МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра теории государства и права и международного права

Заведующий кафедрой
д-р. юрид. наук, профессор
_____ О.Ю. Винниченко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
Магистра

ЗАЩИТА ПРАВ СУБЪЕКТОВ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

40.04.01 Юриспруденция
Магистерская программа «Защита прав человека и бизнеса»

Выполнила работу Студентка 2 курса очной формы обучения		Прозорова Мария Сергеевна
Научный руководитель к.ю.н., доцент		Григорьев Александр Сергеевич
Рецензент и.о. заведующего кафедрой информационного права и цифровых технологий ФГБОУ «СГЮА»,д.ю.н. профессор		Ковалева Наталия Николаевна

Тюмень
2020

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АИС —Автоматизированная информационная система

АСНТИ —Автоматизированная система научно-технической информации

АСОД —Автоматизированная система обработки данных

АСУ —Автоматизированная система управления

ГК —Гражданский Кодекс

ГОСТ —Межгосударственный стандарт

ЕС —Европейский Союз

ЕСЗ; ЕС³ —Европейский центр по борьбе с киберпреступностью

ЕСИА —Единая информационная система идентификации и аутентификации

ИТ;IT —Информационные технологии

НПА —Нормативно-правовой акт

ООН —Организация Объединенных Наций

РОИ —Российская общественная инициатива

РСФСР —Российская Советская Федеративная Социалистическая Республика

РФ —Российская Федерация

СМИ —Средства Массовой Информации

СНГ —Содружество Независимых Государств

США —Соединенные Штаты Америки

УК —Уголовный Кодекс

ФЗ —Федеральный закон

ЭВМ —Электронно-Вычислительная Машина

ВВЕДЕНИЕ

Актуальность темы исследования. Информационные технологии окружают нас. Они объединяют города, страны, народы, планету. Звонок, СМС, email на столько же привычно, на сколько дышать. Быстрее, выгоднее, удобнее и практичнее, а главное – жизненно необходимо. Самоизоляция, связанная со вспышкой COVID-19, явно показала то, что мир уже вполне себе в состоянии жить без выхода на улицу, автономно и независимо от реальности, копируя обыденную реальность. IT откликаются на быстро изменяющуюся реальность. Компьютер, телефон, часы, наушники сегодня больше не просто предмет, для того, чтобы пользоваться, это часть организма, если угодно. Назвать иначе предметы, которые с помощью программок могут сказать нам когда есть, пить, заниматься спортом или принимать таблетки я не могу. То, что было перечислено находится на самом верху айсберга. А ведь с помощью смарт-часов, смарт-браслетов люди отслеживают состояние пульса, состояние здоровья. Если технология понимает, что с вами что-то не так, то она реагирует соответственно – некоторые приборы в состоянии вызвать врача.

А ведь IT влияет на наш мир. Такие слова как «юзать», «блоггер», «софт» «чекать», «ламер» это обычные слова, которые слились с нашей реальностью. Они часть нашей жизни и с этим уже ничего не сделать. Интернет, технологии развивается быстрее, чем реальный мир, он способствует таким эволюционным скачкам, какие мы не творили иногда веками. В частности, способствует ощутимым изменениям права в целом и прав человека в частности.

Российская Федерация является демократическим правовым государством, где за долгие практически 30 лет истории были созданы условия для формирования гражданского общества.

В 2018 году Президент России создал управление по ИТ и развитию цифровой инфраструктуры. Как следует из текста указа «О мерах по оптимизации структуры Администрации Президента РФ» данное управление создано в результате реорганизации ранее существовавшего, аналогичного

управления президента по применению информационных технологий и развитию электронной демократии, которым руководил Андрей Липов. Новое управление является самостоятельным подразделением в составе Администрации Президента.[Указ Президента РФ от 14.06.2018 N 334 "О мерах по оптимизации структуры Администрации Президента Российской Федерации" (вместе с "Положением об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи")[Электронный ресурс]. URL: https://bazanpa.ru/prezident-rf-ukaz-n334-ot14062018-h4073811/ (дата обращения 12.05.2020)]

Цифровая жизнь постепенно привела к появлению «цифровых прав» под которыми В. Зорькин предлагает понимать «…права граждан на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, коммуникационных сетей и сети Интернет, а также право свободно общаться и выражать свое мнение в Сети и право на неприкосновенность частной информационной сферы, включая право на конфиденциальность, анонимность его оцифрованной персональной информации» [Зорькин В. Право в цифровом мире // Российская газета: Столичный выпуск. №7578 (115).]

Сегодня одной из основных задач государства является признание и защита цифровых прав субъектов, пользующихся информационными технологиями.

При внедрении в жизнь современных технологий юридическая незащищенность всех участников данной сферы остается очевидной. Существующая на данный момент ситуация требует разработки концепции по развитию системы законодательства в области защиты прав в сфере цифровых технологий.

Степень научной разработанности темы. . Правовой режим защиты субъектов в сфере информационных технологий является направлением, которое привлекало внимание многих ученых. Значительный вклад в

разработку и совершенствование правового регулирования информационных технологий внесли ряд ученых Зорькин В.Д, Коршунова О.Н., Ломакин А., Степанов О.А, Талапина Э.В. и другие.

Кроме отечественных ученых свой неоценимый вклад внесли и иностранные, чьи труды высоко ценятся на международном уровне: Anderson C., Baskerville R.L., Bouhadana I , Kaul M., Rocha Á, Sousa M.J

Объект и предмет исследования. Объектом данного исследования являются правоотношения в сфере защиты прав субъектов информационных технологий; правовой статус его участников. Предметом исследования служит законодательство Российской Федерации, регулирующее защиту субъектов в сфере информационных технологий, а также различная научная литература, посвященная информационным технологиям и деятельности в сфере информации.

Цель и задачи исследования. Цель настоящей работы заключается в отыскании и анализе различных правовых норм, регулирующих положение субъектов в сфере информационных технологий.

В связи с этим, необходимо разрешить следующие задачи:

1. изучить и проанализировать научные источники, нормативно-правовой и эмпирический материал, имеющийся по теме исследования;
2. исследовать законодательство стран Российской Федерации и иные международные акты, в сфере информационных технологий
3. рассмотреть виды субъектов информационных технологий
4. выявить проблемы правового регулирования защиты субъектов информационных технологий и пути их решения

Методологическая, эмпирическая и теоретическая основы исследования. научного познания, методы анализа, синтеза, сравнительно-правовой, системно-структурный и формально-логический методы.

Теоретической основой исследования являются труды таких учёных-правоведов как Алексеев С.С., Алфёров А.Н, Безкоровайный М.М., Зорькин В.Д., А. К. Костылев, Кочкина Э.Л., Татузов А.Л., Черкасов В.Н., А. Чурилов и др.

Эмпирической основой исследования являются международные правовые акты, Конституция РФ, федеральные конституционные законы, федеральные законы и другие нормативные правовые акты.

На защиту выносятся следующие основные положения, в которых нашла своё отражение и научная новизна исследования:

1. В Российском законодательстве относительно недавно сложилось понимание, что есть «информация» и «информационные технологии», что влечет за собой неоднозначность в законодательстве в отношении IT сферы.
2. Информационное, компьютерное кибернетическое право сливается. По сути, это одно и тоже с некоторыми различаями, которые, по факту, не существенны. На данный момент это синонимичные понятия, которые вытекают одно из другого.
3. Законодательство вынуждено развиваться в силу внешних факторов. Максимально защищенный субъект это государство. В данный момент он старается перенести подобную защищенность и на физических, и на юридических лиц. Подобные действия происходят последние десять лет, когда техническая оснащенность субъектов федерации начала соответствовать необходимому уровню.
4. Реальность вынуждает говорить о необходимости выделения Информационного(компьютерного, кибернетического, право веб-технологий) в отдельную ветвь права, а также нам необходимо создание Информационного кодекса. В. Зорькин , председатель Конституционного суда, также высказывался 2 года назад о том, что нам необходим единый кодифицированный акт в области информационных технологий.

5. Для решения выявленных проблем правового регулирования данной области необходимо модернизировать соответствующие внутригосударственные нормативно правовые акты, а также заключить новые соглашения о защите субъектов информационных технологий, предусматривающие четко прописанные права и обязанности сторон.

Структура работы. Диссертация состоит из ведения, трех глав, шести параграфов, заключения и списка использованных источников и литературы (библиографии).

Во введении излагается актуальность темы исследования, степень её разработанности, объект и предмет, цели и задачи исследования, методологическая, теоретическая и эмпирическая основы исследования.

В первой главе внимание уделяется историко-правовым основам защиты прав субъектов информационных технологий.

Вторая глава подробно рассматривает характеристику субъектов информационных технологий

Третья глава посвящена реальному положению субъектов в данный момент, их положению в законодательстве в компьютерном праве (информационном праве).

В заключении содержатся выводы проведённого исследования, сформулированы рекомендации по решению имеющихся проблем, а также определены пути дальнейшего развития.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ О ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В ПРАВОВОЙ СФЕРЕ

1.1. ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ «ИНФОРМАЦИЯ». ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «ИНФОРМАЦИЯ» В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ

Современная действительность не знает никакую сферу человеческой действительности, которая развивалась бы столь стремительно, практически с нуля, как информатизация и компьютеризация общества. Изначально было заявлено, что компьютеры будут не выгодны, что это бессмысленная трата ресурсов, однако история доказала обратное. Компьютерные технологии живым примером показали возможное быстрое изменение концептуальных представлений, технических средств, методов и сфер применения.

Изначально «программирование» подразумевало умение создавать алгоритм и работать с такими языками, как FORTRAN, BASIC и т.д. В современных реалиях актуально не столько программирование в изначальном смысле слова, сколько умение пользоваться информационными технологиями. Мир упрощается, компьютеризация всех сфер жизни общества убеждает нас в том, что культура общения с компьютером давно стала неотделимым от современной действительности. Терминами «Word», «Excel», «Internet» никого не удивишь, эти слова часть нашего общества и столь же естественны, как слово «бумага». Информационные технологии имеют свои базовые разделы, как архитектура персонального компьютера, операционные системы, теоретическое программирование и др.

Технологии меняют общество, ровно, как и общество диктует свои требования. Всякая деятельность осуществляется по технологии, определяемой целью, предметом, средствами, характером операций и результатами.

В процессе работы мы получаем, а также оперируем различными видами информации. Данный термин происходит от латинского слова "informatio", что означает сведения, разъяснения, изложение. Это слово мы можем слышать достаточно часто, однако определение данного термина достаточно дискуссионное в науке.

В "Большом энциклопедическом словаре» информация определяется как "общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму (генетическая информация). [Большой энциклопедический словарь. 2012[Электронный ресурс]-[Сайт] url: https://slovar.cc/enc/bolshoy/2087819.html) (дата обращения: 20.01.2019)].

Толковый словарь Ожегова определяет информацию в нескольких ключах:

1. Сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством (спец.).

Передача информации. Теория информации (раздел кибернетики, изучающий способы измерения и передачи информации).

2. Сообщения, осведомляющие о положении дел, о состоянии чего-н. Научно техническая и газетная. Средства массовой информации (печать, радио, телевидение, кино). [Толковый словарь Ожегова. С.И. Ожегов, Н.Ю. Шведова.1949-1992.[Электронный ресурс].-[Сайт] url: https://dic.academic.ru/dic.nsf/ogegova/75266) (дата обращения: 20.01.2019)].

В обыденном смысле термин «информация», «информационный» интуитивно ассоциируется с технологиями, компьютерами.

Легально закрепленное определение "информации" впервые появляется в Федеральном законе РФ "Об информации, информатизации и защите информации" от 20 февраля 1995 г., где под "информацией" понимаются "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления". Отметим, что наряду с определением

собственно "информации" Закон также содержит определение "документированной информации", т.е. различает информацию как таковую, как нематериальный объект, и информацию, связанную с материальным носителем.

Сегодня закон дает легальное толкование этого термина в Федеральном законе от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Пункт 1 статьи 2 гласит: «информация - сведения (сообщения, данные) независимо от формы их представления;». [Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" [Электронный ресурс].URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349433&fld=134&dst=1000000001,0&rnd=0.9017852443302901#044410286901490803 (дата обращения 16.09.2019]. Это определение максимально упрощено, в сравнении с теми, что дают словари. Если же сравнивать определение в законах 1995 и 2006, то можно понять, что такое упрощение связано с тем, что таким образом законодатель расширил возможность информации быть в разных воплощениях, а не только в тех, что сказаны в законе.

Кроме того, закон 2006 года выделяет кроме «документированной информации» - «электронный документ». Тем самым еще раз подчеркнув, что стоит разделять информацию, как некий нематериальный объект, и информацию, связанную с материальным носителем. Информатизация общества требует переноса информации все больше и больше на нематериальные носители, тем самым указывая, что для информации, как таковой в принципе материальный объект, как носитель информации, и не всегда обязателен.

До недавнего времени «информация» значилась в ст. 128 Гражданского Кодекса РФ ["Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 16.12.2019, с изм. от 28.04.2020) .[Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&

n=340325&fld=134&dst=554,0&rnd=0.6266534301184712#03687023674239145 (дата обращения 16.09.2019)] , включенная в перечень видов объектов гражданских прав. Иными словами, информация была выделена, как самостоятельный вид объектов, однако никакие специфические характеристики не были приведены. Сегодня же, в выше обозначенном ФЗ от 27.07.2006 N 149-ФЗ в ст. 5 у информации появляются специфические черты, как у объекта правовых отношений. В данной статье в п.1 ст. 5 указано, что «информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу», если законом это не запрещено. В этой же статье в п. 2 и п. 3 выделены категории информации. По сути, под данные категории информации подпадают все знания мира. Информация – это специфический объект права, ему специально оставлена некая свобода, дабы каждый имел право самостоятельно решить, кому, как, когда и в каких объемах возможна передача.

Информация – это то, что позволяет развивать общество, это то, что позволяет двигаться вперед. Основная проблема, которая стоит перед нами, это то, что информации слишком много. Настолько много, что мы тонем в этом потоке. Мы должны понимать, что чрезмерно размытые границы, как в этом случае, не всегда во благо. Нужны более очерченные рамки, чтобы понимать, где новая информация, где переработка, где нечто старое, а где вообще плагиат. Информация нуждается в рамках и границах, как человек в воде и воздухе. Потому что тот, кто владеет информацией - тот владеет миром.

1.2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК ОБЪЕКТЫ ПРАВА. ПОНЯТИЕ «ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Между информационным ресурсом и его потребителем находится именно тот «черный ящик», от состояния которого зависит изготовление информационного продукта, ожидаемого пользователем информационной

системы. Роль этого «черного ящика» и выполняет совокупность средств обработки информации — то, что определяется как информационная технология.

Если мы обратим свое внимание на Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" то в п.2 ст 2. указано понятие “ Информационная технология”. И так, в соответствии с выше обозначенным Федеральным Законом информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Согласно определению ЮНЕСКО, под информационными технологиями(ИТ, IT) нужно понимать комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику, методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, в также связанные со всем этим социальные, экономические и культурные проблемы. [Бобров Евгений Сергеевич, Скрипнюк Джамиля Фатыховна Информационные технологии с позиции технологических укладов в экономическом развитии общества//Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2011. №1 (114)..[Электронный ресурс]. URL:https://cyberleninka.ru/article/n/informatsionnye-tehnologii-s-pozitsii-tehnologicheskih-ukladov-v-ekonomicheskom-razvitii-obschestva (дата обращения: 12.03.2019)].

Сами ИТ требуют сложной подготовки, больших первоначальных затрат и наукоемкой техники. Их введение должно начинаться с создания математического обеспечения, формирования информационных потоков в системах подготовки специалистов.

Выделяют три класса информационных технологий, которые позволяют работать с различного рода предметными областями:

1) Глобальные информационные технологии, которые включают модели, методы и средства, формализирующие и позволяющие использовать информационные ресурсы общества в целом;(таких технологий пока не существует, но в примере масштаба может служить глобальная сеть Интернет);

2) Базовые информационные технологии, которые предназначены для определенной области применения(образование, наука, экономика и т.д.);

3) Конкретные информационные технологии, которые реализуют обработку конкретных данных при решении конкретных функциональных задач пользователя (например, задачи планирования, учёта, анализа и т.д.).

В упомянутом выше Федеральном Законе N 149-ФЗ законодатель дал конкретное, легальное толкование. Своим действием он очертил сферу, в которой могут существовать данные отношения. Дополнительными границами, законодатель подчеркнул, что созданная лицом некая «информационная технология» может пользоваться авторскими правами, как объект авторского права. Кроме того, несмотря на наличие легального определения у нас нет перечня, что же в принципе может подпадать под это определение?

Как пример, это может быть программное обеспечение. В настоящее время программное обеспечение является объектом авторского права. Вместе с тем защита программного обеспечения может осуществляться и другими отраслями права интеллектуальной собственности. Так, в качестве одного из видов защиты может выступать коммерческая тайна или защита нераскрытой информации от незаконного использования. Другой вид защиты – патентная охрана программного обеспечения. Патентное право предоставляет охрану идеям, реализованным в том или ином изобретении, в отличие от авторского права, которое охраняет только само выражение идей. .[А. Чурилов. Режимы охраны программ для ЭВМ: изобретение, коммерческая тайна или литературное произведение? // журнал "ИС. Авторское право и смежные права",N7,июль 2017г.) .[Электронный ресурс]. URL: https://base.garant.ru/77773473/ (дата обращения 15.03.2019)].

В законодательстве понятие изобретения не определено. Однако, в п. 1 ст. 1350 "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ есть определение того, что охраняется в качестве изобретения « техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств), в том числе к применению продукта или способа по определенному назначению.»

Таким образом, программное обеспечение может быть объектом защиты трех различных направлений права интеллектуальной собственности. Сама программа как выражение идей может быть защищена авторским правом и коммерческой тайной. Отдельные же идеи, которые могут быть квалифицированы как изобретения, могут быть защищены патентным правом. Такая тройственная природа защиты имеет свои правовые последствия и часто подвергается критике в академических кругах.

Часть ГК РФ, посвященная правовой охране топологий интегральных микросхем, определяет свой предмет как зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности интегральной микросхемы и связей между ними. "Интегральные микросхемы - микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие". Как видим, здесь дано описание физического представления микросхем, которые используются и в процессе создания информационных технологий. Закон определяет порядок установления авторства и имущественных прав создателя микросхем.

Этот цикл ИТ заранее предполагает разграничение правового внимания на несколько областей регулирования. Первая область связана непосредственно с самим созданием продукта, вторая же с его

использованием для определенных потребительских целей. Исходя из этого, предусмотрено два направления решения правовых проблем информационных технологий.

Первое направлено на урегулирование отношений, которые направлены на создание и включение в сферу использования информационных технологий как составляющей части производства в структуре экономики страны. В данном направлении сосредоточено внимание на правовом обеспечении создания ИТ, упорядочения экономических и организационных проблем, пробелов в данной стадии научной и производственной деятельности. В совокупности всех этих элементов создается комплексная, многогранная, передовая отрасль современной экономики.

Второе же направление определяется проблематикой использования информационных технологий в экономической, социальной, культурной и иных направлениях общественного и экономического развития.

Основная часть технологий ориентирована на выполнение каких-либо конкретных, определенных функций:

- Бухгалтерский учет и контроль
- Ведение системы кадров
- Документооборота
- Финансовых операций,
- Интеллектуальных систем для поддержки изобретательства и стратегического управления и т. д.

Программы для ЭВМ (Электронно-Вычислительных машин), программное обеспечение компьютерной техники и информационных систем с развитием отрасли не прекращают испытывать ряд трудностей, находить проблемы и пробелы в сфере информационных технологий. Ярким примером может являться острая проблема формирования, технического выражения и порядок применения электронно-цифровой подписи.

Кроме того, необходимо привести к правовому порядку такие сферы, как сертификация, стандартизация, лицензирование, организация контроля за

деятельностью производителей информационных технологий, проблемы экспертных оценок качества уже действующих технологий и их соответствия требованиям определенных информационных систем.

Если же мы говорим непосредственно об объектах создания и применения информационных систем, информационных технологий и средств, то к ним мы можем отнести информационные системы и информационные технологии, а также средства их обеспечения.

В соответствии с ФЗ от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" п.2. ст. 2 **“**информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;”

Но какие же “Средства” обеспечивают работу данной сферы? Что вообще подразумевается под этими словами? Обратим свое внимание на “Финансовый словарь”. В соответствии с ним:

Средства обеспечения автоматизированных информационных систем и их технологий – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатации. [Финансовый словарь [Электронный ресурс]. URL:https://dic.academic.ru/dic.nsf/fin_enc/29706 (дата обращения: 16.12.2019)]

К информационным системам относятся и автоматизированные информационные системы разного вида. Первое ,что приходит на ум это - Интернет. Мы настолько привыкли, что воспринимает это как должное, не задумываясь, что это труд многих.

Следующее, о чем мы вспомним, это автоматизированные системы управления (АСУ), автоматизированные системы обработки данных (АСОД), автоматизированные системы научно-технической информации (АСНТИ) и т. п., банки данных, базы знаний, экспертные системы, информационно-вычислительные системы, информационно-телекоммуникационные системы и сети, системы связи и телекоммуникации, а также средства обеспечения этих систем и технологий.

Что касается Субъектов в области Информационных Технологий и средств их обеспечения, мы можем выделить две больше группы:

- Субъекты, которые организуют и осуществляют разработку информационных систем, информационных технологий и средств их обеспечения;
- Субъекты, эксплуатирующие перечисленные выше объекты.

В качестве субъекта, организовавшего и выполняющего разработку, выступают заказчик и разработчики системы. Это может быть кто угодно. И органы государственной власти, и юридические лица, и даже физические лица - организации, предприятия и специалисты. Субъектами, эксплуатирующими информационные системы, информационные технологии, являются органы государственной власти, их подразделения, юридические и физические лица. [Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" [Электронный ресурс].URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349433&fld=134&dst=1000000001,0&rnd=0.9017852443302901#044410286901490803 (дата обращения 20.11.2019].

1.3. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРАВО. ОСНОВНЫЕ ЭТАПЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА В РОССИИ

Основной целью правового регулирования отношений, связанных с применением ИТ, как существующих в данный момент, так и тех, которые будут существовать, является создание эффективной, работающей правовой основы реализации прав граждан, защиты общественных и государственных интересов в соответствующей среде.

Для достижения поставленной цели необходимо понимать, что без скоординированных и согласованных действий органов правотворческой деятельности в сфере развития и использования ИТ должно осуществляться по нескольким направлениям, как то:

– принятие новых законодательных актов, заполняющих пробелы в ранее принятых законах;

– внесение изменений, дополнений в действующие, будущие и иные нормативные акты, которые связаны с ИТ, в соответствии с учетом развития отрасли;

– участие в создании международно-правовых актов в сфере информационных технологий.

Чем же определяется важность изменения законодательства в области ИТ, не считая того, что технологии, как таковые, изменяются не каждый год, а каждое мгновение:

Начнем хотя бы с того, что рост объема услуг связи к 2015 году, в сравнении с 2010 увеличился в 2,6 раза. К 2020, в сравнении с 2015 - в 2,7 раза. За 5 лет произошел рост использования технологий в 0,1 раза, что явно указывает на изменение в современных реалиях, а также изменение в судебной практике

Произошло дополнительное инвестирование в основной капитал операторов связи за период 2008-2020 год. Это оценили в 2,5 трлн рублей.

Объем рынка ИТ к 2020 году увеличен в 5,9 раза, в сравнении с 2007 годом. Кроме того, сокращена доля аппаратных средств при одновременном увеличении доли рынка программных средств и рынка услуг.

К 2020 году увеличено количество компьютеров на 100 человек населения до 87, а пользователей сети Интернет до 90. Стоит также оговорить, что в приведенной статистике не указывается, какого качества, какого года создания данная аппаратура. Однако, сам факт остается фактом - большое количество граждан стали включены в процесс компьютеризации общества.

И в конечном итоге, последнее, о чем стоит сказать, что произошел рост объема продаж продукции радиоэлектронной промышленности в 2015 году в 5 раз.[Прогнозы и аналитика/Экономика/Перспективы развития информационных,коммуникационных технологий в России [Электронный ресурс].URL:https://www.mirprognozov.ru/prognosis/economics/perspektivyi-razvitiya-informatsionnyih-kommunikatsionnyih-tehnologiy-v-rossii(дата обращения 12.12.2019)].

Данные статистики, приведенные выше, явно указывают на то, что произошел довольно серьезный рост информатизации общества, в свою очередь это влечет важность и актуальность обеспечения высокого роста уровня компьютерной безопасности, защиты информации, защиты субъектов.

Люди несут за собой в Интернет среду как позитивное, так и негативное. В свою очередь это вынуждает нас говорить о таких важных аспектах, как “киберпреступность” и “кибербезопасность”.

Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом. Важно правильно сформулировать понятие кибербезопасности, чтобы главные цели работы служб и средств защиты киберпространства от возникающих угроз были точно определены. Однако в концепции приведена формулировка, которая не может удовлетворить этим требованиям. В проекте Концепции говорится следующее: «кибербезопасность – совокупность условий, при которых все составляющие

киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». [Безкоровайный Михаил Михайлович, Татузов Александр Леонидович Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. №1 (2). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 15.05.2019.)].

В свою очередь Киберпреступность - представляет собой совокупность преступлений, где основным непосредственным объектом преступного посягательства выступают общественные отношения в сфере компьютерной информации и информационных технологий, но при этом компьютерная информация, средства создания, хранения, обработки, передачи компьютерной информации являются не только предметами преступного деяния, но и используются, как средства и орудие преступления. [Кочкина Эльвира Леонидовна Определение понятия «Киберпреступление». Отдельные виды киберпреступлений//Сибирские уголовно-процессуальные и криминалистические чтения. 2017. №3 (17). URL: https://cyberleninka.ru/article/n/opredelenie-ponyatiya-ki0berprestuplenie-otdelnye-vidy-kiberprestupleniy (дата обращения: 15.05.2019).].

В Уголовном Кодексе есть 28 Глава «Преступления в сфере компьютерной информации» в которой отражены 4 статьи. Однако, мы считаем, что с развитием общества, еще большим углублением его в информатизацию и кибернетизацию данная глава будет расширяться.

Эксперты считают, что распространение ИТ повлечет увеличение ущерба от деятельности киберпреступников. Ни одна страна не может иметь гарантированной системы защиты от данного вида преступлений, а то и новых преступлений, о которых мы сегодня и подумать не можем. Если мы возьмем цифры, которые зафиксированы в начале, когда преступления только начинались, то в 2004 году было похищено более 105 млрд. долларов, а в 2005 МВД России было зафиксировано свыше 10 тысяч преступлений в сфере высоких технологий. [Центр исследования компьютерной преступности

[Электронный ресурс]. URL: http://www.crime-research.ru/news/06.27.2006/2622/(дата обращения 14.03.2019)].

По данным Генпрокуратуры, самыми популярными преступлениями в сфере ИТ является неправомерный доступ к компьютерной информации((ст. 272 УК РФ)(2016- 994 , 2017 – 1079 2018- 827), распространение вредоносных компьютерных программ (ст. 273 УК РФ)(2016 – 751 , 2017 – 802 , 2018 – 406), а ровно мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ).(2016- 266, 2017 – 228, 2018– 741) [Адвокатская газета. Орган Федеральной палаты адвокатов РФ. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс]. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения 14.03.2019)].

Анализ преступлений, совершаемых в сфере указывает, что наблюдается постоянный рост и развитие преступлений еще с 2000 годов. Борьба против них ведется постоянно, на всех уровнях, хотя совершать эти, да и любые в принципе, стало на порядок проще. Что хоть раз было загружено в Интернет, навсегда останется в нем. Найти практически пошаговую инструкцию, как взломать сайт или провернуть какую-то мошенническую операцию.

Сложившаяся ситуация является следствием расширения российского сегмента глобальной сети Интернет, существенным числом его пользователей. Увеличивается неправомерный доступ к информационным ресурсам государственным и коммерческим организаций в целях копирования(а по факту, хищения) конфиденциальной информации.

Учитывая объективную опасность преступлений в сфере ИТ в мировой практике постоянно происходит развитие законодательства. Наказания становятся строже, приняты соответствующие акты.

В США в июле 2002г Палата представителей Конгресса США одобрила законопроект по повышению компьютерной безопасности (CSEA), Данный акт ужесточает меры, принимаемые в отношении хакеров и в

отношении иных преступлений, совершаемыми ими. Срок увеличили до пожизненного лишения свободы. Конгресс США одобрил в свое время и пожизненное лишение свободы за взлом компьютерных систем. Данный акт, по сути, дал разрешение провайдерам право сообщать, в некоторых случаях обязал сообщать в соответствующие органы об угрозах жизни и здоровья лица, а также и о иных подозрительных случаях. [Американские законодатели одобрили ужесточение антихакерских законов. [Электронный ресурс]. URL: https://internet-law.ru/intlaw/books/crime/2_2.htm (дата обращения 19.04.2019]

В Британии в том же 2002 году впервые хакеры приравнены к террористам не просто в СМИ, для громкого заявления, а на уровне официальных лиц государства. А в это время вступает в силу «Закон о терроризме 2000 года». В Законе впервые распространяется определение и на область киберпространства.[В Великобритании хакеров приравняли к террористам. [Электронный ресурс]. URL:http://www.cnews.ru/news/top/v_velikobritanii_hakerov_priravnyali_1 (дата обращения 19.04.2019)]

Совет Европы, в котором находятся представители 41 государства, близок к заключению первого в истории международного договора, регулирующего борьбу с киберпреступностью. [Европейский центр киберпреступости [Электронный ресурс]. URL:https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата обращения 19.04.2019)]

Деятельность по разработке началась в 1997 году. С 1 января 2013 года по территории Евросоюза (ЕС) работает Европейский центр по борьбе с киберпреступностью (European Cybercrime Centre, EC3).

Центр является структурным подразделением Европола со штабквартирой в Гааге. ЕС планирует создание оперативных и аналитических мощностей, необходимых для быстрого, оперативного реагирования на киберпреступления.

Помимо этого Центр собирает, обрабатывает данные, оказывает информационную, техническую и криминалистическую поддержку правоохранительным органам членов ЕС, координировать расследования,

обучать, подготавливать специалистов вместе с CEPOL.

Центр будет содействовать проведению необходимых исследований и созданию программного обеспечения (R&D), заниматься оценкой и анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений. В сферу деятельности Центра также будет входить помощь судьям и прокурорам.[ЕС открывает центр по борьбе с киберпреступностью [Электронный ресурс]. URL: https://habr.com/ru/post/165253/ (дата обращения 20.04.2019]

На этом фоне поведение России выглядит крайне неоднозначным. К примеру, в 2018 году Россия и США отказались подписать международный договор о борьбе с киберпреступностью.

В декларации президента Франции Макрона говорится: «Мы осуждаем любую злонамеренную кибердеятельность в мирное время, угрожающую как отдельным лицам, так и критическим инфраструктурам, или влекущую за собой значительный неизбирательный или системный ущерб». Франция и большое количество стран, а также государства из состава Евросоюза, и не в ходящие в него государства, к примеру, Япония и Канада подписали акт. В число ИТ-компаний, не оставшихся в стороне, вошли Facebook, Google и Microsoft. Франция сообщила, что приветствует любые предложения по мерам улучшения защиты от киберпреступлений и злоумышленников.

Сам документ это, по сути, призыв к борьбе. Он не содержит в себе ни каких конкретных шагов или действий. Документ представляет собой упоминание всего устава ООН, международного гуманитарного права и международного обычного права. Авторы декларации предполагают, подразумевают, что конкретные действия будут конечно сделаны, но каждой страной на ее усмотрение.

К России и США в своем отказе присоединилось еще ряд стран – Китай Северная Корея, Израиль и Иран.

Отказ подписать французскую декларацию вполне понятен. У России есть отечественный документ, который был внесен на рассмотрение Первого

комитета Генассамблеи ООН еще в конце октября 2018 г. Россия предложила использовать информационные технологии исключительно в мирных целях, предпринимать усилия по предотвращению конфликтов в киберпространстве, с уважением относиться к суверенитету стран и препятствовать увеличению разрыва между ними, а также отказаться от «посредников в контексте применения» ИТ.

Проект Российской резолюции не позиционируется как некий призыв к действию, но содержит перечень мер для реализации целей. В частности, от государств, что подпишутся под ним, будут требовать предоставление весомых доказательств при обвинении субъекта в области кибербезопасности, воздерживаться от провокаций и не использовать киберсреду для нападений.

Суть у этих двух актов одна – защита, помощь, побуждение к активным действиям. Подходы разные.

С одной стороны, конечно, понятно, почему Россия не подписала акт предложенный Францией. Во-первых, мы предложили раньше, во-вторых, были предложены определенные шаги для решения целей и задач, в третьих, страна отстаивает свои интересы.

С другой, когда Россия своим актом создает императивную норму, не позволяющую хоть как-то действовать более-менее свободно, государства могут почувствовать себя «не уютно». Нужно понимать, что, несмотря на то, что государства вынуждены подписывать международные акты, они, тем не менее, желают независимости, развиваться своим путем, независимо и свободно.

То, что предложил президент Франции – это диспозитивный акт, позволяющий государствам двигаться в том ключе, котором им удобно. Каждое государство, каждая компания(а Facebook, Google и Microsoft по силе своего влияния можно сравнить с некоторыми государствами и по некоторым показателям они будут «выигрывать») желает жить без давления.

Нам стоит отметить, что хоть страны не пришли в тот момент к компромиссу, касаемо документов, ситуации и в целом, страны и общество в

лице корпораций понимают, что всем субъектам общества, без исключения, на всех слоях, необходима защита их прав.

Конституция содержит более 30 нормативных правил, устанавливающих основные права и обязанности участников информационных правоотношений. Принципы правового регулирования в сфере ИТ определяются:

- статьей 29 Конституции о праве свободного поиска, получения, передачи и производства, а так распространения информации любым законным способом;
- статья 23 Конституции говорит о принципе на неприкосновенность частной жизни, включая тайну переписки и сообщений;
- статья 24 Конституции – обязует органы власти обеспечить возможность беспрепятственного доступа к документам, затрагивающих права и свободы граждан;
- Статья 44 и статья 128 ГК РФ – гарантии свободы творчества и охраны интеллектуальной собственности, а также связанными с особенностями правовых отношений, связанных с информацией, как отдельным объектом гражданских прав.
- Государственной политикой, которая направлена на приоритетное развитие ИТ при модернизации экономики и повышением эффективности государственного управления, необходимостью обеспечения информационной безопасности
- Определенного рода необходимостью обеспечения информационной безопасности, защиты интеллектуальной собственности и предотвращения нарушений, совершаемых, как в сфере ИТ, так и с их использованием в иных сферах. [Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, № 31, ст. 4398].

Правовые механизмы и процедуры, обеспечивающие реализацию конституционных норм, обязаны быть детализированными нормативно-правовыми актами органов государственной власти.

Общие принципы развития законодательства в сфере ИТ является:

– Верховенство закона

– Системность, согласованность правовых норм, обязывающая участников информационных правоотношений точно и безусловно выполнять нормы законодательства

– Точная, быстрая своевременность кодификации и актуализации законодательства, принятие новых актов, с учетом анализа действующих НПА.

– Последовательная гармонизация правового регулирования

– Обеспечение соответствия российского законодательства общемировой практики регулирования соответствующих правоотношений.

К принципам правового регулирования, которые являются специфическими, относящиеся только к сфере ИТ:

– Презумпция открытости информации

– Обеспечение достоверности, сохранности и эффективного использования информации, являющейся объектом правовых отношений

– Технологическая нейтральность. (подразумевается отказ от законодательного закрепления использования отдельных технологических решений и от создания запретов для развития, применения новых ИТ)

Соответствие НПА перечисленным принципам в сфере ИТ один из важнейших факторов эффективности применения норм и правил.

История становления НПА в сфере ИТ не долгая, но яркая и интересная. На протяжении всей истории, все признавали важность, необходимость ИТ, программ и вообще «полезная штука», но постоянно было что-то не так или не то.

Началом создания в нашей стране законодательной базы регулирующей отношения в сфере компьютерной информации стала разработка в декабре

1991 г. проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией». Закон предусматривал основания для дисциплинарной, гражданской, административной и уголовной ответственности за преступления, которые связаны с компьютерной информацией. [Кравцов К.Н., Этапы развития российского законодательства об ответственности за преступления в сфере компьютерной информации [Электронный ресурс]. URL: https://center-bereg.ru/h1865.html (дата обращения 20.04.2019)]

Однако акт не был принят. Его недостаточно проработали, недостаточно развили, даже для того времени, когда все начинало зарождаться.

Важным этапом направления правотворчества стало принятие Верховным Советом России 23.09.1992 г. закона «О правовой охране программ для электронных вычислительных машин и баз данных». Акт обязал правительство до 01.01.1992 г. внести на рассмотрение Верховного Совета РФ проекты законов РФ с изменениями и дополнениями гражданского, уголовного кодексов РСФСР и иных актов, которые как-либо были связаны с правовой охраной программ электронных вычислительных машин(ЭВМ) и баз данных .

Закон содержал положение об ответственности за выпуск программы для ЭВМ или базы данных под своим именем, а так же за незаконное воспроизведение и распространение аналогичных продуктов.

В 1994 г. был вновь разработан проект закона о внесении дополнений в УК РСФСР. Новый проект предусматривал ответственность за: «…незаконное овладение программами для ЭВМ, файлами и базами данных; фальсификацию или уничтожение информации в автоматизированной системе; незаконное проникновение в автоматизированную информационную систему (АИС), совершенное путем незаконного завладения парольно-ключевой информацией, нарушение порядка доступа или обход механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения; внесение и распространение «компьютерного вируса». Однако проект так и не был реализован в связи с формированием нового Уголовного

кодекса России с учетом преступлений в области компьютерной информации.

В истории НПА в области информационного права важнейшее место занял ФЗ Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. Закон определил основные термины, которые будут использоваться в данной сфере. Позднее был принят ГОСТ Р 50922-96. «Защита информации. Основные термины и определения». Сейчас он не действующий, но он позволил законодательному полю подготовиться к принятию новых понятий, осознанию новых действующих норм, а в перспективе – формированию целостного компьютерного права, как самостоятельной отрасли права.

В феврале 1995 года публикуется проект УК РФ. Впервые за все существование российского права появляется глава, посвященная компьютерным преступлениям.

Ответственность устанавливалась за деяния, такого рода:

1. самовольное проникновение в автоматизированную компьютерную систему (ст. 271);
2. неправомерное завладение программами для ЭВМ, файлами или базами данных (ст. 272);
3. самовольную модификацию, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273);
4. внесение или распространение вирусных программ для ЭВМ (ст. 274);
5. нарушение правил, обеспечивающих безопасность информационной системы (ст. 275).

В 1996г. был принят Модельный Уголовный кодекс государств – участников СНГ, содержащей нормы об ответственности за компьютерные преступления.

В свое время юристам в области ИТ было указано на отсутствие единой правовой концепции, недостаточную связь с отраслевыми законами, слабую проработку терминологии, поэтому, когда ввели в действие УК РФ в его

окончательной редакции осталось только три статьи:

- ст. 272 «Неправомерный доступ к компьютерной информации»;
- ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»;
- ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». [Черкасов В.Н.Компьютеры и преступность. XXI век. (Попытка классификации) [Электронный ресурс]. URL: https://internet-law.ru/intlaw/books/crime/2_1.htm (дата обращения 06.11.2019)].

У ИТ своя собственная специфическая природа права, повышенная социальная опасность преступлений, измененные социальные условия еще с самого начала создания пространства, но это не привело к едином подходу, взгляду на поведение в сфере информационных технологий. При этом, одним из важнейших и одновременно наименее разработанных является направление, связанное с методами и способами защиты информации.

Серьезной проблемой остается криминализация деяний, сопряжённых с компьютерными технологиями, поскольку в российском законодательстве, в основном, речь идет о преступлениях, которые совершены в отношении средств компьютерной техники и информации, а не преступлениях, совершаемых с их использованием.

Этот подход возник с самого начала в этой сфере, что, на наш взгляд, не всегда бывает верным.

ГЛАВА 2. ПОНЯТИЕ И ВИДЫ СУБЪЕКТОВ ИНФОРМАЦИОННОГО ПРАВА (КОМПЬЮТЕРНОГО ПРАВА)

2.1. ПОНЯТИЕ СУБЪЕКТОВ ИНФОРМАЦИОННОГО ПРАВА (ОБЩАЯ ХАРАКТЕРИСТИКА)

В законодательстве отсутствует законодательно закрепленное понятие «субъект информационного права», да собственно это и не нужно. Понятия, которые приводят в научной литературе, которыми пользуются в журналах и учебниках достаточно схожи.

Мы можем сказать, что в соответствии с законодательством РФ Субъекты информационного права – это физические, юридические лица, органы государственной власти, органы местного самоуправления, которые являются участниками публично-правовых и гражданско-правовых отношений в информационной сфере.

Можно сказать, что субъектом информационного права может быть любой, кто обладает информационной право- и дееспособностью.

Под информационной правоспособностью мы можем рассматривать проявление общей правоспособности, в свою очередь под ней понимается установленная и охраняемая государством возможность или способность конкретного субъекта вступать в правовые отношения. В этом случае субъект приобретает юридические права, а соответственно, и обязанности. Если мы используем понятие в таком ключе, то появляются предпосылки правовых отношений с участием данного субъекта.

Но мы должны учитывать, что субъект информационного права может стать субъектом информационных правоотношений только при условии, что есть второй элемент – информационная дееспособность. Под этим следует понимать способность субъекта своими действиями создавать для себя

юридические обязанности, ответственности за свои действия в информационной сфере. Здесь речь пойдет о реальной возможности субъекта реализовать свою информационную правоспособность в условиях конкретных информационных правоотношений.[А. К. Костылев. ИНФОРМАЦИОННОЕ ПРАВО: учебное пособие. 3-е изд., перераб. и доп. Тюмень: Издательство Тюменского государственного университета, 2010. 244 с.]

При осуществлении своих прав субъекты подобных правоотношений обязаны действовать разумно и добросовестно (п.3 ст 157 ГК РФ, п.3 ст. 220 ГК РФ, ст. 234 ГК РФ), соблюдать основы нравственности (ст. 169 ГК РФ) и иные нормы, принятые в обществе(ст. 241 ГК РФ).

Как и говорилось ранее, отсутствует конкретное понятие «субъекта», однако, в НПА и иных актах есть определения конкретных субъектов правоотношений исходя из которых, мы и сделали приблизительное понятие «субъекта».

И так, в соответствии со ст. 2 ФЗ от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" используются определения:

– обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (п .5 ст. 2)

– оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных (п. 12. Ст. 2)

Изучая законодательство РФ, научную литературу и иные источники , выделяются несколько основных групп субъектов информационного права:

– Создатели информации.

Создателем информации может быть любое лицо. Это граждане и их объединения, ученые, писатели, предприятия, органы местного

самоуправления, органы государственной власти, международные организации и т.д.

– Обладатели информации

Следует сразу отметить, что обладатель информации и ее создатель могут не совпадать. Обладатель информации - это субъект, осуществляющий владение, пользование указанными объектами, а также реализующий распоряжения в пределах установленных законом.

В соответствии с п. 1 ст. 6 ФЗ об «Информации» обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

По данному пункту вынесено Постановление Конституционного Суда РФ от 26.10.2017 N 25-П "По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова".

Гражданин А.И.Сушков был принят на работу. В процессе своей трудовой деятельности он переслал с корпоративной почты себе на личную почту информацию, которая являлась конфиденциальной. Сушков был ознакомлен с Положением об обеспечении режима конфиденциальности информации, являющегося неотъемлемой частью трудового договора и обязательного для исполнения. В связи с распространением такой информации Сушков А.И. был уволен.

Суды не согласились с доводами истца и расценили как разглашение конфиденциальной информации то обстоятельство, что он осуществлял пересылку электронных писем, содержащих персональные данные своих коллег по работе, через почтовый сервер, входящий в состав информационно-телекоммуникационной сети, которой владеет ООО "Мэйл.ру"

Сушков обратился в Конституционный Суд РФ, для проверки конституционности п.5 ст. 2 выше обозначенного закона.

Отправка Сушковым А.И. информации, не принадлежащей ему на свой личный адрес электронный почты создает условия неконтролируемого распространения информации. Совершая подобные действия гражданин получает возможность распоряжаться информацией, не получив соответствующего права на основании закона или иного документа. Обладатель же информации, допустивший гражданина без намерений предоставления информации, не сможет в полной мере определить условия и порядок доступа к ней, т.е. осуществлять прерогативы обладателя информации.

Правовые же последствия ситуации различны. Если предоставляя доступ к информации, обладатель информации относился безразлично к ее правовой судьбе, не принимал мер к предотвращению ее выхода из-под контроля, то и оснований нет рассматривать отправку самому себе информации обстоятельства, меняющего правоотношения по поводу этой информации.

Если же обладатель информации принял некие меры для ее сохранности, защиты (включая прямой запрет на отправку на личный адрес(о чем было сказано)), т.е. действовал разумно, то и отправка гражданином информации на личный адрес может рассматриваться в качестве нарушения – в смысле законодательства об информации, информационных технология и о защите информации – его прав и законных интересов именно действием.

Интересно, что Европейский Суд по правам человека не увидел нарушения статьи 8 "Право на уважение частной и семейной жизни" Конвенции о защите прав человека и основных свобод при аналогичном случае. Данные обстоятельства, с точки зрения Европейского Суда по правам человека, позволили работодателю предполагать, что сообщения относятся к профессиональной деятельности работника. (постановления от 3 апреля 2007 года по делу "Коплэнд (Copland) против Соединенного Королевства", от 12 января 2016 года по делу "Бэрбулеску (Barbulescu) против Румынии" и др.).

В итоге Конституционный суд постановил признать п.5 ст.2 Федерального закона "Об информации, информационных технологиях и о защите информации» не противоречащим Конституции РФ, поскольку данное положение не противоречит конституционно-правовому смыслу в системе действующего правового регулирования. [Постановление Конституционного Суда РФ от 26.10.2017 N 25-П "По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова"[Электронный ресурс].URL:http://www.consultant.ru/document/cons_doc_LAW_281568/#dst100028 (дата обращения 10.05.2020)]

– Потребители (пользователи) информации.

В соответствии с ГОСТ 7.73-96 СИБИД, который является межгосударственным стандартом - 3.1.6 потребитель информации: Лицо или коллектив, получающие и использующие информацию в практической деятельности.

Поскольку рассматриваемые далее субъекты могут относиться к любой из трех категорий, в дальнейшем, для более детального, качественного и разумного изучения, мы будем рассматривать субъекты, объединив их в группы:

– РФ; субъекты РФ; муниципальные образования;
– Граждане и другие физические лица;
– Общественные и коммерческие объединения.

2.2. РОССИЙСКАЯ ФЕДЕРАЦИЯ, СУБЪЕКТЫ РФ И МУНИЦИПАЛЬНЫЕ ОБРАЗОВАНИЯ, КАК СУБЪЕКТЫ ИНФОРМАЦИОННОГО ПРАВА

Российская Федерация, субъекты РФ, ее муниципальные образования могут обладать исключительно информационной правоспособность. Иными

словам, РФ является субъектом права, однако не может являться субъектом информационных правоотношений, т.к. данные субъекты реализуют свои права, обязанности через органы государственной или местной власти. Таким образом данный субъект в какой-то мере утрачивает, урезается в своей информационной дееспособности.

Российская Федерация, через органы государственной власти, обязуется обеспечить права и свободы человека и гражданина, юридических лиц, а следовательно, так же обязуется обеспечить и информационные права.

– Обеспечить свободу слова (ст. 29 Конституции РФ)

– Обеспечить достоверное информирование граждан о состоянии экологии (ст. 42 Конституции РФ)

– Публиковать нормативные акты, затрагивающие права, свободы и обязанности человека и гражданина (ст. 15 Конституции РФ)

– Обеспечивать свободу массовой информации. Не допускается цензура (ст. 29 Конституции; ст. 3 Закона РФ от 27.12.1991 N 2124-1 (ред. от 01.03.2020) "О средствах массовой информации")

– Пресекать действия, направленные на сокрытие данных о фактах обстоятельства, создающих угрозу для жизни и здоровья людей (ст. 41 Конституции РФ) ;

– Обеспечить бесплатный доступ к знаниям при обучении (ст. 43 Конституции РФ).

– не допускать использование конфиденциальных данных, третьими лицами.

Непосредственно органы государственной власти субъектов РФ обязаны:

– обеспечивать соблюдение принципа идеологического многообразия, т.е. плюрализма идеологий в России и ее регионах (ст. 13 Конституции)

– обеспечивать соблюдение принципа отделения религии от государства(ст. 4 Конституции);

– не допускать пропаганды, агитации, возбуждающих социальную, религиозную, расовую или национальную ненависть и вражду. Пресекать пропаганду социального, расового, национального или религиозного превосходства (эта обязанность исходит из ч. 2 ст. 29 Конституции РФ);

– в ходе предвыборной кампании обеспечивать кандидатам равные условия в информационной сфере(ст. 48 Конституции)

– обеспечивать полноту, достоверность, своевременность, открытость информации на территории субъекта [Распоряжение Правительства РФ от 30 января 2014 г. N 93-р «О Концепции открытости федеральных органов исполнительной власти» "[Электронный ресурс].URL:http://www.consultant.ru/document/cons_doc_LAW_158273/(дата обращения 05.04.2020)]

Одной из информационных обязанностей субъектов РФ является создание и обеспечение целостности, сохранности, функционирования и развития различного рода информационных фондов.

Однако, давайте разберем на примере Тюменской области, конкретные действия и создание реальной поддержки в сфере информатизации и цифровизации населения.[Постановление Тюменской областной Думы от 27 апреля 1998 г. N 113 «Об утверждении областной целевой программы "Информатизация Тюменской области"»[Электронный ресурс].URL: https://law.admtyumen.ru/law/view.htm?id=203680 (дата обращения 20. 02.2020]

На момент принятия данного постановления в Тюменской области говорили о том, что существует проблема информатизации. Отсутствовала информационно-вычислительная среда, информационное пространство было слабо развито.

Состояние региона, на момент принятия постановления, не соответствовало его возрастающему влиянию во всех сферах общества: политическому, социальному, экономическому. Это довольно сильно сдерживало развитие области. Работы, которые проводили между собой отдельные отрасли и ведомства, были слабо скоординированы, не согласованы

с задачами информатизации региона в целом. В свою очередь все это вело к существенному снижению эффекта производимых затрат, оставляло в стороне нужды, потребности региона.

В регионе отсутствовала современная территориальная инфраструктура информатизации, которая удовлетворяла бы потребности региона в информационно-вычислительном, информационно - аналитическом обслуживании на том уровне, который более-менее считался бы современным.

Однако, Тюменская область развивалась. Мы создали за 20 лет невероятное информационно-технологическое пространство, направленное на все слои общества. Создан Департамент Информатизации Тюменской области, который проводит политику в направлении информатизации, цифровизации общества.

В данный момент вынесено Постановление от 14 декабря 2018 года N 490-п (с изменениями на 17 апреля 2020 года) «Об утверждении государственной программы Тюменской области «Развитие информатизации» и признании утратившими силу некоторых нормативных правовых актов. Программа продлена до 2025 года. [Постановление от 14 декабря 2018 года N 490-п (с изменениями на 17 апреля 2020 года) Об утверждении государственной программы Тюменской области "Развитие информатизации" и признании утратившими силу некоторых нормативных правовых актов [Электронный ресурс].URL:http://docs2.cntd.ru/document/550277090(дата обращения 20. 02.2020]

Таблица, приводимая в Постановлении, является предполагаемым планом, идеальный вариантом, на который рассчитывает правительство Тюменской области.

Исходя из того, что за период с 2015-2020 год доля граждан, которые стали пользоваться электронными услугами составляла 86%, а к 2019 – 93% , количество автоматизированных рабочих мест обеспечивающих работу медицинских работников в медицинской информационной системе, численность населения, охваченного программами подготовки ИТ-кадров и

иные положительные характеристики растут, стоит предположить, что цели если не все, то большая часть имеют шанс быть выполненными.

2.3. ГРАЖДАНЕ И ДРУГИЕ ФИЗИЧЕСКИЕ ЛИЦА, КАК СУБЪЕКТЫ ИНФОРМАЦИОННОГО ПРАВА

Субъект права – это лицо, участник общественных отношений, главные признаки которого – способность быть носителем субъективных юридических прав и обязанностей, а также он может быть участником правоотношений в силу действующего законодательства.

Субъекты информационных правоотношений это или конкретные индивиды, или конкретные коллективы людей.

Индивидами могут быть не только граждане РФ. В это понятие входят также и иностранные граждане, и лица без гражданства. Конституция РФ в главе 2 признает, гарантирует права согласно общепринятым принципам и нормам международного права.

Статья 62 Конституции говорит, что иностранные граждане и лица без гражданства пользуются в Российской Федерации правами и несут обязанности наравне с гражданами Российской Федерации, кроме случаев, установленных федеральным законом или международным договором Российской Федерации.

Чтобы иметь возможность пользоваться своими правами и обязанностями лица обязаны обладать право- и дееспособностью, как и говорилось ранее. В случае физического лица, группы лиц под правоспособностью будет подразумеваться способность лица(создателя программы для ЭВМ, создателя интернет-среды и др.) иметь информационные права и нести соответствующие обязанности. Дееспособность в данном случае будет характеризовать способность лица создавать в реальности, в жизни, на практике, непосредственно своими действиями информационные права и обязанности, которые у данного лица есть. [Алексеев С.С. Общая теория права. Т. 2. М., 1982. С. 138.]

Как видно, правоспособность имеют все граждане. Пол, возраст, раса, национальность, вера значения не имеют. Однако, в информационной сфере правоспособность может быть дополнительно ограничена. Наглядным примером может являться Закон о СМИ ["Закон РФ от 27.12.1991 N 2124-1 (ред. от 01.03.2020) "О средствах массовой информации". [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=346768&fld=134&dst=100027,0&rnd=0.5585991539583091#04053325418179059 (дата обращения 05.04.2020)]

Часть 2 Статья 7 этого закона ограничивает возможность лиц быть учредителем СМИ, в случае, если гражданин является лицом, не достигший восемнадцатилетнего возраста, либо отбывающий наказание в местах лишения свободы по приговору суда, либо душевнобольной, признанный судом недееспособным.

Опять же, дееспособность ровно также возникает не у каждого лица. Таковая может появиться только у тех лиц, что в силу подготовки, способностей, должности и иных активных действий получают в силу информационного законодательства возможность лично использовать свои права и обязанности.

К примеру, граждане с 14 до 18 лет могут, конечно, использовать свои права, но лишь с согласия родителя, законного представителя, опекуна. Соответственно, совершать сделки с программным обеспечением, программными продуктами, компьютерной техникой и т.п. они не могут. Таким образом, данные лица обладают ограниченной дееспособностью.

Однако ряд прав может наступать до рождения (право наследования). В данном случае мы можем говорить о праве на доступ к завещанию. Таким образом, не рожденный субъект, уже имеет права на информацию, о которой говорится в завещании, а также на то имущество, что ему было завещано.

А так же некоторые источники выделяют право на защиту здоровья матери от вредной информации. Однако, данное право кажется неоднозначным. С одной стороны, вне всяких сомнений, во время

вынашивания организм женщины испытывает серьезные изменения, и, вне всяких сомнений, от ряда информации стоит оберегать. С другой стороны, есть информация, типа медицинской, которую сообщать необходимо, и, по сути, происходит нарушение прав лица. Так или иначе, второе выделяемое право нерожденного более спорно, чем первое.

До 6 лет физическое лицо может иметь следующие права:

1) выходить в Internet с разрешения родителей;

2) пользоваться телефонными услугами с соглашения родителей.

Таким образом, права на информацию, на ряд действий связанных с ней появляются у субъекта с рождения и начинают развиваться, добавляться по мере взросления лица. В дальнейшем, когда лицо становится совершеннолетним только от него зависит, появятся ли у него специальные права, а следовательно и обязанности. Единственное чем ограничен субъект в данном случае это законом. Действия гражданина не должны ему противоречить. [Алфёров Андрей Николаевич Человек как явный субъект права в информационной сфере // Сибирский юридический вестник. 2010. №3. ".[Электронныйресурс]. URL:https://cyberleninka.ru/article/n/chelovek-kak-yavnyy-subekt-prava-v-informatsionnoy-sfere (дата обращения: 15.04.2020).]

2.4. ПРАВОВОЙ СТАТУС ОБЩЕСТВЕННЫХ ОБЪЕДИНЕНИЙ И ОРГАНИЗАЦИЙ, КАК СУБЪЕКТОВ ИНФОРМАЦИОННОГО ПРАВА

В предыдущих параграфах мы разобрали такие группы субъектов, как «государство» и « гражданин». В данном параграфе мы хотим обратить свое внимание на третью группу – организации и юридические лица.

В соответствии с ГК РФ п 1 статьи 48. юридическим лицом признается организация, которая имеет обособленное имущество и отвечает им по своим обязательствам, может от своего имени приобретать и осуществлять

гражданские права и нести гражданские обязанности, быть истцом и ответчиком в суде.

За юридическим лицом всегда стоит определённым образом организованный коллектив. Однако, не обязательно, чтобы это было юридическое лицо.

Статья 30 Конституции РФ «Каждый имеет право на объединение, включая право создавать профессиональные союзы для защиты своих интересов. Свобода деятельности общественных объединений гарантируется». Таким образом, объединение людей может быть и община, которая наравне с юридическим лицом становится субъектом информационных отношений.

Свой правовой статус организация реализует через права и обязанности, установленные для всех видов организаций. Для некоторых отдельных юридических лиц установлен специальный статус, с иными правами и обязанностями.

Общий информационный статус юридического лица напрямую связан с информационным обеспечением данного лица. Обеспечение включает в себя создание, приобретение информационных ресурсов, технологий, учет ресурсов и распоряжение своими информационными ресурсами.

Для устранения проблем, которые могут возникнуть в сфере информационного обеспечения, требуется унификация, сведение к единообразию процессов. Общий статус организаций реализуется, в том числе и с помощью субъективных прав юридического лица.

Специальный статус организаций, наделенных специальными полномочиями по сбору, обработке, хранению информации определен и закреплен в законах.

Так обязательному лицензированию подлежат деятельность ряда юридических лиц. Это, к примеру:

– Работа, с информацией персонального характера(конкретным примером может являться медицинская документация);

– проектирование средств защиты информации и обработки персональных данных, а также деятельность, в результате которой вывозятся за пределы РФ государственные информационные ресурсы либо ввозятся.

Развитие интернет-технологий вынуждают предоставлять субъектам специальные статусы. Субъекты, участвующие в международном информационном обмене, требуют серьезного подхода и уточнений.

ГЛАВА 3
ОСНОВНЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ

Как становится ясно из двух предыдущих глав, компьютеризация общества, цифровизация , компьютеризация это действительность, от которой никуда не деться.

Сегодня данный термин используется в нескольких смыслах – узком и широком. В узком смысле мы можем понимать изменение информации, обработку, преобразование в цифровую форму. Это делается для снижения издержек, появлению новых возможностей и т.д. Впервые термин «цифровизация» ввел в употребление в 1995 г. американский информатик Николас Негропонте (Массачусетский университет). Однако реально процессы цифровизации, по крайней мере в экономике, начались уже давно.

Если же мы говорим про цифровизацию в широком смысле, то это можно рассматривать как тренд только в том случае, если цифровая трансформация информации отвечает ряду требований :

1. Охватывается производство, бизнес, наука, социальная сфера, жизнь граждан и прочие отрасли;
2. Сопровождается разумным, рациональным, эффективным использованием результатов
3. Данные результаты доступны пользователям измененной информации;
4. Результаты имеют право использовать не только специалисты, профессионалы, но и так же рядовые граждане;
5. Пользователи цифровой информации имеют навыки работы с ней.

На данный момент мы можем сказать, что цифровизация пришла на смену информатизации и компьютеризации. Изначально речь шла об использовании вычислительной техники, компьютеров, программ и иных

информационных технологий для решения отдельных экономических , социальных, юридических задач.

Развитие возможностей цифрового пространства, как итог, приводит к тому, что создаются целостные «среды существования», в которых пользователь может создать под себя нужное ему дружественное окружение (технологическое, инструментальное, методическое, документальное, партнерское и т. п.) для решения целого класса задач [Принять вызов цифровой экономики [Электронный ресурс]. URL: http://expert.ru/siberia/2017/48/prinyat-vyizov-tsifrovoj-ekonomiki/ (дата обращения:05.04.2020)]

Нормативно-правовая база может стимулировать развитие технологической сферы, а может и существенно сдерживать ее. К примеру, недостаток законодательного регулирования больших данных пока что не дает использовать гражданам использовать свои персональные данные в целях коммерциализации.

Кроме того, у нас отсутствует такое понятие, как «криптовалюта». Это мешает легализации популярных во всем мире цифровых валют в России. Однако, нам предоставлена возможность заключить договор с помощью СМС, а смерт-контракты, работающие на основе блокчейна, позволяют проводить сделки безопаснее, удобнее и прозрачнее с точки зрения борьбы с коррупцией и мошенничеством.

В соответствии с законодательством с 1 октября 2019 года вступили в силу поправки к Гражданскому Кодексу. В соответствии с ними, договор можно заключить в электронной форме, т.е. как было сказано ранее, и в том числе и через СМС. Данные нововведения отражены в статье 160 «Письменная форма сделки» и статье 434 «Форма договора».

Фактически, мы могли такое делать и раньше, но сейчас увеличено количество способов заключения договора.

В классической форме договор заключать не обязательно. Это можно сделать с любым их субъектов с помощью СМС, общения через электронную

почту или мессенджер. Главное, чтобы потом была возможность установить, что желание заключить договор исходило от вас, а не от третьего, неизвестного лица.

Также в силу вступили изменения в статье 309 ГК РФ. Появилась возможность заключать самоисполняемые сделки или смарт-контракты. Сегодня сделку можно заключить с условием исполнения

Также в силу вступили изменения в ст. 309 ГК РФ. Появилась возможность заключения самоисполняемых сделок или смарт-контрактов. Теперь сделку можно заключить с условиями исполнения «без направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления его сторон путем применения информационных технологий, определенных условиями сделки.»

Сфера применения таких договоров максимально обширна и позволяет внедряться в гражданские правоотношения. Данная норма также связана с цифровыми правами.

Типичный пример использования смарт-контракта – размещение на сайте инернет-магазина оферты со ссылкой на специально ПО. Программа может содержать специальный алгоритм, который позволяет списывать с банковской карты необходимую сумму с момента получения товара.

Сегодня все находится в рамках фантазии специалистов в технической сфере и юристов в том числе. Прорывные идеи можно создавать и в рамках закона, благо, для этого появляются возможности.

Таким образом, мы будем использовать под термином «цифровизация» современный, общемировой тренд общества, экономики, юриспруденции, который создан на преобразовании, изменении информации в цифровую составляющую (форму) и как итог - повышение эффективности экономики и улучшение качества жизни.

В 2019 году введено понятие «цифровые права», а также они введены в объекты гражданских прав(ст. 128 ГК РФ), а в Гражданском кодексе это отражено и через отдельную статью 141.1. «Цифровые права». Ими возможно

воспользоваться в рамках инвестиционных платформ, покупая вещь или заказывая услугу.

Правами возможно распоряжаться разными способами, главное, чтобы они были предусмотрены специальной информационной системой, определенной законом.

Распоряжение цифровыми правами осуществляется только в рамках информационной системы, которой может быть только информационная платформа со дня вступления в силу закона «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты РФ». ".[Федеральный закон от 02.08.2019 N 259-ФЗ "О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации" ".[Электронный ресурс]. URL https://bazanpa.ru/gd-rf-zakon-n259-fz-ot02082019-h4470953/ (дата обращения 05.04.2020)].

Данный закон вступил в силу с 1 января 2020 года. Согласно ему, на сайте инвестиционной платформы будут размещаться предложения от различных лиц, желающих получить инвестиции в проекты. При подобного рода заключении сделки заключаются исключительно в экосистеме инвестиционной платформы в электронном виде.

Закон об инвестиционных платформах устанавливает следующие способы инвестирования:

– предоставление займов;

– приобретение эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы, за исключением бумаг кредитных организаций, некредитных финансовых организаций, а также структурных облигаций и предназначенных для квалифицированных инвесторов ценных бумаг;

– приобретение утилитарных цифровых прав.

В соответствии со статьей 2 закона, под утилитарными цифровыми правами понимаются цифровые права, указанные в статье 8 настоящего

Федерального закона. В соответствии со статьей 8 этого закона, утилитарные цифровые права могут содержать следующие цифровые права:

- право требовать передачи вещи (вещей);
- право требовать передачи исключительных прав на результаты интеллектуальной деятельности и (или) прав использования результатов интеллектуальной деятельности;
- право требовать выполнения работ и (или) оказания услуг.

Инвестор с использованием платформы приобретает утилитарное цифровое право за установленную сумму, после чего возникает право требовать выше обозначенного списка.

С использованием инвестиционных платформ ИТ-стартапы смогут привлекать необходимые инвестиции, продавая права требования еще на моменте зарождения идеи, еще на не созданные объекты права, к примеру, право требования на предоставление лицензии на используемый перерабатываемый программный продукт.

Новый закон содержит большое количество требований и ограничений. В частности, операторами подобных платформ могут быть лишь лица, соответствующие требованиям, указанным в законе. Данный перечень установлен в главе 2. Кроме того, при проведении операций обязана происходить идентификация лиц, осуществляющих инвестиции, а физическое лицо имеет право инвестировать не более 600 тыс. рублей в год.

К цифровым правам мы можем отнести право на публикацию цифровых произведений, право на пользование иных электронных устройств. В свою очередь подотрослью цифрового компьютерного права являются авторское, програмное, право доступа к различным данным и защиты при доступе и иное. Нарушение прав возможно с любой из сторон.

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" в статье 7 одним из основных прав гражданина выделяет конфиденциальность анонимных данных персоны . Государство охраняет цифровые права граждан, организаций, к примеру, в области

соответствующего законодательства об информации, информационных технологиях и о защите информации. Ранее уже упоминался соответствующий закон.

Физические и юридические лица имеют право осуществлять поиск, получение информации в любой форме, из любых источников, при условии, что данные действия не противоречат действующим нормам закона. От государственных органов данные субъекты могут получать информацию, затрагивающую их права и обязанности. Государственные органы и органы местного самоуправления обязаны предоставлять информацию о своей деятельности.

В соответствии с законом, информация предоставляется в электронной форме, документ подписывается усиленной квалифицированной электронной подписью, и (или) в форме документа на бумажном носителе. В свою очередь юридические, физические лица предоставляют государственным органам информацию в электронной форме, подписанные, электронной подписью, если иного не установлено законом. [Ломакин А. Цифровизация права // Трудовое право. 2017. № 9. С. 65—74.]

Денную деятельность регламентирует Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [ФЗ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Российская газета от 8 апреля 2011 г. № 75] Еще в 2017 году были внесены соответствующие поправки в законодательство о том, что участники судебного производства имеют право направить в суд документы, а также доказательства по делу в электронном виде, подписанные электронной подписью через сайт суда.

Создание аккаунта на Портал государственных услуг РФ является обязательным условием для того, чтобы воспользоваться данной услугой и подать документы в электронной форме.

В данный момент в электронной форме могут быть так же предоставлены и судебные решения, подписанные усиленной квалифицированной подписью, за исключением особой категории дел.

Вступил в силу законопроект, предусматривающий онлайн-трансляции судебных заседаний, а так же устанавливающий сроки размещения данных актов в сети Интернет. Данные особенности регламентируются в статье 15 Федеральный закон от 22.12.2008 N 262-ФЗ (ред. от 28.12.2017) "Об обеспечении доступа к информации о деятельности судов в Российской Федерации"

При внедрении данной системы обеспечивается доступность правосудия для общества. Растет число кабинетов на сервисе «Электронное правосудие», увеличивается объем документов, поступающих в электронной форме в суды.

К негативным сторонам подобного документооборота стоит отнести то, что часть судебных актов не публикуется вовсе, или появляется несвоевременно.

В данном случае нельзя не сказать и об Электронном правительстве. Основным документом, в соответствии с которым в России формируется электронное правительство, является Концепция формирования в Российской Федерации электронного правительства до 2010 года утвержденная распоряжением Правительства РФ от 06.05.2008 № 632-р (в ред. постановления Правительства РФ от 10.03.2009 №219).В тексте Концепции термин «Электронное правительство» определяется как новая форма деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов.

Главные задачи программы являются повышение эффективности функционирования экономики; государственного, местного управления; создание условий для доступа к информации, а так же получения необходимых услуг.

На данный момент в стране работает единая информационная система идентификации и аутентификации (ЕСИА). ЕСИА обеспечивает доступ

граждан – заявителей и должностных лиц к информации, содержащейся в государственных и иных информационных системах. С помощью данной системы происходит авторизация на сайте Российской общественной инициативы и на Портале госуслуг.

Российская общественная инициатива (РОИ) – Интернет- ресурс, при его помощи граждане РФ, авторизованные через ЕСИА имеют право выдвигать инициативы, а также голосовать за них [Ломакин А. Цифровизация права // Трудовое право. 2017. № 9. С. 65—74.]

Государство работает в сфере защиты информации от неправомерного использования, изменения, уничтожения, распространения, а также иных неправомерных действий. Закон предусматривает различную ответственность, вплоть до уголовной.

К вопросам информационной безопасности государство относит защиту информации, ее сохранность, но в первую очередь реализацию гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере.

Кроме гарантированных Конституцией прав и свобод гражданам гарантированы такие права, как право на личную и семейную тайну, тайну телефонных переговоров, переписки, почтовых и иных сообщений, защиту чести и достоинства. Необходимо заботиться не только о повышении безопасности граждан, но и о повышении безопасности информационных систем государственных органов, финансовой и банковской отраслей, а также о защите сведений, составляющих государственную тайну.

Если рассматривать правоотношения физических, юридических лиц и государства, то ранее, в Федеральным законом «Об информации, информатизации и защите информации» от 20.02.95 г. определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являются объектами отношений данных лиц и подлежат обязательному учету и защите как материальное имущество собственника (статьи 4.1, 6.1), в его обновленной редакции от 27

июля 2006 г. N 149-ФЗ данные статьи отсутствуют. Однако это не значит, что законодатель оставил стороны без возможности взаимодействия. В обновленном ФЗ, в ст.6 сказано, что «Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.». Таким образом, информация приравнивается к материальным благам и появляется возможность совершать действия с информационными ресурсами.

Законодательство рассматривает заключение гражданско-правовых договоров или оформление иных правоотношений, где присутствует обмен электронными сообщениями, подписанными электронной подписью, как обмен документами.

С точки зрения права выделяется информация без ограниченного права доступа (к примеру, законы РФ, обязательные к публикованною; информации о ЧС; информации о состоянии борьбы с преступностью) и информация с ограниченным доступом(коммерческая, государственная, банковская, профессиональная тайна и персональные данные), запрещенная к распространению информация, объекты интеллектуальной собственной и прочая информация.

Засекречивание информации, которая должна быть должна быть донесена до граждан, нарушение объема информации, ее содержания, не опубликование сведений, нарушение прав граждан на получение бесплатной информации, не предоставление сведений, создающих опасности для жизни и здоровья граждан, искажение сведений, сокрытие информации и в иных случаях предусматривается ответственность по закону.

Защита лиц на доступ к информации происходит путем направления жалобы на конкретное должностное лицо или государственный орган в Судебную палату по информационным спорам при Президенте РФ или путем предоставления искового заявления или жалобы для рассмотрения в гражданском, административном или уголовном судопроизводстве.

Стоит отметить, что помимо информационной безопасности государства, существует безопасность предприятия. Предполагается, что каждая организация заинтересована в защите корпоративных сведений, сохранении их конфиденциальности [Ломакин А. Цифровизация права // Трудовое право. 2017. № 9. С. 65—74].

Новые возможности использования цифровых технологий открываются и для оптимизации государственных функций на основе конституционных принципов верховенства права и народовластия.

В скором времени времени IT-технологии позволят с помощью программного кода обеспечить однозначность содержания законов и НПА. Сторонники подобных разработок пока что преувеличивают способности кодировки и недооценивают вариативность общественных отношений, подлежащих регулированию в современной реальности. Сегодня существует потребность благоприятных условий для безопасного функционирования информационных систем.

Повсеместная цифровизация, кибернизация общества создала необходимость развития эффективного механизма защиты частной жизни человека и гражданина, включая обработку персональных данных.

В данном ключе мы не можем обойти тему, которая коренным образом повлияла на Информационное право. 1 мая 2019 года был принят Федеральный закон № 90-ФЗ. Он внес существенные изменения в ФЗ «О связи» и «Об информации, информационных технологиях и о защите информации» (далее – «Закон»). Он направлен на создание инфраструктуры, которая необходима для создания устойчивого, безопасного, целостного функционирования сети Интернет на территории РФ. Это что-то вроде защитной подушки безопасности на случай, если РФ отключат от сети Интернет.

Закон практически полностью вступил в силу 1 ноября 2019 года. Он устанавливает дополнительные обязанности для ряда субъектов. В частности для операторов связи собственников, иных владельцев элементов инфраструктуры, как технологические сети связи, точки обмена трафиком,

линии связи, пересекающие границу РФ, и иных лиц, имеющих номер автономной системы. В случае угрозы или попытки отключения РФ от сети Интернет, Роскомнадзор вправе выдать указания операторам, какие действия им нужно предпринять.

Подобный порядок утверждается Правительством. Закон предусматривает создание реестра точек обмена трафиком. Он так же утверждается Правительством.

Положения Закона детализируются на уровне подзаконных актов, регулирующих технические параметры, требования к сетям связи, порядок предоставления информации и др.

В целях обеспечения устойчивого и безопасного использования доменных имен предусматривается создание национальной системы доменных имен. Туда домены: .RU, .РФ, .SU и иные домены верхнего уровня иные домены верхнего уровня, управление которыми осуществляется зарегистрированными на территории РФ юридическими лицами, являющимися зарегистрированными владельцами баз данных указанных доменов в международных организациях распределения сетевых адресов и доменных имен. [Приказ Роскомнадзора от 29.07.2019 N 216 "Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону".[Электронный ресурс].URL http://www.consultant.ru/law/hotdocs/59001.html/(дата обращения 01.05.2020].

Внедрение средств обеспечения безопасности и достоверности операций требуют дальнейшего совершенствования.

Применение современных технологий требует от законодателя более качественного подхода, понимания, что у участников «цифровых» отношений отсутствуют как таковые права и обязанности, а кроме того, необходимо пересмотреть отношение к технологиям, признать, что это давно не сфера для развлечений, а естественная среда обитания человечества, а также многое и многое другое.

Практически все государства, а также межгосударственные объединения и организации уделяют значительное внимание проблемам цифровизации. Анализ актов позволяет создавать достаточно целостную картину современной действительности, часть из которой мы отказываемся признавать.

Известный факт, что в европейских странах право на защиту персональных данных это «логический вывод» из права на защиту частной жизни. [Bouhadana I. The right to the respect of privacy in digital age in the French law system // Эволюция государственных и правовых институтов в условиях развития информационного общества / Сборник научных работ. М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. С. 135—153.]

Право на частную жизнь – это азбучная истина континентального права. [Sousa M.J., Rocha Á. Digital learning: Developing skills for digital transformation of organizations // Future Generation Computer Systems. February 2019. Vol.91. P. 327—334. doi: 10.1016/j.future.2018.08.048]. .

К примеру, французская доктрина различает несколько составляющих частной жизни (персонально-интимная) жизнь и социальная частная жизнь. Конкретно в такую логику частной жизнь идеально вписываются социальны сети, в то время как с личной жизнью они в основном в противоречивых отношениях. Европейский суд по правам человека подтвердил право любого индивида строить отношения с другими людьми. Через некоторое время, в это неотъемлемое право так же вошло право на электронную переписку. Одним из примеров может в частности Copland против Соединённого Королевства, §§41-42.[Постановление ЕСПЧ от 03.04.2007 "Дело "Копланд (Copland) против Соединенного Королевства" (жалоба N 62617/00) По делу обжалуется мониторинг использования государственным служащим телефона, электронной почты и Интернета в отсутствие законодательной базы. По делу допущено нарушение требований статьи 8 Конвенции о защите прав человека и основных свобод.".[Электронный ресурс].URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=43155#02765821414200842(дата обращения 02.05.2020)].

Краткий анализ ситуации таков, заявительница работала в колледже пост-высшего образования, статутном учебном заведении, управляемом государством, в качестве личного помощника директора. Начиная с конца 1995 года ей пришлось тесно сотрудничать с заместителем директора. По требованию заместителя директора был установлен контроль использования ею телефона, электронной почты и Интернета. По утверждению государства-ответчика, это было сделано для того, чтобы убедиться в том, что она не использует оборудование колледжа в личных целях. Мониторинг использования телефона предусматривал анализ телефонных счетов колледжа, указывавших вызываемые телефонные номера, дату и время звонков, а также их продолжительность и стоимость; мониторинг использования Интернета заключался в анализе посещающихся сайтов, дат и продолжительности визитов, а мониторинг электронной почты - в анализе адресов, дат и времени отправки электронных сообщений. В период этих событий правила мониторинга в колледже не были разработаны. В английском праве также отсутствовали общие гарантии защиты личной жизни, но впоследствии было принято законодательство, регулировавшее перехват сообщений и обстоятельства, при которых работодатели могли записывать или контролировать сообщения работников без их согласия.

Аналогичный случай можно привести и в Румынии. Постановлении ЕСПЧ от 12.01.2016 по делу "Бэрбулеску (Barbulescu) против Румынии" (жалоба N 61496/08). .[Информация о Постановлении ЕСПЧ от 12.01.2016 по делу "Бэрбулеску (Barbulescu) против Румынии" (жалоба N 61496/08) По делу обжалуются мониторинг использования работником Интернета по месту работы и использование собранных данных как обоснование для его увольнения. Дело передано на рассмотрение Большой Палаты Европейского Суда.[Электронный ресурс].URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=483770#017658648190953596(дата обращения 02.05.2020)].

Подобного рода действия, нарушающие права неотъемлемые права субъектов происходят по всему миру. Россия не должна разбираться с последствиями, мы должны думать на опережение.

Директива Европейского парламента и Совета Европейского союза от 15 декабря 1997 г. № 97/66/ЕС [Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector // OJ. L 24. 30 January 1998. Vol. 41.P.1—8],. которая связана с обработкой персональных данных и защиты неприкосновенности частной жизни в области телекоммуникации обязывает «…государства на уровне национального законодательства обеспечивать конфиденциальность коммуникаций, осуществляемых посредством общедоступной телекоммуникационной сети и общедоступных телекоммуникационных услуг» (п. 1 ст. 5).

Все это является право на частную жизнь.

В некоторой мере, подобное взаимодействие частной и персональной жизни используется и на более высоком уровне. К примеру, в деятельности ООН.

24.03.2015 Комитет по правам человека принимает решение и учреждает трехлетний период должности Специального докладчика по вопросу о праве на неприкосновенность частной жизни. В его обязанности в том числе входит защита персональных данных .

Данному учреждению предшествует доклад Верховного комиссара ООН по правам человека о праве на неприкосновенность частной жизни в цифровой век. [Доклад Управления Верховного комиссара ООН по правам человека по вопросу о праве на неприкосновенность частной жизни в цифровой век [Электронный ресурс].URL https://www.ohchr.org/RU/Issues/DigitalAge/Pages/ReportDigitalAge.aspx (дата обращения 12.05. 2020]

В работе отмечается, что государства, как таковые, обязаны обеспечить охрану частной жизни, соблюдение прав человека. Однако, исходя из разделения ответственности с частным сектором, определенные обязательства

несут юридические лица, бизнес-структуры. В частности, на их уровне должна обеспечиваться защита персональных данных. Стоит отметить, что различается защита персональных данных вообще и защита данных при автоматизированной обработке. ["Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)[Электронный ресурс].URLhttp://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349294&fld=134&dst=100007,0&rnd=0.2347151870002857#04129920255011832(дата обращения 12.05.2020)]

В правовом поле России действуют в основном правовые нормы общего характера, потребность в конкретизации содержания нормы в современных условиях объясняется необходимостью технологических особенностей цифровизации. На ряду с этим, на данном этапе юридическая наука отстает от реальной практики.

В должной мере проблема конкретизации права применительно к сфере цифровизации сетей и технологий связанная с противоправной деятельностью не изучена во всех отраслях ни на каком из уровней.

Переход на электронное управление обществом уже находится в производстве и, по мнению ряда экспертов, является предпосылкой к развитию террористических действий с использованием информационно-телекоммуникационных сетей.

Во время VII Московской конференции, в 2018 году, глава ФСБ Александр Бортников заявил, что мессенджеры активно используются для террористических актов выходцами из Ирака и Сирии. По его мнению, только за 2017 год было предотвращено 25 терактов, которые координировались посредством мессенджеров. Конкретные названия приложений глава ФСБ не назвал. [Комсомольская правда. ФСБ: Террористы готовят атаки через мессенджеры [Электронный ресурс].URL https://www.tumen.kp.ru/daily/26814/3850911/ (дата обращения 13.05.2020)]

При рассмотрении конкретизации как фактора придания праву(в субъективном смысле) максимальной определенности в процессе

правоприменительной деятельности следует обратить внимание так же и на систему взглядов на угрозы в сфере компьютерной информации. [Степанов О.А. О проблеме конкретизации права в условиях цифровизации общественной практики // Право. Журнал Высшей школы экономики. 2018. № 3. С. 4—23].

Наиболее актуальные исследования различного рода проблем, возникающих при применении современных информационных средств, позволило обосновать необходимость совершенствования норм российского законодательства. Учитывая важность соблюдения прав человека в современном мире, осознавая важность для нашего государства и общества, юридических лиц, признавая ,что информационные технологии стали не просто частью нашей жизни, а стали второй, а для кого-то и первой жизнью, считаем, что опасность для общества и государства посягательств на права субъектов в области информационных технологий диктует необходимость признать в полной мере их специфичность, а также тот факт, что в российском законодательстве практически отсутствуют меры по предупреждению подобного рода преступлений и правонарушений. Считаем ,что подобная отрасль права должна быть выделена в отдельную ветвь и развиваться самостоятельно, по возможности без внешнего влияния, на сколько это возможно. Таким образом, мы получим еще одну попытку для улучшения общества, хотя бы в виртуальном мире.

ЗАКЛЮЧЕНИЕ

Проанализировав международные и внутригосударственные нормативно-правовые акты научную и учебную литературу, а также судебную практику, относящуюся к рассматриваемой нами теме, приходим к следующим выводам:

Общество сегодня живет в новой цифровой реальности, созданной информационными технологиями. Цифровые технологии проникли во все сферы деятельности человека и уже сегодня идет речь о создании новой реальности, которая не будет иметь аналогов в прежнем мире. Цифровизация общества, его политической и экономической составляющих говорит о том, что назрела необходимость наполнения национальных правовых систем стандартами, которые приобретут иную степень совместимости в рамках формирования макросреды правого регулирования.

Практически любая деятельность в сфере информационных технологий регулируется законодательством. Однако в процессе нарушается часть прав субъектов, которые не учитываются, в силу того факта, что информационное общество развивается на много быстрее общества реального. Нарушаются права физических лиц, юридических, в некоторых случаях, государств.

РФ необходимо иметь кодифицированный акт, а также заключать международные договора, которые создадут базу принципов и покажут, что мы готовы развиваться. Развиваться не только в рамках государства, а также и за его приделами.

Все сказанное говорит о том, что сегодня необходимо искать оптимальный компромисс между возможностью доступа спецслужб и правоохранительных органов к компьютерной информации и правом граждан на ее конфиденциальность.

Общий объем преступлений и правонарушений против конституционных прав и свобод человека, совершаемых в РФ в сфере цифровых технологий, из года в год растет.

Вместе с тем, имеется ряд проблем в правовом регулировании цифровых взаимоотношений, о которых мы уже упоминали выше. Для их решения необходимо модернизировать вышеозначенные внутригосударственные нормативно правовые акты путем внесения соответствующих статей, а также заключить новые соглашения о информационном сообщении Хочется надеяться, что после того, как это будет сделано, уровень защищенности субъектов информационных технологий вырастет и информационное общество, кибернетическое общество будет развиваться если не параллельно реальности, то в более позитивном ключе, не перенимая негативный опыт реальности .

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция РФ о 12.12.1993 г. (ред. от 21.07.2014). URL:http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 28.04.2020).
2. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 16.12.2019, с изм. от 12.05.2020) URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения 20.04.2020)
3. "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 18.07.2019) URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=329334&fld=134&dst=100007,0&rnd=0.3261387195529242#07836601592046473
4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) "Об информации, информационных технологиях и о защите информации" URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349433&fld=134&dst=1000000001,0&rnd=0.9017852443302901#044410286901490803 (дата обращения 16.09.2019
5. Закон РФ от 27.12.1991 г. № 2124-1 (ред. от 01.03.2020) «О средствах массовой информации». URL: http://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения 05.04.2020).
6. Указ Президента РФ от 14.06.2018 N 334 "О мерах по оптимизации структуры Администрации Президента Российской Федерации" (вместе с "Положением об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи")[Электронный ресурс]. URL: https://bazanpa.ru/prezident-rf-ukaz-n334-ot14062018-h4073811/ (дата обращения 12.05.2020)

7. [Распоряжение Правительства РФ от 30 января 2014 г. N 93-р «О Концепции открытости федеральных органов исполнительной власти» "[Электронный ресурс].URL:http://www.consultant.ru/document/cons_doc_LAW_158273/(дата обращения 05.04.2020)
8. [Постановление Тюменской областной Думы от 27 апреля 1998 г. N 113 «Об утверждении областной целевой программы "Информатизация Тюменской области"»[Электронный ресурс].URL: https://law.admtyumen.ru/law/view.htm?id=203680 (дата обращения 20. 02.2020]
9. [Постановление от 14 декабря 2018 года N 490-п (с изменениями на 17 апреля 2020 года) Об утверждении государственной программы Тюменской области "Развитие информатизации" и признании утратившими силу некоторых нормативных правовых актов [Электронный ресурс].URL:http://docs2.cntd.ru/document/550277090(дата обращения 20. 02.2020]
10. ".[Федеральный закон от 02.08.2019 N 259-ФЗ "О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации" ".[Электронный ресурс]. URL https://bazanpa.ru/gd-rf-zakon-n259-fz-ot02082019-h4470953/ (дата обращения 05.04.2020)].
11. [ФЗ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Российская газета от 8 апреля 2011 г. № 75]
12. Приказ Роскомнадзора от 29.07.2019 N 216 "Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону".[Электронный ресурс].URL http://www.consultant.ru/law/hotdocs/59001.html/(дата обращения 01.05.2020].
13. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection

of privacy in the telecommunication sector // OJ. L 24. 30 January 1998. Vol. 41.P.1—8]

14.. ["Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)[Электронный ресурс].URLhttp://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349294&fld=134&dst=100007,0&rnd=0.2347151870002857#04129920255011832(дата обращения 12.05.2020)]

15. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных"".[Электронный ресурс]. URL http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286959&fld=134&dst=100008,0&rnd=0.8697923426396312#07717267132625225 (дата обращения 10.04.2020)

16. Федеральный закон от 22.12.2008 N 262-ФЗ (ред. от 28.12.2017) "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" .[Электронный ресурс]. URL http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286518&fld=134&dst=100008,0&rnd=0.9231249379225657#0619823889888319

17. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 07.04.2020) "О связи" .[Электронный ресурс]. URL http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=349739&fld=134&dst=100009,0&rnd=0.3252726417721159#05436248263303041

18. Приказ Роскомнадзора от 29.07.2019 N 216 "Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону".[Электронный ресурс].URL http://www.consultant.ru/law/hotdocs/59001.html/(дата обращения 01.05.2020].

19. [Распоряжение Правительства РФ от 06.05.2008 N 632-р (ред. от 10.03.2009) «О Концепции формирования в Российской Федерации электронного правительства до 2010 года» Электронный ресурс].URL

http://www.consultant.ru/document/cons_doc_LAW_76942/ (дата обращения 10.05.2020].

20. ГОСТ 7.73-96 СИБИД. Поиск и распространение информации. Термины и определения ".[Электронный ресурс].URL http://docs.cntd.ru/document/1200004733(дата обращения 15.04.2020)

Научная литература

21. Бобров Евгений Сергеевич, Скрипнюк Джамиля Фатыховна Информационные технологии с позиции технологических укладов в экономическом развитии общества // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2011. №1 (114). .[Электронный ресурс]. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-s-pozitsii-tehnologicheskih-ukladov-v-ekonomicheskom-razvitii-obschestva (дата обращения: 12.03.2019)
22. Зорькин В. Право в цифровом мире // Российская газета: Столичный выпуск. №7578 (115)
23. А. Чурилов. Режимы охраны программ для ЭВМ: изобретение, коммерческая тайна или литературное произведение? // журнал "ИС. Авторское право и смежные права",N7,июль 2017г.) .[Электронный ресурс]. URL: https://base.garant.ru/77773473/ (дата обращения 15.03.2019)
24. Безкоровайный Михаил Михайлович, Татузов Александр Леонидович Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. №1 (2). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 15.05.2019.)
25. Кочкина Эльвира Леонидовна Определение понятия «Киберпреступление». Отдельные виды киберпреступлений//Сибирские

уголовно-процессуальные и криминалистические чтения. 2017. №3 (17). URL: https://cyberleninka.ru/article/n/opredelenie-ponyatiya-ki0berprestuplenie-otdelnye-vidy-kiberprestupleniy (дата обращения: 15.05.2019

26. Черкасов В.Н.Компьютеры и преступность. XXI век. (Попытка классификации) [Электронный ресурс]. URL: https://internet-law.ru/intlaw/books/crime/2_1.htm (дата обращения 06.11.2019)].
27. [Алексеев С.С. Общая теория права. Т. 2. М., 1982. С. 138.]
28.. [Алфёров Андрей Николаевич Человек как явный субъект права в информационной сфере // Сибирский юридический вестник. 2010. №3. ".[Электронныйресурс]. URL:https://cyberleninka.ru/article/n/chelovek-kak-yavnyy-subekt-prava-v-informatsionnoy-sfere (дата обращения: 15.04.2020).]
29. [Ломакин А. Цифровизация права // Трудовое право. 2017. № 9. С. 65—74.]
30. [Bouhadana I. The right to the respect of privacy in digital age in the French law system // Эволюция государственных и правовых институтов в условиях развития информационного общества / Сборник научных работ. М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. С. 135—153.]
31. [Sousa M.J., Rocha Á. Digital learning: Developing skills for digital transformation of organizations // Future Generation Computer Systems. February 2019. Vol.91. P. 327—334. doi: 10.1016/j.future.2018.08.048]. .
32. Доклад Управления Верховного комиссара ООН по правам человека по вопросу о праве на неприкосновенность частной жизни в цифровой век [Электронный ресурс].URL https://www.ohchr.org/RU/Issues/DigitalAge/Pages/ReportDigitalAge.aspx (дата обращения 12.05. 2020

33.. [Степанов О.А. О проблеме конкретизации права в условиях цифровизации общественной практики // Право. Журнал Высшей школы экономики. 2018. № 3. С. 4—23].

34.[Кравцов К.Н., Этапы развития российского законодательства об ответственности за преступления в сфере компьютерной информации [Электронный ресурс]. URL: https://center-bereg.ru/h1865.html (дата обращения 20.04.2019)]

35..[А. К. Костылев. ИНФОРМАЦИОННОЕ ПРАВО: учебное пособие. 3-е изд., перераб. и доп. Тюмень: Издательство Тюменского государственного университета, 2010. 244 с.]

Материалы практики

36.Постановление ЕСПЧ от 03.04.2007 "Дело "Копланд (Copland) против Соединенного Королевства" (жалоба N 62617/00) По делу обжалуется мониторинг использования государственным служащим телефона, электронной почты и Интернета в отсутствие законодательной базы. По делу допущено нарушение требований статьи 8 Конвенции о защите прав человека и основных свобод.".[Электронный ресурс].URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=43155#02765821414200842

37..[Информация о Постановлении ЕСПЧ от 12.01.2016 по делу "Бэрбулеску (Barbulescu) против Румынии" (жалоба N 61496/08) По делу обжалуются мониторинг использования работником Интернета по месту работы и использование собранных данных как обоснование для его увольнения. Дело передано на рассмотрение Большой Палаты Европейского Суда. [Электронный ресурс].URL:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=483770#017658648190953596 (дата обращения 02.05.2020)].

38. Постановление Конституционного Суда РФ от 26.10.2017 N 25-П "По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова"[Электронный ресурс].URL:http://www.consultant.ru/document/cons_doc_LAW_281568/#dst100028(дата обращения 10.05.2020)

Электронные ресурсы

39. Большой энциклопедический словарь. 2012[Электронный ресурс]-[Сайт] url: https://slovar.cc/enc/bolshoy/2087819.html) (дата обращения: 01.10.2019).
40. Толковый словарь Ожегова. С.И. Ожегов, Н.Ю. Шведова.1949-1992.[Электронный ресурс].-[Сайт] url: https://dic.academic.ru/dic.nsf/ogegova/75266) (дата обращения: 20.01.2019).
41. Финансовый словарь [Электронный ресурс]. URL:https://dic.academic.ru/dic.nsf/fin_enc/29706 (дата обращения: 16.12.2019)
42. Прогнозы и аналитика/Экономика/Перспективы развития информационных, коммуникационных технологий в России [Электронный ресурс].URL:https://www.mirprognozov.ru/prognosis/economics/perspektivyi-razvitiya-informatsionnyih-kommunikatsionnyih-tehnologiy-v-rossii (дата обращения 12.12.2019)
43. Центр исследования компьютерной преступности [Электронный ресурс]. URL: http://www.crime-research.ru/news/06.27.2006/2622/(дата обращения 14.03.2019)

44. Адвокатская газета. Орган Федеральной палаты адвокатов РФ. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс]. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения 14.03.2019)
45. Американские законодатели одобрили ужесточение антихакерских законов. [Электронный ресурс]. URL: https://internet-law.ru/intlaw/books/crime/2_2.htm (дата обращения 19.04.2019]
46. В Великобритании хакеров приравняли к террористам. [Электронный ресурс]. URL:http://www.cnews.ru/news/top/v_velikobritanii_hakerov_priravnyali_1 (дата обращения 19.04.2019)
47. Европейский центр киберпреступости [Электронный ресурс]. URL:https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата обращения 19.04.2019)
48. ЕС открывает центр по борьбе с киберпреступностью [Электронный ресурс]. URL: https://habr.com/ru/post/165253/ (дата обращения 20.04.2019)
49. Принять вызов цифровой экономики [Электронный ресурс]. URL: http://expert.ru/siberia/2017/48/prinyat-vyizov-tsifrovoj-ekonomiki/ (дата обращения:05.04.2020)
50. Комсомольская правда. ФСБ: Террористы готовят атаки через мессенджеры [Электронный ресурс].URL https://www.tumen.kp.ru/daily/26814/3850911/(дата обращения 13.05.2020)