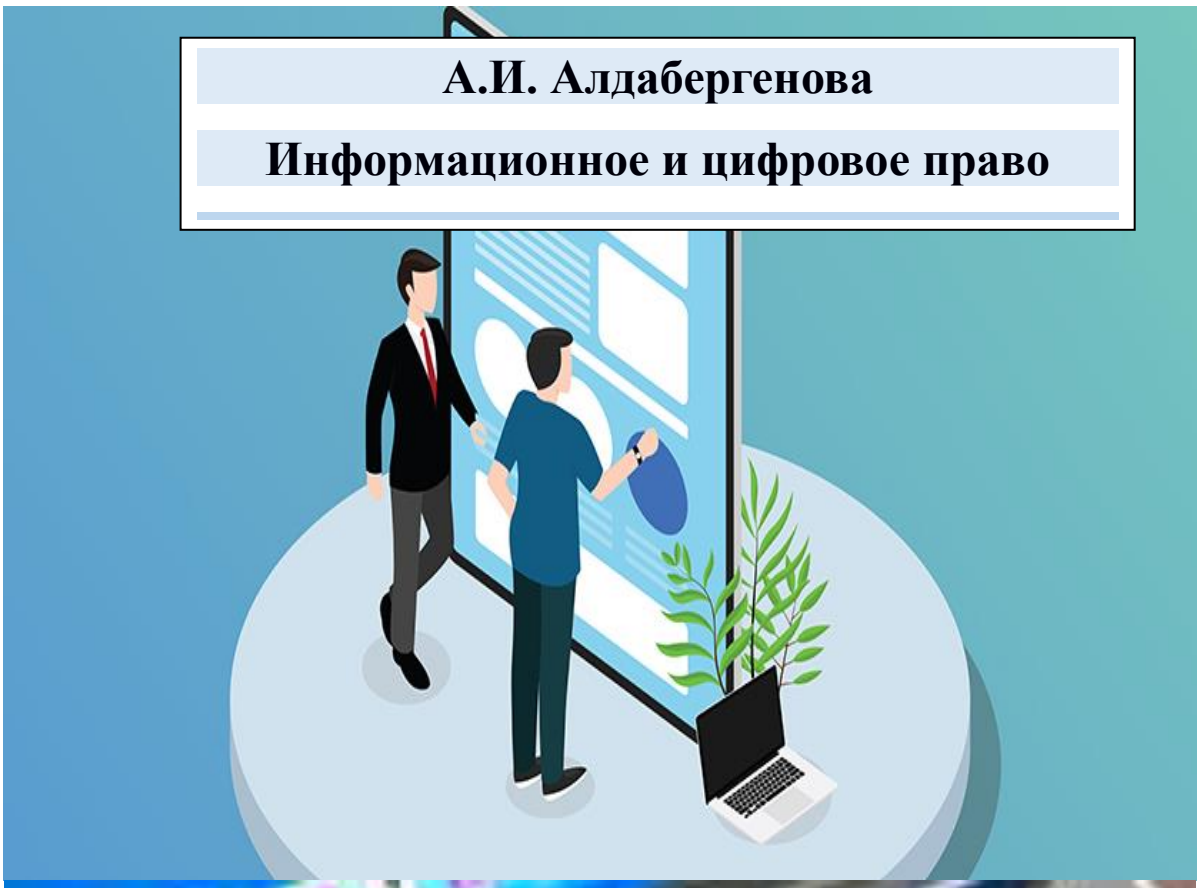
А.И. Алдабергенова

Информационное и цифровое право



Костанай, 2022

Институт экономики и права имени П.Чужинова

Кафедра гражданского права и процесса

А.И. Алдабергенова

Информационное и цифровое право

Учебно-методическое пособие

Костанай, 2022

УДК 342.951
ББК 67.401.114

Автор:
Алдабергенова Айгуль Ибрахимовна, магистр юридических наук, заведующая кафедрой гражданского права и процесса

Рецензенты:
Брылевский Андрей Владимирович - кандидат юридических наук, и.о.ассоциированного профессора кафедры уголовного права и процесса КРУ имени А. Байтурсынова
Хакимова Гульнара Еркеновна - кандидат юридических наук, и.о.ассоциированного профессора кафедры гражданского права и процесса КРУ имени А. Байтурсынова
Байзакова Гульсум Муратовна - кандидат юридических наук, доцент кафедры права Костанайского филиала ФГБОУ ВО «ЧелГУ»

Алдабергенова А.И.
А 40 Информационное и цифровое право. Учебно-методическое пособие. Костанай: КРУ им.А.Байтурсынова, 2022. - 90 с.

ISBN 978-601-356-213-1

В учебно-методическое пособие включены основные характеристики цифровых технологий, правовых режимов информатизации и цифровизации, развития цифровой инфраструктуры; в данном пособии раскрываются проблемы идентификации субъектов интернет-отношений, основные подходы к решению проблем информационной безопасности на современном этапе развития Казахстана.

Учебно-методическое пособие предназначено для студентов образовательной программы «Юриспруденция»; оно может быть рекомендовано преподавателям высших учебных заведений при проведении учебных занятий по информационному и цифровому праву.

ББК 67.412.1
А 40

Утверждено и рекомендовано к изданию Учебно-методическим советом Костанайского регионального университета имени А.Байтурсынова, ___.___.2022 г. протокол № ___

ISBN 978-601-356-213-1

Содержание

Введение

Прежде всего хотелось бы заметить, что появление интернета, являющегося ничем иным, как информационной технологией, оказало и продолжает оказывать колоссальное воздействие буквально на все сферы отношений, традиционно подвергающиеся правовому регулированию. В связи с этим нельзя не вспомнить известное высказывание американского юриста Роберта Дж. Амброги, в начале 2000-х написавшего: «Интернет породил свою собственную сферу права. Интернет-право - это динамичная, гибкая и неизведанная область практики, где правила еще не определены окончательно. На самом деле это даже не отдельная область права, фактически это смесь теории и практики, взятых из различных сфер, - мешанина из частей, взятых из интеллектуальной собственности, гражданских свобод, деликтного, уголовного, имущественного, телекоммуникационного, международного торгового, коммерческого и коллизионного права» [1, с.76].

Таким образом, в зарубежной юриспруденции информационное и цифровое право изначально рассматривалось не как самостоятельная отрасль права, а как некая совокупность разнонаправленных правовых норм и институтов, относящихся к различным отраслям (областям) права и регулирующих отношения, которые так или иначе связаны с интернетом.

Важно обратить внимание на следующее: в определенный момент стало очевидным, что влияние технологий на право не ограничивается исключительно интернетом – значимыми для права могут оказаться разнообразные информационные технологии. При этом понятие «информационные технологии» в широком смысле употребляется для обозначения вычислений, под которыми в рассматриваемом контексте понимаются не расчеты и подсчеты, а «проектирование и создание аппаратных и программных систем для широкого спектра целей; обработку, структурирование и управление различного рода информацией; проведение научных исследований с использованием компьютеров; обеспечение интеллектуального поведения компьютерных систем; создание и использование средств связи и развлечений; поиск и сбор информации, относящейся к какой-либо конкретной цели, и т.д.» [3]. В узком же смысле термин «информационные технологии» («информационно-коммуникационные технологии») используют для обозначения технологий, обеспечивающих доступ, хранение, поиск, передачу и манипулирование данными (информацией) и необходимых для удовлетворения практических, повседневных потребностей бизнеса и пользователей.

Изложенное, на наш взгляд, свидетельствует о том, что информационное и цифровое право - это уже не прежний набор правовых норм и институтов, характерный для интернет-права: интернет-право теперь становится лишь одной из составляющих цифрового права. Кроме того, внедрение и использование цифровых технологий требует не только правовой регламентации, но и технического, и этического регулирования, что должно учитываться при разработке нормативно-правовых положений.

Резюмируя, можно заключить, что информационное и цифровое право следует понимать, как совокупность правовых норм и институтов, регулирующих разнообразные отношения, связанные с внедрением и использованием цифровых и информационных технологий, но эти нормы не объединены единым методом регулирования и относятся к различным отраслям права. Причем информационное и цифровое право представляет собой динамично расширяющееся правовое образование: на сегодня оно охватывает, в частности, проблематику электронных платежей, электронных и мобильных денег, электронного банкинга, защиты прав потребителей на платежных рынках, искусственного интеллекта, аналитики больших данных, конкурентных отношений в эпоху больших данных, блокчейна, криптовалюты, смарт-контрактов, цифровой идентификации и аутентификации, конфиденциальности, пересечения законодательства о конкуренции и интеллектуальной собственности, поисковых систем, уберизации, цифровизации интеллектуальной собственности, электронных доказательств, международной торговли и цифровой торговли, электронных услуг, интернет-платформ, цифровых товаров, управления контрактами, национальной безопасности, глобальных потоков данных, договорных отношений и условий контрактов, незаконного присвоения интеллектуальной собственности, защиты коммерческой тайны, авторских и смежных прав, прав на товарные знаки, доменных имен и ip-адресов, патентных прав, лицензирования, переговоров и заключения договоров в электронной форме, киберспорта, программного обеспечения, азартных игр, геномов, телемедицины и данных о здоровье, баз данных и контента, распределения рисков, управления и обслуживания сети, диффамации, кибербулинга, онлайн-сервисов, агрегаторов, онлайн-арбитража и онлайн-посредничества, налогов и пр.

Модуль 1. Общие положения информационного права Республики Казахстан

Тема 1.1. Информационное право - правовая основа информационного общества

Цель: ознакомить студентов с целью и назначением курса, его ролью и местом в системе учебных дисциплин. Раскрыть понятие информации, роль информации в жизни личности

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- умением анализировать основные положения информационного права и соотносить их с иными отраслями права, содержащимися в специальных законах;
- умением решать базовые задачи по данной тематике на практических занятиях;
- способностью использовать углубленные специализированные теоретические знания, практические навыки и умения для организации научных и научно-прикладных исследований, учебного процесса, аналитической деятельности.

План:

1. Понятие информации.
2. Понятие и признаки информационного общества.
3. Государственная информационная политика: цели, задачи, особенности реализации.

1. Понятие информации

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

В общем смысле информация представляет собой сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком; сообщения, осведомляющие о положении дел, о состоянии чего-либо. Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно.

В соответствии с Законом Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации» информация - это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, полученные или созданные обладателем информации, зафиксированные на любом носителе и имеющие реквизиты, позволяющие ее идентифицировать.

И.Л. Бачило в одном из своих учебников упоминает, что наука об информации - информатика - стала формироваться несколько веков назад. Ее

упрощенно трактуют как научную дисциплину, изучающую закономерности получения, отбора, хранения, передачи, преобразования и применения информации (знаний) в самых разных областях общественной деятельности… Разрешение правовых проблем информатики можно рассматривать как сферу информационного права.

Информация является основным объектом, по поводу которого возникают общественные отношения между различными субъектами в информационной сфере. Являясь разновидностью правовых отношений, информационные отношения регулируются информационно-правовыми актами, которые устанавливают порядок распространения информации, доступа к ней, ограничения, защиты и т.п.

В настоящее время для регулирования информационных отношений действует значительное количество норм, регламентирующих технические и правовые аспекты информационного обмена, информационных технологий и обеспечения информационной безопасности как на уровне нормативных правовых актов, так и на уровне различных ведомственных нормативных и ненормативных актов.

Реализация права на осуществление, поиск, получение и передачу информации (право на доступ к информации или право знать) является важнейшим определяющим институтом информационного права. Юридический фундамент этого института составляют информационно-правовые нормы Конституции РК. Право на доступ к информации содержится в ст. 20 Конституции: «Каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом».

К числу признаков, свойств информации можно отнести:

а) ее системность. Информация, как и любой другой объект реальности, обладает системной структурой. Совокупность информации о чем-либо формирует понятие «знание»;

б) неисчерпаемость информации;

в) материальность информации (информация - это нечто, что может объективно существовать (к примеру, на материальном носителе), кроме того, она отражает многообразие материального мира;

г) объективность информации: информация - отражение внешнего объективного мира;

д) идеальность информации - часто информацию мы воспринимаем с помощью технических средств.

Существует множество критериев классификации информации.

1) по степени организованности (упорядоченности) выделяют документированную и иную информацию; информационные ресурсы и свободную информацию, не находящуюся в информационных системах; систематизированную информацию (каталоги, энциклопедии, рубрикаторы и т.п.) и несистематизированную;

2) по виду носителя (форме закрепления) - на бумажном носителе, видео- и звуковая, компьютерная информация, в объемно-пространственной форме, устная, энергетическая (биологическая) при энергоинформационном обмене;

3) по степени доступа - информация с ограниченным доступом, информация без права ограничения доступа, объекты интеллектуальной собственности, «вредная информация» с ограничением по распространению, иная общедоступная информация;

4) по функциональному предназначению (по сфере применения) - массовая информация, распространяемая через СМИ, и отраслевая, профессиональная (по интересам) информация и т.д.

2. Понятие и признаки информационного общества

Информационное общество - это термин, применяемый для обозначения современного состояния индустриально развитых стран, связанного с новой ролью информации во всех сторонах их жизнедеятельности, качественно новым уровнем производства, переработки и распространения информации.

Своим названием термин «информационное общество» обязан профессору Токийского технологического института Ю. Хаяши, чей термин был использован в появившихся практически одновременно - в Японии и США - в работах Ф. Махлупа (1962) и Т. Умесао (1963). Теория «информационного общества» была развита такими известными авторами, как М. Порат, Й. Массуда, Т. Стоунер, Р. Карц и др.

Как отмечает В.А. Копылов, в соответствии с концепцией З. Бжезинского, Д. Белла, О. Тоффлера, поддерживаемой и другими зарубежными учеными, информационное общество - разновидность постиндустриального общества. Рассматривая общественное развитие как «смену стадий», сторонники этой концепции информационного общества связывают его становление с доминированием «четвертого», информационного сектора экономики, следующего за тремя известными секторами - сельским хозяйством, промышленностью и экономикой услуг. При этом они утверждают, что капитал и труд, как основа индустриального общества, уступают место информации и знаниям в информационном обществе.

К признакам информационного общества можно отнести:

1) высокий уровень развития информационных технологий и их интенсивное использование гражданами, бизнесом и государственными органами;

2) получение гражданами и организациями преимуществ от применения информационных технологий за счет:

а) обеспечения равного доступа к информационным ресурсам;

б) развития цифрового контента;

в) применения инновационных технологий и радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе.

И.Л. Бачило акцентирует внимание на вопросе синтеза информационного и гражданского, а, следовательно, и правового общества.

И.М. Рассолов видит структуру информационного общества двухуровневой, включающей:

- интересы и ценности;

- индивиды, территория и социальные структуры.

При этом важным фактором формирования информационного общества являются общественные связи или информационные отношения.

Охарактеризуем основные элементы представленной структуры информационного общества.

Интересы - это причины действий или поступков, а также выражение значимости объектов окружающего мира для человека.

Ценности - это установки и оценки, императивы и запреты, цели и проекты, выраженные в форме нормативных представлений, т.е. «ориентиры деятельности человека».

Индивид является основным элементом любого общества, в том числе и информационного, а территория является основой социального информационного пространства.

Под социальными структурами понимаются устойчивые социальные образования, социальные общности и социальные институты. К примеру, приобретший сегодня особенную популярность твиттер.

3. Государственная информационная политика: цели, задачи, особенности реализации

Государственную информационную политику определяют как совокупность целей, отражающих национальные интересы в информационной сфере, стратегии, тактики управленческих решений и методов их реализации, разрабатываемых и реализуемых государственной властью для регулирования и совершенствования, как непосредственно процессов информационного взаимодействия во всех сферах жизнедеятельности общества и государства, так и процессов технологического (в широком смысле) обеспечения такого взаимодействия.

При этом цели государственной политики определяют необходимость решения задач не только в сфере информационных технологий, но и в других отраслях экономики, науке и технике, социальной сфере и государственном управлении.

Повышение качества жизни граждан и улучшение условий развития бизнеса в информационном обществе предусматривает:

- развитие сервисов для упрощения процедур взаимодействия общества и государства с использованием информационных технологий;
- перевод государственных услуг в электронный вид;
- развитие инфраструктуры доступа к сервисам электронного государства;
- повышение открытости деятельности государственных органов;
- создание и развитие электронных сервисов в области здравоохранения, а также в областях жилищно-коммунального хозяйства, образования и науки, культуры и спорта.

Построение электронного правительства и повышение эффективности государственного управления предусматривает:

- формирование единого пространства электронного взаимодействия;

- создание и развитие государственных межведомственных информационных систем, предназначенных для принятия решений в реальном времени;

- создание справочников и классификаторов, используемых в государственных информационных системах;

- повышение эффективности внедрения информационных технологий;

- создание инфраструктуры пространственных данных РК;

- развитие системы учета результатов научно-исследовательских и опытно-конструкторских работ, выполненных в рамках государственного заказа;

- обеспечение перевода в электронный вид государственной учетной деятельности;

- создание и развитие специальных информационных и информационно-технологических систем обеспечения деятельности государственных органов, в том числе защищенного сегмента сети Интернет и системы электронного документооборота.

Развитие рынка информационных технологий, обеспечение перехода к экономике, осуществляемой с помощью информационных технологий, предусматривает:

- стимулирование отечественных разработок в сфере информационных технологий;

- подготовку квалифицированных кадров в сфере информационных технологий;

- развитие экономики и финансовой сферы на основе использования информационных технологий;

- формирование социально-экономической статистики развития информационного общества;

- развитие технопарков в сфере высоких технологий. Преодоление высокого уровня различия в использовании информационных технологий различными слоями общества и создание базовой инфраструктуры информационного общества предусматривает:

- развитие телерадиовещания;

- развитие базовой инфраструктуры информационного общества;

- популяризацию возможностей и преимуществ информационного общества;

- повышение готовности населения и бизнеса к возможностям информационного общества, в том числе обучение использованию современных информационных технологий.

Обеспечение безопасности в информационном обществе предусматривает:

- противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам Республики Казахстан;

- обеспечение технологической независимости в отрасли информационных технологий;

- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасность информации ограниченного доступа;

- обеспечение развития законодательства РК и совершенствование правоприменительной практики в сфере информационных технологий.

Контрольные вопросы:

1. Определите соотношение понятий: «информация», «информационные ресурсы», «информатизация», «информационные технологии».

2. Какие признаки присущи информации?

3. Охарактеризуйте информационную деятельность государства и органов местного самоуправления.

4. Какими нормами Конституции РК закреплены основы информационной деятельности государства.

5. В чем заключается особенность информационной политики государства?

Тестовые задания:

1. Укажите неверный ответ. К свойствам информации относятся:
A) системность;
B) неисчерпаемость;
C) материальность;
D) объективность;
E) актуальность.

2. Укажите признак информации:
A) специфичность;
B) комплектность;
C) идеальность;
D) качество;
E) актуальность.

3. Укажите критерий информации, классифицирующий систематизированную информацию (каталоги, энциклопедии, рубрикаторы и т.п.) и несистематизированную:
A) по виду носителя;
B) по степени организованности;
C) по форме закрепления;
D) по степени доступа;
E) по функциональному предназначению.

4. По функциональному предназначению (по сфере применения) информация делится на:
A) массовую и отраслевую;
B) информационные ресурсы и свободную информацию;

C) видео- и звуковую;
D) полезную и вредную;
E) каталоги и энциклопедии.

5. Информация с ограниченным доступом, информация без права ограничения доступа классифицируется в соответствии с критерием:
A) по виду носителя;
B) по степени доступа;
C) по степени упорядоченности;
D) по форме закрепления;
E) по функциональному предназначению.

6. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, полученные или созданные обладателем информации, зафиксированные на любом носителе и имеющие реквизиты, позволяющие ее идентифицировать – это?
A) секреты производства;
B) коммерческая тайна;
C) информация;
D) государственные секреты;
E) инструкция.

7. Укажите признак информационного общества:
A) специфика образовательной деятельности;
B) обеспечение безопасности эксплуатации строительных объектов;
C) предоставление конечного результата проектно-изыскательских работ;
D) высокий уровень развития информационных технологий;
E) актуальность темы научной статьи.

8. Развитие цифрового контента относится к признакам:
A) капиталистического общества;
B) индустриального общества;
C) информационного общества;
D) современного общества;
E) постиндустриального общества.

9. Нормативно-правовой акт, содержащий нормы о праве на доступ к информации:
A) Закон о некоммерческих организациях;
B) Уголовно-процессуальный кодекс;
C) Земельный кодекс;
D) Конституция;
E) Кодекс о недрах.

10. Определите признак информации, отражающий внешний объективный мир:

A) системность;
B) неисчерпаемость;
C) материальность;
D) объективность;
E) идеальность.

Тема 1.2. Понятие, предмет, методы, принципы информационного права и его место в правовой системе казахстанского права

Цель: раскрыть понятие, предмет, методы и принципы информационного права.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате изучения данной темы студент должен обладать следующими компетенциями:

- осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- быть способным юридически правильно квалифицировать факты и обстоятельства.
- анализировать и соотносить нормы, регулирующие методы, принципы информационного права.

План:

1. Понятие информационного права, его предмет и метод. Принципы информационного права.
2. Система и источники информационного права.
3. Информационное право в системе казахстанского права. Информационное право как наука.

1. Понятие информационного права, его предмет и метод. Принципы информационного права

Информационное право - это отрасль казахстанского права, нормы которой регулируют общественные отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

К определению информационного права как отрасли права, его содержанию современные специалисты подходят неоднозначно. Информационное право можно рассматривать: 1) как отрасль права; 2) как науку; 3) как учебную дисциплину.

И.Л. Бачило подчеркивает, что отрасль информационного права отличается от других отраслей права тем, что имеет свой ярко выраженный предмет отношений. В состав предмета она включает отношения, воплощенные:

1) в информации при разнообразии форм ее проявления и формируемых на этой основе информационных ресурсах;

2) средствах и технологиях работы с информацией (информационных технологиях);

3) средствах и технологиях передачи информации по сетям связи.

Таким образом, подводя итог, можно определить предмет информационного права как общественные отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Предмет и метод правового регулирования органически связаны между собой. Если предмет отрасли права отвечает на вопрос «что?», то сущность метода правового регулирования соответствует вопросам «как?», «каким образом происходит правовое регулирование отношений, складывающихся между их участниками?».

По общему правилу методом правового регулирования называется совокупность приемов и способов, с помощью которых осуществляется воздействие на участников правовых отношений. Метод правового регулирования можно определить как специфический способ, при помощи которого государство на основе данной совокупности юридических норм обеспечивает нужное ему поведение людей как участников правоотношения.

Метод правового регулирования влияет на выбор способов установления прав и обязанностей субъектов, степень свободы действий субъектов в рамках правоотношения, их правовое положение по отношению друг к другу, а также на возможность использования тех или иных средств защиты субъективных прав участников правоотношения. Эффект подобного влияния достигается с помощью двух приемов правового регулирования: императивного и диспозитивного.

В теории права встречаются различные наименования базовых методов правового регулирования: императивный (авторитарный, метод централизации, или субординации, административно-правовой, метод властных предписаний, метод власти и подчинения) и диспозитивный (автономный, метод децентрализации или координации, гражданско-правовой, метод равенства сторон). Определим различия между ними.

При императивном регулировании правовое положение участников правоотношения строится на началах неравенства. Один из участников всегда наделяется властными полномочиями по отношению к другому. Как правило субъект, наделенный властными полномочиями, является государственным органом либо органом, уполномоченным государством на совершение определенных действий и наделенным правом издания односторонне-властных предписаний, адресованных другому участнику. Права и обязанности субъектов правоотношения, построенного на принципах власти-подчинения, подлежат жесткой регламентации со стороны государства, и объем правомочий не может быть изменен участниками самостоятельно.

При диспозитивном регулировании правоотношений участники находятся в равном, равноправном положении, наделяются правом выстраивать свои

взаимоотношения на взаимовыгодных условиях или отказаться от участия в подобных отношениях. Государство предоставляет возможность участникам диспозитивных отношений выбирать для себя наиболее приемлемый вариант поведения, ограничивая этот выбор лишь соображениями законности. Отношения между субъектами строятся не на основе односторонне-властных предписаний, а на базе свободного договора.

Теория разделения методов правового регулирования на диспозитивные и императивные тесно связана с разделением всего правового массива на частное и публичное право. Императивное регулирование традиционно присуще публично-правовым отраслям права, соответственно диспозитивное - отраслям, относящимся к разряду частноправовых.

Трансформируясь из базовых методов правового регулирования в отраслевые, каждый из методов приобретает специфическую окраску, уникальный набор приемов и способов правового регулирования, свойственный только данной отрасли права.

Отрасль информационного права обладает методом правового регулирования, сочетающим в себе элементы императивного и диспозитивного начал.

Проиллюстрируем сказанное на примере норм Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

Диспозитивное регулирование, к примеру, установлено в ст. 10 данного закона, согласно которой доступ к персональным данным определяется условиями согласия субъекта или его законного представителя, предоставленного собственнику и (или) оператору на их сбор и обработку. При этом субъект вправе дать согласие на сбор, обработку персональных данных через кабинет пользователя на веб-портале «электронного правительства», сервис обеспечения безопасности персональных данных, а также посредством зарегистрированного на веб-портале «электронного правительства» абонентского номера сотовой связи субъекта путем передачи одноразового пароля или путем отправления короткого текстового сообщения в качестве ответа на уведомление веб-портала «электронного правительства».

Императивное регулирование установлено в достаточно большом числе норм указанного закона. Например, согласно, ст. 24 право субъекта персональных данных на доступ к его персональным данным может:

- знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую:

- подтверждение факта, цели, источников, способов сбора и обработки персональных данных;

- перечень персональных данных;

- сроки обработки персональных данных, в том числе сроки их хранения;

- требовать от собственника и (или) оператора изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами;

- требовать от собственника и (или) оператора, а также третьего лица блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;

- требовать от собственника и (или) оператора, а также третьего лица уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

- дать согласие (отказать) собственнику и (или) оператору на распространение своих персональных данных в общедоступных источниках персональных данных;

- на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда.

Таким образом, специфика метода информационного права отражается в уникальном сочетании способов правового регулирования, определенном основными направлениями и принципами государственной информационной политики.

Находясь на этапе своего становления, информационное законодательство нуждается в серьезной методологической «подпитке», разработке основ теории информационного права. На сегодняшний день действующие нормативные акты не представляют собой систему информационного законодательства, в полной мере обеспечивающую регулирование складывающихся правоотношений в информационной сфере.

Одним из важнейших аспектов методологии является вопрос правовых принципов, в которых заложена суть правовых норм. Под принципами права понимаются выраженные в праве исходные нормативно-руководящие начала, характеризующие его создание, его основы, закрепленные в нем закономерности общественной жизни.

Решение задачи определения основополагающих принципов сегодня наиболее актуально для одного из десяти выделяемых блоков проблем информационного законодательства: информационная деятельность, информационные отношения (формирование и использование информационных ресурсов, информационных систем; специализация организаций на информационной деятельности; обеспечение информационных потребностей граждан, юридических лиц; регулирование рынка информации и услуг и т.д.).

Поскольку принципы - это основополагающие идеи (требования), определяющие в своей совокупности идеальную конструкцию (модель) регулирования конкретной области общественных отношений, вопросу их детальной регламентации необходимо самое пристальное внимание. При этом необходим учет всех существенных признаков понятия «принципы права», разработанных философами и юристами, таких как:

а) закрепленность принципа в нормативном правовом акте, т.е. конкретном источнике информационного права;

б) предметная определенность. Она означает, что объективным критерием для определения принципа служит специфика предмета правового

регулирования, т.е. особенности информационных правоотношений, регулируемых нормами права. Другими словами, принцип должен выражать сущность совокупности каких-то норм с точки зрения того, что они регулируют;

в) целевая направленность. Этот принципообразующий признак даёт возможность выделить принципы правовой защиты по направлениям и желаемым результатам в области правового регулирования информационных правоотношений. Признак целенаправленности означает, что принцип должен выражать сущность определенной совокупности норм права не только в статике, но и в динамике, в направлении достижения целей;

г) нормативность. Как признак, она, в конечном счете, сводится к указанию того, что в общем случае может человек как субъект права и что обязаны и не могут государство, общество и другие люди по отношению к нему как субъекту права. Нормативность означает, что принципы права не только выражают ее существенные свойства, но также выступают и в качестве общего правила поведения субъектов общественных отношений, что, будучи закрепленными в правовых нормах, они приобретают значение общих правил поведения, имеющих регулятивный характер, и что, кроме того, они являются нормами прямого действия;

д) выражение внутреннего единства совокупности правовых норм института правовой защиты. Принципы права вносят единообразие во всю систему юридических норм правового института и придают глубокое единство правовому регулированию общественных отношений, цементируют все элементы механизма правовой защиты данных отношений, когда ими пронизываются не какие-либо отдельные, а все ее нормы;

е) стабильность. Этот признак означает, что принцип права действует в течение определенного, относительно длинного времени. Отражая качественное состояние системы права, он не может быть изменчив в такой же мере, как правовые нормы. При этом устойчивость не означает неподвижность. Напротив, устойчиво то, что способно к изменениям, к развитию;

ж) универсальность. Данный признак является ведущим при выделении принципа из норм права. Это важнейшее свойство, которое отличает его от правовой нормы. Универсальность принципа базируется на его общезначимости, общеобязательности, высшей императивности и прямом действии;

з) истинность. Принципом может быть только такое положение, которое не противоречит иным принципам права и правовой защиты, опыту и юридической практике;

и) взаимосвязь и взаимообусловленность принципов правовой защиты. Взаимосвязь принципов предполагает их взаимное воздействие Характер связи может быть различным: содержание, причина, следствие, прямая, косвенная, непосредственная связь принципов определяется единой целью;

к) стабильные нормативно-руководящие положения должны быть присущи правовой действительности, формируются под воздействием экономических и социально-политических факторов и определяющей

качественные особенности правового регулирования специфической группы общественных отношений;

л) сложившиеся на базе социально-политических и экономических явлений стабильные нормативно-руководящие начала выступают основой практической деятельности правотворческих органов, субъектов права;

м) принципы права олицетворяют собой объективные закономерности развития общественных отношений и служат правильным ориентиром отражения и использования указанных закономерностей, воплощая в себя функцию единства правового регулирования.

Базовые принципы регулирования информационных отношений сформулированы в Законе Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» - это:

1) законность;

2) соблюдение прав, свобод и законных интересов физических лиц, а также прав и законных интересов юридических лиц;

3) равенство прав физических и юридических лиц на участие в деятельности в сфере информатизации и использование ее результатов;

4) обеспечение свободного доступа к электронным информационным ресурсам, содержащим информацию о деятельности государственных органов (презумпция открытости), и обязательного их предоставления, кроме электронных информационных ресурсов, доступ к которым ограничен в соответствии с законами Республики Казахстан;

5) своевременность предоставления, объективности, полноты и достоверности электронных информационных ресурсов, в отношении которых законами Республики Казахстан установлен обязательный характер их публичного распространения либо предоставления государственными органами;

6) свобода поиска, формирования и передачи любых электронных информационных ресурсов, доступ к которым не ограничен в соответствии с законами Республики Казахстан;

7) обеспечение безопасности личности, общества и государства при применении информационно-коммуникационных технологий;

8) создание условий для развития отрасли информационно-коммуникационных технологий и добросовестной конкуренции;

9) обеспечение централизованного управления объектами информатизации «электронного правительства»;

10) осуществление деятельности по информатизации на территории Республики Казахстан на основе единых стандартов, обеспечивающих надежность и управляемость объектов информатизации.

Как известно, имея общеобязательный характер, принципы права способствуют укреплению внутреннего единства и взаимодействия различных его отраслей и институтов, правовых норм и правовых отношений.

Проанализируем, например, внутриотраслевые принципы формирующегося института предоставления государственных услуг, в том

числе, в электронной форме, института, в котором в большей мере проявляется публично-правовой аспект информационных правоотношений.

Не вызывает сомнений, что основным характеризующим признаком совокупности норм, определяющих правовое обеспечение формирования и использования информационных ресурсов, является ее комплексность. Правовое регулирование общественных отношений в рассматриваемой области человеческой деятельности осуществляется нормами и методами конституционного, административного, гражданского права, а также иных отраслей права. Институт предоставления государственных услуг - не исключение, к нему в полной мере присущ признак комплексности.

2. Система и источники информационного права

Информационное право, являясь отраслью права, состоит из множества отдельных информационно-правовых норм, совокупность которых выражается в сложной целостной системе. Внутри этой единой системы информационно-правовые нормы в определенной последовательности и взаимосвязи группируются в различные институты и более крупные подразделения.

Система информационного права - это объективно обусловленное системой общественных информационных отношений внутреннее строение, объединение и расположение информационно-правовых норм в определенной последовательности.

В системе информационного права выделяются части, разделы, институты. Наиболее крупные подразделения информационного права - это его общая и особенная части.

К Общей части относятся нормы информационного права, которые закрепляют основные принципы, формы и методы информационной деятельности граждан, государства, государственных органов, органов местного самоуправления.

Нормы Общей части информационного права конкретизируются в его Особенной части. Особенная часть состоит из нескольких разделов, включающих соответствующие информационно-правовые институты. Каждое из этих подразделений представляет собой совокупность информационно-правовых норм, регулирующих группу однородных информационных отношений. Информационно-правовой институт объединяет правовые нормы, регулирующие узкую и близкую по содержанию группу информационных отношений.

Особенную часть информационного права составляют разделы, в которых сгруппированы нормы, регулирующие отношения в области:

- реализации основных информационных прав и свобод, например, права на информацию;
- организации и деятельности средств массовой информации;
- обработки персональных данных;
- электронного документооборота;
- обеспечения информационной безопасности и др.

Остановимся на вопросе понятия института информационного права. Признаками правового института являются:

а) юридическое единство правовых норм, определяемое предметной средой отношений;

б) возможность обеспечить полноту регулирования совокупности однородных отношений;

в) возможность обособить нормы, образующие институт в одном акте или существенно связанных между собой нескольких нормативных правовых актов.

Итак, институт информационного права - это относительно устойчивая группа информационно-правовых норм, регулирующая определенную группу информационных отношений. Так, институтами информационного права будут являться: институт правового режима информационных ресурсов, институт права на информацию, институт средств массовой информации и т.д. При этом особенная часть кодекса представлена тремя суперинститутами:

1) правовой режим информации, информационных ресурсов, информационных технологий и коммуникаций;

2) право на информацию;

3) правовое обеспечение информационной безопасности. Нормы информационного права РК содержатся в большом числе разнообразных правовых нормативных актов или источниках.

Источники информационного права - это правовые акты представительных и исполнительных органов и местного самоуправления, в которых содержатся нормы информационного права.

Немаловажную роль в регулировании информационных правоотношений играют международно-правовые акты, среди которых основополагающее значение имеет Окинавская хартия глобального информационного общества от 22 июля 2000 г. Согласно положениям хартии «все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей».

Актуален как никогда вывод профессора В.А. Копылова, сделанный в одном из докладов еще в 2000 г. о том, что поскольку в информационном обществе практически отсутствуют географические и геополитические границы и даже временные рамки и часовые пояса, а также, как правило, не действуют национальные законодательства, то информационное право как правовое отображение такого общества должно строиться главным образом на нормах международного права, регулирующих основные группы информационных отношений на межгосударственном уровне. Так, посредством норм международного права государствами должны быть приняты определенные обязательства в области защиты информационных прав и свобод, в регламентации таких глобальных вопросов, как трансграничная передача

персональных данных, когда главной целью становится адекватная защита прав субъектов данных.

Главный источник информационного права в национальном законодательстве - Конституция РК. Она включает основные принципиальные положения информационного права, поэтому нормы Конституции имеют высшую силу.

Источниками информационного права являются также многочисленные законы, регулирующие различные виды информационных отношений.

Информационно-правовые нормы могут содержаться также в локальных актах, принимаемых администрацией или иными органами предприятий, организаций, учреждений (например, положение о персональных данных).

Необходимо помнить, что информационное право и информационное законодательство - не тождественные понятия: последнему свойственна комплексность, так как помимо информационно-правовых оно содержит нормы и других отраслей права, и прежде всего - административного права.

Сегодня идет активный процесс формирования информационного права соответственно современным условиям жизни общества. Вопросы системы этой отрасли права и систематизации информационного законодательства приобрели высокую степень актуальности. К тому же далеко не все сферы информационной деятельности получили необходимое правовое регулирование.

3. Информационное право в системе казахстанского права. Информационное право как наука

Каждая из отраслей казахстанского права распространяется на свой, особый вид общественных отношений, требующих соответствующих предметов и методов правового регулирования. Определим место информационного права в системе права путем его сопоставления и отграничения от других отраслей права.

В юридической науке должен быть внимательно рассмотрен вопрос о месте информационного права в системе права на современном этапе.

Подчеркнем особенности информационного права, рассмотрев вопрос его связи с другими отраслями права и отграничения от них. В связи с тем, что информационное право распространяется на одну из областей деятельности государства, оно тесно соприкасается с конституционным и административным правом.

Конституционное право, являясь ведущей отраслью в системе права, закрепляет основы общественного строя РК, правовое положение личности, систему и принципы организации и деятельности государственных органов и органов местного самоуправления. Как и все отрасли, информационное право базируется и развивается на этих нормах. Конституционное право содержит также нормы, непосредственно относящиеся к информационному праву. Так, право на информацию - это гарантированная Конституцией РК возможность граждан получать достоверные сведения о деятельности государственных органов и организаций, общественных объединений и должностных лиц. Конституция РК в п. 2 ст. 20 закрепляет право каждого человека свободно

получать и распространять информацию любым, не запрещенным законом способом.

Сходство информационного права с административным проявляется в использовании сходных методов правового регулирования, главным образом метода властных предписаний. Основное разграничение этих отраслей права - по предмету правового регулирования. В предмет информационного права входят отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношений.

Предмет административного права составляют общественные отношения в сфере управленческой деятельности государственных органов и должностных лиц по исполнению публичных функций государства. Сегодня, в условиях развития электронного правительства, механизмов предоставления государственных услуг в электронном виде связь информационного права с административным является особенно тесной.

В вопросе ответственности за правонарушения в информационной сфере информационное право связано с уголовным правом.

Обозначая место информационного права в системе права, И.Л. Бачило подчеркивает два существенных момента: с одной стороны - его системообразующую роль для всех норм, связанных с проблемой информации и информатизации, и с другой - его системоорганизующую роль… Это как бы обратная связь особой социальной сферы через ее отрасль права со всеми остальными структурами права… например, создание новых норм об ответственности за правонарушения в области информации, связи, информатизации, защиты информации и прав субъектов в этой области (УК РК, КоАП РК).

В условиях формирования информационного общества обнаруживается тесная связь информационного права как самостоятельной отрасли права как с базовыми отраслями российского права (конституционным, гражданским, уголовным), так и с другими, причем среди «смежных» с информационной отраслью права особенно явно проявляются имеющие ярко выраженный социальный аспект. Это трудовое право - в вопросе права на информацию субъектов трудового права, защиты персональных данных работника, право социального обеспечения - в аспекте предоставления качественных государственных услуг.

Информационное право, ставшее в настоящее время одной из наиболее современных и актуальных отраслей отечественного права, отличается интенсивностью формирования своего нового содержания, масштабностью перемен, интенсивностью развития информационного законодательства. Наука информационного права еще молода, и многие проблемы информационного права еще не получили должной научной оценки.

Необходимо подчеркнуть, что правовая основа информационных отношений недостаточно разработана, нестабильна: в информационное законодательство постоянно вносятся многочисленные изменения и дополнения, что затрудняет его применение, а также и изучение. Важную роль в

продолжающемся процессе формирования информационного права призвана выполнить наука информационного права.

В числе наиболее актуальных проблем науки информационного права - исследование вопросов предмета и системы информационного права, принципов информационно-правового регулирования.

Контрольные вопросы:

1. Сформулируйте определение понятия «информационное право».
2. Охарактеризуйте предмет информационного права.
3. В чем выражается специфика метода правового регулирования информационного права?
4. Какие принципы лежат в основе информационного права? Каково их значение?
5. Что понимается под системой и источниками информационного права?

Тестовые задания:

1. Какие отношения входят в предмет информационного права?
A) основанные на автономии воли участников;
B) возникающие в процессе поиска, получения, передачи, производства и распространения информации;
C) предусмотренные договором возмездного оказания услуг;
D) по использованию технической документации;
E) связанные с неимущественными отношениями.

2. Назовите главный источник информационного права в национальном законодательстве:
A) Закон о СМИ;
B) Закон о доступе к информации;
C) Конституция РК;
D) Закон о персональных данных;
E) ГК РК.

3. Укажите разделы, составляющие особенную часть информационного права:
A) понятие информации;
B) электронный документооборот;
C) классификация обязательств;
D) история развития имущественных отношений;
E) функциональное предназначение залоговых отношений.

4. Перечислите институты информационного права:
A) доказательства, третьи лица, суд;
B) юридические лица, обязательства, вещные права;
C) налоги, сборы, акцизы;
D) наказание, проступок, категории преступлений;

E) институт права на информацию, институт средств массовой информации и т.д.

5. Отрасль права, нормы которой регулируют общественные отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения – это?
A) международное частное право;
B) гражданское право;
C) информационное право;
D) земельное право;
E) конституционное право.

6. Один из участников всегда наделяется властными полномочиями по отношению к другому – один из признаков ... метода:
A) дедуктивного;
B) логического;
C) диспозитивного;
D) императивного;
E) аналитического.

7. Назовите характерные черты диспозитивного регулирования правоотношений:
A) наделенным правом издания односторонне-властных предписаний;
B) участники находятся в равном, равноправном положении;
C) подлежат жесткой регламентации со стороны исполнительных органов;
D) строятся на началах неравенства;
E) объем правомочий не может быть изменен участниками самостоятельно.

8. В каком нормативно-правовом акте содержатся базовые принципы регулирования информационных отношений?
A) Закон о СМИ;
B) Закон об информатизации;
C) Конституция РК;
D) Закон о персональных данных;
E) ГК РК.

9. Укажите принцип, не относящийся к регулированию информационных отношений:
A) законность;
B) свобода договора;
C) равенство прав физических и юридических лиц;
D) обеспечение свободного доступа к электронным информационным ресурсам;
E) обеспечение безопасности личности, общества и государства.

10. Основополагающие идеи (требования), определяющие в своей совокупности идеальную конструкцию (модель) регулирования конкретной области общественных отношений:
A) элементы;
B) свойства;
C) признаки;
D) методы;
E) принципы.

Тема 1.3. Информационные правоотношения. Информационно-правовые нормы

Цель: раскрыть понятие и структуру информационного правоотношения; юридические факты как основания возникновения, изменения и прекращения информационных правоотношений

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате изучения данной темы студент должен обладать следующими компетенциями:

- умением ориентироваться в условиях постоянного изменения правовой базы.
- способностью анализировать большой объем информации, юридической литературы.
- способностью использовать углубленные специализированные теоретические знания, практические навыки и умения для организации научных и научно-прикладных исследований, учебного процесса, аналитической деятельности.

План:

1. Информационные правоотношения: понятие, содержание, субъекты. Условия возникновения, изменения и прекращения информационных правоотношений.
2. Понятие и признаки информационно-правовых норм.

1. Информационные правоотношения: понятие, содержание, субъекты. Условия возникновения, изменения и прекращения информационных правоотношений

В результате воздействия информационно-правовых норм на информационные отношения последние приобретают форму правоотношения. Правоотношения - это общественные отношения, урегулированные нормами права.

Информационные правоотношения - это общественные отношения, урегулированные нормами информационного права, возникающие в процессе

поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Прежде всего, информационное право, как отдельная отрасль права регулирует однородную группу общественных отношений. Специфику данных отношений можно определить следующими признаками:

1) они возникают, изменяются и прекращаются в информационной сфере при обращении информации;

2) складываются по поводу обладающих определенной спецификой объектов, к которым относятся информация, информационные объекты, информационные технологии. И такие объекты в силу их особенностей невозможно поставить в один ряд с другими объектами правового регулирования.

Информационные правоотношения имеют характерное внутреннее строение (структуру). Структура показывает, из каких элементов состоит правоотношение и как эти элементы взаимосвязаны друг с другом. Правоотношение (в том числе и информационное) состоит из трех элементов: объект, субъект, содержание.

Важнейший элемент правоотношения - субъекты. Субъектами информационного права выступают участники (стороны) регулируемых нормами информационного права общественных отношений. К ним относятся физическое лицо (включая граждан, лиц без гражданства и иностранных граждан), юридическое лицо, государство, государственный орган, орган местного самоуправления.

Субъект информационного правоотношения должен обладать информационной правосубъектностью. Понятие «информационная правосубъектность» включает в себя понятие «информационная правоспособность» и «информационная дееспособность».

Информационная правоспособность рассматривается как проявление общей правоспособности, под которой понимается установленная и охраняемая государством возможность или способность данного субъекта вступать в правовые отношения. В этом случае субъект приобретает юридические права, обязанности, а также обязанность нести ответственность за реализацию таких прав и обязанностей. В таком понимании правоспособность является предпосылкой возникновения правовых отношений с участием этого субъекта.

Предпосылкой для возникновения информационных правоотношений является информационная правоспособность, которая выражается в определяемой информационно-правовыми нормами возможности данного субъекта приобретать информационные права и обязанности (права и обязанности в информационной сфере) и нести юридическую ответственность за их практическую реализацию. Каждый, кто нормами информационного права наделен правами и обязанностями в информационной сфере, может рассматриваться в качестве субъекта информационного права.

Однако субъект информационного права может стать субъектом информационных правоотношений тогда, когда он обладает вторым элементом информационной правосубъектности - информационной дееспособностью.

Информационная дееспособность подразумевает способность субъекта своими действиями приобретать права, создавать для себя юридические обязанности, а также нести ответственность за свои действия в информационной сфере. В нашем случае речь идет о практической способности субъекта реализовывать свою информационную правоспособность в условиях конкретных информационных правоотношений.

При этом «гражданин, физическое лицо, вне зависимости от его трудовых и иных аналогичных контактов, всегда является членом социального коллектива, единицей в геополитических, административно-территориальных, культурологических структурах, деятельность которых регулируется либо морально-нравственными нормами, либо нормами законодательства. И все они связаны с информационным фоном потребностей этого лица в информации и являются активными приемниками информации, идущей от гражданина. Чем определеннее развиты различные институты демократии, тем прочнее связи гражданина с государством, государственной организацией».

Рассматриваемая область общественных отношений, т.е. отношений, складывающихся в процессе реализации электронным государством своих функций, безусловно, обладает определенной спецификой, при этом упоминаемые И.Л. Бачило связи гражданина с этим государством становятся еще более тесными - с одной стороны, и более прозрачными и открытыми - с другой.

Объект правоотношения представляет собой то, на что воздействуют правоотношения. Это все те материальные, духовные и иные социальные блага, явления и процессы, по поводу которых субъекты информационного права вступают в информационно-правовые отношения. К примеру, объектом информационных правоотношений будут выступать государственные услуги в электронном виде.

Содержание, как третий элемент правоотношений, образует юридические права и обязанности участников (субъектов) информационных правоотношений. В нашем примере - это права и обязанности получателей услуг (заявителей) и тех, кто их предоставляет (орган государственного внебюджетного фонда, Правительство РК и местные исполнительные органы, орган местного самоуправления).

Информационные правоотношения возникают, изменяются и прекращаются на основании юридических фактов. Юридические факты - это конкретные жизненные обстоятельства, с которыми связывается возникновение, изменение или прекращение правоотношений. Их можно подразделить на события и действия.

События - это юридические факты, которые не связаны с волей людей (стихийные бедствия, смерть человека, достижение совершеннолетия и т.д.). Как пример события можно привести ситуацию аппаратного или программного сбоя.

Действия - это юридические факты, наступление которых связано с волей и сознанием участников правоотношений (в свою очередь подразделяются на правомерные и неправомерные). Правомерным действием, к примеру, будет

являться соответствующее нормам закона предоставление (получение) государственной услуги в электронном виде. Примером неправомерного действия будет уголовно наказуемое деяние - неправомерный доступ к компьютерной информации.

2. Понятие и признаки информационно-правовых норм

Информационно-правовые нормы, также как и иные нормы права, представляют собой установленные (в указах Президента РК, постановлениях Правительства РК и других нормативных актах) и охраняемые государством (в лице своих правоохранительных органов) правила поведения участников общественных отношений, выраженные в их юридических правах и обязанностях.

Информационно-правовая норма - это установленное государством и обеспеченное мерами государственного принуждения правило поведения в общественных информационных отношениях, возникающих в процессе поиска, получения, передачи, производства и распространения информации, а также связанных с ними отношений.

Классификацию информационно-правовых норм можно провести по нескольким основаниям.

В зависимости от способа воздействия на участников информационных отношений, информационно-правовые нормы подразделяются:

- на обязывающие информационно-правовые нормы - это нормы, содержащие требования на совершение каких-либо действий.
- запрещающие информационно-правовые нормы - это нормы, содержащие запрет на совершение каких-либо действий.
- уполномочивающие информационно-правовые нормы - они устанавливают права участников правоотношений на совершение каких-либо определенных действий.

В зависимости от своего содержания информационно-правовые нормы можно подразделить на два вида: 1) материальные; 2) процессуальные.

Материальные информационно-правовые нормы закрепляют материальное информационно-правовое содержание прав и обязанностей участников информационных отношений.

Процессуальные (процедурные) нормы информационного права порядок и действие норм материального права, например, порядок предоставления государственных услуг в электронном виде.

Структура нормы права поясняет, из каких структурных частей (элементов) состоит норма права и как эти части между собой взаимосвязаны. Как и норма всякой другой отрасли права информационно-правовая норма состоит из трех элементов: 1) гипотезы, 2) диспозиции, 3) санкции.

1. Гипотеза - это элемент информационно-правовой нормы, который указывает на условия действия информационно-правовой нормы. Определяет обстоятельства, при которых могут возникнуть информационные правоотношения, и указывает на субъектов - участников этих правоотношений.

2. Диспозиция - это элемент информационно-правовой нормы, который устанавливает содержание самого правила поведения, т.е. определяет содержание прав и обязанностей участников информационных отношений.

3. Санкция - это элемент информационно-правовой нормы, который указывает на меры воздействия за нарушение информационно-правовой нормы. К примеру, согласно ст. 205 Уголовного кодекса РК умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, - наказывается штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

Контрольные вопросы:

1. Сформулируйте понятие «информационно-правовая норма». Какие признаки отличают информационно-правовые нормы от других норм права?
2. Какие виды информационно-правовых норм выделяются в зависимости от способа воздействия на участников информационных отношений?
3. Из каких структурных элементов состоит информационно-правовая норма? Охарактеризуйте каждый из этих элементов.
4. Что понимается под информационными правоотношениями? Какие особенности им свойственны?
5. Определите понятие «субъект информационного правоотношения».
6. Охарактеризуйте субъектный состав информационных правоотношений.

Тестовые задания:

1. Элемент информационно-правовой нормы, который указывает на условия действия информационно-правовой нормы - это?
A) гипотеза;
B) диспозиция;
C) санкция;
D) указание;
E) протест.

2. Укажите нормы информационного права, закрепляющие порядок и действие норм материального права:
A) обязывающие;
B) процессуальные;
C) материальные;
D) закрепляющие;

E) правоизменяющие.

3. Санкция – это?
A) элемент информационно-правовой нормы, который определяет содержание прав и обязанностей участников информационных отношений;
B) элемент информационно-правовой нормы, который устанавливает содержание самого правила поведения;
C) элемент информационно-правовой нормы, который указывает на классификацию информации;
D) элемент информационно-правовой нормы, который указывает на меры воздействия за нарушение информационно-правовой нормы;
E) элемент информационно-правовой нормы, который указывает на функциональное предназначение залоговых отношений.

4. Перечислите структурные элементы информационно-правовой нормы:
A) гипотеза, диспозиция, санкция;
B) факты, события, действия;
C) указание, предписание, инструкция;
D) условие, содержание, форма;
E) раздел, институт, принцип и т.д.

5. Назовите деление информационно-праовых норм в зависимости от способа воздействия на участников информационных отношений:
A) материальные, процессуальные;
B) императивные, диспозитивные;
C) правовозникающие, правоизменяющие, правопрекращающие;
D) обязывающие, запрещающие, уполномочивающие;
E) условные, срочные, временные.

6. Нормы, содержащие требования на совершение каких-либо действий – это?
A) запрещающие;
B) обязывающие;
C) уполномочивающие;
D) материальные;
E) процессуальные.

7. Дайте характеристику уполномочивающим информационно-правовым нормамм:
A) строятся на издании односторонне-властных предписаний;
B) участники находятся в равном положении;
C) подлежат жесткой регламентации со стороны исполнительных органов;
D) устанавливают права участников правоотношений на совершение каких-либо определенных действий;
E) содержат требования на совершение каких-либо действий.

8. Программный сбой – это событие или действие?
A) действие;
B) событие;
C) условие;
D) правонарушение;
E) форма.

9. Что из перечисленного относится к правомерным действиям?
A) стихийное бедствие;
B) компьютерный взлом системы программного обеспечения;
C) предоставление государственной услуги в электронном виде;
D) интернет-мошенничество;
E) взлом аккаунта в социальных сетях.

10. Что будет служить примером неправомерного действия?
A) меры по охране окружающей среды;
B) компьютерный взлом системы программного обеспечения;
C) чтение лекций о вреде курения;
D) достижение совершеннолетия;
E) установление сертифицированного программного обеспечения.

Тема 1.4. Право на информацию как институт информационного права

Цель: раскрыть содержание права на информацию, рассмотреть и проанализировать основные подходы к обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- умением критически оценивать информацию, переоценивать накопленный опыт и конструктивно принимать решение на основе обобщения информации;
- умением решать базовые задачи по данной тематике на практических занятиях;
- умением анализировать правовые нормы, регулирующие содержание права на информацию и цифрового неравенства.

План:

1. Общая характеристика права на информацию.
2. Доступ к информации о деятельности государственных органов и органов местного самоуправления.

1. Общая характеристика права на информацию

Основополагающий институт информационного права - это институт права на информацию.

Под данным институтом понимается совокупность правовых актов и отдельных норм, определяющих порядок реализации прав субъектов информационного права в области производства (создания) информации, поиска и получения (доступа) информации, сбора, хранения, передачи, использования, распространения информации в целях, не противоречащих свободам, правам и интересам человека, государства, общества и обеспечивающих создание информационных ресурсов, необходимых для реализации других прав и обязанностей субъектов права, предусмотренных и гарантированных законодательством РК и нормами международного права.

При этом доступ к информации должен подразумевать и доступ к открытой информации, общедоступной информации, и доступ к информации, являющейся общественным достоянием, информации особой социальной значимости, и доступ к информации в сфере средств массовой информации.

Несомненно, в условиях развития «электронного государства» можно говорить о расширении правоспособности человека как участника информационных правоотношений. И речь уже идет о правоспособности, основанной на транспарентности и открытости государственного управления.

Транспарентность можно определить как состояние информированности (наличие полного, достаточного и достоверного знания) о той или иной деятельности (ее объектах или результатах) любого заинтересованного в этом субъекта.

Состояние информированности возникает вследствие получения соответствующей информации, которое возможно посредством доступа к информации, под которым следует понимать ознакомление с информацией либо предоставление ее для ознакомления, т.е. анализируемому состоянию предшествует информационный процесс, состоящий в совершении действий по доступу к информации. Субъектами такого информационного процесса выступают две стороны: сторона, обладающая информацией, и сторона, заинтересованная в ее получении.

Так, субъектами информационного процесса «электронного государства» выступают, с одной стороны - человек, с другой - государственные органы, составляющие «электронное правительство». И государство должно обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения государственных органов. Сегодня возможно лишь констатировать недостаточный уровень информированности общества в целом и каждого человека в отдельности.

Второй немаловажный аспект - это обеспечение равного доступа к информационным технологиям.

Термины «цифровое неравенство» или «цифровой разрыв» (в англоязычной литературе digital divide) трактуются по-разному. Чаще всего под

цифровым неравенством понимается неравный доступ к информационным технологиям, разделение на тех, кому эти технологии доступны, а кому нет, деление на «информационно богатых» и «информационно бедных».

ЮНЕСКО считает проявлением цифрового неравенства наличие на карте мира стран, где информационные технологии развиты и доступны гражданам, и стран, или даже целых регионов, где уровень развития информационных технологий низок и большинство населения не имеет к ним доступа.

Другие исследователи считают, что цифровое неравенство, это социально-экономический феномен, являющийся следствием разницы в уровне дохода, грамотности и образования, степени развития определенных навыков, различия в сфере бизнеса, культуры, законодательства.

Принято рассматривать цифровое неравенство как сложное социально-экономическое явление, имеющее множество форм:

1. Региональное или территориальное неравенство. Оно выражается в разделение мира на регионы, где информационные технологии доступны большинству населения и где нет. Границы информационно богатых и информационно бедных регионов практически совпадают с границами индустриально развитых регионов (Северная Америка, Западная Европа, развитые страны Юго-Восточной Азии) и стран «третьего мира» (Африка, Азия, Южная Америка).

Другим проявлением регионального неравенства является разная степень информатизации отдельных регионов внутри страны, деление ее на «информационно богатые» индустриальные регионы и «информационно бедные» сельские, малонаселенные или труднодоступные территории.

2. Социальное неравенство. Выражается в одновременном присутствии в обществе социальных групп, которые активно используют информационные технологии, и групп, которые не могут себе этого позволить по причине низкого дохода, недостатка образования и культуры, отсутствия необходимых навыков, ограниченных физических возможностей, в силу преклонного возраста и т.д.

Итак, для обеспечения цифрового равенства и цифрового единства граждан необходимыми условиями являются:

- равенство в доступности технических средств;
- равенство в навыках использования ИКТ;
- равенство в способах и целях использования ИКТ.

По аналогии, «как социальное государство обеспечивает социальное равенство, так электронное государство берет на себя обязанность обеспечить цифровое равенство… Проблема «цифрового равенства» по своей природе тесно связана с социальным равенством. Ее решение зависит от того, как государство решает вопрос выравнивания социального положения населения. Любое социальное неравенство способно существенно дестабилизировать нормальное функционирование общественного процесса и государственного управления… Принцип «цифрового равенства» должен не только получить законодательное воплощение, но пронизать собой все законодательство. Этот принцип исходит из того, чтобы лицо выбирало, в какой форме получать информацию - в традиционной бумажной или электронной»

2. Доступ к информации о деятельности государственных органов и органов местного самоуправления

В настоящее время необходимым является изменение характера информационного взаимодействия общества и государства, выражающееся в расширении прав граждан путем не только предоставлении доступа к разнообразной информации, но и увеличении возможностей людей участвовать в процессе принятия решений. Центральной фигурой в процессах информатизации государственных органов должен быть человек как источник, потребитель информации и субъект гражданского общества, его интересы и потребности. И это должно как никогда осознаваться государственными служащими.

Размещение в свободном доступе информации о деятельности органов исполнительной власти и органов местного самоуправления, а также формируемых ими информационных ресурсах позволяет сделать деятельность указанных органов более понятной и предсказуемой для граждан и организаций, а также уменьшить нагрузку на указанные выше органы за счет снижения количества поступающих обращений.

В случае нарушения порядка предоставления информации о деятельности государственных органов и органов местного самоуправления, содержащей сведения, относящиеся к информации ограниченного доступа, а также незаконное взимание платы за предоставление информации о деятельности государственных органов и органов местного самоуправления либо нарушение порядка взимания платы за предоставление информации о деятельности государственных органов и органов местного самоуправления в случаях, если законом такая плата установлена КоАП РК, предусмотрена административная ответственность в виде штрафа на должностных лиц.

Контрольные вопросы:

1. Каково содержание права на информацию?
2. Раскройте понятие цифрового неравенства, определите уровень доступности информационных технологий для граждан.
3. Назовите и охарактеризуйте формы цифрового неравенства.
4. Определите основные направления нормативно-правового обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления.

Тестовые задания:

1. Укажите неверный ответ. Институт права на информацию включает в себя?
A) производство информации;
B) создание информации;
C) поиск и получение информации;
D) сбор и хранение информации;
E) аналитическая работа с инормацией.

2. Институт права на информацию – это основополагающий институт:

A) уголовного права;
B) криминалистики;
C) информационного права;
D) прокурорского надзора;
E) социологии.

3. Разделение мира на регионы, где информационные технологии доступны большинству населения и где нет – это?
A) социальное неравенство;
B) территориальное неравенство;
C) экономическое неравенство;
D) политическое неравенство;
E) смешанное неравенство.

4. Укажите неверный ответ. Для обеспечения цифрового равенства и цифрового единства граждан необходимыми условиями являются:
A) равенство в доступности технических средств;
B) равенство в доступности финансовых средств;
C) равенство в навыках использования ИКТ;
D) равенство в способах использования ИКТ;
E) равенство в целях использования ИКТ.

5. Низкий доход, недостаток образования и культуры, отсутствие необходимых навыков, ограничение физических возможностей – это характерные признаки ...:
A) процессуального неравенства;
B) регионального неравенства;
C) социального неравенства;
D) территориального неравенства;
E) условного неравенства.

6. Состояние информированности (наличие полного, достаточного и достоверного знания) о той или иной деятельности (ее объектах или результатах) любого заинтересованного в этом субъекта – это?
A) состязательность;
B) обязанность;
C) коммуникабельность;
D) транспарентность;
E) сплоченность.

7. Неравный доступ к информационным технологиям, разделение на тех, кому эти технологии доступны, а кому нет, деление на «информационно богатых» и «информационно бедных» - это?
A) автономия воли участников;
B) равенство сторон;

C) социальное неравенство;
D) цифровое неравенство;
E) цифровизация.

8. Что не относится к признакам социального неравенства?
A) низкий доход;
B) недостаток образования и культуры;
C) отсутствие необходимых навыков;
D) свободный доступ к интернету;
E) преклонный возраст.

9. Какая организация считает, что цифровое неравенство проявляется в странах, где информационные технологии развиты и доступны гражданам или, где уровень развития информационных технологий низок и большинство населения не имеет к ним доступа?
A) МВФ;
B) ЕАЭС;
C) ЮНЕСКО;
D) ВОЗ;
E) НАТО.

10. Лицо выбирает в какой форме получать информацию - в традиционной бумажной или электронной» - это принцип?
A) законности;
B) цифрового равенства;
C) свободы договора;
D) состязательности сторон;
E) демократизма.

Тема 1.5. Институт правового режима информационных ресурсов

Цель: раскрыть понятие информационного ресурса, правового режима информационных ресурсов. Рассмотреть понятие государственных секретов.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- умение правильно применять нормы права.
- умение анализировать юридическую литературу по вышеуказанным темам.
- умение решать задачи по вышеуказанным темам.

План:

1. Понятие информационного ресурса.

2. Основные категории информационных ресурсов. Общедоступная информация и информация ограниченного доступа.

1. Понятие информационного ресурса

Информационный ресурс - это массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения (информацию), сформированные по определенному признаку или критерию.

Любой субъект (мировое сообщество, конкретное государство, регион, город или район, организация, предприятие или хозяйство, отдельный человек или группа лиц) для своей деятельности располагает определенными объемами и видами ресурсов.

Последние подразделяются на отдельные виды ресурсов относительно определенных предметных областей жизни и деятельности человека. Например:

- материальные (совокупность предметов труда, используемых в процессе производства общественного продукта - сырье материалы, топливо, полуфабрикаты и т. п.),
- природные (естественные ресурсы - объекты, процессы, условия природы, используемые для удовлетворения материальных и духовных потребностей людей),
- энергетические (носители энергии - нефть, газ и др.),
- трудовые (люди, владеющие общеобразовательными и профессиональными знаниями),
- финансовые, товарные, нематериальные (духовные или интеллектуальные) и др.

Перечисленные ресурсы имеют первостепенное значение для материального производства особенно в эпоху индустриального общества.

В отличие от большинства перечисленных выше ресурсов информационные ресурсы (ИР) являются продуктом интеллектуальной деятельности наиболее квалифицированной и творческой части населения, составляют значительную часть национального богатства и относятся к числу возобновляемых благ, так как имеют способность к тиражированию в зависимости от общественной потребности.

В большей своей части эти ресурсы материализованы в виде книг, статей, документов, баз данных, баз знаний, алгоритмов, компьютерных программ, произведений искусства, литературы и т.п. По существу, эти накопленные людьми знания на протяжении своей истории существования и развития, зачастую отчужденные от своих создателей, рассматриваются как общие стратегические ресурсы, принадлежащие всему человечеству.

Информационные ресурсы объединяют первичную информацию, отражающую знания человека об опыте своей деятельности и сведения об окружающей среде, а также всю вторичную информацию, образующуюся в результате обработки и переработки всей получаемой информации.

С одной стороны, определенный объем ИР составляют знания людей, специалистов (экспертные знания). Объем этих знаний неуклонно возрастает в

результате более совершенных и целенаправленных научных исследований, ведущих к открытиям и научно-техническим достижениям, более глубокого и широкого образования населения, развития и повсеместно используемых современных средств вычислительной техники, коммуникаций, связи и других факторов.

С другой стороны, основная и большая часть ресурсов представляет собой накопленную информацию, которая фиксировалась на различных носителях на протяжении всего исторического пути развития человечества и продолжает накапливаться и фиксироваться в настоящее время весьма быстрыми темпами (за счет использования современных компьютерных и коммуникационных средств).

Следует отметить, что обмен информацией в результате общения и коммуникаций присущ всей живой природе (по некоторым учениям нематериалистического характера и неживой), однако только человеку принадлежит свойство глубокого познания окружающего мира, извлечения из него разнообразной информации, ее анализа и на этой базе генерирования и накапливания новых знаний. Именно это - формирование и использование ИР - отличает человека от всего живого и позволяет ему не только осознанно ориентироваться в окружающей обстановке, но и создавать вокруг себя общественные богатства, строить социальные отношения и обеспечивать свою жизнедеятельность с помощью научно-технических достижений.

Чрезвычайно важно то обстоятельство, что определенным образом собранная и целенаправленно обработанная информация порождает новые знания. Таким образом, информация обладает уникальным свойством репродуцировать (воспроизводить) знания и усиливать эффект их накопления (суммирования), что приводит к постоянному росту ИР.

Следует отметить, что практически до последней четверти XX в. ИР не рассматривались с позиций общественно значимой экономической или иной категории, влияющей на состояние и развитие страны. В основном обращалось внимание на культурное наследие той или иной национальности или государства. В настоящее время в эпоху постиндустриального развития общества по своей эффективности использования, важности, полезности и степени значимости ИР играют все большую роль и рассматриваются как приоритетные стратегические ресурсы, сопоставимые с материальными и энергетическими ресурсами.

2. Основные категории информационных ресурсов. Общедоступная информация и информация ограниченного доступа

Можно выделить ряд классификаций информационных ресурсов по различным основаниям.

Основной подход к классификации информационных ресурсов - это критерий доступа к ним пользователей. Итак, по категории доступа информационные ресурсы могут быть открытыми (общедоступными) или с ограниченным доступом.

Общедоступная информация предоставляется свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных, предоставленных законом прав.

В свою очередь, документированная информация с ограниченным доступом подразделяется на отнесенную к государственной тайне и конфиденциальную. Данное разграничение, в частности, отмечено в п. 2 ст. 20 Конституции: «Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом».

В соответствии со ст. 1 Закона Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах» под государственными секретами понимаются защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.

К сведениям, составляющим государственные секреты Республики Казахстан, относятся следующие составляющие:

1) Сведения в военной области, относимые к государственным секретам Республики Казахстан.

2) Сведения в области экономики, образования, науки и техники, относимые к государственным секретам Республики Казахстан.

3) Сведения во внешнеполитической и внешнеэкономической области, относимые к государственным секретам Республики Казахстан.

4) Сведения в области разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, относимые к государственным секретам Республики Казахстан.

Согласно п. 1 ст. 126 и п. 1 ст. 1017 Гражданского кодекса (далее - «ГК РК») к коммерческой тайне относится ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства, управленческую модель, а также способы и методы для увеличения прибыли.

При этом предприятие не может включать любую информацию в перечень объектов коммерческой тайны. К этому вопросу нужно подойти избирательно и вдумчиво, соблюдая три главных критерия в выборе:

- сведения должны иметь для предприятия действительную или потенциальную коммерческую ценность;
- сведения должны быть неизвестными третьим лицам;
- в отношении сведений должен быть установлен режим коммерческой тайны.

К объектам коммерческой тайны также можно отнести сведения о субъектах предпринимательства и сферах их деятельности, а также производственную, управленческую, научно-техническую и финансово-хозяйственную информацию о деятельности компании. Однако стоит отменить,

что в казахстанском законодательстве нет определенного перечня объектов, которые нельзя относить к коммерческой тайне.

В некоторых странах законодательство отдельно предусматривает список сведений, не относящихся к коммерческой тайне. К таким сведениям относятся:

1) Устав юридического лица, а также документы, дающие право заниматься предпринимательской деятельностью (свидетельство о государственной регистрации, лицензии, патенты);

2) сведения по занятости работников, информация обо всех свободных рабочих местах (вакансиях), о предстоящем высвобождении работников, их количестве и категориях, о создании дополнительных рабочих мест;

3) сведения о состоянии условий и охраны труда на рабочих местах, нарушениях установленных норм технике безопасности и гигиены труда, производственных травмах;

4) сведения об экологическом состоянии, соблюдении установленных санитарно-эпидемиологических норм пожарной, технической безопасности и других объектов, и техники, представляющих опасность для жизни и здоровья населения;

5) сведения о нарушениях законодательства;

6) иные сведения, свободный доступ к которым, предусмотрен законодательными актами.

К коммерческой тайне также нельзя относить общедоступную информацию, к которой относятся общеизвестные сведения, а также иную информацию, доступ к которой не ограничен.

Таким образом, ГК определяет перечень объектов, которые относятся к коммерческой тайне, но в то же время, в нормативно-правовых актах нет перечисленных объектов, которые не могут быть отнесены к коммерческой тайне. Также стоит отменить, что перечень коммерческой тайны, указанный в ГК, не является исчерпывающим, что создает некоторые неудобства.

Право на защиту коммерческой тайны действуют до тех пор, пока сохраняются условия, предусмотренные п. 1 ст. 126 ГК РК, а именно предпринимаются меры по сохранению коммерческой ценности информации и ее защите против доступа третьих лиц. Данное требование содержится в п. 4 ст. 1017 ГК РК, где говорится, что правообладатель имеет право на защиту этой информации от незаконного использования, если соблюдены условия п. 1 ст. 126 ГК РК.

Таким образом, у правообладателя есть обязанность принимать меры к установлению режима конфиденциальности к информации, имеющей ценность для предприятия. Согласно п. 4 ст. 28 Предпринимательского кодекса РК (далее - «ПК РК») под установлением режима коммерческой тайны следует понимать следующие действия: 1) определение перечня информации, составляющей коммерческую тайну; 2) ограничение доступа к коммерческой тайне путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка; 3) учет лиц, получивших доступ к коммерческой тайне, и (или) лиц, которым эта информация была представлена или передана.

Если ли же сравнивать законодательство Казахстана и других стран в отношении коммерческой тайны, то, к примеру, в российском законодательстве установлены более расширенные требования по установлению режима коммерческой тайны. Согласно закону «О коммерческой тайне» Российской Федерации от 29.07.2004 г., обладатель коммерческой тайны обязан принять следующие меры:

1. определить перечень сведений, составляющих секрет производства и относящихся к информации, составляющей коммерческую тайну;

2. оградить доступ к таким сведениям путем установления порядка обращения с ними и контроля за соблюдением установленного порядка;

3. вести учет лиц, получивших доступ к секрету производства, и (или) лиц, которым информация о нем была предоставлена или передана;

4. регулировать отношения по использованию информации, составляющую коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5. наносить на материальные носители информацию о содержании коммерческой информации, с указанием обладателя такой информации.

Как мы можем видеть в законодательстве РФ есть требования наносить маркировку на материальные носители о содержании коммерческой информации, в отличие от казахстанского законодательства.

В случае если же, вышеуказанные меры не будут приняты обладателем коммерческой тайны, то в России режим коммерческой тайны не будет считаться установленным. В свою очередь, в Казахстане нет таких жестких требований, по установлению режима коммерческой тайны. Минимальные требования по установлению мер по охране коммерческой тайны содержатся в п. 4 ст. 28 ПК, согласно которому меры по охране информации, составляющей коммерческую тайну, могут включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к коммерческой тайне путем установления порядка обращения с этой информации и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к коммерческой тайне, и (или) лиц, которым эта информация была представлена или передана.

Не соблюдение вышеуказанных минимальных мер правообладателем по охране коммерческой тайны могут повлечь риски для субъекта предпринимательства. Так. в случае обращения правообладателя в суд о нарушении прав на коммерческую тайну, суд может прийти к выводу о том, что сам правообладатель не принял достаточных (должных) мер для охраны коммерческой тайны и отказать в иске, так как сам правообладатель допустил халатность в отношении собственной коммерческой тайны.

Согласно ПК РК, порядок отнесения к категориям доступа, условия хранения и использования информации, составляющей коммерческую тайну, определяется субъектом предпринимательства.

Контрольные вопросы:

1. Раскройте понятие информационного ресурса.
2. Определите категории информационных ресурсов.
3. Определите признаки информации ограниченного доступа.
4. Какие сведения составляют государственную тайну?
5. Определите понятие конфиденциальной информации, охарактеризуйте ее виды.

Тестовые задания:

1. Укажите нормативно-праовой акт, определяющий установление режима коммерческой тайны?
A) УПК РК;
B) АППК РК;
C) Предпринимательский кодекс РК;
D) Закон РК «О доступе к информации»;
E) Закон РК «О нотариате».

2. Какие действия не относятся к установлению режима коммерческой тайны?
A) контроль за соблюдением порядка обращения с коммерческой тайной;
B) ограничение доступа к коммерческой тайне путем установления порядка обращения с этой информацией;
C) определение перечня информации, составляющей коммерческую тайну;
D) учет лиц, получивших доступ к коммерческой тайне;
E) регистрация лиц, распространивших сведения о коммерческой тайне.

3. У правообладателя информации, имеющей ценность для предприятия есть обязанность:
A) передать сторонней организации во временное пользование;
B) принимать меры к установлению режима конфиденциальности;
C) своевременно разрешать споры по разглашению информации;
D) безвозмездно исправить допущенные ошибки;
E) открывать отдельный банковский счет.

4. Укажите правильный ответ. Ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства, управленческую модель, а также способы и методы для увеличения прибыли – это?
A) секрет компании;
B) коммерческая тайна;
C) государственный секрет;
D) страховая тайна;
E) нотариальная тайна.

5. К сведениям, составляющим государственные секреты Республики Казахстан, относятся:
A) сведения в военной области;

B) коммерческая тайна;
C) ноу-хау;
D) лекционный комплекс;
E) протокол заседания совета директоров.

6. По категории доступа информационные ресурсы делятся на:
A) бумажные и электронные;
B) открытые (общедоступные) или с ограниченным доступом;
C) аудио- и видео;
D) документированные и недокументированные;
E) официальные и свободные.

7. Государственные секреты - это?
A) информация, предоставляемая в силу прямого указания закона в случаях реализации гражданином своих конституционных прав;
B) защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права;
C) массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения;
D) ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства;
E) перечень сведений, составляющих секрет производства.

8. Объекты, процессы, условия природы, используемые для удовлетворения материальных и духовных потребностей людей, относятся к:
A) свободным ресурсам;
B) природным ресурсам;
C) трудовым ресурсам;
D) энергетическим ресурсам;
E) информационным ресурсам.

9. Что относится к материальным ресурсам?
A) сырье материалы, топливо;
B) биткоин, токен, искусственный интеллект;
C) нефть, газ;
D) работник, предприниматель, руководитель;
E) мировое сообщество, конкретное государство, регион.

10. Массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения (информацию), сформированные по определенному признаку или критерию - это?
A) трудовой ресурс;
B) информационный ресурс;
C) природный ресурс;
D) средство производства;
E) общественный продукт.

Тема 2.1. Цифровые технологии и цифровые активы

Цель: рассмотреть понятие и особенности технологических понятий, связанных с цифровизацией.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- демонстрировать углубленные знания и понимание содержания дисциплины, которые дают возможность нестандартно подходить к разработке и применению идей в исследовательских работах.
- владение навыками самостоятельной, творческой работы; умение организовать свой труд; способность порождать новые идеи, находить подходы к их реализации.
- умением анализировать гражданско-правовые нормы, регулирующие процесс цифровизации.

План:

1. Понятие и особенности технологических понятий, связанных с цифровизацией.
2. Развитие цифровой инфраструктуры.
3. Цифровизация деятельности государственных органов.
4. Глобальные тренды цифровизации и международный опыт.

1. Понятие и особенности технологических понятий, связанных с цифровизацией

Цифровые технологии стремительными темпами вторгаются в нашу жизнь. Уже привычными стали Интернет, искусственный интеллект, роботы, социальные сети, Амазон, облачные технологии, кибербезопасность и т.п.

Однако все большее распространение получают развитие и становятся более привычными новые понятия и явления.

Но есть масса понятий, о которых основная масса обывателей даже и не слышала и которые известны узкому кругу технологически подкованных людей. Например: блокчейн, токен, смарт-контракты, нода, майнинг, верификация, валидация, хэш-код, фиатная валюта и т.п.

Но сейчас сосредоточимся на анализе уже существующих и даже внедренных проектов изменений в гражданское законодательство, связанных с цифровизацией.

Предметом рассмотрения будет Закон Республики Казахстан от 25 июня 2020 г. № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» (далее - Закон о цифровых технологиях).

Приведем расшифровку некоторых понятий, используемых в цифровой технологии.

Блокчейн (blockchein - цепочка блоков) - распределенный реестр или связанные блоки. То есть это цифровой реестр или база данных, причем эти данные распределены по всем компьютерам пользователей. Блокчейн можно сравнить с бисерным ожерельем, где каждая бусинка - это блок, запись действия. Например, оплаты кем-то чего-то или сдачи домашнего задания. Такое ожерелье - или «чейн» (цепь) - не может быть уничтожено или повреждено. Каждый новый блок добывается путем математических вычислений в процессе майнинга (добычи), и нанизывается на существующую цепочку блоков. Каждый пользователь в любой момент может увидеть всю цепочку блоков. Подделать и обмануть в блокчейне невозможно.

Начался блокчейн с биткоина и первоначально применялся только как платформа для криптовалют. Но со временем блокчейн стал использоваться и в других сферах: банковский сектор (Дойче - банк, ВТБ, Сбербанк), платежные системы (Visa, Master card, SWIFT), земельная сфера и сфера недвижимости (земельный реестр, реестр недвижимости), государственные услуги (удостоверение личности, нотариат, электронное гражданство) и т.д.

В Казахстане блокчейн внедрен, например, для формирования очереди в детский сад. Каждый подавший заявление - это новый блок в цепочке блоков, составляющей очередь. Новый блок прикрепляется к предыдущему, а предыдущий прикреплен к следующему. Создается жесткая сцепка, которая позволяет четко знать свою очередь. Эта очередь никак, никем и никогда не может быть сдвинута или переставлена.

Криптовалюта - цифровая (виртуальная) валюта, единица которой - монета (англ.- coin). Защищена от подделки, так как представляет собой зашифрованную информацию, скопировать которую невозможно.

Фиатные деньги тоже могут существовать как электронные деньги, но для этого они должны сначала быть внесены на счет в физическом воплощении, например, через банк или платежный терминал. А криптовалюта выпускается непосредственно в сети и никак не связана ни с какой-либо обычной валютой, ни с любой государственной валютной системой.

Основной криптовалютой является Биткоин (более 90% рынка), разработанный в 2009 г. человеком или группой людей под псевдонимом Сатоши Накамото (личность до сих пор не установлена). Затем появились другие криптовалюты, которые называются альткойны (от англ. Altcoin, alternative coin). Наиболее известными альткойнами являются Litecoin, Namecoin, Novacoin, Ethereum, Ripple, Dash и другие.

Биткоин (от англ. bitcoin, от bit - бит и coin - монета) - криптовалюта, платежная система, использующаяся одноименную единицу для учета операций. Биткоины никто не печатает, как фиатные деньги. Эмиссия биткоинов возможна только в цифровом виде и любой желающий может начать добывать или, как говорят, майнить биткоины в любое время. Майнинг биткоинов происходит посредством использования вычислительных мощностей компьютеров в распределенной сети.

Майнинг (от англ. mining - добыча полезных ископаемых) - деятельность по созданию новых структур (обычно новых блоков в блокчейне). Суть майнинга заключается в том, что компьютеры, находящиеся в разных точках земли, решают математические задачи, в результате которых создаются биткоины. Работа майнеров заключается в том, чтобы подобрать из миллионов комбинаций один-единственный хэш (цифровой код), подходящий ко всем новым транзакциям, и секретному ключу, который и обеспечит майнеру получение награды.

С ростом количества добытых блоков сложность майнинга растет, так как приходится вкладывать все больше усилий в добычу блоков. Первоначально (когда было несколько блоков) для майнинга хватало простого персонального компьютера, но теперь, с фантастическим количеством блоков, майнинг можно проводить только на специализированных устройствах (фермах).

Основная проблема майнинга сейчас заключается в громадных затратах на электричество. Поэтому майнеры объединяются в пулы, в которые входят несколько десятков, сотен или тысяч майнеров, составляющих единое звено (пул).

Токен (англ., от нем. Zeichen - знак, символ). Если говорить очень просто, токен - это жетон, который можно обменять на какую- то услугу или товар.

В качестве примера жетонов можно назвать жетон в метро или для игрового автомата или аттракциона. Купив жетон, вы потом меняете его на услугу в виде прохода через турникет метро или в виде возможности воспользоваться услугами аттракциона.

Токен - это тот же жетон, только цифровой. Компания, которая хочет внедрить какой-либо проект и желая раздобыть для этого средства, выпускает цифровые жетоны - токены, проводит так называемое ICO (Initial Coin Offerring) - первичное размещение токенов). Можно сравнить ICO с IPO (первичное размещение акций). Отличие в том, что при IPO покупатели, приобретая акции, получают доли в компании. При ICO они получают токены - жетоны, которые в последующем они могут обменять на какие - либо блага от компании.

По сути участники ICO финансируют развитие компании сейчас для того, чтобы получить от нее какие-то блага в будущем.

Это можно приравнять к краудфандингу (народное финансирование, от англ. Crowd-funding, crowd - толпа,funding - финансирование) - коллективное сотрудничество людей (доноров), которые добровольно объединяют свои деньги вместе, чтобы поддержать усилия других людей или организаций (реципиентов). Если проект удачен, то инвесторы могут получить выгоду от

продажи токенов на бирже, если проект проваливается, то токены не больше чем цифирки, не имеющие ценности.

Смарт-контракт (умный договор) (Smart contract) - компьютерный протокол, посредством которого происходит исполнение условий соглашения участников. Смарт-контракт - это запрограммированный договор, условия которого прописаны в программном коде и который автоматически исполняется с помощью блокчейна.

При этом применяются простые правила «если, то»: «если» определенное условие будет исполнено, «то» будет совершено определенное действие. Примером может быть смарт-контракт (программный код), согласно которому мотор арендованного автомобиля заработает только в случае своевременного внесения арендной платы.

Смарт-контракт подписывается с помощью электронных подписей и размещается на платформе блокчейн. Исполнение производится автоматически, без участия сторон.

С правовой точки зрения смарт-контракт может классифицироваться как письменная форма сделки, совершенная с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки.

Верификация (от англ. Veritas - истина) означает проверку или тестирование.

Валидация (от англ. Validus - здоровый, сильный, крепкий) - подтверждение, аттестация.

Отличие верификации от валидации заключается в том, что верификация означает подтверждение общим требованиям, а валидация - подтверждение требованиям, установленным в данном конкретном случае.

Валидация означает в данном случае комплексную проверку изделия требованиям заказчика самим заказчиком. То есть валидация - это тестирование изделия на физическую функциональность в процессе передачи его заказчику (едет или не едет - проводятся испытания).

Фиатные (от лат. - декрет, указание), они же фидуциарные (от лат. -fiducia - доверие) деньги - деньги, номинальная стоимость которых устанавливается и гарантируется государством, традиционные деньги.

Законом РК о цифровых технологиях Закон об информатизации дополнен статьей 33-1 «Правовой режим оборота цифровых активов», которая гласит:

«Статья 33-1. Правовой режим оборота цифровых активов.

1. Цифровой актив не является средством платежа.

2. Цифровые активы являются обеспеченными и необеспеченными.

К обеспеченным цифровым активам относятся цифровой токен и иные цифровые активы, являющиеся цифровым средством удостоверения имущественных прав на товары и (или) услуги, выпускаемые (предоставляемые) лицом, выпустившим обеспеченный цифровой актив. Виды обеспеченных цифровых активов, а также перечень прав, удостоверяемый токеном, устанавливаются лицом, выпускающим цифровой токен, в порядке, установленном законодательством Республики Казахстан.

К необеспеченным цифровым активам относятся цифровые токены, полученные как вознаграждение за участие в поддержании консенсуса в блокчейне в порядке, установленном законодательством Республики Казахстан.

3. Выпуск и оборот необеспеченных цифровых активов на территории РК запрещается, за исключением случаев, предусмотренных законами Республики Казахстан.

4. Цифровой актив не обеспечивает права на ценные бумаги, производные финансовые инструменты, базовым активом которых являются ценные бумаги, и не предоставляют его собственнику или владельцу соответствующих прав в отношении юридического лица.

5. Право на цифровой актив удостоверяется посредством записи в блокчейне лицом, выпускающим цифровой актив на распределенной платформе данных, в соответствии с законодательством Республики Казахстан.

6. Внесение в информационную систему сведений о передаче цифрового актива или прав на него допускается при выполнении следующих условий:

1) лицо, осуществившее внесение сведений, обладает доступом в информационную систему лица, выпускающего цифровой актив на распределенной платформе данных, в соответствии с установленными требованиями;

2) информационная система лица, выпускающего цифровой актив на распределенной системе данных.

Собственник, владелец и пользователь, обладающие доступом в информационную систему выпускающих цифровых активов, обладают равными правами на внесение изменений в соответствии с заданным алгоритмом валидации. При этом изменения синхронизируются у всех пользователей информационной системы.

Кроме того, ст. 1 Закона об информатизации дополнена подпунктом 56-1) следующего содержания:

«56-1) цифровой токен - вид цифрового актива, являющийся цифровым средством учета, обмена и удостоверения имущественных прав».

В цифровой практике рассматриваются различные варианты соотношения токена и криптовалюты (например, биткоина).

Кроме понятия «цифровой токен», в Закон об информатизации включен еще ряд технологических терминов.

Статья 1 Закона об информатизации дополнена подпунктом 55-2) следующего содержания:

«55-3) цифровой майнинг - процесс проведения вычислительных операций с использованием компьютерных, энергетических мощностей согласно заданным алгоритмам шифрования и обработки данных, обеспечивающий подтверждение целостности блоков данных в объектах информатизации посредством блокчейна».

Нашлось место и блокчейну. Ст. 1 Закона об информатизации дополнена подпунктами 38-2) и 39-1):

«38-2) блокчейн - информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе

данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования».

«39-1) распределенная платформа данных - технологическая платформа, компоненты которой связаны между собой заданными алгоритмами, размещаются на различных узлах сети, могут иметь одного или более владельцев, а также могут обладать различным уровнем тождественности данных».

2. Развитие цифровой инфраструктуры

Основной составляющей развитой ИКТ инфраструктуры является широкополосный доступ в Интернет. Широкополосный доступ обеспечивается проводными технологиями, такие как FTTx, ADSL и беспроводными технологиями 3G, 4G и спутниковой связью. Для обеспечения населения и бизнеса широкополосным доступом к сети интернет в городах и областях Республики Казахстан создана телекоммуникационная инфраструктура; однако на сегодняшний день она не удовлетворяет потребностям сельских жителей. В целях снижения цифрового неравенства необходимо более качественно и всеохватно обеспечить сетями широкополосного доступа сельские населенные пункты.

Правительства многих стран мира рассматривают широкополосный доступ в интернет как ключевой элемент своих программ развития. Европейский союз реализует инициативу «Цифровая повестка дня», входящую в стратегию «EU 2020», где инфраструктура высокоскоростного доступа в интернет обозначена как основа современной экономики Европейского Союза. США финансирует из федерального бюджета проекты по расширению доступа сельского населения к оптоволоконной инфраструктуре. Канада в стратегии «Цифровая Канада 150» - инвестирует в расширение услуг высокоскоростного интернета для 280 тыс. домохозяйств в сельских и отдаленных населенных пунктах.

Преодоление информационного неравенства регионов осложняется размерами страны, наличием более 6 600 сельских населенных пунктов, часть которых расположена в удаленных и труднодоступных местностях. В мировом опыте эта проблема решается развитием спутниковой связи и вещания, которые предоставляют:

- возможность равноправного доступа населения страны к информации, в том числе к государственным услугам, информационным ресурсам отечественного телевещания;

- опережающее удовлетворение растущих информационных потребностей населения, бизнеса и государства.

Включение Казахстана в мировую систему информатики и телекоммуникаций уже повлекло многократное увеличение объектов информационно-коммуникационной инфраструктуры в государственном управлении, бизнесе, системах управления промышленными объектами, расширило сферы оказания услуг ИКТ операторами, обрабатывающими персональные данные граждан.

Одновременно с развитием сетей широкополосного доступа, преобразованиями в информационно-коммуникационной инфраструктуре, переводом бизнес-процессов хозяйствующих субъектов в «онлайн» среду и автоматизацией технологических процессов в промышленности, энергетике, банковской деятельности и сфере ИКТ-услуг необходимо одновременно проводить продуманную и последовательную политику обеспечения безопасности информационного пространства и инфраструктуры связи.

Основные проблемы и угрозы безопасности в сфере использования ИКТ, влияющие на эффективность процессов цифровизации экономики Казахстана, меры по их преодолению нашли отражение в Концепции кибербезопасности «Киберщит Казахстана» и предусматривают использование доверенных технологий обеспечения целостности, конфиденциальности, доступности информации и аутентификации пользователей при ее обработке.

Эффективная реализация мероприятий по цифровизации экономики Республики Казахстан будет обеспечена только при обеспечении единства, устойчивости и безопасности информационно-коммуникационной инфраструктуры, сохранности данных и доверии граждан к процессам, в основе которых лежат решения, основанные на использовании ИКТ.

3. Цифровизация деятельности государственных органов

На предыдущем этапе информатизации государство создало «Электронное Правительство» Республики Казахстан в виде базовой инфраструктуры и информационных систем государственных органов, прямо или косвенно задействованных в оказании государственных услуг.

На июль 2017 года в электронную форму переведено более 740 услуг и сервисов, реализованы 83 мобильные услуги. В 2015 году объем оказанных государственных услуг в электронной форме на веб-портале составил более 36 миллионов, в 2016 году - около 40 миллионов. На сентябрь 2017 года количество зарегистрированных уникальных пользователей достигло более 6,6 миллионов человек.

По состоянию на октябрь 2017 года в стране функционирует 349 центров обслуживания населения. В 2013 году на базе Call-центра «электронного правительства» был создан Единый контакт-центр с бесплатным номером телефона 1414. В Единый контакт-центр ежедневно поступает не менее 14 тысяч обращений от граждан, с прогнозируемым ростом в среднем на 15% от общего количества обращений ежегодно. Это создает большую нагрузку на операторов, приводит к проблемам с дозвоном и снижает качество услуг. Большое количество звонков содержит однотипные обращения, их можно было бы перевести в режим автоматической обработки или самообслуживания.

На веб-портале электронного правительства создана площадка Открытого правительства. По состоянию на октябрь 2017 года на портале «открытых данных» размещены 2 376 наборов данных, обсуждены 17 132 проекта нормативных правовых актов и концепций законопроектов, опубликованы 14 928 бюджетных документов.

Несмотря на достигнутые результаты, остаются актуальными проблемы, связанные с недостаточным уровнем открытости, клиентоориентированности и проактивности. Так, например, государственные органы неохотно раскрывают информацию, которая может быть использована для создания добавочной стоимости в виде актуальных и востребованных открытых данных.

Профильная деятельность государственных органов автоматизируется - однако, до сих пор есть сферы деятельности, недостаточно охваченные информатизацией. Появление новых технологий дает возможность предоставлять услуги более высокого качества, чем те, которые реализованы на текущий момент. Например, использование технологий больших данных может привести к принципиально новому подходу к анализу потребностей населения, и, как следствие, повышению качества обслуживания.

Непременными условиями вхождения Казахстана в топ-30 развитых стран мира являются не только рост ВВП до уровня развитых стран, но и преодоление разрыва в социально-экономическом развитии, в частности, достижение прогресса в улучшении показателей системы здравоохранения, и, соответственно, поддержание высокого уровня здоровья, продолжительности и качества жизни населения.

Цифровые технологии в здравоохранении могут помочь решить основные блоки проблем: доступность и качество медицинской помощи, а также вопросы профилактики заболеваний.

Здравоохранение напрямую влияет на длительность и качество жизни населения страны, включая сохранение возраста трудоспособности и экономической активности. Цифровизация здравоохранения позволяет снизить количество медицинских ошибок, повысить качество и скорость обслуживания, а также качество принятия управленческих решений.

В настоящее время государственные проекты, реализуемые в развитых странах, ориентированы на формирование целостной архитектуры национального уровня, обеспечивающей сбор, обработку и обмен данными о здоровье граждан и системе здравоохранения. Основные цели - получение единой информационной среды с возможностью мониторинга здоровья каждого человека, повышения эффективности системы здравоохранения в целом, повышение качества и доступности медицинской помощи, снижение количества медицинских ошибок, построения системы, в центре которой находятся пациент и информация о его здоровье.

Однако система здравоохранения все еще имеет достаточно большие сферы, неохваченные цифровизацией и не использующие современные возможности увеличения эффективности.

Также существуют проблемы в нормотворческом процессе, в том числе отсутствует единое информационное пространство; недостаточная прозрачность и разрыв связи между мониторингом и процессом нормотворчества, где ведение правового мониторинга осуществляется вручную; отсутствуют инструменты для проведения анализа перед разработкой НПА, в связи с чем существует необходимость дальнейшего совершенствования

информационных систем, которые будут прозрачными и работать в едином информационном пространстве.

4. Глобальные тренды цифровизации и международный опыт

Усилия по цифровизации приводят к созданию нового общества, где активно развивается человеческий капитал - знания и навыки будущего воспитываются с самых юных лет, повышаются эффективность и скорость работы бизнеса за счет автоматизации и других новых технологий, а диалог граждан со своими государствами становится простым и открытым.

Эти изменения вызваны внедрением за последние годы множества технологических инноваций, применяемых в разных отраслях. Кардинальным образом меняются способы производства и получения добавленной стоимости, появляются новые требования к образованию и трудовым навыкам людей. Промышленный интернет вещей формирует будущее производственных отраслей, используя возможности гибкого и умного производства, обеспечивает революционный рост производительности. Искусственный интеллект внедряется, в том числе, в консервативных отраслях, таких как финансовые услуги и медицина. Технология 3D-печати уже сегодня способствует трансформации таких отраслей, как авиация, логистика, биомедицина и автомобильная промышленность. Блокчейн имеет все предпосылки совершить глобальную трансформацию денежной системы. Большие данные и повсеместная доступность связи являются одними из факторов, на основе которых строится «экономика совместного потребления», распространяющаяся в глобальных масштабах ускоренными темпами. Компании-лидеры сегмента «совместного потребления при отсутствии физических активов» по размерам капитализации превышают стоимость традиционных компаний с многомиллиардными физическими активами на балансе.

Эти перемены радикальны и происходят за считанные годы и даже месяцы, а не десятилетия, как раньше. Но это только начало, и миру еще предстоит пережить основную массу перемен. Темп изменений нарастает, но еще не поздно быть частью этих изменений.

Процесс цифровизации сегодня затрагивает практически все страны мира. В то же время, каждая страна сама определяет приоритеты цифрового развития. Более 15 стран мира реализуют на текущий момент национальные программы цифровизации. Передовыми странами по цифровизации национальных экономик являются Китай, Сингапур, Новая Зеландия, Южная Корея и Дания. Китай в своей программе «интернет плюс» интегрирует цифровые индустрии с традиционными, Канада создает ИКТ-хаб в Торонто, Сингапур формирует «Умную экономику», драйвером которой становится ИКТ, Южная Корея в программе «Креативная экономика» ориентируется на развитие человеческого капитала, предпринимательство и распространение достижений ИКТ, а Дания фокусируется на цифровизации госсектора.

В этих странах государство играет ключевую роль в запуске и реализации программы, при этом успех зависит от вовлечения частных игроков - то, что называется «цифровая приватизация». Сегодня мы наблюдаем все больше

примеров, когда государства осознанно подталкивают участников экономической системы к цифровому будущему. Государство объявляет своего рода «тендер» на закрытие тех или иных «неэффективностей», идентифицированных как приоритетные. Игроки представляют свои «биды», концепции пилотов и подходы к возможной реализации проектов. Государство квалифицирует предложения и выбирает победителя по итогам конкурса пилотных проектов. Победитель, как правило, не получает прямых государственных субсидий, но получает право реализовать свой проект «под ключ» (по тому или иному направлению, в той или иной отрасли, в том или ином регионе). Государство обеспечивает поддержку в области нормативной базы, синхронизацию и кооперацию с ключевыми стейкхолдерами (региональные власти и др.), а также создание стимулов для «цифровизируемых» отраслей. Также возможен выбор консорциума победителей, который позволяет снижать риски при реализации, в то же время, поддерживая конкуренцию между 2-3 игроками.

Наиболее ярким примером подхода цифровой приватизации является Сингапур. Так, в 2014 г. государство инициировало разработку концепции Smart Nation и пригласило бизнес и экспертное сообщество к сотрудничеству для ее уточнения и реализации. Smart Nation - инициатива государства по повышению качества жизни посредством внедрения цифровизации в повседневную жизнь граждан. Государство сформировало исходный запрос на решение целого ряда задач, которые были определены как первостепенные для запуска основных инициатив в рамках Smart Nation. Так, одна из ключевых инициатив, определенных изначально, - развитие национальной сенсорной сети для построения «умного города». Под каждую из задач государство организовывает тендер для выбора подрядчика на разработку технического решения. Участие в тендере открыто для всех участников, отвечающих требованиям брифинга: таким образом, государство обеспечивает фокус не только на крупный бизнес, но и на привлечение малого и среднего бизнеса. Примечательно, что в 2015-2016 гг. более половины контрактов были подписаны с малым и средним бизнесом.

Государство может обеспечить «цифровой скачок» в стране за счет ускоренного развития конкретных технологий. В таких случаях государство принимает на себя роль инвестора, определяющего ключевые, наиболее перспективные направления финансирования, исходя из оценки долгосрочного возврата на инвестиции, конкурентной позиции, трендов, а также вкладывается в фундаментальные условия успеха, такие как образование и переквалификация кадров.

В Южной Корее при активной позиции государства опорные компании начинают самостоятельно осуществлять инвестиции в прорывные цифровые технологии. Так, один из крупнейших телеком-операторов страны - SKT - обозначил намерения инвестировать в технологии искусственного интеллекта и «интернета вещей» более 4 млрд. долларов США. Оператор отмечает необходимость партнерств в развитии новых технологий, а также планирует привлечение местных стартапов для разработки точечных решений.

Еще один глобальный тренд - «самоцифровизация государства», т.е. цифровизация операций государства и государственных компаний. Самоцифровизация - задача, которую необходимо реализовать любому государству, нацеленному на максимизацию создания стоимости в экономике, рост благосостояния, достойное место в рейтингах ведения бизнеса и уровня жизни.

У самоцифровизации на уровне страны существует два ключевых направления:

- Цифровизация государственного управления: цифровой документооборот, принципы digital by default и digital first, пересмотр неэффективных процессов. В этой логике самоцифровизация охватывает весь спектр сервисов: внутреннее взаимодействие госструктур - G2G, взаимодействие с гражданами - G2C, взаимодействие с бизнесом - G2B.

- Цифровизация субъектов квазигосударственного сектора, что особенно актуально для таких стран, как Казахстан, где государство по-прежнему в той или иной форме отвечает за большинство рабочих мест в экономике, а значит и за рост производительности труда. Поскольку зачастую традиционные конкурентные рыночные механизмы для таких компаний не работают, разрабатываются и устанавливаются измеримые КПЭ, связанные с реализацией цифровой трансформации (внедрение технологий индустрии 4.0 и соответствующее создание стоимости, % выручки от новых продуктов, обучение и переквалификация персонала).

Так, Дания активно инвестирует в цифровизацию госорганов. В настоящее время каждый гражданин и каждый бизнес имеют личный кабинет, с помощью которого происходит общение с госорганами в режиме реального времени. С 2015 г. все граждане обязаны общаться с госорганами только через интернет (в Дании 95% домохозяйств имеют доступ в интернет), каждый гражданин имеет цифровой паспорт (digital ID), а все госорганы и муниципалитеты связаны в единую сеть, что позволяет взаимодействовать со всеми ведомствами с помощью единого личного кабинета. Бизнес, кроме коммуникации, имеет возможность осуществлять все операции через интернет, получать выписки, оплачивать налоги и отправлять отчеты (в электронном виде отправка и получение документов занимает 5 минут в сравнении с 5-ю днями при отправке в бумажном виде). Подобная система позволяет ежегодно экономить 10-20% бюджета.

Все эти изменения имеют долгосрочные экономические и социальные последствия. Такое явление, как «экономика совместного потребления», распространяющаяся в глобальных масштабах ускоренными темпами, оказывает не только прямое влияние на каждого потребителя, но и косвенное влияние на страну в целом. Она является решением для самозанятых граждан, мотивирует к ведению предпринимательской деятельности и способствует росту экономической активности. Данный тренд получит дальнейшее развитие по мере того, как новые активы и предметы потребления будут использоваться совместно в целях сокращения индивидуальных издержек.

Контрольные вопросы:

1. Определение понятия и особенностей технологических понятий, связанных с цифровизацией (блокчейн, токен, биткоин, смарт-контракты и пр.).
2. Назовите направления развития цифровой инфраструктуры.
3. Глобальные тренды цифровизации.
4. Международный опыт в сфере цифровизации госорганов.

Тестовые задания:

1. Укажите вид цифрового актива, являющийся цифровым средством учета, обмена и удостоверения имущественных прав:
A) майнинг;
B) цифровой токен;
C) блокчейн;
D) биткоин;
E) искусственный интеллект.

2. Процесс проведения вычислительных операций с использованием компьютерных, энергетических мощностей согласно заданным алгоритмам шифрования и обработки данных, обеспечивающий подтверждение целостности блоков данных в объектах информатизации посредством блокчейна - это?
A) цифровой токен;
B) блокчейн;
C) смарт-контракт;
D) цифровой майнинг;
E) биткоин.

3. Дайте определение блокчейну:
A) ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства;
B) массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения;
C) информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;
D) вид цифрового актива, являющийся цифровым средством учета, обмена и удостоверения имущественных прав;
E) процесс проведения вычислительных операций с использованием компьютерных, энергетических мощностей согласно заданным алгоритмам шифрования.

4. Укажите правильный ответ. Технологическая платформа, компоненты которой связаны между собой заданными алгоритмами, размещаются на

различных узлах сети, могут иметь одного или более владельцев, а также могут обладать различным уровнем тождественности данных – это?
A) секрет компании;
B) распределенная платформа данных;
C) блокчейн;
D) IPO;
E) цифровой майнинг.

5. Умный договор – это?
A) публичный договор;
B) смарт-контракт;
C) ноу-хау;
D) договор присоединения;
E) протокол заседания совета директоров.

6. Цифровая (виртуальная) валюта, единица которой является монета – это?
A) криптовалюта;
B) блокчейн;
C) валюта Западной Европы;
D) национальная валюта;
E) токен.

7. Краудфандинг - это?
A) информация, предоставляемая в силу прямого указания закона в случаях реализации гражданином своих конституционных прав;
B) коллективное сотрудничество людей (доноров), которые добровольно объединяют свои деньги вместе, чтобы поддержать усилия других людей или организаций (реципиентов);
C) распределенный реестр или связанные блоки;
D) ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства;
E) платежная система, использующаяся одноименную единицу для учета операций.

8. Запрограммированный договор, условия которого прописаны в программном коде и который автоматически исполняется с помощью блокчейна – это?
A) реальный договор;
B) протокол заседания совета директоров;
C) консенсуальный договор;
D) ноу-хау;
E) смарт-контракт.

9. Что означает проверку или тестирование?
A) верификация;
B) смарт-контракт;

C) валидация;
D) майнинг;
E) блокчейн.

10. Под валидацией понимается:
A) подтверждение, аттестация;
B) проверка, тестирование;
C) регистрация;
D) идентификация;
E) реализация, сертификация.

Тема 2.2. Институт электронного документооборота

Цель: рассмотреть значение электронного документооборота в условиях развития цифровизации, сущность и значение электронной цифровой подписи.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- анализировать и соотносить нормы, регулирующие сущность электронного документооборота в условиях развития цифровизации.
- применять свои знания и понимание для решения проблем гражданско-правового регулирования по вопросам юридической значимости электронных документов.
- быть способным юридически правильно квалифицировать факты и обстоятельства.

План:

1. Значение электронного документооборота в современных условиях развития электронного государства. Электронная цифровая подпись.
2. Понятие электронного документооборота. Электронный документ.

1. Значение электронного документооборота в современных условиях развития электронного государства. Электронная цифровая подпись

Немаловажное значение в вопросе полноценного функционирования электронного правительства приобретает электронный документооборот (ЭДО), который можно определить как «систему ведения документации, при которой массив создаваемых электронных документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сеть, дающую возможность формирования и ведения распределенной базы данных».

Тем не менее проблемы, связанные с введением электронного документооборота, очевидны. В числе таких проблем можно назвать:

1) доказывание права авторства на информацию;

2) обнаружение и доказывание факта распространения контрафактных экземпляров;

3) идентификация содержания электронного документа с его творцом;

4) утверждение факта и даты ввода в Интернет документа;

5) определение и фиксация понятия электронного документа.

Необходимы комплексные решения в сфере безопасного электронного документооборота. Сегодня общественность заинтересована в предоставлении услуг «электронного правительства» при условии конфиденциальности и секретности при взаимодействии с государственной службой (при прозрачности для финансовых органов), гарантиях против мошенничества или взлома компьютеров.

В то же время в опубликованных сегодня документах по построению электронного правительства вопросы информационной безопасности учтены не в полной мере. На стадии реализации проекта это может привести к таким инцидентам, как нарушение прав граждан на получение услуг, нарушение конфиденциальности, подмена сайтов или документов в электронном виде при выполнении государственными органами своих функций и оказании услуг. В случае даже единичного взлома, ставшего достоянием широкой общественности, доверие граждан и предприятий к электронному правительству может быть подорвано, что увеличит период перевода государственных услуг в электронную форму.

В настоящее время система электронного документооборота развита главным образом в банковской сфере, а также при взаимодействии хозяйствующих субъектов и контролирующих органов (например, при подаче налоговых деклараций).

В большинстве случаев организации и граждане обращаются в государственные органы для регистрации и подтверждения своих прав, для защиты своих интересов и т.д. Совершение этих действии сопровождается огромным количеством документов, и их конечным результатом также чаще всего является документ. Чтобы граждане и организации согласились общаться через интернет с государством, они должны быть уверены, что все их права будут документированы в электронном виде не менее надежно, чем на бумаге. Сами государственные органы должны быть уверены в целостности и аутентичности представленных гражданами и организациями электронных документов.

Положительно на системе электронного документооборота сказывается принятие 7 января 2003 г. Закона РК № 370-II «Об электронном документе и электронной цифровой подписи». Этот Закон расширяет сферу использования и допустимые виды электронной подписи. Прежний закон разрешал применять только сертифицированные средства электронной подписи, а область ее использования ограничивалась гражданско-правовыми отношениями.

Законом установлены принципы использования электронной цифровой подписи:

1) Электронная цифровая подпись равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия при выполнении следующих условий:

- удостоверена подлинность электронной цифровой подписи при помощи открытого ключа, имеющего регистрационное свидетельство;

- лицо, подписавшее электронный документ, правомерно владеет закрытым ключом электронной цифровой подписи;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в регистрационном свидетельстве;

- электронная цифровая подпись создана и регистрационное свидетельство выдано аккредитованным удостоверяющим центром Республики Казахстан или иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне Республики Казахстан.

2) Закрытые ключи электронной цифровой подписи являются собственностью лиц, владеющих ими на законных основаниях.

Лицо может иметь закрытые ключи электронной цифровой подписи для различных информационных систем. Закрытые ключи электронной цифровой подписи не могут быть переданы другим лицам.

Допускается хранение закрытых ключей электронной цифровой подписи в удостоверяющем центре в соответствии с правилами создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

3) Владелец регистрационного свидетельства электронной цифровой подписи юридического лица - руководитель юридического лица или лицо, его замещающее, вправе передавать работнику данного юридического лица или назначенному им лицу полномочия на использование электронной цифровой подписи от имени данного юридического лица.

Согласно закону выделяются два вида ключа электронной цифровой подписи: открытый и закрытый.

Открытый ключ электронной цифровой подписи - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

Закрытый ключ электронной цифровой подписи - последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи.

Иностранная электронная цифровая подпись, имеющая иностранное регистрационное свидетельство, признается на территории Республики Казахстан в следующих случаях:

- удостоверена подлинность иностранной электронной цифровой подписи доверенной третьей стороной Республики Казахстан;

- лицо, подписавшее электронный документ, правомерно владеет закрытым ключом иностранной электронной цифровой подписи;

- иностранная электронная цифровая подпись используется в соответствии со сведениями, указанными в регистрационном свидетельстве;

- сформирована средствами электронной цифровой подписи иностранного удостоверяющего центра, зарегистрированного в доверенной третьей стороне Республики Казахстан, или иностранного удостоверяющего центра, зарегистрированного в доверенной третьей стороне иностранного государства, зарегистрированной в доверенной третьей стороне Республики Казахстан.

Кроме того, развитые информационно-коммуникационные технологии могут явиться мощным инструментом подавления населения и стать предпосылкой возникновения антидемократического режима. Поэтому законодательство становящегося электронного государства должно содержать гарантии пресечения противоправного вмешательства в жизнь и сознание людей в определенных интересах, а также быть готово к информационным изменениям и отражать основные вопросы его функционирования».

2. Понятие электронного документооборота. Электронный документ

Итак, под электронным документооборотом понимают систему ведения документации, при которой массив создаваемых электронных документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сеть, дающую возможность формирования и ведения распределенной базы данных.

В соответствии со ст. 1 Закона РК от 7 января 2003 г. № 370-II «Об электронном документе и электронной цифровой подписи» выделяются следующие понятия:

- электронный документ - документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;

- электронный документооборот - обмен электронными документами между государственными органами, физическими и юридическими лицами;

- система электронного документооборота - система обмена электронными документами, отношения между участниками которой регулируются нормативными правовыми актами Республики Казахстан.

Электронный документ состоит из двух частей:

- реквизитной, содержащей идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т.д.) и электронную подпись;

- содержательной, включающей в себя текстовую, числовую и/или графическую информацию, которая обрабатывается в качестве единого целого.

Характеризуя основные проблемные области в сфере электронного документооборота, С.И. Семилетов отмечает: юридическая сила как официальных документов, так и прочих индивидуальных актов, обеспечивается их соответствием требованиям, установленным зако- ном и наличием вытекающих из них необходимых реквизитов. Одним из обязательных и важных реквизитов документа, обеспечивающим юридическую силу документа, является собственноручная подпись физического или должностного лица, составившего документ, отображающая волю и согласие подписавшего лица по отношению к содержанию документа. По реквизиту (подпись)

идентифицируется подписавшее документ лицо, оцениваются его полномочия. Такая же функция электронной подписи и в электронном документе.

Электронный документооборот осуществляется в государственных и негосударственных информационных системах на основе следующих принципов:

1) функционирования различных систем электронного документооборота;

2) использования электронных документов в любых сферах деятельности, где применяются информационно-коммуникационные технологии для создания, обработки, хранения и передачи данных;

3) передачи электронных документов с использованием любых информационных систем.

Требования к электронному документообороту:

1. Электронный документ, соответствующий требованиям настоящего Закона и удостоверенный посредством электронной цифровой подписи лица, имеющего полномочия на его подписание, равнозначен подписанному документу на бумажном носителе.

2. Электронный документ считается отправленным с момента его передачи через сети телекоммуникаций.

3. Входящий электронный документ считается поступившим после его фиксации в информационной системе адресата.

4. Уведомление о получении должно содержать данные о факте и времени получения электронного документа и его отправителе. В случае непоступления его автору считается, что документ не получен адресатом.

В случаях, установленных законодательством Республики Казахстан, для оказания государственной услуги представляется электронная копия документа.

5. Порядок электронного документооборота определяется Правительством Республики Казахстан.

6. Порядок сбора, обработки, хранения, передачи, поиска, распространения, использования, защиты, регистрации и уничтожения электронных документов и иных данных, содержащих сведения, составляющие государственные секреты, с использованием информационных систем в защищенном исполнении, отнесенных к государственным секретам, а также порядок создания, аккредитации и прекращения деятельности специального удостоверяющего центра определяются Комитетом национальной безопасности Республики Казахстан.

Электронные документы хранятся в государственных и (или) негосударственных информационных системах в порядке, установленном законодательством Республики Казахстан.

Участник системы электронного документооборота вправе:

- обратиться в удостоверяющий центр за подтверждением принадлежности и действительности открытого ключа электронной цифровой подписи, зарегистрированного данным удостоверяющим центром;

- обслуживаться несколькими удостоверяющими центрами.

Участник системы электронного документооборота обязан соблюдать установленные правила электронного документооборота.

Безусловно, нормативно-правовое обеспечение юридической значимости электронных документов должно осуществляться с учетом правового режима электронного документа и его функционального назначения. В целях законодательного определения правового статуса электронных документов, по мнению Е.В. Семизоровой, необходимо:

- установить правовые критерии признания электронного документа юридически значимым;
- предусмотреть ответственность за умышленное уничтожение электронных документов или их реквизитов, обеспечивающих качество юридической значимости электронного документа;
- определить и стандартизировать основные типы файлов, используемых для обработки, хранения и передачи документированной электронной информации, в целях обеспечения их адекватного отображения у всех участников электронного документооборота и взаимного обмена документированной информацией в рамках деятельности электронного правительства. Данный перечень должен носить открытый характер;
- предусмотреть меры, направленные на обеспечение доступности к информации в случае исключения каких-либо файловых типов из данного перечня;
- разработать и закрепить законодательно порядок осуществления третьей независимой стороной процедур перевода документов из традиционной формы в электронную и наоборот, в том числе в случаях, когда документ изначально был создан и существовал до момента перевода исключительно в электронной форме.

Контрольные вопросы:

1. Охарактеризуйте роль электронного документооборота на современном этапе развития Казахстана.
2. Дайте характеристику электронному документообороту.
3. В чем специфика электронного документа? Каковы его реквизиты?
4. Определите понятие и признаки электронной цифровой подписи.
5. Охарактеризуйте виды электронной подписи.

Тестовые задания:

1. Когда был принят Закон РК № 370-II «Об электронном документе и электронной цифровой подписи»?
A) 30 августа 1995 г.;
B) 7 января 2003 г.;
C) 7 января 2022 г.;
D) 1 июля 1999 г.;
E) 16 декабря 1991 г.

2. Из каких частей состоит электронный документ?
A) письменной и устной;
B) интерактивной и ссылочной;

C) вводной и резолютивной;
D) реквизитной и содержательной;
E) описательной и заключительной.

3. Дайте понятие реквизитной части электронного документа:
A) включает в себя технологию создания;
B) содержит идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т.д.) и электронную подпись;
C) обеспечивает неизменность информации на платформе данных;
D) является средством учета и обмена имущественных прав;
E) содержит порядок проведения вычислительных операций с использованием алгоритмов шифрования.

4. Укажите правильный ответ. Содержательная часть электронного документа включает в себя:
A) секреты компании;
B) текстовую, числовую и/или графическую информацию, которая обрабатывается в качестве единого целого;
C) статистическую и аналитическую информацию;
D) описательную и идентифицирующую характеристику;
E) цифровые данные.

5. Электронная цифровая подпись равнозначна:
A) печати организации;
B) уставу организации;
C) собственноручной подписи подписывающего лица;
D) подписи исполняющего обязанности подписывающего лица;
E) решению совета директоров.

6. Обмен электронными документами между государственными органами, физическими и юридическими лицами – это?
A) делопроизводство;
B) электронная почта;
C) электронный документооборот;
D) корпоративная связь;
E) технология производства.

7. Электронный документ - это?
A) информация, предоставляемая в силу прямого указания закона в случаях реализации гражданином своих конституционных прав;
B) документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;
C) распределенный реестр или связанные блоки;
D) ценная информация, которая включает в себя секреты производства (ноу-хау), технологию производства;

E) платежная система, использующаяся одноименную единицу для учета операций.

8. Система электронного документооборота – это?
A) порядок сбора, обработки электронных документов;
B) система поиска, распространения информации;
C) система обмена электронными документами, отношения между участниками которой регулируются нормативными правовыми актами Республики Казахстан;
D) запрограммированный договор, условия которого прописаны в программном коде;
E) система защиты, регистрации и уничтожения протоколов заседаний органов управления.

9. Укажите виды ключей электронной цифровой подписи:
A) простой и сложный;
B) открытый и закрытый;
C) временный и постоянный;
D) условный и срочный;
E) электронный и бумажный.

10. Под последовательностью электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи понимается:
A) блокчейн;
B) открытый ключ ЭЦП;
C) закрытый ключ ЭЦП;
D) майнинг;
E) валидация.

Тема 2.3. Глобальные информационные системы. Интернет. Средства массовой информации. Интернет-СМИ

Цель: раскрыть основные подходы к определению Интернета, понятие и признаки средства массовой информации.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- применять свои знания и понимание для решения проблем правового регулирования по вопросам специфики Интернет-СМИ.
- умение правильно применять нормы права.
- умение анализировать юридическую литературу по заданным темам.

План:

1. Правовая природа Интернета и Интернет-отношений.
2. Понятие средств массовой информации. Конституционные гарантии свободы массовой информации.
3. Средства массовой информации, функционирующие в сети Интернет.
4. Интернет-диффамация: вопросы юридической ответственности.
5. Договор банковского вклада.

1. Правовая природа Интернета и Интернет-отношений

В последние годы, как в Казахстане, так и во всем мире Интернет активно используется хозяйствующими субъектами в самых различных областях предпринимательской деятельности. Это обусловлено в первую очередь тем, что использование современных телекоммуникационных технологий позволяет существенно снизить материальные издержки, связанные с осуществлением предпринимательской деятельности, сократить временные затраты на осуществление хозяйственных операций, увеличить объем реализации товаров, работ и услуг посредством Интернета за счет новых потребителей, способствует более эффективному использованию Интернета в рекламных целях. Растет количество зарегистрированных доменных имен. Появляются все новые виды услуг, связанных с использованием Интернета, увеличивается объем инвестиций в телекоммуникационные технологии.

Вместе с тем заметим, что на сегодняшний день национальное законодательство отстает от бурного развития технологий. В первую очередь это касается сферы интернет-регулирования правоотношений, возникающих в глобальной Сети. Однако многие проблемы, существующие в социальной и экономической сфере, также получили свое преломление в виртуальном пространстве. Являясь, по сути, принципиально новым институтом общественной жизни, Интернет поставил перед правовой наукой целый комплекс проблем. Возникла необходимость переосмыслить правовую доктрину с учетом последствий функционирования Сети, которые вызывают массу вопросов юридического характера. Среди них - проблема определения понятия «Интернет», пределы правового регулирования Сети, вопросы юрисдикции по спорам, возникающим из сетевых отношений, вопросы квалификации сделок и правонарушений, совершенных в Интернете, используемых доказательств и множество других.

Интернет (от англ. Internet) - это всемирная система объединённых компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (World Wide Web, WWW) и множества других систем (протоколов) передачи данных. Интернет представляет собой сеть взаимосвязанных компьютерных систем и ряда различных компьютерных служб.

При этом Интернет - глобальная информационная система, части которой логически взаимосвязаны друг с другом посредством единого адресного

пространства. Интернет состоит из множества взаимосвязанных компьютерных сетей и обеспечивает удаленный доступ к компьютерам, электронной почте, доскам объявлений, базам данных и дискуссионным группам.

Основанием для перехода служит постоянное движение страны от компьютеризации к информатизации и созданию единого развитого информационного пространства в глобальной сети Интернет казахстанского сегмента Интернета - Казнета (далее - Казнет).

Развитие единого информационного пространства Казнет является межотраслевой, межведомственной и государственной задачей, требующей координации действий множества участников данного процесса. Такая координация возможна только на основе единой концепции, определяющей и обосновывающей необходимые действия и их последовательность.

Официальная история Казнета имеет своей точкой отсчета 19 сентября 1994 года - день, когда в базе данных IANA был зарегистрирован домен верхнего уровня KZ. В июне 1995 года появляется первый каталог казахстанских веб-сайтов - Kazakh Internet Yellow & White Pages (ныне несуществующий). В декабре 1997 года запускается проект наиболее популярного в настоящее время каталога рубрикатора казахстанских веб-ресурсов - «Весь WWW-Казахстан» (Catalog.Site.KZ).

К объектам развития и регулирования Казнета можно отнести:

1) информационные ресурсы вне зависимости от форм хранения и собственности, содержащие как сведения, составляющие коммерческую тайну, конфиденциальную информацию, так и открытую общедоступную информацию;

2) права физических и юридических лиц, государства на получение, распространение и пользование информацией, защиту конфиденциальной информации и интеллектуальной собственности;

3) систему формирования общественного сознания (мировоззрение, политические взгляды, моральные и этические ценности и прочие), базирующуюся на информации, распространяемой в глобальной сети Интернет;

4) систему воздействия на процесс принятия политических решений, во многом зависимую от качества и своевременности ее информационного обеспечения;

5) систему информирования государственными органами населения об общественно-политических и социально-экономических аспектах жизни страны;

6) систему участия общественных объединений в пропаганде своих взглядов в средствах массовой информации, размещенных в сети Интернет;

7) общенациональную, региональные и локальные информационно-телекоммуникационные системы сети передачи данных, в том числе и специального назначения, а также спутниковые системы связи;

8) системы электронной торговли - торговля товарами и услугами посредством Интернета.

Пространство Казнет объединяет в себе следующие типы ресурсов: самостоятельные интернет-ресурсы доменной зоны KZ; сетевые ресурсы

других доменных зон, расположенные на площадках казахстанских провайдеров; иностранные ресурсы, направленные на казахстанскую аудиторию; ресурсы казахстанских компаний, расположенные в других доменных зонах.

Не прекращаются дискуссии по поводу главного вопроса: что есть Интернет? Объект права? Или, может быть, субъект?

Одна из точек зрения относит Интернет к средствам массовой информации. Эта точка зрения основана на положениях Закона «О средствах массовой информации», согласно которому:

- под массовой информацией понимаются предназначенные для неограниченного круга лиц печатные, аудиовизуальные и иные сообщения и материалы;

- под средством массовой информации понимается периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая интернет-ресурсы;

- под сетевым изданием понимается интернет-ресурс, прошедший процедуру постановки на учет в уполномоченном органе, информационно-коммуникационная инфраструктура которого размещена на территории Республики Казахстан.

Второй подход основан на признании Интернета субъектом права, однако субъект права должен обладать рядом существенных признаков, например, правосубъектностью, которыми сеть в полной мере не обладает.

Третья точка зрения более обоснована, и заключается она в признании Интернета объектом права. Действительно, Интернет как инфраструктура информационного общества, скорее всего, очевидно, будет выступать в качестве объекта правового регулирования, причем даже не специального, а самого обычного.

Существует немало подходов к определению понятия Интернета. В Казахстане термин «Интернет» используется в многочисленных нормативных правовых актах, легальное определение Интернета дается в Законе Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»: «Интернет - всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов».

По мнению И.Л. Бачило, Интернет - это сфера непрерывного информационно-коммуникационного процесса, обеспечивающего обращение информации (сведений) в цифровой форме в неограниченном пространстве через связанные между собой сети связи, и реализации обмена информационным ресурсом любых субъектов (потребителей) в целях получения, накопления знаний или осуществления электронных операций субъектов в разных областях реализации их интересов, прав и обязанностей.

Специфика Интернета предопределена особенностями кибернетического пространства, к числу которых, по мнению И.М. Рассолова, относится:

1) отсутствие географических границ;

2) анонимность в киберпространстве;

3) возможность ускользать от контроля (пользователи Сети могут «выйти» из режима, определенного национальным законом, чтобы избежать выявления совершенных ими правонарушений… Субъекты преступлений стараются осуществлять свою преступную деятельность в наиболее свободных зонах Интернета, т.е. вне судебной юрисдикции собственного государства (например, в зонах .com, .net, .org, .ag, .sc)

4) иерархия и структурные зоны (Интернет представляет пространственную структуру, включающую иерархию различных участников: учреждений регистрации доменных имен и множества посредников, распределенных ассиметричным способом (интернет-провайдеры, торговые информационные посредники и др. Все они обеспечивают возможность доступа потребителям информации к информационным разделам и наполнениям Сети);

5) растущее взаимодействие, интерактивность и динамизм;

6) наличие интерактивных информационных связей (Интернет характеризуется огромным числом электронных соединений, коммуникаций. Одним из характерных элементов этой среды является сетевой договор).

В юридической литературе выделяют четыре регулятора правоотношений в сети Интернет (поведения участников сети). Поведение в данной сфере может быть урегулировано следующими типами регуляторов:

- напрямую законом;
- социальными (корпоративными) нормами;
- законами рынка и конкуренции;
- техническими нормами.

В виду того, что сеть Интернет и отношения в рамках сети Интернет развиваются гораздо быстрее, чем законодатель успевает создавать соответствующие законные конструкции и формулы, в настоящее время регулирование большой части отношений строится на деловых обыкновениях, «Интернет-обычаях».

Безусловно, начинать правовое урегулирование сети Интернет необходимо с норм международных - единых для всех цивилизованных государств. Правоотношения, складывающиеся в сети Интернет, не могут регулироваться только нормами национального законодательства.

В числе их особенностей:

1. Особый субъектный состав. Интернет-отношения могут возникать между особыми субъектами (операторы связи, провайдеры, разработчики сетей, международные организации, отвечающие за развитие протоколов Интернета и т.д.).

2. Субъекты интернет-отношений могут находиться в разных странах, а их деятельность регулироваться законодательствами разных стран.

3. Интернет-отношения невозможны без использования информационно-коммуникационных технологий и сетей. Они имеют информационное наполнение, т.е. складываются по поводу информации в Интернете. Объектом этих отношений является не всякая информация, а только обрабатываемая в киберпространстве.

4. Интернет-отношения выделяются на современном этапе развития общества, государства и технологий… для целей автоматизации управления различными информационными системами, в нашем случае сложной кибернетической системы - Интернета.

Очевидно, что Интернет сегодня прочно вошел в современную жизнь практически каждого человека. Однако нерешенных проблем в этой области еще достаточно. Остановимся на некоторых их них.

Безусловно, в числе проблем - проблема цифрового равенства. И здесь будет полезен опыт зарубежных государств, в которых работают специализированные программы соответствующей подготовки.

Проблема номер один сегодня - защита персональных данных в сети Интернет.

Анонимность интернет - отношений предопределяет и наличие проблемы установления личности субъекта Интернет-отношений, т.е. проблема идентификации.

Для вступления в некоторые коммуникационные интернет-отношения субъекты должны быть определенным образом идентифицированы. Многие интернет-ресурсы и сервисы предлагают или требуют для использования их пройти процедуру регистрации. Можно сказать, что для деятельности в виртуальном пространстве Интернета человек создает свой виртуальный образ или виртуальное лицо. По аналогии с реальным человеком виртуальное лицо будет иметь свое «имя», под которым действует (имя пользователя) и аналог фотографии и подписи в удостоверении личности - пароль.

Поскольку субъект виртуальных отношений определяется только этими двумя параметрами, то виртуальные лица и реальные люди не соотносятся между собой как один к одному: один пользователь может иметь несколько виртуальных лиц, и за одним виртуальным лицом может стоять несколько людей. Основная возникающая в этом случае проблема: сложно установить реального человека, стоящего за виртуальным лицом, еще сложнее эту связь процессуально доказать. В механизме электронной подписи также не предусмотрено наличие идентифицирующего признака, непосредственно связанного с человеком, неотчуждаемого от него.

2. Понятие средств массовой информации. Конституционные гарантии свободы массовой информации

Основной нормативный акт, регулирующий отношения, складывающиеся в сфере массовой информации, с участием средств массовой информации - это Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации».

Под массовой информацией, согласно данному закону, понимаются предназначенные для неограниченного круга лиц печатные, аудиовизуальные и иные сообщения и материалы.

Под средством массовой информации понимается периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная

запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая интернет-ресурсы.

Распространение продукции средства массовой информации включает: продажу, подписку, доставку, раздачу периодического печатного издания, аудио- или видеозаписи программы, вещание телеканала, радиоканала (телевизионное вещание, радиовещание), вещание телепрограммы, радиопрограммы в составе соответственно телеканала, радиоканала, демонстрацию кинохроникальной программы, предоставление доступа к сетевому изданию, иные способы распространения.

В ст. 2 Закона РК «О средствах массовой информации» четко определено, что свобода слова, творчества, выражения в печатной и иной форме своих взглядов и убеждений, получения и распространения информации любым не запрещенным законом способом гарантируются Конституцией Республики Казахстан. Цензура запрещается.

Государственные органы, общественные объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации.

Средства массовой информации обязаны содействовать государственным органам, осуществляющим противодействие терроризму.

Разглашение сведений, составляющих государственные секреты или иную охраняемую законом тайну, пропаганда и оправдание экстремизма или терроризма, распространение информации, раскрывающей технические приемы и тактику антитеррористических операций в период их проведения, пропаганда наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также культа жестокости, насилия и порнографии запрещаются.

Основными принципами деятельности средств массовой информации являются:

- объективность;
- законность;
- достоверность;
- уважение частной жизни, чести, достоинства человека и гражданина.

Распространение не соответствующих действительности сведений, порочащих честь и достоинство гражданина или организации (государственного органа, общественного, творческого, научного, религиозного либо иного объединения граждан и юридических лиц), воздействие средствами массовой информации на суд влекут ответственность, предусмотренную законодательными актами Республики Казахстан.

Ответственность за нарушение законодательства о средствах массовой информации несут виновные в этом должностные лица государственных органов и иных организаций, а также собственник, распространитель, главный редактор (редактор) средства массовой информации, авторы распространяемых сообщений и материалов.

Собственник, главный редактор (редактор) средства массовой информации несут установленную законодательными актами Республики

Казахстан ответственность за распространение сообщений и материалов, содержащих пропаганду или агитацию насильственного изменения конституционного строя, нарушения целостности Республики Казахстан, подрыва безопасности государства, войны, социального, расового, национального, религиозного, сословного и родового превосходства, культа жестокости, насилия и порнографии, независимо от источника их получения.

Собственник, главный редактор (редактор), журналист средства массовой информации, в том числе физические или юридические лица, использующие интернет-ресурсы, не вправе разглашать в распространяемых сообщениях и материалах информацию, указанную в пункте 3-4 статьи 14 Закона «О СМИ», за исключением случаев, если распространение такой информации осуществляется в целях защиты прав и законных интересов ребенка, пострадавшего в результате противоправных действий (бездействия), и несовершеннолетних, подозреваемых и (или) обвиняемых в совершении административных и (или) уголовных правонарушений, за исключением несовершеннолетних, признанных судом виновными в совершении тяжких или особо тяжких преступлений, включая информацию об их родителях и иных законных представителях.

Информация, указанная в части первой настоящего пункта, может распространяться в средствах массовой информации с согласия:

- несовершеннолетнего, достигшего четырнадцатилетнего возраста, пострадавшего в результате противоправных действий (бездействия), и его законных представителей;

- законных представителей несовершеннолетнего, не достигшего четырнадцатилетнего возраста, пострадавшего в результате противоправных действий (бездействия);

- несовершеннолетнего, достигшего шестнадцатилетнего возраста, совершившего административные и (или) уголовные правонарушения, и его законных представителей.

В случае, если одно из лиц, указанных в части второй настоящего пункта, не дает своего согласия на распространение информации в средствах массовой информации, распространение данной информации запрещено, за исключением следующих случаев:

- без согласия несовершеннолетнего, достигшего четырнадцатилетнего возраста и пострадавшего в результате противоправных действий (бездействия), или его законных представителей, если законный представитель является подозреваемым или обвиняемым в совершении данных противоправных действий (бездействии);

- с согласия одного законного представителя пострадавшего несовершеннолетнего в случае, если второй законный представитель находится за пределами Республики Казахстан и его согласие получить не представляется возможным.

Средства массовой информации вправе в целях содействия расследованию преступления, установлению лиц, причастных к совершению преступления, розыску пропавших несовершеннолетних в объеме, необходимом

для достижения указанных целей, и с соблюдением требований, установленных Уголовно-процессуальным кодексом Республики Казахстан, на основании процессуальных документов, полученных от органов, ведущих уголовный процесс, распространять в средствах массовой информации сведения, относящиеся к несовершеннолетнему.

Воспрепятствование законной профессиональной деятельности журналиста влечет установленную законами Республики Казахстан ответственность.

3. Средства массовой информации, функционирующие в сети Интернет

Реалии развития Интернет-отношений позволяют с уверенностью утверждать: справедливо считать свершившимся появление нового средства массовой информации, объединяющего в себе черты теле- и радионовостей (оперативность обновления) с газетными и журнальными публикациями (объём предоставляемой информации).

Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает сегодня один из самых активных этапов своего развития.

Развитие единого информационного пространства Республики Казахстан является одной из важнейших задач, стоящей перед государством, которое должно решать вопросы не только своего развития и как следствие - развития информационного пространства, но и обеспечения информационной безопасности.

Источником распространения массовой информации в сети является любой общедоступный и открытый информационный ресурс. Это может быть Интернет-страница или сайт, on-line конференция, электронная почтовая рассылка и т.д.

Безусловно, новые технологии заставили нас изменить традиционное представление о средствах массовых коммуникаций. Традиционные формы коммуникаций - телевидение и радио - с приходом глобальных компьютерных сетей и применением цифровых технологий обработки вещательного сигнала дали качественно новые возможности. А главное - увеличилась пропускная способность радио- и телеканалов и, в конечном счете, значительно увеличились возможности ресурса распространения электронных СМИ.

Свобода Интернета от коммерческих и политических ограничений вместе с его доступностью и интерактивностью придает электронным средствам коммуникаций громадный демократизирующий потенциал, поскольку позволяет избегать цензуры и регламентации. Однако, с другой стороны, эти возможности являются основой существующих угроз информационной безопасности, а также нелегальной деятельности хозяйствующих субъектов, бесконтрольного распространения рекламы, в том числе рекламы криминального характера.

Проанализируем средства массовой информации, функционирующие в сети Интернет, определим их правовой режим, акцентируя внимание на возможности применения норм действующего законодательства для регулирования правоотношений с участием таких СМИ.

Мы наблюдаем всплеск активности анализируемых СМИ в масштабах всей страны (что особенно наглядно в период предвыборных агитаций). Нельзя не принимать во внимание и предсказаний ежегодного удвоения «населения» Сети.

Говоря о регулировании средств массовой информации, функционирующих в Интернет, возникает вопрос: насколько правомерно считать средствами массовой информации такие издания вообще?

Активное развитие средств массовой информации в Сети очевидно. Тем не менее, до сих пор не выработано единого представления о содержании и формах деятельности таких СМИ, единого подхода к терминологии.

Прежде всего, необходимо отметить многовариантность правовых ответов на терминологическое выражение смыслового наполнения Интернета. Нет единого подхода и у специалистов, занимающихся проблемами правового урегулирования интернет-отношений.

Средства массовой информации в сети Интернет закон «О средствах массовой информации» определяет как сетевые издания. Под сетевым изданием согласно «букве закона» понимается сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с законом.

Средства массовой информации, функционирующие в Интернет, разнообразны по характеру своей деятельности, по тематике и т.д. В связи с этим представляется необходимым проанализировать возможность их классификации. Проанализируем уже имеющие подходы.

И. Давыдов еще в 2000 г. осуществил попытку охарактеризовать масс-медиа Интернета и предложил варианты классификации медийных ресурсов, представленных в Интернете. Им были выделены собственно сетевые издания (т.е. те, которые выходят только в Интернете и сетевые версии традиционных СМИ).

Кроме того, сетевые СМИ могут быть подразделены по типу представленного в них контента. Здесь возможны две классификации:

1) новостные; комментарийные; смешанные;

2) авторские; редакционные; смешанные.

Возможны также классификации по тематике: монотематические (внутри этой группы деление может стать почти бесконечным ввиду обилия вариантов представленных монотематических ресурсов); политематические; и классификация по принадлежности: принадлежащие государству; принадлежащие медийным группам; политическим группам; бизнес - группам; независимые.

Кроме того, существенно деление, которое, несмотря на используемую терминологию, относится не столько к географическому положению редакций конкретных ресурсов, сколько к аудитории, на которую данные ресурсы

ориентированы в первую очередь: общие ресурсы, региональные ресурсы (к данному типу могут быть отнесены также зарубежные русскоязычные ресурсы, ориентированные на относительно узкие диаспоры).

Необходимо отметить, что в последнее время появилось много новых информационных объектов: домашняя интернет-страница, сайт, портал, электронная библиотека, он-лайн конференция, чаты, службы мгновенного сообщения типа ICQ и MSN, электронная почтовая рассылка в популярном формате RSS или столь модный сегодня блог.

Такие СМИ представляют собой информационные объекты, содержанием которых являются размещаемые на них и периодически обновляемые сведения, сообщения и материалы, по общему правилу предназначенные для неопределенного круга лиц. Иными словами эти объекты распространяют не что-нибудь, а именно «массовую ин формацию» в понимании нормы ст. 1 Закона РК «О средствах массовой информации».

Отмечая роль и оценивая влияние средств массовой информации в сети Интернет на общество в целом, исследователи подчеркивают, что «если на Западе в блогах больше речь идет о том, например, «как я провел лето» или «как я купил себе новый макинтош», то в Казахстане блоги совершенно особенная вещь - здесь проявляется наш особый путь. Политическая дискуссия, пропавшая со страниц газет, из ТВ и радио, она вся сейчас там. Люди интеллектуального труда пользуются Livejournal, и у них нет ощущения, что в стране отсутствует политическая дискуссия - она есть, просто она не в том месте, где была раньше».

Известно, что «для сетевых информационных процессов характерны широта охвата аудитории, высокая оперативность, многообразие форм информационного воздействия при наличии обратных связей пользователя с поставщиком информации. Такое сочетание приводит к тому, что глобальные компьютерные сети становятся мощным инструментом выражения и формирования общественного мнения. В этом качестве они приближаются по своим возможностям к традиционным средствам массовой информации, а в некоторых случаях и превосходят их. Нередко электронные газеты сообщают о произошедших событиях раньше, чем традиционные СМИ.

По мнению А.Г. Рихтера, «между Интернетом и средствами массовой информации нельзя ставить знак равенства: признаки информации, распространяемой по телекоммуникационным сетям, не совпадают с признаками традиционной массовой информации». Прежде всего, для Интернет-страниц не подходит формула «форма периодического распространения массовой информации», характеризующая традиционные средства массовой информации.

Как представляется, наиболее логичную и обоснованную позицию по данной проблеме предложил В. Наумов. В логике его подхода, - любой сайт - источник массовой информации, но отнюдь не любой сайт - средство массовой информации. Поскольку, как правильно отмечает В. Наумов, переход в правовое положение СМИ с неизбежностью сопряжен с соответствующими обременениями (новый баланс прав и обязанностей), то это серьезное и

юридически значимое действие должно проводиться собственниками и менеджментом тех или иных сетевых ресурсов осознанно и добровольно.

Размышляя о статусе СМИ, В. Наумов метафорично интерпретирует его в качестве своеобразных «погон» или «униформы» для СМИ. А за красивые «погоны и униформу», дающие определенные права и преференции, как, впрочем, и за все в жизни, «надо платить». В частности, - повышенной юридической ответственностью за то, чем отзовется виртуальное слово и\или изображение.

В настоящее время в мире имеют место различные подходы к определению отношения государства к Интернет-СМИ. Например, китайский вариант, в той или иной степени распространённый в ряде государств Юго-Восточной Азии и Ближнего Востока. Суть его в строгом (сама степень строгости определяется исключительно мнениями руководства государства со ссылкой на национальные традиции) контроле за деятельностью в Интернете, или цензуре. Государство контролирует большую часть информации, циркулирующей в сети, а само существование Интернет-СМИ в ряде случаев невозможно.

Другой вариант (характерен для государств Западной Европы и Северной Америки) подразумевает государственный контроль, сводящийся к пресечению преступной деятельности в Интернете. Однако такой вариант не охватывает всего многообразия общественных отношений.

В настоящий момент трудно судить, какой вариант будет избран для Казахстана в качестве наиболее оптимального. Согласно Конституции, в нашей стране необходим баланс интересов с одной стороны общества и Интерне-СМИ, имеющих право на информацию, и государства, призванного защищать общество от преступности, насилия и других негативных явлений. Формирование такого баланса зависит от позиции не только государственных ведомств, юристов и журналистов, но и рядовых граждан-пользователей Интернета.

Известно, что в рамках поручений Первого Президента, данных в статье «Социальная модернизация Казахстана: двадцать шагов к обществу всеобщего труда» от 23 июля 2012 года № 961 утверждена новая программа «Информационный Казахстан - 2020», основной целью которой выступает создание условий, обеспечивающий переход страны к информационному обществу. Программа направлена на обеспечение эффективности системы государственного управления, доступности инновационной и информационно-коммуникационной инфраструктуры, создание информационной среды для социально-экономического и культурного развития общества, а также развитие отечественного информационного пространства.

Действующее законодательство о средствах массовой информации было принято тогда, когда журналистика была практически полностью профессиональной. Сейчас, с развитием Интернета, журналистика доступна каждому пользователю: популярные блоги и микроблоги имеют аудиторию больше, чем некоторые традиционные СМИ. Представляется, что концепция интернет-ресурсов как СМИ, сыграв положительную роль в развитии

казахстанского законодательства, полностью себя исчерпала. Интернету «тесно» в рамках Закона РК «О СМИ», что требует специфических методов правового регулирования информационных аспектов Интернета. Право на получение и распространение информации посредством глобальных информационно-коммуникационных сетей нуждается в самостоятельном закреплении, так как имеет ряд особенностей: оно, в отличие от традиционных СМИ, интерактивно, требует специального технического обеспечения, может реализовываться анонимно, соответствующая информация распространяется мгновенно, борьба с злоупотреблениями здесь затруднена. Таким образом, статус интернет-ресурсов как источников информации мог бы стать объектом отдельной главы нового закона.

Существенными характеристиками современного развития Интернет-отношений Казахстана являются:

- большой рост количества новых веб-сайтов, компаний и предприятий в отрасли;
- появление оцифрованных информационных ресурсов;
- активизация работы традиционных отраслей экономики в виртуальном пространстве;
- «переток» финансовых средств из традиционной торговли в электронную;
- существенное влияние политической ситуации в мире на информационное пространство Казахстана;
- русскоязычное и казахскоязычное информационные пространства, которые часто не пересекаются друг с другом;
- отсутствие крупных сетей ритейла и слабость организованной торговли;
- малая доля численности городского населения и наличие всего двух городов-миллионеров;
- направленность государства к организованной торговле, безналичным расчетам и развитию электронной коммерции;
- развитие электронного правительства и перевод государственных услуг в Интернет;
- значительный государственный информационный заказ;
- присутствие в казахстанской информационной среде пользователей из России, с Украины и из других стран СНГ;
- распространенность международных карточек типа Visa, Mastercard и других, позволяющих делать покупки в интернет-магазинах;
- слабое производство контента, что видно по количеству издаваемых книг.

4. Интернет-диффамация: вопросы юридической ответственности

Среди специалистов уже несколько лет развивается дискуссия о природе юридической ответственности в Интернет-праве. Под системой юридической ответственности понимают совокупность и взаимодействие норм и институтов права, соблюдение которых обеспечивает правопорядок, а применение их при совершении правонарушения восстанавливает правопорядок. Юридическая

ответственность выражается, прежде всего, в ответственном отношении к своим обязанностям самих участников общественных отношений и добросовестной реализации имеющихся прав и возложенных на них обязанностей.

Исследователями подчеркивается, что отсутствие отлаженных правовых механизмов влияния на представляемую информацию позволяет размещать в Интернете противоправные материалы откровенно националистического, фашистского, расистского содержания, различного рода дезинформацию, анонимные клеветнические публикации и т.д.

В свете этой полемики актуальной и своевременной представляется проблема цивилизованного правового регулирования деятельности средств массовой информации в сети, в частности, их ответственности за оглашение каких-либо фактов, не соответствующих действительности, и сведений, порочащих честь, достоинство, репутацию и доброе имя.

Под распространением сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, следует понимать опубликование таких сведений в печати, трансляцию по радио и телевидению, демонстрацию в кинохроникальных программах и других средствах массовой информации, распространение в сети Интернет, а также с использованием иных средств телекоммуникационной связи, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение в той или иной, в том числе устной, форме хотя бы одному лицу.

Диффамация, или опозорение в печати, известна буржуазному уголовному законодательству как преступление, близкое к клевете, но отличающееся от нее двумя признаками:

1. Диффамация есть оглашение каких-либо позорящих фактов в печати, тогда как клевета может быть совершена на словах или в письме;

2. В диффамации преступный момент заключается в самом оглашении в печати позорящих сведений, независимо от их правильности, клевета же всегда рассматривается как сообщение заведомо ложных сведений. Поэтому против обвинения в клевете можно защищаться, доказывая правильность сообщенных сведений, а против диффамации указанием на это защищаться нельзя.

Диффамация была известна законодательству как «оглашение в печати о частном или должностном лице, обществе или установлении такого обстоятельства, которое может повредить их чести, достоинству или доброму имени». В таком виде диффамация являлась средством ограничения свободы печати не только против вторжения последней в частную жизнь граждан, но и против разоблачения в прессе неправильных действий должностных лиц. В отношении должностных лиц допускалась защита против обвинения в диффамации указанием на истинность оглашенного в печати позорящего обстоятельства, касающегося служебной деятельности опозоренного лица. Однако обвиняемый мог защищаться только путем представления письменных доказательств, что практически представлялось почти невозможным

Интернет-диффамация, кибер-диффамация, диффамация в Сети - можно по-разному определить обозначенное явление, главная опасность которого - в реальной угрозе задекларированных конституционных принципов общества и государства. До настоящего времени нет единого понимания, что такое Интернет-диффамация и каковы механизмы ее урегулирования правовыми мерами.

Интернет-диффамацию можно определить как распространение посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, деловую репутацию, доброе имя.

Неотъемлемый атрибут диффамационного деликта - признак порочности. Если распространенные сведения не носят порочащего характера, даже при условии, что они не соответствуют действительности, то не будет и состава диффамационного деликта.

Суть любого диффамационного спора - в разрешении коллизии между правом на защиту чести и достоинства, с одной стороны, и правом на свободу слова и массовой информации, - с другой.

Постулируя незыблемость прав и свобод человека, мировое сообщество, тем не менее, прекрасно осознает, что свобода не может быть безгранична. Она в любом случае будет ограничена аналогичной свободой других лиц. Отметим, что международные акты о правах человека разрешают государствам при определенных условиях вводить ограничения некоторых прав. Однако подобные меры должны приниматься только в той степени, в какой это необходимо государству в интересах безопасности его граждан и его собственной безопасности. Нормы, позволяющие ограничить действие некоторых прав человека, вводятся с целью установления равновесия между правами отдельных лиц и интересами общества и государства в целом, а также в том случае, когда между ними могут возникать противоречия. Проблема - в поиске ответа о соразмерности таких ограничений.

Итак, в связи с бурным развитием интернет-отношений представляется важным обращение к проблемам диффамационного права. Неслучайно сегодня неведомый большинству практикующих юристов термин «диффамация» все чаще используется не только в научных публикациях, но и в решениях Европейского Суда по правам человека.

Обязанность доказывать соответствие действительности распространенных в Интернете сведений лежит на ответчике. Истец же обязан доказать факт распространения сведений лицом, к которому предъявлен иск, а также порочащий характер этих сведений. Гражданское законодательство предусматривает возможность требования истцом прекращения распространения информации в Сети, ее опровержения, а также компенсации морального вреда.

В числе нерешенных вопросов - возможность обеспечения доказательств. Как доказать факт размещения клеветнической информации в Интернете? Практика показывает, что предъявить обоснованные претензии собственнику сайта очень сложно, практически невозможным представляется и требование об

опубликовании опровержения. Неслучайно в условиях анонимного присутствия в Сети, так популярны интерактивные «гостевые книги», предоставляющие посетителям безграничные возможности реализации права на свободу слова. Как следствие, честь, достоинство и доброе имя граждан нередко выступают объектами посягательств в Интернете.

Затруднительность применения к средствам массовой информации, функционирующим с сети Интернет, обоснованных санкций превращает виртуальное пространство в привлекательное поле для диффамационных утверждений.

Дискуссионность вопроса о природе средств массовой информации, функционирующих в сети Интернет, определяет отсутствие правовых механизмов контроля их деятельности в виртуальном пространстве. Речь о цивилизованном правовом регулировании деятельности «иных средств массовой информации». Пока же законодательство в отношении средств массовой информации, функционирующих в сети Интернет, не обеспечивает соблюдение конституционных прав и свобод человека и гражданина.

Итак, интернет-диффамация - это распространение посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя. Честь, достоинство, репутация, доброе имя в случае распространения диффамационных материалов выступают специфичным объектом анализируемого правоотношения. Возможность анонимного присутствия в Сети позволяет скрыть подлинные имена автора, источника и лица, разместившего информацию. В связи с отсутствием соответствующего законодательства, четко определенного перечня субъектов деятельности в Интернете и их правового статуса реальная судебная защита прав личности, нарушаемых в Сети, в настоящее время не может быть обеспечена в полном объеме.

Проблема заключается в том, что для доказанности в суде факта распространения порочащих сведений конкретными лицами требуется проведение достаточно сложных процедур: просмотр протоколов доступа, проверка учетных записей провайдеров доступа, определение телефонных номеров и их владельцев, просмотр содержимого серверов, установление владельцев серверов, зачастую находящихся в разных странах, что связано с исполнением международных поручений, и т.д.

Сложность и в том, что географический размах связей в Интернете способен породить принципиальные вопросы, которые могут заставить пересмотреть само понятие «репутация». Что означает чья-то репутация в глобальном сообществе, и кого можно считать «разумным и благонамеренным представителем общества как целого», чьими критериями и стандартами, как предполагается, должен руководствоваться суд?

Подводя итог, отметим, что только тщательная проработка юридического механизма реализации конституционных гарантий прав, свобод и иных нематериальных благ в контексте функционирования в сети Интернет средств

массовой информации позволит обеспечить эффективную и всестороннюю защиту прав и свобод граждан.

Контрольные вопросы:

1. В чем специфика Интернета, интернет-отношений?
2. Охарактеризуйте основные подходы к определению Интернета.
3. Назовите основные проблемы правового регулирования интернет-отношений.
4. В чем проблематичность взаимоотношений человека с сетью Интернет?
5. Раскройте понятия «массовая информация», «средство массовой информации», «сетевое издание». Соотнесите их между собой.
6. Осветите конституционные гарантии свободы массовой информации.
7. В чем специфика средств массовой информации, функционирующих в сети Интернет?
8. Каковы основные подходы к определению отношения государств к Интернет-СМИ?

Тестовые задания:

1. Под распространением посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя понимается:
A) сетевое издание;
B) интернет-диффамация;
C) массовая информация;
D) интернет-ресурс;
E) средство массовой информации.

2. По типу представленного в них контента сетевые СМИ делятся на:
A) новостные; комментарийные; смешанные;
B) драматические, детективные;
C) государственные, частные;
D) содержательные, описательные;
E) комедийные, документальные.

3. Дайте понятие диффамации:
A) опровержение фактов в печати;
B) идентифицирующий атрибут;
C) обеспечение неизменности информации на платформе данных;
D) оглашение каких-либо позорящих фактов в печати;
E) использование алгоритмов шифрования.

4. Укажите неверный ответ. Основными принципами деятельности средств массовой информации являются:
A) автономия воли участников;
B) объективность;

C) законность;
D) достоверность;
E) уважение частной жизни, чести, достоинства человека и гражданина.

5. Что понимается под средством массовой информации:
A) рецензия на научную статью в сфере науки и техники;
B) электронный учебно-методический комплекс по дисциплине для обучающихся;
C) периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая интернет-ресурсы;
D) пост рекламного характера известного блогера;
E) листовки о кандидатах в депутаты в областные представительные органы.

6. Сетевое издание – это?
A) сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с законом;
B) аккунт в социальных сетях;
C) электронный документооборот;
D) вид корпоративной связи;
E) вид печатного издания рекламного характера.

7. Всемирная система объединённых компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов означает:
A) портал;
B) интернет;
C) токен;
D) блокчейн;
E) аккаунт.

8. Когда был принят Закон РК «О СМИ»?
A) 30 августа 1995 г.;
B) 23 июля 1999 г.;
C) 1 января 1999 г.;
D) 16 декабря 1991 г.;
E) 22 июля 2020 г.

9. Назовите основной нормативный акт, регулирующий отношения, складывающиеся в сфере массовой информации:
A) Закон РК «О средствах массовой информации»;
B) ГК РК;
C) Закон РК «О рекламе»;
D) УПК РК;

E) ГПК РК.

10. Укажите признак диффамационного деликта:
A) равноправие сторон;
B) состязательность;
C) оперативность;
D) порочность;
E) законность.

Тема 2.4. Электронное государство как институт информационного и цифрового права

Цель: раскрыть определение, понятие электронного государства и электронного правительства; рассмотреть значение предоставления государственных услуг в электронном виде.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- анализировать и решать юридические проблемы в сфере предоставления государственных услуг в электронном виде.

План:

1. Понятие электронного государства. Электронный парламент и электронное голосование.
2. Электронное правительство. Вопросы предоставления государственных услуг в электронном виде.
3. Электронное правосудие как форма реализации судебной власти в электронном государстве.

1. Понятие электронного государства. Электронный парламент и электронное голосование

Наряду с построением правового, конституционного, социального государства провозглашаемая сегодня задача - построение государства электронного.

В определении понятия «электронное государство» принципиальным вопросом является вопрос - или скорее немалая проблема - соответствующей терминологии. Особого внимания и поддержки заслуживает мнение П.У. Кузнецова о том, что «без научного осмысления в обиход «вбрасываются» такие новые словосочетания, как «электронное правительство», «электронное

государство», «сервисное государство», «электронное правосудие», «электронный нотариат», «электронный сервис» и др., которые затем вписываются в документы официальной государственной политики. Казалось бы, это нормальный процесс создания терминологического поля, без которого невозможно выстраивать государственную политику в области формирования и развития информационного общества. Однако концептуальные рабочие термины не переходят в разряд нормативных правовых, где они должны наполняться праворегулирующим либо правообеспечивающим содержанием».

Как соотносятся между собой понятия «электронное правительство» и «электронное государство»? В правовой литературе английский термин E-Government получил несколько переводов. Чаще он переводится как «электронное правительство». Такой перевод допустим, но он сужает понятие, по существу сводя вопрос только к исполнительной власти. Термин «электронное государство» не только больше соответствует английскому эквиваленту, но и подчеркивает, что речь идет о всех трех ветвях власти - законодательной, исполнительной и судебной.

Предполагается, что «электронное государство» в своей основе является и конституционным, и правовым, и социальным. При этом пример, где в силу исторических особенностей поступательное развитие конституционного государства не сложилось, показывает трудность одновременного построения и конституционного, и правового, и социального, и «электронного государства». Отсутствие предшествующего социального опыта и проработанной модели конституционного государства затрудняет и тормозит развитие электронного государства, для которого необходимы не только развитая система ИКТ, но и высокий уровень правового развития. Усложнение социальных отношений (как следствие развития ИКТ) требует их дальнейшей юридизации, однако именно правовая основа электронного государства вырабатывается с наибольшим трудом.

Основой формирования электронного государства является информационное общество - качественно новое состояние элементарных ячеек социума, отдельного государства и человечества в целом, обусловленное развитием информационных технологий, коммуникационных систем, отражающее новый уровень развития научного знания, представляющее собой новый тип организации общества, общества нового века. Народ как субъект демократии в теории электронного государства имеет специфические черты.

Ученые ведут речь о возникновении «народа-избирателя» как единого субъекта демократии, а также о его качественном преобразовании - приобретении свойств диджитальной публики. Диджитальная публика, по мнению С. Московичи, представляет собой рассредоточенную массу избирателей, состоящих из индивидов-избирателей, которые ведут постоянный диалог между собой. Это самоорганизованная система, способная к выработке независимых решений. В.Н. Руденко утверждает, что способность такой публики к взаимодействию и самоорганизации есть переход из сообщества «управляемых» к сообществу «управляющих», которое составит альтернативу правительствам и парламентам. Вопросы о том, существует ли

информационное общество и обладает ли население свойствами диджитальной публики, являются неоднозначными.

Соответственно, субъектами информационного процесса «электронного государства» выступают, с одной стороны - человек, с другой - государственные органы, составляющие «электронное правительство». И государство должно обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения государственных органов. Сегодня возможно лишь констатировать недостаточный уровень информированности общества, конкретного человека.

Электронное государство - прежде всего, социальное государство, в свою очередь социальное государство - и эта позиция И.Л. Бачило вызывает уважение - в определенной части является сервисным государством. При этом нужно иметь в виду, что только сервисные задачи и работа в этом направлении не исчерпывают функций государственных органов в области социальной сферы. Это, пожалуй, конечный итог каждой социальной функции - предоставить условия для граждан и организаций реализовать свои социальные и иные права. Для этого необходимо неуклонное выполнение базовых государственных функций. Конституционной основой социальности государства является раздел второй Конституции РК о правах и обязанностях человека и гражданина, где содержится основной перечень социальных прав каждого, находящегося под юрисдикцией Казахстана. Социальность государства обеспечивается, прежде всего, законами, актами Президента и Правительства, деятельностью местных представительных и исполнительных органов, актами органов местного самоуправления.

Необходимо отметить, что Казахстан переживает один из наиболее сложных этапов информатизации - процесс адаптации и коренной перестройки государства на пути к его «электронной версии». И в этом процессе далеко не последняя роль должна отводиться полноценному обеспечению прав и свобод человека. Действительно, «во всех подходах к понятию электронного государства прослеживается его негативная черта - ориентация на общеуниверсальное представление о личности и человеке, отсутствие индивидуальных особенностей при совершении каких-либо юридических действий. Развитые информационно-коммуникационные технологии могут явиться мощным инструментом подавления населения и стать предпосылкой возникновения антидемократического режима. Поэтому законодательство становящегося электронного государства должно содержать гарантии пресечения противоправного вмешательства в жизнь и сознание людей в определенных интересах, а также быть готово к информационным изменениям и отражать основные вопросы его функционирования».

Речь идет о развитии в Казахстане электронной демократии. Именно сегодня «наряду с тем, что в большинстве сфер деятельности государства происходят позитивные изменения в реализации реформ, развитие информационной организации государства объективно переживает сложный

период. В результате информационная сфера, ее ресурсы, в том числе и их защищенность, отстают в развитии от других институтов современного общества. Данное обстоятельство негативно сказывается не только на информационной организации государства, но и на состоянии информационной безопасности Казахстана, информационной безопасности личности и всего общества в целом. Не вызывает сомнений, что процесс внедрения инструментов электронной демократии в реалии необратим.

Под электронной демократией понимается такая форма организации общественно-политической деятельности граждан, которая обеспечивает за счет широкого применения информационно-коммуникационных технологий качественно новый уровень взаимодействия граждан друг с другом, с государственными органами, органами местного самоуправления, общественными организациями и коммерческими структурами.

Кроме того, «самым активным и часто уязвимым субъектом в эпоху перемен, а информатизация, цифровизация и сетевая жизнь информационной среды - это не что иное, как революция в развитии социума, остается человек, индивид, гражданин. И понять, что изменяется под воздействием информационно-технологических факторов чрезвычайно важно».

Безусловно, «плюсов» в применяемых технологиях электронного голосования больше, чем достаточно. Тем не менее возможных проблем тоже предостаточно. Так, электронные технологии могут быть использованы и в качестве средств фальсификации результатов голосования; кроме того, не исключены серьезные сбои в функционировании автоматизированных комплексов, обеспечивающих электронное голосование. Поэтому крайне важно в рамках внедрения электронного голосования разрабатывать не только процедуры голосования, подсчета голосов, но и процедуры контроля данных процессов, а также процедуры верификации результатов голосования. И, безусловно, важнейшей проблемой электронного голосования продолжает оставаться проблема цифровой идентификации граждан, являющихся пользователями систем электронной демократии. Во многом данная проблема является главным препятствием на пути повсеместного внедрения механизмов электронного голосования на уровне выборов субъектов государственной власти.

Эта проблема - не только проблема электронного голосования: идентификация гражданина при общении с органами власти - одна из наиболее сложных, требующих своего четкого решения проблема e-government.

2. Электронное правительство. Вопросы предоставления государственных услуг в электронном виде

Процессы формирования информационного общества и электронного правительства в Казахстане динамично развиваются. Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития.

Сегодня происходит ценностная переориентация в отношениях власти и человека. Если на предшествующих этапах развития отсчет шел от государства к человеку, то теперь обозначился новый подход: истинным моментом становится человек. В этом контексте, информационные права - особый и специфический вид прав человека. В системе этих прав человека электронного государства на одно из ведущих мест выходит право на предоставление государственных услуг в электронной форме.

Закон Республики Казахстан от 15 апреля 2013 года № 88-V «О государственных услугах» действительно призван совершить революцию во взаимоотношениях государства и человека.

Правительственное веб-присутствие (согласно классификации Европейской комиссии) характеризуется последовательным прохождением пяти этапов:

1. Информационный (Information) - означает 20%-ное веб-присутствие и предполагает создание регулярно обновляемых правительственных веб-сайтов с публикацией на них основной правительственной информации (нормативные акты, распоряжения, постановления и пр.), ссылок на министерства и государственные департаменты (образования, здравоохранения, финансов и т.п.).

2. Интерактивный односторонний (One way interaction) - предполагает 40%-ное веб-присутствие и заключается в организации пассивного взаимодействия между клиентами и правительством. Он подразумевает, например, предоставление доступа в электронной форме к различным формулярам документов, которые требуются гражданам и бизнесу для взаимодействия с государством. Нужную форму можно распечатать, но отправлять ее придется традиционным образом, а не через Интернет. Или, например, поиск вакансий в государственных организациях на основе заданных пользователем критериев.

3. Интерактивный двусторонний (Two way interaction) - означает 60%-ное веб-присутствие и реализуется посредством интерактивного двустороннего взаимодействия. На этой стадии онлайновые сервисы приобретают интерактивность и появляется возможность запрашивать информацию по тем или иным выступлениям и обсуждениям, обращаться к госчиновникам по электронной почте, участвовать в онлайновых дискуссиях или оставлять комментарии на досках сообщений и т.п.

4. Транзакционный (Transaction) - предполагает 80%-ное веб-присутствие и характеризуется транзакционным взаимодействием, благодаря чему возможно предоставление услуг, выполнимых в онлайне на всех стадиях. Примером может служить подача заявок в электронной форме на получение лицензий на ведение профессиональной деятельности, подача налоговых деклараций, заявлений на обмен документов и т.п.

5. Проактивный (Targetisation) - означает 100%-ное веб-присутствие и отличается тем, что правительство не только предоставляет гражданам и коммерческим структурам сервисные услуги, но и привлекает граждан к принятию решений и двустороннему диалогу на базе интерактивных сервисов.

Проанализировав данную классификацию, можно утверждать, что сегодня для Казахстана характерен переход от первого, информационного этапа, ко второму, интерактивному одностороннему. Согласно закону «О государственных услугах» сформирована основа для четвертого, транзакционного этапа правительственного веб-присутствия.

Предлагая электронные услуги, государство должно сделать доступным онлайновый публичный сектор информации, чтобы большая часть административных процедур (оптимально - все) была доступна электронным способом. Государство обязано обеспечить универсальные услуги. Сеть «Интернет» должна быть доступна всем гражданам, включена в универсальные услуги и предлагаться пользователю по допустимой цене.

Закон «О государственных услугах» предусматривает, что государственные услуги оказываются на основе следующих основных принципов:

- равного доступа услугополучателям без какой-либо дискриминации по мотивам происхождения, социального, должностного и имущественного положения, пола, расы, национальности, языка, отношения к религии, убеждений, места жительства или по любым иным обстоятельствам;
- недопустимости проявлений бюрократизма и волокиты при оказании государственных услуг;
- подотчетности и прозрачности в сфере оказания государственных услуг;
- качества и доступности государственных услуг;
- постоянного совершенствования процесса оказания государственных услуг;
- экономичности и эффективности при оказании государственных услуг.

Государственные услуги подлежат включению в реестр государственных услуг. Порядок ведения реестра государственных услуг, а также его структура определяются уполномоченным органом в сфере оказания государственных услуг.

Для обеспечения единых требований к качеству оказания государственных услуг центральными государственными органами разрабатываются и утверждаются подзаконные нормативные правовые акты, определяющие порядок оказания государственных услуг, в том числе для государственных услуг, оказываемых загранучреждениями Республики Казахстан, местными исполнительными органами областей, городов республиканского значения, столицы, районов, городов областного значения, акимами районов в городе, городов районного значения, поселков, сел, сельских округов.

Подзаконный нормативный правовой акт, определяющий порядок оказания государственной услуги, разрабатывается и утверждается в течение двух месяцев со дня утверждения реестра государственных услуг или внесения в него изменений и дополнений.

Разработка и согласование проектов подзаконных нормативных правовых актов, определяющих порядок оказания государственных услуг,

осуществляются в соответствии с Законом Республики Казахстан «О правовых актах».

Проект подзаконного нормативного правового акта, определяющего порядок оказания государственной услуги, подлежит публичному обсуждению. Принятие, изменение, дополнение и отмена подзаконных нормативных правовых актов, определяющих порядок оказания государственных услуг, осуществляются на основе предложений уполномоченного органа по оценке и контролю за качеством оказания государственных услуг, уполномоченного органа в сфере оказания государственных услуг, уполномоченного органа в сфере информатизации, центральных государственных органов, местных исполнительных органов областей, городов республиканского значения, столицы, районов, городов областного значения, акимов районов в городе, городов районного значения, поселков, сел, сельских округов, а также по итогам общественного мониторинга качества оказания государственных услуг и (или) рассмотрения обращений услугополучателей по вопросам оказания государственных услуг.

Подзаконный нормативный правовой акт, определяющий порядок оказания государственной услуги, предусматривает:

- описание порядка:

- действий структурных подразделений (работников) услугодателя в процессе оказания государственной услуги;

- взаимодействия структурных подразделений (работников) услугодателя в процессе оказания государственной услуги;

- взаимодействия с Государственной корпорацией и (или) иными услугодателями, а также использования информационных систем в процессе оказания государственной услуги;

- порядок обжалования решений, действий (бездействия) центральных государственных органов, местных исполнительных органов областей, городов республиканского значения, столицы, районов, городов областного значения, акимов районов в городе, городов районного значения, поселков, сел, сельских округов, а также услугодателей и (или) их должностных лиц, Государственной корпорации и (или) ее работников по вопросам оказания государственных услуг;

- приложение в форме стандарта государственной услуги, который содержит: наименование государственной услуги; наименование услугодателя; способы предоставления государственной услуги; срок оказания государственной услуги; форму оказания государственной услуги; результат оказания государственной услуги; размер платы, взимаемой с услугополучателя при оказании государственной услуги, и способы ее взимания в случаях, предусмотренных законодательством Республики Казахстан; график работы услугодателя; перечень документов, необходимых для оказания государственной услуги; основания для отказа в оказании государственной услуги, установленные законами Республики Казахстан;

- иные требования с учетом особенностей оказания государственной услуги, в том числе оказываемой в электронной форме и через Государственную корпорацию.

При оказании государственных услуг через Государственную корпорацию, оказание которых предусматривает отправку заявления и документов услугополучателя услугодателям на бумажном носителе, день приема заявлений и документов не входит в срок оказания государственной услуги, установленный подзаконным нормативным правовым актом, определяющим порядок оказания государственной услуги.

Работник Государственной корпорации обязан принять заявление услугополучателя при наличии у него полного пакета документов согласно перечню, предусмотренному подзаконным нормативным правовым актом, определяющим порядок оказания государственной услуги.

В случае представления услугополучателем неполного пакета документов согласно перечню, предусмотренному подзаконным нормативным правовым актом, определяющим порядок оказания государственной услуги, а также документов с истекшим сроком действия работник Государственной корпорации отказывает в приеме заявления.

При оказании государственной услуги через Государственную корпорацию идентификацию личности услугополучателя осуществляют работники Государственной корпорации. При оказании государственных услуг через Государственную корпорацию взаимодействие с услугодателями осуществляется с использованием информационной системы мониторинга оказания государственных услуг.

Работники Государственной корпорации при оказании государственных услуг обязаны получать письменное согласие услугополучателя на использование сведений, составляющих охраняемую законом тайну, содержащихся в информационных системах.

Оказание государственных услуг в электронной форме осуществляется посредством веб-портала «электронного правительства» и объектов информатизации, интегрированных с сервисами, размещенными на шлюзе «электронного правительства», внешнем шлюзе «электронного правительства», в соответствии с законодательством Республики Казахстан.

Результатом оказания государственной услуги в электронной форме является выдача электронного документа или документа на бумажном носителе либо сведения из информационной системы «электронного правительства».

Результаты оказания государственных услуг в электронной форме, полученных посредством абонентского устройства сотовой связи, направляются в кабинет пользователя на веб-портале «электронного правительства» в форме электронного документа, а также по выбору услугополучателя на его абонентский номер в виде короткого текстового сообщения.

Обязательные реквизиты результатов оказания государственных услуг в электронной форме, полученных посредством абонентского устройства сотовой связи, а также порядок проверки их достоверности регулируются законодательством Республики Казахстан об информатизации.

Результаты оказания государственных услуг в электронной форме, полученных посредством абонентского устройства сотовой связи, используются услугополучателем для подтверждения фактов, имеющих юридическое значение, без необходимости их представления на бумажном носителе.

При оказании государственной услуги в электронной форме через Государственную корпорацию на основании письменного согласия услугополучателя его запрос в форме электронного документа заверяется электронной цифровой подписью работника Государственной корпорации, выданной ему для использования в служебных целях.

Услугополучателям может быть оказано несколько государственных услуг в электронной форме по принципу «одного заявления» в порядке, определяемом уполномоченным органом в сфере информатизации.

Для оказания государственных услуг в электронной форме государственные органы обязаны на постоянной основе поддерживать в актуальном состоянии электронные информационные ресурсы, находящиеся в их информационных системах.

3. Электронное правосудие как форма реализации судебной власти в электронном государстве

В связи с развитием новых медиа, актуально стало говорить и о их применении в правовой сфере, а именно в отправлении правосудия.

Основополагающими целями судебной реформы были определены: доступность правосудия, быстрое и качественное рассмотрение дел, максимальное исключение какого-либо воздействия на судей извне.

На современном этапе развития науки и техники особое значение приобретает интеграция информационных технологий в те сферы жизни, от которых напрямую зависит стабильное существование общества и его граждан. Если говорить о праве как об основном социальном регуляторе, то внедрение технологий, позволяющих наиболее эффективно кодифицировать, анализировать, применять и исполнять правовые нормы, является необходимым условием совершенствования правовой системы как в Казахстане, так и за рубежом.

Сегодня для судопроизводства актуальны как никогда: открытость и доступность; формирование информационных ресурсов, включая ход судебных заседаний; организация оперативного доступа к информационным ресурсам в рамках формирования единого информационного пространства судов общей юрисдикции и Верховного суда РК; реализация новых требований судебного законодательства; оперативная организация мониторингов и аналитической работы на больших массивах консолидированной информации от всех участников информационного пространства.

Согласимся, что государство, внедряя информационные технологии в судопроизводство, реализуя модели электронного правосудия в целом, должно ставить в качестве стратегической задачи изменение взаимоотношений между государством и обществом, между судом как ветвью государственной власти и остальными гражданами. Все это требует глубокого теоретического

исследования проблемы внедрения электронных технологий в гражданское и арбитражное судопроизводство для выработки научных рекомендаций по совершенствованию процессуального законодательства, по повышению эффективности правоприменительной практики.

Так, в 2015 году Верховным судом Республики Казахстан был открыт для широкого доступа единый интернет-портал судебных органов, сервис «Судебный кабинет» а также множество электронных информационных сервисов, призванных обеспечить доступность и прозрачность судебной системы.

Современное электронное правосудие в Казахстане развивается достаточно быстро. Такое развитие обусловлено совершенствованием законодательства в этой сфере, а также выявлением новых сервисов и увеличением их производительности.

Электронное правосудие в Республике Казахстан это и «Судебный кабинет», форум «Талдау», который формируется на основе Единого классификатора категорий дел и материалов, это и новая автоматизированная информационно-аналитическая система «Төрелік», единая система судов Республики Казахстан, это и система видеоконференцсвязи между судами.

В республике все залы судебного заседания оснащены системами аудио-видео фиксации (АВФ), практикуется ведение электронного протокола. И, что актуально, исключена возможность для корректировки записи АВФ, обеспечена гарантированная сохранность. В казахстанских судах запустили удобный сервис «Мобильный судебный кабинет». Это дает возможность стороне не являться лично в суд, а поучаствовать в судебном процессе через мобильные устройства с выходом в Интернет, в том числе и из-за рубежа.

Работает единая система мониторинга работы судов, которая дает возможность в онлайн-режиме круглосуточно собирать и анализировать судебную информацию. Через данный центр Верховный суд имеет возможность видеть в реальном времени сбои в работе судов. Поступающая информация сегментирована в четыре блока показатели по делопроизводству, систему мониторинга компонентов «Терелік», информационная безопасность и применение АВФ.

Развитие электронного правосудия имеет множество преимуществ для участников судебного процесса: представляет собой систему, увеличивающую эффективность судопроизводства, позволяющую экономить время участников процесса и уменьшающую затраты на судопроизводство.

Достоинство подачи искового заявления в электронном виде: позволяет сэкономить временной ресурс, так как отправка возможна при помощи сети Интернет, не выходя из дома, вместе с тем, экономия денежных средств, особенно в, случае нахождения в разных городах.

После направления искового заявления можно получить электронное подтверждение об этом.

Второй этап технического достижения извещения посредством электронной почты или смс-рассылки, конечно, более, оперативные и менее затратные.

Видеоконференцсвязь при рассмотрении дела в суде.

Достоинства: экономия временного и денежного ресурса, особенно для участников иного места жительства.

Уже сейчас: судебная повестка приходит вам на телефон, а судебное решение на электронную почту; не выходя из дома можно направить документы и оплатить госпошлину, в любой суд страны в любое время суток. Система позволяет производить поиск по номеру дела, наименованию сторон. Активно внедряется информационная технология в судопроизводстве.

Можем уверенно говорить, что в Казахстане цифровизация судов состоялась. 91% гражданских исков подается электронно. 6,5 млн судебных актов доступно через интернет. Участники судебных процессов могут «держать на цифровом контроле» весь процесс: от подачи заявления в суд до окончательного разрешения дела. В этом им помогает ряд сервисов.

Первый из них - «Судебный кабинет», казахстанский аналог системы «Мой Арбитр». Это единое электронное окно доступа ко всем судебным услугам. Через него можно с любого гаджета направить в суд более 90 видов электронных обращений, увидеть регистрацию обращения, узнать его статус и в конце получить судебный акт. Более того, достаточно подать соответствующее заявление, чтобы участие в заседании было без выезда в суд.

Сервис «Суды-Gis» позволяет найти контакты судов, адвокатов, медиаторов, нотариусов в конкретном регионе. Удобно. Через Telegram-бот «Smart-сот» можно получить ответы на многие вопросы. В Казахстане считают важным мнение каждого получателя судебных услуг.

Проект Digital Agent дает возможность оценить комфорт, сервис, судебные процедуры и работу персонала судов, оставить жалобы и предложения. Это мобильное приложение позволяет любому пользователю в режиме онлайн связаться с судом и на месте решить возникающие вопросы.

Сейчас Верховный суд республики совместно с Национальной палатой предпринимателей «Атамекен» разрабатывает IT-программу по судебной аналитике и прогнозированию исхода судебного дела. Цель - сделать правосудие предсказуемым и повысить инвестиционную привлекательность Казахстана.

Контрольные вопросы:

1. В чем особенности формирующегося электронного государства? Назовите основные нормативные акты, направленные на развитие основ электронного государства.
2. Дайте характеристику документу «Правосудие Казахстана: реалии, тренды, перспективы».
3. Охарактеризуйте порядок предоставления государственных услуг в электронном виде.
4. В чем состоит назначение электронного правосудия?
5. Каковы основные направления развития электронного правосудия в Казахстане?

Тестовые задания:

1. Назовите казахстанский аналог системы РФ «Мой Арбитр»:
A) «Судебный кабинет»;
B) «Суды-Gis»;
C) «Атамекен»;
D) «Терелік»;
E) «Digital Agent».

2. Сервис, позволяющий осуществлять поиск контактов судов, адвокатов, медиаторов, нотариусов в конкретном регионе:
A) «Platonus»;
B) «Суды-Gis»;
C) «egov.kz»;
D) «Терелік»;
E) «Digital Agent».

3. Укажите количество этапов прохождения правительственного веб-присутствия (согласно классификации Европейской комиссии):
A) три;
B) пять;
C) два;
D) семь;
E) десять.

4. Какой этап характеризуется 20%-ным веб-присутствием и предполагает создание регулярно обновляемых правительственных веб-сайтов?
A) транзакционный;
B) проактивный;
C) интерактивный двусторонний;
D) информационный;
E) интерактивный односторонний.

5. Сколько процентов веб-присутствия предполагает интерактивный односторонний этап?
A) 20%;
B) 40%;
C) 60%;
D) 100%;
E) 80%.

6. Какой этап предполагает 80%-ное веб-присутствие?
A) конечный;
B) информационный;
C) проактивный;
D) транзакционный;

E) интерактивный.

7. Форма организации общественно-политической деятельности граждан, которая обеспечивает за счет широкого применения информационно-коммуникационных технологий качественно новый уровень взаимодействия граждан друг с другом, с государственными органами, органами местного самоуправления, общественными организациями и коммерческими структурами означает?
A) общественное согласие;
B) электронную демократию;
C) рекламную деятельность;
D) электронную торговлю;
E) активность в социальных сетях.

8. Когда был принят Закон РК «О государственных услугах»?
A) 30 августа 1995 г.;
B) 23 июля 1999 г.;
C) 1 июля 2015 г.;
D) 16 декабря 1991 г.;
E) 15 апреля 2013 г.

9. Государственные услуги подлежат включению в:
A) единый реестр;
B) государственный кадастр;
C) реестр государственных услуг;
D) журнал регистрации входящих документов;
E) журнал регистрации исходящих документов.

10. Укажите принцип оказания государственных услуг:
A) аккуратность;
B) состязательность;
C) бюрократизм;
D) качество и доступность;
E) постоянство.

Тема 2.5. Персональные данные как институт информационного и цифрового права

Цель: раскрыть определение персональных данных и содержание понятия «обработка персональных данных».

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- умение правильно применять нормы права.
- умение анализировать юридическую литературу по вышеуказанным темам. - умение решать задачи по вышеуказанным темам.

План:

1. Основные подходы к регулированию правоотношений по поводу персональных данных в зарубежных странах.
2. Закон РК «О персональных данных и их защите» - основа действующего законодательства в сфере защиты персональных данных.

1. Основные подходы к регулированию правоотношений по поводу персональных данных в зарубежных странах

Защита персональных данных - условный термин, применяемый для обозначения права индивида на доступ к своему персональному досье, имеющемуся в распоряжении государственных или частных «пользователей информации», с целью обеспечения точности, своевременности и соотносимое имеющейся информации с целями, для которых она хранится, и проверки того, не может ли получить доступ к информации лицо, не обладающее соответствующими полномочиями. Таким образом, защита персональных данных связана также с личным характером информации.

В 60-х и 70-х гг. XX в. с приходом информационных технологий стал возрастать интерес к приватности. Возможность использования мощных компьютеров для слежки и контроля означала необходимость принятия особых правил, регулирующих сбор и обработку персональных данных. Во многих странах новые конституции отразили, это право. Процесс обновления законодательства в данной области можно проследить со времени появления первого закона о защите данных, изданного в Германии в земле Гессен в 1970 г. После этого были приняты законы в Швеции (1973), Соединенных Штатах (1974), Германии (1977) и Франции (1978).

Из этих законов «выросли» два важных международных документа. Первый - Конвенция Совета Европы о защите прав личности в связи с автоматической обработкой персональных данных. Второй - Руководящие принципы Организации по экономическому сотрудничеству и развитию о защите приватности в связи с трансграничной передачей персональных данных. Эти положения определяют персональную информацию как данные, которые нуждаются в защите на каждом этапе от сбора до хранения и распространения. Право граждан на доступ к своим данным и внесение в них изменений стало главной составляющей этих правил.

В разных законах и правилах по-разному определяются условия защиты данных. Повсеместно принято считать, что персональная информация должна быть:

- получена честным и законным путем;
- использована только для заранее определенных целей;

- соответствовать задаче, ради которой она собиралась;
- точной и свежей;
- обрабатываться только с согласия субъектов ее получения;
- доступна субъекту данных;
- защищена от несанкционированного доступа;
- уничтожена после того, как цель достигнута.

Два упомянутых соглашения сильно повлияли на развитие законодательства во всем мире. Почти 30 стран признали Конвенцию Совета Европы и еще несколько государств собираются сделать это в ближайшем будущем. Руководящие принципы Организации по экономическому сотрудничеству и развитию также широко используются законодателями разных стран, в том числе и не входящих в эту международную структуру.

Мировой опыт позволяет назвать три главные причины для принятия специальных законов о защите приватности и персональных данных:

1) приведение законодательства значительного числа стран к общемировым цивилизованным стандартам, отражающим высокий уровень защиты прав человека. Многие государства, особенно в Центральной и Восточной Европе (включая Россию), Южной Африке и Южной Америке, приняли соответствующие законы, чтобы исправить последствия нарушений прав человека при тоталитарных режимах прошлых лет;

2) создание благоприятных условий для развития электронного бизнеса. Многие страны, особенно в Азии, уже приняли (или разрабатывают) законы, направленные на развитие электронной коммерции. Правительства понимают, что в современном мире, насыщенном высокотехнологичными коммуникациями, персональные данные потребителей находятся под угрозой - особенно когда они пересылаются по Интернету. Поэтому в законах об электронном бизнесе появляются гарантии приватности;

3) приведение национального законодательства в соответствие с европейскими соглашениями. Большинство стран Центральной и Восточной Европы принимает законы, основываясь на Конвенции Совета Европы 1981 г. и Директиве Европейского Союза о защите данных. Многие из этих стран в ближайшем будущем надеются стать членами ЕС. В других регионах мира государства приводят свои законы в соответствие требованиям ЕС просто потому, что иначе могут пострадать их торговые отношения с членами Евросоюза.

В имеющих сейчас базовое значение документах, регулирующих работу с персональными данными в мире, сформулированы основные принципы работы с персональными данными:

- персональные данные должны собираться и обрабатываться (храниться, использоваться, раскрываться, стираться и т.д.) только в соответствии с законом и наделенными соответствующими полномочиями органами;
- персональные данные должны быть адекватными заранее определенным целям и распоряжение ими должно ограничиваться по срокам, соответствующим указанным целям;
- персональные данные должны быть точны;

- персональные данные должны обрабатываться только с согласия субъектов этих данных;

- персональные данные должны быть доступны субъектам этих данных, в том числе и для внесения уточнения в эти данные;

- персональные данные должны быть должным образом защищены.

В международном праве существует большое число законов, отраслевых стандартов для финансовых институтов, телекоммуникационных компаний, учреждений здравоохранения и обязательных и рекомендательных документов, затрагивающих защиту информации от внутренних угроз и управление операционными рисками:

PCI DSS - обязательный стандарт для операторов данных платежных карт систем VISA, MasterCard, American Express, JCB, Discover. Во-первых, в стандарте регламентируется необходимость шифрования носителей информации, содержащих данные платежных карт, и надежной защиты ключей шифрования. Также в PCI DSS определена необходимость генерации стойкого ключа и разделение криптографического ключа между несколькими лицами. Во-вторых, согласно стандарту операторы платежных карт должны защищать информацию от утечек по различным каналам, жестко регламентировав использование внешних устройств и перемещение конфиденциальных данных. В-третьих, в PCI DSS определена необходимость использования двухфакторной аутентификации для доступа к данным.

Basel II - довольно давно и успешно применяющийся в Евросоюзе, Северной Америке и Японии нормативный акт, регламентирующий банковскую деятельность. В частности, в стандарте описана необходимость ведения архива конфиденциальной информации и создания системы управления операционными рисками.

SOX - Sarbanes-Oxley Act of 2002 является обязательным для всех публичных компаний, акции которых котируются на фондовых биржах США. За несоблюдение закона топ-менеджеры компании несут персональную финансовую (штраф до 25 млн долларов) и уголовную ответственность (до 20 лет лишения свободы). Секция 404 закона регламентирует необходимость внедрения системы внутреннего контроля для предотвращения и защиты информационных активов компании от утечек и несанкционированного использования.

SEC Rule 17a-4 и NASD 3010/3110 - своды правил для компаний, акции которых котируются на биржах США. В правилах регламентируется создание архива электронной корреспонденции и переписки через службы мгновенных сообщений. Требования NASD 3010/3110 еще более жесткие - требуется архивировать не только корреспонденцию участников системы, но и все транзакции брокеров, трейдеров и лиц, действующих от их имени.

Combined code on corporate governance - Кодекс корпоративного управления Великобритании пока не является обязательным для всех организаций, однако уже давно де-факто является стандартом для корпораций, чьи акции представлены на Лондонской фондовой бирже. Combined code регламентирует создание и поддержку системы внутреннего контроля и

необходимость как минимум один раз в год проводить независимый аудит такой системы. Также в Кодексе говорится о необходимости постоянного мониторинга самой системы внутреннего контроля, а в случае возникновения какого-либо инцидента ИБ, высшее руководство компании должно быть немедленно информировано.

Американский закон HIPAA - затрагивает учреждения здравоохранения, страховые компании и посредников, хранящих, обрабатывающих и передающих конфиденциальные данные. Закон конкретизируют правила HIPAA, The Security Rule, в которых в частности регламентируется необходимость создания системы внутреннего контроля, написания правил использования рабочих компьютеров и внешних устройств и организации системы контроля доступа к информации.

GBLA & FACTA - защита непубличной информации клиентов финансовых корпораций регламентируется законами Gramm-Leach-Bliley Act of 1999 и Fair and Accurate Credit Transactions Act of 2003. Стандарт «Interagency Guidelines Establishing Information Security Standards» вносит дополнительные уточнения в приведенные законы и требует от финансовых институтов США защищать непубличные данные граждан в процессе хранения, использования, пересылки и утилизации от всех прогнозируемых рисков информационной безопасности, а также обеспечивать надежный контроль доступа к этой информации.

Архивирование информации (data retain) является распространенным требованием многих стандартов и законов, касающихся информационной безопасности. Сохранение переписки сотрудников, отправленных через Интернет данных, записанных на периферийные устройства файлов и копий распечатанных на принтерах документов является важной задачей как с точки зрения внутреннего контроля и управления операционными рисками, так и как самостоятельная задача. Очевидно, что часто для различных целей требуется провести ретроспективный анализ использованной и перемещенной за пределы корпоративной сети информации.

Несоблюдение требований архивирования информации в большинстве нормативных документов в большинстве случаев является прямым нарушением законодательства страны, за что предусматриваются солидные штрафы для компаний, а топ-менеджмент несет персональную уголовную и финансовую ответственность. Часто из-за невозможности предоставить электронные копии документов в суд компании проигрывают процессы и теряют огромные суммы. Одним из наиболее известных дел, показывающих необходимость архивирования информации, является процесс с участием Morgan Stanley. Первоначально присяжные приняли решение о взыскании с компании Morgan Stanley 1,5 млрд долларов за невозможность предоставления копий электронных писем, затребованных адвокатами другой стороны. Позже эта цифра была сокращена в сто раз и составила 15 млн. долл.

2. Закон РК «О персональных данных и их защите» - основа действующего законодательства в сфере защиты персональных данных

Закон РК «О персональных данных и их защите» регулирует общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных.

Согласно ст. 1 Закона под персональными данными понимаются сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

В свою очередь, под обработкой персональных данных понимаются действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных.

Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами:

1) соблюдения конституционных прав и свобод человека и гражданина;

2) законности;

3) конфиденциальности персональных данных ограниченного доступа;

4) равенства прав субъектов, собственников и операторов;

5) обеспечения безопасности личности, общества и государства.

Сбор персональных данных - действия, направленные на получение персональных данных.

Обработка персональных данных - действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных.

Использование персональных данных - действия с персональными данными, направленные на реализацию целей деятельности собственника, оператора и третьего лица.

Хранение персональных данных - действия по обеспечению целостности, конфиденциальности и доступности персональных данных.

Распространение персональных данных - действия, в результате совершения которых происходит передача персональных данных, в том числе через средства массовой информации или предоставление доступа к персональным данным каким-либо иным способом.

Под блокированием понимаются действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных.

Обезличивание персональных данных - это действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно.

Персональные данные по доступности подразделяются на общедоступные и ограниченного доступа.

Общедоступными персональными данными являются персональные данные или сведения, на которые в соответствии с законодательством Республики Казахстан не распространяются требования соблюдения

конфиденциальности, доступ к которым является свободным с согласия субъекта.

В целях информационного обеспечения населения используются общедоступные источники персональных данных (в том числе биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации).

Сведения о субъекте, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, исключаются из общедоступных источников персональных данных в любое время по требованию субъекта или его законного представителя либо по решению суда или иных уполномоченных государственных органов.

При этом расходы, возникающие при уничтожении персональных данных с общедоступных источников персональных данных, возлагаются на собственника и (или) оператора, третье лицо.

Объем расходов, возникающих при отзыве согласия субъекта или его законного представителя на распространение его персональных данных в общедоступных источниках персональных данных, связанных с уничтожением персональных данных с общедоступных источников персональных данных, а также лица, на которые возлагаются данные расходы, в случае возникновения необходимости определяются в судебном порядке.

Персональными данными ограниченного доступа являются персональные данные, доступ к которым ограничен законодательством Республики Казахстан.

Сбор, обработка персональных данных осуществляются собственником и (или) оператором, а также третьим лицом с согласия субъекта или его законного представителя в порядке, определяемом уполномоченным органом. Сбор, обработка персональных данных умершего (признанного судом безвестно отсутствующим или объявленного умершим) субъекта осуществляются в соответствии с законодательством Республики Казахстан.

Особенности сбора, обработки персональных данных в электронных информационных ресурсах, содержащих персональные данные, устанавливаются в соответствии с законодательством Республики Казахстан об информатизации. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Доступ к персональным данным определяется условиями согласия субъекта или его законного представителя, предоставленного собственнику и (или) оператору на их сбор и обработку. Доступ к персональным данным должен быть запрещен, если собственник и (или) оператор, и (или) третье лицо отказываются принять на себя обязательства по обеспечению выполнения требований или не могут их обеспечить.

Обращение (запрос) субъекта или его законного представителя относительно доступа к своим персональным данным подается собственнику и (или) оператору письменно или в форме электронного документа либо иным способом с применением элементов защитных действий, не противоречащих законодательству Республики Казахстан. Третьи лица могут получать персональные данные, содержащиеся в информационных системах

государственных органов, через веб-портал «электронного правительства» при условии согласия субъекта, предоставленного через кабинет пользователя на веб-портале «электронного правительства», а также посредством зарегистрированного на веб-портале «электронного правительства» абонентского номера сотовой связи субъекта путем передачи одноразового пароля или путем отправления короткого текстового сообщения в качестве ответа на уведомление веб-портала «электронного правительства» или сервиса обеспечения безопасности персональных данных.

При сборе, обработке персональных данных для проведения статистических, социологических, научных, маркетинговых исследований собственник и (или) оператор, а также третье лицо, передающие персональные данные, обязаны их обезличить в соответствии с правилами сбора, обработки персональных данных. При сборе, обработке персональных данных для осуществления аналитики данных в целях реализации функций государственными органами обезличивание персональных данных осуществляется оператором информационно-коммуникационной инфраструктуры «электронного правительства» в соответствии с правилами по сбору, обработке, хранению, передаче электронных информационных ресурсов для осуществления аналитики данных в целях реализации функций государственными органами, утверждаемыми уполномоченным органом в сфере информатизации, за исключением случаев, когда обезличивание персональных данных произведено собственником и (или) оператором.

Персональные данные подлежат уничтожению собственником и (или) оператором, а также третьим лицом:

- по истечении срока хранения;
- при прекращении правоотношений между субъектом, собственником и (или) оператором, а также третьим лицом;
- при вступлении в законную силу решения суда;
- в иных случаях.

Контрольные вопросы:

1. Раскройте понятия «персональные данные», «обработка персональных данных», «оператор обработки персональных данных».
2. Охарактеризуйте законодательство в сфере защиты персональных данных.
3. Назовите и раскройте принципы защиты персональных данных.
4. Раскройте особенности обработки персональных данных, а также биометрических персональных данных.
5. Какими правами обладает субъект персональных данных?
6. В чем состоят обязанности оператора при обработке персональных данных?

Тестовые задания:

1. Укажите принцип сбора, обработки и защиты персональных данных:
А) состязательность;

B) законность;
C) демократизм;
D) прозрачность;
E) открытость.

2. Действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных означают:
A) использование больших данных;
B) обработку персональных данных;
C) защиту личной информации;
D) архивирование данных;
E) регистрацию учетных данных.

3. По истечении срока хранения персональные данные подлежат:
A) хранению;
B) учету;
C) уничтожению;
D) восстановлению;
E) перерегистрации.

4. Укажите виды персональных данных по доступности:
A) прямые и косвенные;
B) основные и дополнительные;
C) свободные и активные;
D) общедоступные и ограниченного доступа;
E) учетные и зачетные.

5. Сведения, относящиеся к определенному или определяемому на их основании субъекту, зафиксированные на электронном, бумажном и (или) ином материальном носителе - это?
A) коммерческая тайна;
B) государственные секреты;
C) персональные данные;
D) секреты производства;
E) ноу-хау.

6. Укажите требование многих стандартов и законов, касающихся информационной безопасности:
A) регистрация учетных данных;
B) архивирование информации;
C) подготовка презентации;
D) обработка больших данных;
E) сбор секретов производства.

7. В каких случаях персональные данные подлежат уничтожению собственником и (или) оператором:
A) при регистрации юридического лица;
B) при изменении личных данных;
C) при вступлении в законную силу решения суда;
D) при смене собственника;
E) при толковании договора.

8. Хранение персональных данных означает действия по:
A) реализации функций государственных органов обезличивания персональных данных;
B) обеспечению целостности, конфиденциальности и доступности персональных данных;
C) передаче электронных информационных ресурсов для осуществления аналитики данных;
D) уничтожению собственником и (или) оператором;
E) сохранению переписки сотрудников, отправленных через Интернет.

9. Действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно – это?
A) сбор статистических данных;
B) обезличивание персональных данных;
C) обработка социологических данных;
D) передача научных знаний;
E) блокировка личных данных.

10. Укажите принцип сбора, обработки и защиты персональных данных:
A) конфиденциальность персональных данных ограниченного доступа;
B) состязательность;
C) бюрократизм;
D) качество и доступность;
E) постоянство при проведении социологических исследований.

Тема 2.6. Общая характеристика и значение информационной безопасности

Цель: раскрыть определение информационной безопасности человека и общества, основные подходы к решению проблем информационной безопасности на современном этапе развития Казахстана.

Связь темы лекционного и семинарского занятия с компетенциями, приобретаемыми студентами после освоения данной темы.

В результате освоения настоящей темы студент должен обладать следующими компетенциями:

- интегрировать знания и справляться со сложными вопросами, связанные с информационной безопасностью государства

- умением решать базовые задачи по данной тематике на практических занятиях;

- способностью использовать углубленные специализированные теоретические знания, практические навыки и умения для организации научных и научно-прикладных исследований, учебного процесса, аналитической деятельности.

План:

1. Подходы к определению понятия «информационная безопасность». Задачи и гарантии обеспечения информационной безопасности.

2. Информационная безопасность личности как приоритетная задача государства.

1. Подходы к определению понятия «информационная безопасность». Задачи и гарантии обеспечения информационной безопасности

Понятие «информационной безопасности» сегодня - одно из базовых понятий информационного права. Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития. А значит, актуально все, что связано с понятием безопасности в информационном обществе и в условиях формирования электронного правительства.

Понятие безопасности является очень широким и сужается в зависимости от контекста. Существует безопасность государства, личности, предприятия, общества в целом, а также пожарная безопасность, промышленная безопасность, радиационная и так далее - все они формируют общую систему национальной безопасности государства. В общем, под безопасностью следует понимать отсутствие недопустимого риска, связанного с возможностью нанесения ущерба. Национальная безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Центральным направлением в обеспечении национальной безопасности является формирование безопасной среды для реализации прав и свобод человека и гражданина.

Национальная безопасность включает в себя: государственную безопасность, общественную, техногенную, экологическую и защиту от угроз стихийных бедствий, экономическую безопасность, энергетическую, информационную, безопасность личности.

Информационная безопасность является неотъемлемой частью национальной безопасности. Это связано с тем, что информация во все времена играла ключевую роль в обеспечении стабильности и безопасности любого государства. В свете бурного развития информационных технологий

информационный ресурс превратился в важнейший актив государства, который нуждается в надежной защите.

В этой связи взаимосвязаны термины «информационная безопасность» и «защита информации».

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации. Под защитой информации может подразумеваться:
- программно-аппаратная защита (установка антивирусного программного обеспечения, межсетевых экранов, аппаратных модулей защиты);
- техническая защита информации;
- инженерная защита информации (создание инженерных и коммуникационных средств защиты);
- правовая защита информации;
- криптографическая защита информации;
- организационная защита информации.

Данные способы защиты информации представляют собой комплексную деятельность организации, направленную на сохранение информационных ресурсов, представляющих ценность для организации.

Под информационной безопасностью в широком смысле понимается деятельность, направленная на обеспечение защищенного состояния объекта. В качестве такого объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства.

Необходимость защиты информации сформировалась под влиянием угроз информационной безопасности. В результате возникновения таких угроз возникает проблема эффективного обеспечения информационной безопасности, для создания которой требуется создание развитого методологического базиса, позволяющего решить следующие комплексные задачи:

- создать систему органов, ответственных за безопасность информации;
- разработать теоретико-методологические основы обеспечения безопасности информации;
- решить проблему управления защитой информации и ее автоматизации;
- создать нормативно-правовую базу, регламентирующую решение всех задач обеспечения безопасности информации;
- наладить производство средств защиты информации;
- организовать подготовку специалистов по защите информации;
- подготовить нормативно-методическую базу для проведения работ по обеспечению информационными технологиями.

Стандартная модель безопасности, в том числе информационной, состоит в обеспечении доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Это три важнейших базовых принципа, которые должны обеспечивать информационную безопасность.

Доступность информационных ресурсов является важнейшим элементом информационной безопасности и представляет собой гарантию получения требуемой информации или информационной услуги пользователем за определенное время. Информационные системы создаются и приобретаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это наносит ущерб всем субъектам информационных отношений.

Целостность подразумевает собой актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - это гарантия доступности конкретной информации только кругу лиц, для которых она предназначена.

При обеспечении информационной безопасности участники информационных систем должны стремиться к реализации именно данных понятий, так как они составляют основу защиты информации.

Появление и научное закрепление дефиниции «информационная безопасность» непосредственно связано с осмыслением феномена информатизации и изучением содержания процесса формирования информационного общества.

Представляет интерес вопрос анализа, наряду с правовым аспектом, подходов философов, политологов, социологов, исследователей технических наук к определению понятия «информационная безопасность». Остановимся на некоторых из них.

Подход философов основывается на выделении трех составляющих информационной безопасности:

- удовлетворение информационных потребностей субъектов;
- обеспечение безопасности информации;
- обеспечение защиты субъектов.

Таким образом, в сущностном плане информационная безопасность, согласно философскому подходу, есть такое состояние объекта, при котором состояние информационной среды, в которой он находится, позволяет ему сохранять способность и возможность принимать и реализовывать решения сообразно своим целям, направленным на прогрессивное развитие. Это означает, что информационная безопасность может достигаться как в результате проведения мероприятий, направленных на поддержание информационной среды в безопасном для объекта защиты состоянии, защиту объекта от деструктивного воздействия, так и путем укрепления иммунитета и развития способности объекта уклоняться от деструктивного информационного воздействия (в том числе за счет предвидения их возможности).

Следовательно, задача обеспечения информационной безопасности государства состоит в том, чтобы создать такие условия функционирования информационной инфраструктуры (главным элементом которой является не компьютер, а человек), при которых отдельные граждане, коллективы, органы власти могли бы принимать управленческие решения и добиваться их реализации сообразно целям, направленным на прогрессивное развитие всего общества.

Политический анализ проблематики информационной безопасности - сегодня один из наиболее активных и указывает, прежде всего, на растущую необходимость объединения усилий частного сектора, политических институтов и правоохранительных структур, экспертно-аналитических сообществ в поиске способов противостояния многообразным угрозам в данной области. Адекватная запросам времени политика в области безопасности должна опираться на приоритеты взаимовыгодного сотрудничества и развития гражданской инициативы при руководящей и направляющей роли государства. Сегодня сложились все предпосылки к тому, чтобы стратегии социального партнерства и гражданского участия заняли достойное место в процессах выработки и реализации комплексной политики информационной безопасности.

Технический подход основывается, прежде всего, на проблеме разработки требований безопасности сайтов, включающих защиту серверов, лицензирование, сертификацию и аттестацию объектов информатизации, применение криптографических механизмов при передаче данных по каналам связи, использование методов идентификации и аутентификации пользователей на сайте. Кроме того, подчеркивается, что системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности и вместе с тем максимально учитывались национальные интересы.

Социологи развивают понятие информационной безопасности в рамках одного из направлений социологии - социологии информатики, тем самым взаимосвязывая социологический и информационный подходы.

Среди юристов также пока не выработано единого подхода к определению понятия «информационной безопасности».

«Информационная безопасность является важнейшей составляющей национальной безопасности в целом… В структуре информационного права проблема обеспечения информационной безопасности является одним из институтов. Суть этого института информационного права состоит в осуществлении правовых, организационных, технических мер, обеспечивающих безопасное состояние всех составляющих информационно-коммуникационного комплекса государства, отдельных организаций и каждого человека».

2. Информационная безопасность личности как приоритетная задача государства

Сегодня, наряду с такими понятиями, как «безопасность», «национальная безопасность», «информационная безопасность» как никогда актуализируется понятие «информационной безопасности личности». В современных условиях эта проблема выдвигается на уровень общенациональной.

Анализ основных правомочий человека электронного государства позволяет сделать вывод о приоритетности решения вопроса информационной безопасности личности.

Неслучайно Модельный информационный кодекс для государств-участников СНГ в ст. 1 в числе основных целей информационного законодательства называет в том числе - обеспечение и защиту конституционных прав и свобод человека в информационной сфере; обеспечение информационной безопасности человека, общества и государства; создание правовых условий для эффективного информационного обеспечения физических и юридических лиц, государственных органов и органов местного самоуправления.

При этом информатизация общества и проблема информационной безопасности личности тесно взаимосвязаны. К сожалению, в свете проблем «информационной безопасности государства», «информационной безопасности госструктур», «информационной безопасности бизнеса» и т.п. предмет нашего исследования остается как бы «в тени», за рамками внимания как законодателя, так и многих исследователей. Однако можно с уверенностью утверждать, что постепенно эта проблема выйдет на первый план и будет требовать скорейшего решения.

Формирующееся глобальное информационное пространство, в котором циркулируют информационные потоки, создаваемые всей человеческой цивилизацией, ставит в повестку дня решение не только технических, но и нравственных проблем, порождаемых самим фактом существования этого пространства. Активизация и глобализация информационных взаимодействий в современном обществе предъявляют все более высокие требования к обеспечению информационной безопасности личности.

Поскольку сегодня человек - хочет он этого или нет - начинает жить в электронном Казахстане, необходим целый комплекс специальных мер для обеспечения допустимого уровня безопасности жизни и деятельности человека в таком государстве. Данный комплекс должен включать мониторинг всех аспектов электронного государства, осуществляемый в режиме реального времени с целью своевременного выявления существующих и возникающих в нем информационных угроз, их предотвращения и нейтрализации, а также ликвидации негативных последствий этих угроз. Такой мониторинг станет возможным, если основная масса субъектов электронного государства станет сознательно в нем участвовать и возьмет на себя долю ответственности за безопасность этого государства. Это означает, что должна быть соответствующая этика - этика электронного государства, которой будут

следовать субъекты данного государства и без которой безопасность человека в информационном обществе будет практически недостижима.

При этом, безусловно, должен соблюдаться определенный баланс интересов личности, интересов общества в целом и интересов самого электронного государства.

Застрахованы ли граждане, получив универсальную электронную карту, от мошенничества? Насколько обеспечена будет защита персональных данных?

Для сравнения. Во многих странах, преуспевающих в сфере информационных технологий, нет унифицированной электронной карты. Так, в Германии нет такой карты - это законодательно запрещено по соображениям безопасности граждан. В Англии для безопасности граждан в 2010 г. законодательно упразднен Регистр идентификации и уничтожены базы данных. В Южной Корее создали электронное правительство, но из-за высокого уровня электронного мошенничества население отказалось пользоваться этими услугами.

Формирование электронного Казахстана как электронного государства по-новому расставляет акценты в вопросе реализации прав субъектов информационных отношений, и, прежде всего, человека как основного, первичного их участника.

Вывод: гарантии прав и интересов в информационной сфере приобретают далеко немаловажное значение. И эта проблема требует своего решения как никогда. К примеру, Модельный информационный кодекс для государств-участников СНГ в качестве таковых гарантий называет следующее:

1. Обеспечение информационных прав и свобод человека в информационной сфере, обеспечение информационной безопасности является важнейшей функцией государства.

2. Обеспечение права каждого человека на свободу поиска, получения, использования, создания, распространения и хранения информации любыми законными способами и средствами возлагается на органы государственной власти и местного самоуправления.

3. Государственные органы и органы местного самоуправления, юридические лица обязаны предоставлять информацию по запросу субъектов информационных отношений и информационно-инфраструктурных отношений, за исключением информации, доступ к которой ограничен законом.

Проблем больше, чем достаточно. Не вызывает сомнений одно: развивающееся законодательство в сфере регулирования информационных правоотношений должно быть ориентировано прежде всего на человека как основного, первичного их участника. Этот самый «главный» участник - человек электронного государства, человек информационного общества - не должен остаться в стороне, и его права, и свободы, которые в условиях развития электронного государства актуализируются как никогда, законодателем в полной мере должны быть обеспечены. Понятия «права человека», «законность» должны стать лидирующим ядром в ряду институциональных признаков «электронного государства».

Принцип правовой защищенности человека и гражданина, как основополагающий принцип правового государства, должен лечь в основу решения проблемы «человек в информационном обществе», «человек и общество».

Дела о защите чести, достоинства и деловой репутации граждан в нашем обществе имеют тенденцию к увеличению. Прежде всего, в последние годы новое звучание приобрела проблема интернет-диффамации, т.е. распространения в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя.

Право на неприкосновенность частной жизни относится к числу основных прав человека и защищено Всеобщей декларацией прав человека и Конституцией РК.

Соблюдение конституционных прав и свобод человека и гражданина - задача любого государства, позиционирующего себя в мировом сообществе как демократическое. Перечень и содержание основных прав и свобод человека закреплены во Всеобщей декларации прав человека, которую называют совестью мира, нравственным эталоном человечества. В этом историческом документе, как и в Уставе ООН, подтверждена истина: все люди рождаются свободными и равными в своем человеческом достоинстве и основных, естественных правах. Во всеобщей декларации утверждается право каждого человека на жизнь без нужды и страха на личную неприкосновенность, свободу слова и убеждений.

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Единое мировое информационное пространство, создавая условия безграничной свободы и отсутствия должного правового регулирования, ставит под сомнение ряд закрепленных основным законом государства прав и свобод.

Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, информационные ресурсы доступны всем слоям населения, при этом полноценно решена проблема признания, реализации и защиты прав и свобод субъектов информационных правоотношений, переживает сегодня один из самых активных этапов своего развития. В процессе формирования информационного общества вступившие в силу изменения ГК РК - очередной значимый шаг.

Контрольные вопросы:

1. Дайте характеристику информационной безопасности.
2. Раскройте понятия «информационная безопасность», «информационная безопасность личности», «информационная безопасность общества», «информационная безопасность государства».
3. Какова роль международно-правовых актов в решении вопросов информационной безопасности.

Тестовые задания:

1. Комплекс мероприятий, направленных на обеспечение информационной безопасности – это?
A) блокировка информации;
B) защита информации;
C) обработка личных данных;
D) анализ социологических данных;
E) сбор и накопление аналитического материала.

2. Укажите неверный ответ. Национальная безопасность включает в себя:
A) государственную;
B) персональную;
C) энергетическую;
D) экологическую;
E) информационную.

3. В каком документе содержится перечень и содержание основных прав и свобод человека?
A) в Хартии Европейского союза;
B) в Международном пакте о гражданских и политических правах;
C) во Всеобщей декларации прав человека;
D) в Международном пакте об экономических, социальных и культурных правах;
E) в Декларации ООН о правах коренных народов.

4. Гарантия доступности конкретной информации только кругу лиц, для которых она предназначена:
A) исключительность;
B) доступность;
C) конфиденциальность;
D) открытость;
E) прозрачность.

5. Что понимается под национальной безопасностью?
A) перечень и содержание основных прав и свобод человека;
B) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;
C) информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий;
D) состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз;
E) обеспечение информационных прав и свобод человека в информационной сфере.

6. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения означает:
A) публичность;
B) первостепенность;
C) целостность;
D) объективность;
E) формальность.

7. Укажите неверный ответ. Один из способов защиты информации:
A) программно-аппаратная защита;
B) техническая защита;
C) предварительная защита;
D) инженерная защита;
E) криптографическая защита.

8. Назовите общество, в котором информационные процессы осуществляются главным образом на основе использования информационно коммуникационных технологий:
A) индустриальное общество;
B) информационное общество;
C) социальное общество;
D) постиндустриальное общество;
E) высокоразвитое общество.

9. К какому виду защиты относится установка антивирусного программного обеспечения?
A) к инженерной;
B) к программно-аппаратной;
C) к криптографической;
D) к правовой;
E) к технической.

10. Укажите три базовых принципа, обеспечивающие информационную безопасность:
A) относимость, допустимость и системность;
B) состязательность, независимость и гласность;
C) доступность, целостность и конфиденциальность;
D) качество, профессионализм и доступность;
E) постоянство, системность и оперативность.

Список использованных источников

1 Бачило И.Л. Информационное право: учебник / И.Л. Бачило. - М.: Юрайт, 2013. – 376 с.
2 Рассолов И.М. Информационное право: учебник / И. М. Рассолов. - М.: Юрайт, 2011. - 379 с.
3 Сулейменов М.К. Цифровизация и совершенствование гражданского законодательства (статья третья, исправленная и откорректированная в связи с принятием Закона о цифровых технологиях) // https://online.zakon.kz/
4 Конобеевская И.М. Цифровые права как новый объект гражданских прав // Известия Сарат.ун-та. Экономика. Управление. Право. 2019. Т. 19, вып.3. - С. 330-334. // https://cyberleninka.ru/
5 Ситдикова Р.И., Ситдиков Р.Б. Цифровые права как новый вид имущественных прав // https:cyberleninka.ru/
6 Москеле А. Перспективы законодательного внедрения криптовалюты в Казахстане с учетом опыта зарубежных стран // https://www.zakon.kz/
7 Карагусов Ф.С. О правовом режиме денег в качестве одного из основных видов объектов гражданских прав, создании национальной платежной системы и контроле рынка криптовалют // https://www.zakon.kz/

Нормативные правовые акты:

1 Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.) // http://online.zakon.kz/
2 Закон Республики Казахстан от 25 июня 2020 года № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» // http://online.zakon.kz/
3 Гражданский кодекс Республики Казахстан (Общая часть), принят Верховным Советом Республики Казахстан 27 декабря 1994 года (с изменениями и дополнениями по состоянию на 24.11.2022 г.) // http://online.zakon.kz/
4 Кодекс Республики Казахстан от 2 января 2021 года № 400-VI «Экологический кодекс Республики Казахстан» (с изменениями и дополнениями от 27.12.2021 г.) // http://online.zakon.kz/
5 Бюджетный кодекс Республики Казахстан от 4 декабря 2008 года № 95-IV (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
6 Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
7 Кодекс Республики Казахстан от 29 октября 2015 года № 375-V «Предпринимательский кодекс Республики Казахстан» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/

8 Кодекс Республики Казахстан от 26 декабря 2017 года № 123-VI «О таможенном регулировании в Республике Казахстан» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
9 Кодекс Республики Казахстан от 27 декабря 2017 года № 125-VI «О недрах и недропользовании» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
10 Закон Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 12.09.2022 г.) // http://online.zakon.kz/
11 Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» (с изменениями и дополнениями по состоянию на 25.06.2022 г.) // http://online.zakon.kz/
12 Закон Республики Казахстан от 18 января 2012 года № 545-IV «О телерадиовещании» (с изменениями и дополнениями по состоянию на 27.06.2022 г.) // http://online.zakon.kz/
13 Закон Республики Казахстан от 15 апреля 2013 года № 88-V «О государственных услугах» (с изменениями дополнениями по состоянию на 04.09.2022 г.) // http://online.zakon.kz/
14 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
15 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
16 Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации» (с изменениями и дополнениями по состоянию на 18.11.2022 г.) // http://online.zakon.kz/
17 Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации» (с изменениями и дополнениями по состоянию на 03.05.2022 г.) // http://online.zakon.kz/