронных устройств для перехвата информации и т. д.);

- нарушение правил в сфере оборота информации;

- увеличение оттока за границу специалистов и правообладателей интеллектуальной собственности; усиление зависимости различных сфер жизнедеятельности общества от зарубежных информационных структур.

Основные угрозы воздействия информации на государство (угрозы интересам государства в информационной сфере):

- разрушение единого информационного пространства государства;

- вытеснение национальных информационных агентств, СМИ и производителей средств информатизации с внутреннего информационного рынка;

- монополизация информационного рынка государства отечественными и зарубежными информационными структурами;

- блокирование деятельности государственных СМИ по информированию отечественной и зарубежной аудитории, низкая эффективность информационного обеспечения государственной политики и др.

2. Правовая защита от угроз воздействия информации на личность, общество, государство.

Обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

В рамках изучения метода правового обеспечения информационной безопасности исследователями предлагается оперировать методами регулирования публично-правовых отношений.

В условиях неоконченного оформления информационных отношений нормами права основным социальным регулятором обеспечения информационной безопасности представляются принципы, которые определяют методологические границы деятельности по ее обеспечению.

Общими принципами являются:

- 1) законность;
- 2) открытость и гласность;
- 3) правовое равенство всех участников процесса информационного взаимодействия;
- 4) комплексность мер по обеспечению информационной безопасности и последовательность их реализации;
- 5) обоснованность мер обеспечения информационной безопасности;
- 6) взаимная ответственность человека, общества и государства.

Исследователями проблем национальной безопасности обосновывается ряд специальных принципов, применимых для обеспечения информационной безопасности:

- 1) приоритет мер предупреждения при реализации политики безопасности;
- 2) соотношение прав и свобод на информацию с их самоограничениями, ограничениями и ответственностью;
- 3) технико-технологическая обусловленность информационных процессов;
- 4) гуманизм, социальная справедливость, сочетание гласности и тайны;
- 5) свобода поиска, получения, передачи, производства и распространения информации любым законным способом, установление ограничений доступа к информации только законом;
- 6) открытость информации о деятельности государственных органов;
- 7) достоверность информации и своевременность ее предоставления;
- 8) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 9) глобальность.

Обеспечение информационной безопасности осуществляется посредством непрерывно действующего комплекса организационных, правовых и технических мер.

Организационные меры обеспечения информационной безопасности включают:

- 1) выработку стратегии и тактики обеспечения информационной безопасности: разработку государственных и отраслевых программ, финансирование деятельности по обеспечению информационной безопасности;
- 2) формирование системы субъектов, осуществляющих деятельность по обеспечению информационной безопасности, организацию их координации и взаимодействия, развитие международного сотрудничества;
- 3) установление режимов информационной безопасности, в том числе режимов ограничения доступа к информации;
- 4) лицензирование деятельности, регистрацию и стандартизацию работ и услуг, сертификацию товаров в области обеспечения информационной безопасности, создание системы страхования информационных рисков;
- 5) формирование системы мониторинга показателей и характеристик информационной безопасности в основных сферах жизнедеятельности.

К техническим мерам обеспечения информационной безопасности относятся:

- 1) разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, в том числе создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих блокирование, уничтожение, искажение информации;
- 2) выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем;

3) формирование единой защищенной системы электронного документооборота и средств ЭЦП (электронной цифровой подписи) государственных органов;

4) создание системы обеспечения надежности и устойчивости функционирования критически важных объектов информатизации, отказ или разрушение которых могут причинить ущерб национальной безопасности.

К правовым мерам обеспечения информационной безопасности относятся:

1) разработка правовых механизмов регулирования отношений в информационной сфере;

2) правовое закрепление категорий информации, информационных ресурсов и систем, оснований и порядка доступа к ним;

3) закрепление общеобязательных правил поведения в области обеспечения информационной безопасности, определение круга противоправных деяний, формирование перечня ограничений возможностей реализации информационных отношений в целях защиты прав и законных интересов субъектов взаимодействия, определение условий введения данных ограничений;

4) принятие НПА, в том числе устанавливающих ответственность за преступления против информационной безопасности;

5) определение статуса субъектов обеспечения информационной безопасности, законодательное разграничение их полномочий;

6) определение и применение механизмов выявления и расследования правонарушений в информационной сфере, процедур привлечения к уголовной, административной и иным видам ответственности;

7) осуществление надзора и контроля за законностью деятельности граждан, организаций, государственных органов и должностных лиц в информационной сфере.

Классическими способами правового обеспечения информационной безопасности являются введение необходимых ограничений (запретов) и предписаний.

В сфере обеспечения информационной безопасности можно выделить следующие основные запреты:

1) на распространение информации:

– экстремистского характера, порнографического содержания;

– пропагандирующего культ насилия и жестокости, содержащей призывы к насильственному свержению конституционного строя, к организации или проведению массовых беспорядков, к незаконной организации или проведению массовых беспорядков;

– содержащей сведения, которые могут быть использованы для причинения вреда здоровью или нарушения общественной безопасности, в том числе информации о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия;

– причиняющей вред здоровью и развитию детей, оказывающей деструктивное информационное воздействие на личность;

– содержащей пропаганду войны, социальной, национальной, религиозной и расовой вражды или розни, информации, содержащей персональные данные гражданина, служебную информацию ограниченного распространения, коммерческую тайну, государственные секреты;

– заведомо ложной, позорящей другое лицо, информации, унижающей честь и достоинство лица, а также честь и достоинство представителя власти, дискредитирующей деловую репутацию хозяйствующего субъекта;

– содержащей ложные сведения о товарах и услугах;

– содержащей заведомо ложное сообщение, в том числе об опасности;

– содержащей угрозы причинения вреда правам и интересам лица, в том числе угрозу убийства или причинения другого вреда здоровью, уничтожения имущества, совершения акта терроризма;

– при отсутствии у получателя возможности отказаться от ее получения.

2) на сбор информации:

– содержащей тайну личной жизни лица, персональные данные гражданина, служебную информацию ограниченного распространения (служебную тайну), коммерческую тайну, профессиональную тайну, государственные секреты;

– для передачи ее иностранному государству, иностранной организации или их представителю в ущерб национальной безопасности.

3) на использование информации:

– в нарушение прав ее обладателей, составляющей объекты авторского права и смежных прав, права промышленной собственности;

– образующей коды вредоносных программ.

4) на сдерживание свободного оборота информации – ограничение распространения общедоступной информации и осуществление цензуры.

В сфере обеспечения информационной безопасности выступают базовыми следующие предписания:

1) на обязательное распространение общедоступной информации:

– по запросу граждан, о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;

– о деятельности государственных органов, о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– о состоянии преступности, а также о фактах нарушения законности;

– накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

2) на соблюдение порядка:

– распространения продукции СМИ, религиозной информации, информации о нацистской символике или атрибутике;

– распространения рекламы, документирования информации и ее использования, в том числе на соблюдение порядка получения и использования материалов скрытой аудио- и видеозаписи, кино- и фотосъемок;

– хранения документированной информации, использования радио-, теле-, видео- и кинопрограмм, документальных и художественных фильмов, а также информационных компьютерных файлов и программ обработки информационных текстов, относящихся к специальным СМИ;

– хранения информации в компьютерной системе, сети или на машинных носителях;

– связанного с применением скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и оказывающих вредное влияние на их здоровье;

– возрастных ограничений при распространении продукции СМИ;

– лицензирования отдельных видов деятельности, сертификации отдельных элементов и комплексов информационно-коммуникационной инфраструктуры.

Важнейшим вопросом является определение субъектного состава отношений в области обеспечения информационной безопасности. Особое место среди субъектов обеспечения информационной безопасности занимает государство. Это обусловлено его уникальными средствами и силами противодействия угрозам. Несмотря на то, что эту деятельность оно осуществляет совместно с гражданами и обществом, влияние государства на обеспечение безопасности является определяющим. Следовательно, в

целях обеспечения информационной безопасности (как комплексного социально-правового явления) государство выстраивает политику развития информационного общества, стратегию информационной безопасности и формирует соответствующую правовую основу.

3. Правовая защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц.

Правовое обеспечение информационной безопасности – это разработка и применение правовых средств и механизмов правовой системы государства в области защиты информационных систем и ресурсов в целях поддержания их свойств в состоянии гарантированной устойчивости и соблюдения законности информационного взаимодействия субъектов в процессе развития информационного общества, создания условий реализации прав и интересов личности, защиты интересов государства, в том числе в рамках международного сотрудничества.

Важнейшим практическим аспектом правового регулирования выступает нормативное обеспечение информационной безопасности. Оценка качественного состояния нормативного обеспечения информационной безопасности должна учитывать ряд параметров, к которым относятся:

1) охват нормативного обеспечения таких основных сфер информационной безопасности. Как защита информационных ресурсов, обеспечение государственной политики в информационной сфере, безопасности критически важных объектов информационно-коммуникационной инфраструктуры, противодействие деструктивному информационному воздействию, преступлениям в информационной сфере, обеспечение безопасности международного информационного обмена;

2) степень юридической силы нормативных актов, регулирующих отношения в сфере информационной безопасности;

3) конституционную закрепленность отношений, возникающих по поводу защиты базовых прав и интересов взаимодействующих субъектов;

4) законодательную регламентацию системы субъектов обеспечения информационной безопасности, нормативное закрепление их функций и полномочий;

5) нормативное закрепление ответственности за нарушение норм, регулирующих отношения в области информационной безопасности;

6) ратификацию основных международных соглашений в области информационной безопасности, имплементацию в национальное законодательство модельных законов и рекомендательных актов в данной сфере.

Проблема нормативного обеспечения информационной безопасности во многих государствах, в том числе в Беларуси, заключается в том, что в этой сфере не проводилась систематизация законодательства и нормы «размазаны» по разным сферам и отдельным нормативным правовым актам.

Отправной точкой для систематизации законодательства может являться классификация норм, регулирующих отношения по обеспечению информационной безопасности, включающая следующие направления:

1. Нормативное обеспечение международной информационной безопасности.

Республика Беларусь активно участвует в глобальных и региональных инициативах по обеспечению международной информационной безопасности. Так в 2013 году подписано двустороннее белорусско-российское соглашение о сотрудничестве в сфере обеспечения международной информационной безопасности, а также Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности. В Республике Беларусь 1 апреля 2019 г. вступило в силу Соглашение о сотрудничестве государств – членов ОДКБ в области обеспечения информационной

безопасности. Решением глав правительств СНГ 25 октября 2019 г. утверждена Стратегия обеспечения информационной безопасности государств – участников СНГ.

2. Регулирование основ обеспечения информационной безопасности.

В Республике Беларусь нормы, регулирующие конкретные аспекты информационной безопасности, инкорпорированы в отраслевое законодательство. Специальные НПА об обеспечении информационной безопасности сводятся исключительно к законам о ратификации международных соглашений в данной области. Единственным специальным правовым актом, регулирующим сегодня вопросы информационной безопасности, является Концепция информационной безопасности Республики Беларусь. Информационной безопасности также касаются акты технического регулирования (например, постановление Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 «об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»).

3. Нормативное закрепление прав в информационной сфере.

Законодательство Республики Беларусь в качестве одного из способов правового обеспечения информационной безопасности предусматривает закрепление неотчуждаемых прав на нематериальные блага (ст. 151 ГК). Осуществляется правовая охрана таких неимущественных «информационных» прав, как право на тайну (ст. 28 Конституции Республики Беларусь), право на защиту информации (ст. 31, 32 Закона об информатизации), права на результаты интеллектуальной деятельности (ст. 51 Конституции Республики Беларусь). Защита указанных прав не только осуществляется посредством их признания, но и обеспечивается ответственностью за их нарушение. Также правовой мерой обеспечения информационной безопасности является признание конституционного права на информацию и закрепление свободы сбора, обработки и распространения информации (ст. 33 Конституции Республики Беларусь).

4. Нормативное регулирование обеспечения информационной безопасности в СМИ.

С развитием коммуникационных технологий начал обособливаться институт правового обеспечения СМИ, так называемое медиа-право. В рамках данного института нормативное обеспечение информационной безопасности реализуется посредством законодательного закрепления ряда запретов. Кроме этого, в республике созданы организационно-правовые механизмы предупреждения распространения посредством СМИ деструктивной информации.

Концептуальным принципом безопасности белорусского информационного общества является запрет цензуры, включающий в себя запрет на ограничение свободы информации (особенно касающейся безопасности граждан), на монополизацию СМИ и воспрепятствование их деятельности. Данный запрет облечен в конституционную форму и предусматривает уголовную ответственность в случае нарушения.

С учетом того, что информационная безопасность включает в себя безопасность коммуникации общества, нормативное регулирование информационной безопасности предусматривает положения, защищающие деятельность СМИ. Кроме того, нормативно регулируется обеспечение информационной безопасности от таких рисков, как использование СМИ в деструктивных целях (например, для нарушения избирательных прав).

5. Нормативное регулирование обеспечения информационной безопасности в сети Интернет.

Новыми и наиболее сложными для правового регулирования отношениями является социальное взаимодействие в сети Интернет. Обществом пока не согласованы границы правового опосредования «сетевых» отношений. Однако в этих условиях общество уже сформулировало и облекло в правовую форму основные запреты, формирующие основу обеспечения информационной безопасности в сети Интернет. Среди них запрет на распространение посредством сети Интернет деструктивной либо ложной информации,

запрет на использование сети Интернет для совершения компьютерных преступлений. В то же время правовое обеспечение безопасности строится не только на запретах. Большую роль играют законодательно закрепленные правила правомерного использования сети Интернет, включающие реализацию государственной политики в коммуникационной среде, архитектуру общественного взаимодействия, обеспечение прав и интересов субъектов отношений и ответственность за нарушение правил использования сети Интернет.

6. Нормативное регулирование обеспечения информационно-психологической безопасности.

Деструктивное информационное воздействие на общество и государственные институты является одной из основных потенциальных угроз национальной безопасности Республики Беларусь. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государств, рассматривается как угроза информационной безопасности в международных правовых актах.

Предупреждение деструктивного информационно-психологического воздействия на население не может эффективно осуществляться исключительно затруднением деструктивных информационных потоков, дозированием вредной информации или иными ограничительными мерами, поскольку они, как правило, малоэффективны с технической точки зрения и почти никак не регулируются на межгосударственном уровне. В этих условиях важнейшим средством обеспечения информационной безопасности становится правовое регулирование, в первую очередь, посредством введения запретов на осуществление информационно-психологического воздействия и ответственности за такую противоправную деятельность, как деструктивная пропаганда, призывы и иное побуждение к совершению преступлений и антисоциальных деяний, распространение ложной информации, сокрытие общественно важной информации, публичные оскорбления, унижение чести и достоинства.

7. Нормативное регулирование защиты информационных ресурсов.

Обеспечение безопасности информационных ресурсов является одной из важнейших составляющих обеспечения информационной безопасности. Защита информационных ресурсов осуществляется посредством ряда регламентов, а также запретов, связанных с обеспечением правовой принадлежности информации, ее доступности и целостности (неизменности).

Нормативное обеспечение безопасности информационных ресурсов также включает в себя обеспечение безопасности архивного дела и делопроизводства. Под безопасностью в данном случае понимается не только надежность функционирования систем документооборота, но и обеспечение реализации основных интересов личности, общества и государства, связанных с документированной информацией. В первую очередь, это обеспечение доступности документов, их сохранности, защита информации в электронном документообороте.

В правовом обеспечении безопасности информационных ресурсов одним из древнейших и наиболее устоявшихся является институт тайн. Защита конфиденциальности информации рассматривается как один из столпов обеспечения информационной безопасности. В связи с этим развитость нормативного регулирования тайн отчасти отражает уровень обеспечения информационной безопасности в целом. Институт тайн в национальном законодательстве Республики Беларусь представлен в основном конституционно закрепленной тайной личной жизни, включая тайну корреспонденции и тайну телефонных переговоров. Необходимо отметить значительную нормативную развитость и детализацию отношений в области государственных секретов, как и юридическую полноту ответственности за правонарушения в данной сфере. Также законодательно регулируются использование коммерческой тайны и ее защита. Нормативно закреплены категории банковской тайны, служебной информации

ограниченного распространения, налоговой тайны, тайны голосования. Регламентируется ответственность за разглашение врачебной тайны, тайны усыновления, тайны следственных действий. Отдельного внимания заслуживает такой вид информации ограниченного распространения, как персональные данные. Отнесение персональных данных к тайнам достаточно условно, поскольку в основе их природы лежит не свойство конфиденциальности информации, а режим ее использования, учитывающий интересы личности.

8. Нормативное регулирование безопасности информационных систем.

Правовое регулирование в области связи и коммуникаций отличается обособленностью, трансграничным характером и спецификой регулирования. В Республике Беларусь нормативное обеспечение безопасности систем электросвязи традиционно базируется на системе регламентов, предписаний и запретов, обеспеченных ответственностью за их неисполнение. Помимо обеспечения безопасности коммуникационных систем, белорусский законодатель в поле правового внимания удерживает безопасность информационной инфраструктуры в целом. В этих целях используется распространенный подход выделения критически важных объектов информатизации.

9. Законодательство о противодействии преступлениям против информационной безопасности.

Нормативное обеспечение правоохранительной составляющей информационной безопасности основывается не только на криминализации общественно опасных деяний, создающих угрозу интересам личности, общества и государства в информационной сфере, но и на закреплении норм, создающих условия для эффективного противодействия данным преступлениям в силу их латентности, технической обусловленности и соразвития с процессами информатизации.

В целом оценивая состояние нормативного обеспечения информационной безопасности в Беларуси, необходимо отметить, что национальное законодательство является развитым, соответствует современному уровню и отвечает темпам информатизации белорусского общества.

Что касается стратегического уровня обеспечения информационной безопасности, то в Республике Беларусь действует Концепция информационной безопасности.

Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности.

Предметом Концепции выступают общественные отношения, складывающиеся при обеспечении безопасной реализации конституционных прав и свобод гражданина, формирования информационного общества, государственной политики, инновационного развития Республики Беларусь, совершенствования информационной инфраструктуры государства, распоряжения информационными ресурсами, международного информационного обмена.

Концепция обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере.

Положения Концепции служат основой для отраслевых программ, планов работы заинтересованных государственных органов, проектов вовлеченных общественных организаций, инициатив граждан. В контексте реализации Концепции в качестве приоритетных мер обеспечения информационной безопасности следует рассматривать:

- совершенствование системы органов обеспечения информационной безопасности, в том числе определение уполномоченного органа по обеспечению информационной безопасности;
- разработку специального нормативного правового акта, формулирующего нормы и правила правомерного поведения в информационной среде, необходимые регламенты, ограничения и запреты, а также регулирующие деятельность государственных органов по обеспечению информационной безопасности;
- совершенствование системы доведения объективной и достоверной информации о деятельности государственных органов, реализации государственной информационной политики;
- совершенствование комплекса мер по нейтрализации негативных последствий распространения ложной информации, информации с признаками разжигания национальной и религиозной розни, пропаганды терроризма и экстремизма и деструктивного информационного воздействия на личность, общество, государство;
- интегрирование объектов информатизации в критически важную информационную инфраструктуру с созданием единых стандартов обеспечения ее безопасности, формированием системы координации и контроля;
- развитие системы обеспечения безопасности электронного документооборота, совершенствование защиты охраняемой в соответствии с законом информации;
- совершенствование глобальных правил безопасного и ответственного поведения в информационной сфере.

ТЕМА 12

ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

- 1. Понятие юридической ответственности за правонарушения в информационной сфере.**
- 2. Дисциплинарная и материальная ответственность за правонарушения в информационной сфере.**
- 3. Административная ответственность за правонарушения в информационной сфере.**
- 4. Гражданско-правовая ответственность за правонарушения в информационной сфере.**
- 5. Уголовная ответственность за преступления в информационной сфере.**

1. Понятие юридической ответственности за правонарушения в информационной сфере.

Понятие юридической ответственности относится к числу общетеоретических и применяемых в различных отраслях права. Являясь одним из юридических средств, нейтрализующих последствия ненадлежащего поведения субъектов, выступающего в качестве нарушения прав и законных интересов других лиц, юридическая ответственность выступает как реакция государства на совершение правонарушения. Эта реакция имеет властный, принудительный характер, понуждающий правонарушителя претерпеть неблагоприятные для него последствия в виде лишения определенных материальных или нематериальных благ.

Юридическая ответственность – предусмотренная правовыми нормами обязанность субъекта права претерпеть неблагоприятные для него последствия правонарушения.

Юридическая ответственность – мера государственного принуждения за совершенное правонарушение, связанная с претерпеванием виновным лишения личного (организационного) или имущественного характера.

Содержание юридической ответственности выступает как государственно-властное принуждение, проявляющееся в различных формах. Юридическая ответственность за нарушение законодательства, регулирующего отношения в информационной сфере, имеет ряд специфических особенностей:

1) правонарушения, попадающие под применение тех или иных мер, всегда связаны с информацией;

2) правонарушения можно рассматривать в качестве информационно-правовых, если их связь с информацией является не только непосредственной, но и опосредованной наличием материального носителя.

Под **правонарушением в информационной сфере** принято понимать виновное, противоправное деяние (действие или бездействие) конкретного субъекта, посягающее на установленный информационный порядок и причиняющее вред информационной сфере либо создающее реальную угрозу такого причинения.

За информационные правонарушения может наступать дисциплинарная, материальная, административная, гражданско-правовая, уголовная ответственность.

2. Дисциплинарная и материальная ответственность за правонарушения в информационной сфере.

Дисциплинарная ответственность – это специфический вид юридической ответственности, возникающий при неисполнении работником возложенных на него трудовых обязанностей без уважительных причин, выражающийся в осуждении поведения работника путем объявления ему властью нанимателя или уполномоченного им лица дисциплинарного взыскания.

Дисциплинарная ответственность наступает за совершение дисциплинарного проступка.

Дисциплинарный проступок – противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей (ст. 197 ТК).

Состав дисциплинарного проступка включает четыре элемента:

- 1) субъект;
- 2) субъективную сторону;
- 3) объект;
- 4) объективную сторону.

Субъектом дисциплинарного проступка является работник, т.е. лицо, состоящее в трудовых правоотношениях с нанимателем.

Субъективная сторона дисциплинарного проступка определяется отношением работника к своему поведению. При привлечении работника к дисциплинарной ответственности наниматель обязан установить наличие вины работника.

В соответствии с п. 3 Постановления Пленума ВС Республики Беларусь от 28 июня 2012 г. № 4 «О практике применения судами законодательства о трудовой дисциплине и дисциплинарной ответственности работников» Вина работника в совершении противоправного деяния может выражаться как в форме умысла, так и неосторожности. Неисполнение работником трудовых обязанностей по не зависящим от него причинам не может рассматриваться как дисциплинарный проступок.

Объект дисциплинарного проступка – это благо, на которое посягает нарушитель (права и обязанности сторон трудового отношения, интересы нанимателя, государства, имущество нанимателя, правила внутреннего трудового распорядка и т.п.).

Объективную сторону дисциплинарного проступка образуют вредные последствия, состоящие в причинной связи с действием (бездействием) работника-правонарушителя.

Отказ от выполнения работы, не входящей в круг трудовых обязанностей работника, либо выполнение которой противопоказано по состоянию здоровья, а также от выполнения общественного поручения не является нарушением трудовой дисциплины и не влечет применение мер дисциплинарного взыскания.

Виды дисциплинарной ответственности:

1) общая дисциплинарная ответственность, возникающая на основании Трудового кодекса Республики Беларусь и правил внутреннего трудового распорядка и распространяющаяся на всех работников, в том числе на тех, для которых установлена специальная дисциплинарная ответственность;

2) специальная дисциплинарная ответственность, возникающая на основании уставов и положений о дисциплине и распространяющаяся на отдельные категории работников (государственных служащих, сотрудников органов внутренних дел и т.д.).

К нарушителям трудовой дисциплины применяются следующие меры дисциплинарной ответственности (дисциплинарные санкции):

- 1) меры дисциплинарного взыскания;
- 2) иные меры дисциплинарной ответственности.

За совершение дисциплинарного проступка наниматель может применить к работнику следующие меры дисциплинарного взыскания:

- 1) замечание;
- 2) выговор;
- 3) лишение полностью или частично стимулирующих выплат на срок до двенадцати месяцев;
- 4) увольнение (пп. 6–11 ст. 42, пп. 1, 1², 5¹, 9 и 10 ч. 1 ст. 47 ТК).

Указанные меры дисциплинарного взыскания могут применяться ко всем работникам. Данный перечень является исчерпывающим в отношении работников, на которых не распространяется специальная дисциплинарная ответственность.

Для работников, на которых распространяется специальная дисциплинарная ответственность, согласно ч. 2 ст. 198 ТК могут применяться и другие дисциплинарные взыскания, предусмотренные уставами и положениями о дисциплине, а также иными актами законодательства.

Например, согласно Закону Республики Беларусь «О государственной службе в Республике Беларусь» к государственному служащему, помимо предусмотренных трудовым законодательством, могут применяться такие взыскания, как понижение в классе на срок до 6 месяцев, понижение в должности до 6 месяцев. Для адвокатов – порицание.

Право выбора меры дисциплинарного взыскания принадлежит нанимателю. При выборе меры дисциплинарного взыскания должны учитываться тяжесть дисциплинарного проступка, обстоятельства, при которых он совершен, предшествующая работа и поведение работника на производстве.

При применении к работнику меры дисциплинарного взыскания нанимателю следует исходить из положений ч. 3 ст. 198 ТК о строго индивидуальном подходе к каждому случаю совершения дисциплинарного проступка.

Если при рассмотрении дела будет установлено, что примененная нанимателем мера дисциплинарного взыскания не соответствует тяжести дисциплинарного проступка, степени вины работника, его предшествующей работе и поведению на производстве, суд может признать применение такого дисциплинарного взыскания незаконным и отменить его (ч. 2 ст. 202 ТК). При этом суд не вправе указывать, какое более мягкое дисциплинарное взыскание может быть применено к работнику, поскольку право выбора меры дисциплинарного взыскания принадлежит нанимателю.

К работникам, совершившим дисциплинарный проступок, независимо от применения мер дисциплинарного взыскания могут применяться: лишение премий, изменение времени предоставления трудового отпуска и другие меры. Виды и порядок применения этих мер определяются правилами внутреннего трудового распорядка, коллективным договором, соглашением, иными локальными правовыми актами (ч. 4 ст. 198 ТК).

В соответствии со ст. 200 ТК дисциплинарное взыскание применяется не позднее одного месяца со дня обнаружения дисциплинарного проступка, не считая времени болезни работника или ухода за больным членом семьи, подтвержденных листком нетрудоспособности или справкой о временной нетрудоспособности, пребывания работника в отпуске, нахождения на военных или специальных сборах.

Днем обнаружения дисциплинарного проступка считается день, когда о проступке стало известно лицу, которому работник непосредственно подчинен.

Доказательствами совершения дисциплинарного проступка могут являться, в частности, докладные записки, составленные в установленном порядке акты о допущенных нарушениях, материалы проверок, ревизий, проводимых вышестоящими в порядке подчиненности организациями, а также государственными органами.

Алкогольное, наркотическое или токсическое опьянение могут быть подтверждены медицинским заключением и другими видами доказательств, в том числе актом, свидетельскими показаниями, которые должны быть оценены судом.

При рассмотрении материалов о дисциплинарном проступке правоохранными органами дисциплинарное взыскание применяется не позднее одного месяца со дня отказа в возбуждении или прекращения уголовного дела.

Дисциплинарное взыскание не может быть применено позднее шести месяцев, а по результатам ревизии, проверки, проведенной компетентными государственными органами или организациями, – позднее двух лет со дня совершения дисциплинарного проступка. В указанные сроки не включается время производства по уголовному делу.

Дисциплинарное взыскание применяется органом (руководителем), которому предоставлено право приема (избрания, утверждения, назначения на должность) и увольнения работников, либо по поручению иным органом (руководителем).

В соответствии со ст. 199 ТК до применения дисциплинарного взыскания наниматель обязан затребовать письменное объяснение работника.

Отказ работника от дачи письменного объяснения не является препятствием для применения дисциплинарного взыскания и оформляется актом с указанием присутствовавших при этом свидетелей.

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

Дисциплинарное взыскание оформляется приказом (распоряжением, постановлением, решением, протоколом).

Дисциплинарное взыскание, предусмотренное п. 3 ч. 1 ст. 198 ТК, применяется с месяца, следующего за месяцем издания приказа (распоряжения, постановления, решения, протокола) о дисциплинарном взыскании.

Приказ (распоряжение, постановление, решение, протокол) о дисциплинарном взыскании с указанием мотивов объявляется работнику под роспись в пятидневный срок со дня издания, не считая времени болезни работника или ухода за больным членом семьи, подтвержденных листком нетрудоспособности или справкой о временной нетрудоспособности, пребывания работника в отпуске, нахождения на военных или специальных сборах. Работник, не ознакомленный в указанный срок с приказом (распоряжением, постановлением, решением, протоколом) о дисциплинарном взыскании, считается не имеющим дисциплинарного взыскания. Отказ работника от ознакомления с приказом (распоряжением, постановлением, решением, протоколом) о дисциплинарном взыскании оформляется актом с указанием присутствовавших при этом свидетелей.

Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, он считается не подвергавшимся дисциплинарному взысканию. При этом дисциплинарное взыскание погашается автоматически без издания приказа (распоряжения, постановления, решения, протокола).

Орган (руководитель), применивший взыскание, имеет право снять его досрочно до истечения года по собственной инициативе, по ходатайству непосредственного

руководителя, профсоюза или иного представительного органа (представителя) работников, а также по просьбе работника.

Досрочное снятие дисциплинарного взыскания оформляется приказом (распоряжением, постановлением, решением, протоколом).

Дисциплинарное взыскание может быть обжаловано в комиссию по трудовым спорам, суд, вышестоящий орган.

Органы, рассматривающие трудовые споры, вправе отменить взыскание. Наниматель после этого может применить более мягкое дисциплинарное взыскание, если не истекли сроки привлечения к дисциплинарной ответственности. При этом сроки рассмотрения трудового спора в органах по рассмотрению трудовых споров в них не включаются.

Вышестоящий орган (руководитель), рассматривающий трудовые споры отдельных категорий работников с особым характером труда вправе отменить, смягчить или усилить дисциплинарное взыскание, наложенное нижестоящим органом, если установит, что это взыскание не соответствует тяжести совершенного проступка.

Усиление не допускается, если вопрос о наложении взыскания рассматривается по жалобе работника.

Дисциплинарная ответственность в виде увольнения в информационных отношениях может применяться, например, за:

1) неоднократное (два и более раза в течение шести месяцев) представление в уполномоченные органы неполных либо недостоверных сведений (п. 11 ст. 42 ТК);

2) нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных (п. 10 ст. 47 ТК).

Материальная ответственность – это самостоятельный вид юридической ответственности, она выступает одной из составляющих механизма реализации прав и обязанностей субъектами трудовых правоотношений.

Материальная ответственность в трудовом праве состоит в обязанности одной стороны возместить ущерб, причиненный другой стороне трудового правоотношения, в случаях и порядке, предусмотренных трудовым законодательством.

В теории трудового права называют следующие признаки материальной ответственности:

- возникновение материальной ответственности обуславливается трудовым договором;
- ее субъектами являются только стороны трудового договора;
- ответственность возникает в результате обязанностей по трудовому договору;
- каждая из сторон несет материальную ответственность только за виновные нарушения своих обязанностей, если это повлекло ущерб у другой стороны;
- обе стороны могут возместить причиненный ущерб добровольно.

В соответствии со ст. 400 ТК работник может быть привлечен к материальной ответственности при одновременном наличии следующих условий:

- 1) ущерба, причиненного нанимателю при исполнении трудовых обязанностей;
- 2) противоправности поведения (действия или бездействия) работника;
- 3) прямой причинной связи между противоправным поведением работника и возникшим у нанимателя ущербом;
- 4) вины работника в причинении ущерба.

При определении размера ущерба учитывается только реальный ущерб, упущенная выгода не учитывается, за исключением случая причинения ущерба не при исполнении трудовых обязанностей (пункт 6 статьи 404 ТК). Под реальным ущербом понимаются утрата, ухудшение или понижение ценности имущества, влекущие необходимость для нанимателя произвести затраты на восстановление, приобретение имущества или иных

ценностей либо произвести излишние денежные выплаты (за исключением штрафов, взыскиваемых с нанимателя).

Противоправным признается такое поведение (действие или бездействие) работника, при котором он не исполняет или ненадлежащим образом исполняет обязанности, возложенные на него ТК, иными актами законодательства о труде, коллективным договором, иными локальными правовыми актами, трудовым договором.

Обязанность доказать факт причинения ущерба, а также наличие других условий материальной ответственности лежит на нанимателе.

Работники, которые несут полную материальную ответственность на основании пунктов 1, 2, 4 и 6 ст. 404 ТК, обязаны доказать отсутствие своей вины в причинении ущерба.

Недопустимо возложение на работника ответственности за вред, который относится к категории нормального производственно-хозяйственного риска (экспериментальное производство, введение новых технологий и др.).

Наниматель обязан создавать работникам условия, необходимые для нормальной работы и обеспечения сохранности вверенных им ценностей.

Работник, причинивший ущерб, может добровольно возместить его полностью или частично.

С согласия нанимателя работник может передать для возмещения причиненного ущерба равноценное имущество или исправить поврежденное.

Работники, как правило, несут полную материальную ответственность за ущерб, причиненный по их вине нанимателю.

Трудовым кодексом, коллективными договорами, соглашениями может устанавливаться ограниченная материальная ответственность работников за ущерб, причиненный нанимателю по их вине, за исключением случаев, предусмотренных ст. 404 ТК.

3. Административная ответственность за правонарушения в информационной сфере.

Административная ответственность выражается в порицании лица, совершившего административное правонарушение, и наложении административного взыскания на физическое лицо, совершившее административное правонарушение, юридическое лицо, подлежащее административной ответственности (ст. 4.1 КоАП).

В КоАП административная ответственность за нарушения в информационной сфере предусмотрены главой 23 «Административные правонарушения в области связи и информации»:

Статья 23.1. Несоблюдение порядка использования радиочастотного спектра и нарушение порядка ввоза радиоэлектронных средств и (или) высокочастотных устройств.

Несоблюдение порядка использования радиочастотного спектра, в том числе регистрации радиоэлектронных средств и (или) высокочастотных устройств, несоблюдение установленных параметров излучений радиоэлектронных средств и (или) высокочастотных устройств, а равно нарушение порядка ввоза на территорию Республики Беларусь радиоэлектронных средств и (или) высокочастотных устройств – *влекут наложение штрафа в размере до четырех базовых величин с конфискацией предмета административного правонарушения или без конфискации, а на индивидуального предпринимателя или юридическое лицо – наложение штрафа в размере до двадцати базовых величин с конфискацией предмета административного правонарушения или без конфискации.*

Статья 23.2. Нарушение правил охраны линий и сооружений связи.

1. Нарушение правил охраны линий и сооружений связи, если оно не повлекло перерыва связи, теле- и радиовещания, – *влечет наложение штрафа в размере до четырех базовых величин.*

2. Повреждение по неосторожности линий и сооружений связи, телевидения и радиовещания, повлекшее перерыв связи, теле- и радиовещания, – *влечет наложение штрафа в размере от десяти до тридцати базовых величин.*

Статья 23.3. Самовольное использование сетей электросвязи.

1. Самовольное использование сетей электросвязи или подключение к ним любых средств электросвязи или устройств, а равно подключение к сетям электросвязи не прошедших подтверждение соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации, технических регламентов Таможенного союза, Евразийского экономического союза средств электросвязи – *влекут наложение штрафа в размере до четырех базовых величин.*

2. Те же действия, совершенные повторно в течение одного года после наложения административного взыскания за такие же нарушения, – *влекут наложение штрафа в размере от десяти до тридцати базовых величин.*

Статья 23.4. Несанкционированный доступ к компьютерной информации.

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, – *влечет наложение штрафа в размере от двадцати до тридцати базовых величин.*

Статья 23.5. Нарушение законодательства о средствах массовой информации.

1. Нарушение законодательства о средствах массовой информации, выразившееся в незаконном ограничении свободы массовой информации, – *влечет наложение штрафа в размере от двадцати до тридцати базовых величин.*

2. Нарушение установленного порядка рассылки обязательных бесплатных экземпляров периодических печатных изданий – *влечет наложение штрафа в размере до двадцати базовых величин.*

3. Незаконное изготовление и (или) распространение продукции средств массовой информации – *влекут наложение штрафа в размере от двадцати до тридцати базовых величин с конфискацией предмета административного правонарушения или без конфискации.*

4. Распространение средством массовой информации информации, распространение которой запрещено в средствах массовой информации в соответствии с законодательными актами, за исключением случаев, когда ответственность за распространение такой информации предусмотрена иными статьями Особенной части КоАП, – *влечет наложение штрафа на юридическое лицо в размере до двухсот базовых величин.*

5. Распространение владельцем интернет-ресурса, не зарегистрированного в качестве сетевого издания, информации, распространение которой запрещено на интернет-ресурсах в соответствии с законодательными актами, за исключением случаев, когда ответственность за распространение такой информации предусмотрена иными статьями Особенной части КоАП, – *влечет наложение штрафа в размере до двадцати базовых величин, а на юридическое лицо – до ста базовых величин.*

6. Получение денежных средств и (или) другого имущества в целях финансирования средств массовой информации от иностранных юридических лиц, иностранных граждан и лиц без гражданства, постоянно не проживающих в Республике Беларусь, в случаях, когда это запрещено законодательными актами, а также от анонимных источников – *влечет наложение штрафа на юридическое лицо в размере до пятидесяти базовых величин с конфискацией полученных средств и (или) другого имущества.*

Статья 23.6. Разглашение коммерческой или иной охраняемой законом тайны.

Умышленное разглашение коммерческой или иной охраняемой законом тайны без согласия ее владельца лицом, которому коммерческая или иная охраняемая законом тайна

известны в связи с его профессиональной или служебной деятельностью, – влечет наложение штрафа в размере от четырех до двадцати базовых величин.

Статья 23.7. Нарушение законодательства о защите персональных данных.

1. Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных, – влекут наложение штрафа в размере до пятидесяти базовых величин.

2. Деяния, предусмотренные частью 1 настоящей статьи, совершенные лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью, – влекут наложение штрафа в размере от четырех до ста базовых величин.

3. Умышленное незаконное распространение персональных данных физических лиц – влечет наложение штрафа в размере до двухсот базовых величин.

4. Несоблюдение мер обеспечения защиты персональных данных физических лиц – влечет наложение штрафа в размере от двух до десяти базовых величин, на индивидуального предпринимателя – от десяти до двадцати пяти базовых величин, а на юридическое лицо – от двадцати до пятидесяти базовых величин.

Статья 23.8. Разглашение служебной тайны по неосторожности.

Разглашение служебной тайны либо утрата документов или компьютерной информации, содержащих сведения, составляющие такую тайну, или предметов, сведения о которых составляют такую тайну, совершенные по неосторожности лицом, имеющим или имевшим к ним доступ, если утрата явилась результатом нарушения установленных правил обращения с указанными документами, компьютерной информацией или предметами, – влекут наложение штрафа в размере от четырех до двадцати базовых величин.

Статья 23.9. Нарушение требований по использованию национального сегмента сети Интернет.

1. Осуществление деятельности по реализации товаров, выполнению работ, оказанию услуг на территории Республики Беларусь с использованием информационных сетей, систем и ресурсов, имеющих подключение к сети Интернет, не размещенных на территории Республики Беларусь и (или) не зарегистрированных в установленном порядке, – влечет наложение штрафа на индивидуального предпринимателя или юридическое лицо в размере от десяти до двадцати пяти базовых величин.

2. Нарушение требований законодательных актов по осуществлению идентификации абонентских устройств при оказании интернет-услуг и (или) пользователей интернет-услуг в пунктах коллективного пользования интернет-услугами, учету и хранению сведений об абонентских устройствах, персональных данных пользователей интернет-услуг, а также сведений об оказанных интернет-услугах – влечет наложение штрафа в размере от пяти до пятнадцати базовых величин.

3. Нарушение требований законодательства по ограничению доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами, – влечет наложение штрафа на индивидуального предпринимателя или юридическое лицо в размере от десяти до двадцати пяти базовых величин.

4. Невыполнение поставщиком интернет-услуг предусмотренных законодательными актами обязанностей по формированию и хранению актуальных сведений о посещаемых пользователями интернет-услуг информационных ресурсах – влечет наложение штрафа в размере от пяти до тридцати базовых величин, на индивидуального предпринимателя – от пятидесяти до ста базовых величин, а на юридическое лицо – до двухсот базовых величин.

Статья 23.10. Нарушение правил оборота специальных технических средств, предназначенных для негласного получения информации.

Незаконное изготовление или приобретение без цели сбыта, а также нарушение правил ввоза в Республику Беларусь и вывоза из Республики Беларусь специальных технических средств, предназначенных для негласного получения информации, – *влекут наложение штрафа в размере от пяти до тридцати базовых величин с конфискацией специальных технических средств, предназначенных для негласного получения информации.*

Правонарушения в информационной сфере содержатся и в иных главах КоАП. Например, в главе об административных правонарушениях, посягающих на права и свободы человека и гражданина (глава 10) предусмотрена ответственность за:

Статья 10.2. Оскорбление

1. Оскорбление, то есть умышленное унижение чести и достоинства личности, выраженное в неприличной форме, – *влечет наложение штрафа в размере до тридцати базовых величин.*

2. Оскорбление в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, распространенной в глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования или выделенной сети электросвязи, – *влечет наложение штрафа в размере от десяти до двухсот базовых величин, или общественные работы, или административный арест, а на юридическое лицо – наложение штрафа в размере от тридцати до двухсот базовых величин.*

Статья 10.5. Отказ в предоставлении гражданину информации.

Незаконный отказ должностного лица в предоставлении гражданину собранных в установленном порядке документов и материалов, непосредственно затрагивающих его права, свободы и законные интересы, либо предоставление ему неполной или умышленно искаженной информации – *влекут наложение штрафа в размере от пяти до тридцати базовых величин.*

Статья 10.10. Нарушение законодательства об обращениях граждан и юридических лиц.

1. Отказ в приеме обращения гражданина, индивидуального предпринимателя или юридического лица, либо нарушение установленных сроков рассмотрения такого обращения, либо непринятие в пределах своей компетенции мер по восстановлению нарушенных прав, свобод и (или) законных интересов заявителя – *влекут наложение штрафа в размере до четырех базовых величин.*

2. Отсутствие книги замечаний и предложений или непредъявление книги замечаний и предложений по первому требованию гражданина – *влекут наложение штрафа в размере до четырех базовых величин.*

4. Гражданско-правовая ответственность за правонарушения в информационной сфере.

Гражданско-правовая ответственность – это обеспеченное силой государственного принуждения возложение на правонарушителя неблагоприятных последствий совершенного им правонарушения в виде предусмотренных законодательством и (или) договором санкций имущественного характера, взыскиваемых по требованию потерпевшей стороны и направленных на восстановление ее имущественного положения.

Так в зависимости от основания различают договорную и внедоговорную ответственность. Договорная ответственность представляет собой санкцию за нарушение договорного обязательства. Внедоговорная ответственность имеет место тогда, когда соответствующая санкция применяется к правонарушителю, не состоящему в договорных отношениях с потерпевшим.

В соответствии с п. 4 ст.140 ГК информация, составляющая служебную тайну или коммерческую тайну, защищается способами, предусмотренными законодательством. В

случае незаконного ознакомления или незаконного использования, а также разглашения информации, которая составляет служебную тайну или коммерческую тайну, физические и юридические лица, государственные органы и их должностные лица обязаны возместить ее обладателю причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную тайну или коммерческую тайну вопреки обязательству о неразглашении коммерческой тайны, трудовому договору (контракту), и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Статьей 1010 ГК определено, что лицо, правомерно обладающее сведениями, составляющими секрет производства (ноу-хау), имеет право на защиту этих сведений от незаконного использования. Сведения, составляющие секрет производства (ноу-хау), охраняются в режиме коммерческой тайны в случае, если они соответствуют требованиям, определенным п. 2 ст. 140 ГК. Право на защиту таких сведений возникает независимо от выполнения в отношении этих сведений каких-либо формальностей (регистрации, получения свидетельства и т.п.).

Статья 1011 ГК предусматривает ответственность за незаконное использование секрета производства (ноу-хау). Лицо, правомерно обладающее секретом производства (ноу-хау), вправе потребовать от лица, незаконно его использующего, немедленного прекращения такого использования, а также вправе использовать иные способы защиты, предусмотренные законодательством.

В случае использования секрета производства (ноу-хау) лицом, которое в соответствии с законодательством является добросовестным приобретателем, суд с учетом средств, израсходованных таким лицом на использование секрета производства (ноу-хау), может разрешить его дальнейшее использование на условиях возмездности.

Лицо, самостоятельно и правомерно получившее сведения, составляющие секрет производства (ноу-хау), вправе использовать эти сведения независимо от прав обладателя соответствующего секрета производства (ноу-хау) и не отвечает перед ним за такое использование.

Кроме того за нарушение личных неимущественных прав гражданское законодательство предусматривает возмещение морального вреда (ст. 152 ГК). Например, в соответствии со ст.19 Закона о защите персональных данных моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, установленных указанным Законом, подлежит возмещению. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

5. Уголовная ответственность за преступления в информационной сфере.

Уголовная ответственность является наиболее строгим видом юридической ответственности. Основанием для ее наступления является совершение преступления, т.е. виновного общественно опасного деяния (действия или бездействия), характеризующегося признаками, предусмотренными УК, и запрещенного им под угрозой наказания.

Преступления против компьютерной безопасности, предусмотрены в главе 31 УК, которая состоит из 5 действующих статей.

Статья 349. Несанкционированный доступ к компьютерной информации.

1. Несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, –

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Уничтожение, блокирование или модификация компьютерной информации.

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, разрушение, блокирование либо нарушение работы компьютерной системы, сети или машинного носителя либо модификация компьютерной информации при отсутствии признаков преступления против собственности, повлекшие причинение существенного вреда, –

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, –

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 УК, –

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 352. Неправомерное завладение компьютерной информацией.

1. Умышленные несанкционированное копирование, перехват компьютерной информации либо иное неправомерное завладение компьютерной информацией, повлекшие причинение существенного вреда, –

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, –

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 УК, –

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств.

1. Разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения

компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, –

наказываются штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Те же действия, совершенные группой лиц по предварительному сговору, –
наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 УК, –
наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности причинение существенного вреда, –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, повлекшее по неосторожности последствия, указанные в части 2 статьи 349 УК, –

наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

К статьям других глав УК, в которых предусматривается ответственность за преступления в информационной сфере относятся:

Статья 188. Клевета.

Распространение заведомо ложных, порочащих другое лицо сведений (клевета) в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, размещенной в глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования или выделенной сети электросвязи, либо клевета, содержащая обвинение в совершении тяжкого или особо тяжкого преступления, –

наказываются штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Статья 198¹. Нарушение законодательства о средствах массовой информации.

Распространение владельцем интернет-ресурса, не зарегистрированного в качестве сетевого издания, информации, распространение которой запрещено на интернет-ресурсах в соответствии с законодательными актами, совершенное в течение года после наложения административного взыскания за такое же нарушение, –

наказывается общественными работами, или штрафом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 203. Нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений.

1. Умышленное незаконное нарушение тайны переписки, телефонных или иных переговоров, почтовых, телеграфных или иных сообщений граждан –

наказывается общественными работами, или штрафом, или исправительными работами на срок до одного года, или арестом.

2. То же деяние, совершенное с использованием специальных технических средств, предназначенных для негласного получения информации, либо должностным лицом с использованием своих служебных полномочий, –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или лишением свободы на срок до двух лет.

Статья 203¹. Незаконные действия в отношении информации о частной жизни и персональных данных.

1. Умышленные незаконные сбор, предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина, –

наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Умышленное незаконное распространение информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшее причинение существенного вреда правам, свободам и законным интересам гражданина, –

наказывается ограничением свободы на срок до трех лет или лишением свободы на тот же срок со штрафом.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга, –

наказываются ограничением свободы на срок до пяти лет или лишением свободы на тот же срок со штрафом.

Статья 203². Несоблюдение мер обеспечения защиты персональных данных.

Несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий, –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до одного года, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на срок до одного года.

Статья 204. Отказ в предоставлении гражданину информации.

Незаконный отказ должностного лица в предоставлении гражданину собранных в установленном порядке документов и материалов, непосредственно затрагивающих его права, свободы и законные интересы, либо предоставление ему неполной или умышленно искаженной такой информации, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина, –

наказываются штрафом или лишением права занимать определенные должности или заниматься определенной деятельностью.

Статья 373. Умышленное разглашение государственной тайны.

1. Умышленное разглашение сведений, составляющих государственную тайну, лицом, имеющим или имевшим доступ к этим сведениям, при отсутствии признаков измены государству или шпионажа –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, повлекшее тяжкие последствия, –

наказывается ограничением свободы на срок до пяти лет или лишением свободы на тот же срок.

Статья 374. Разглашение государственной тайны по неосторожности.

1. Разглашение сведений, составляющих государственную тайну, лицом, имеющим или имевшим доступ к этим сведениям, либо утрата документов или компьютерной информации, содержащих сведения, составляющие такую тайну, или предметов, сведения о которых составляют такую тайну, совершенные по неосторожности лицом, имеющим или имевшим к ним доступ, если утрата явилась результатом нарушения установленных правил обращения с указанными документами, компьютерной информацией или предметами, –

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до одного года, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на срок до одного года.

2. Те же деяния, повлекшие тяжкие последствия, –

наказываются ограничением свободы на срок до трех лет или лишением свободы на тот же срок.

Статья 375. Умышленное разглашение служебной тайны.

1. Умышленное разглашение экономических, научно-технических или иных сведений, составляющих служебную тайну, лицом, имеющим или имевшим доступ к этим сведениям, при отсутствии признаков преступлений, предусмотренных статьями 226¹, 254, 255, 356 и 358 УК, –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, повлекшее тяжкие последствия, –

наказывается ограничением свободы на срок до пяти лет или лишением свободы на тот же срок.

Статья 375¹. Незаконные собирание либо получение сведений, составляющих государственные секреты.

1. Незаконные собирание либо получение сведений, составляющих государственные секреты Республики Беларусь, а равно сведений, составляющих государственные секреты других государств, переданных Республике Беларусь в соответствии с законодательством Республики Беларусь, с целью их распространения при отсутствии признаков измены государству или шпионажа –

наказываются штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет.

2. Действия, предусмотренные частью 1 настоящей статьи, совершенные с использованием специальных технических средств, предназначенных для негласного получения информации, либо повлекшие тяжкие последствия, –

наказываются ограничением свободы на срок до пяти лет или лишением свободы на тот же срок.

Отдельно внимание заслуживает такое преступление как хищение имущества путем модификации компьютерной информации, предусмотренное в ст. 212 УК и отраженное в главе 24 преступления против собственности.

Статья 212. Хищение имущества путем модификации компьютерной информации.

1. Хищение имущества путем модификации компьютерной информации –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, –

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, –

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, –

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.