Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Саратовская государственная юридическая академия»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных статей
по материалам Всероссийской научной Интернет-конференции студентов, магистрантов, аспирантов, молодых ученых, посвященной 85-летию
ФГБОУ ВО «Саратовская государственная юридическая академия»

2-11 апреля 2016 года

Саратов

2016

УДК 340:004(082)
ББК 67:32.81я43
И74

И74 Информационные технологии и право: сборник материалов Всероссийской научной Интернет-конференции, посвященной 85летию ФГБОУ ВО «Саратовская государственная юридическая академия». Саратов, 2016. – 295 с.

ISBN 978-5-9758-1644-3

В сборнике представлены материалы Всероссийской научной Интернет-конференции студентов, магистрантов, аспирантов, молодых ученых «Информационные технологии и право», посвященной 85-летию ФГБОУ ВО «Саратовская государственная юридическая академия».

В статьях приведены результаты исследований по актуальным проблемам защиты информации в Интернете и корпоративных сетях, защиты персональных данных, борьбы с преступлениями в сфере компьютерной информации, противодействия экстремизму и терроризму в сети, защиты авторских прав, применения информационных технологий в политологических исследованиях, избирательных кампаниях, криминалистике, судебной экспертизе.

Материалы публикуются в авторской редакции.

УДК 340:004(082)
ББК 67:32.81я43

ISBN 978-5-9758-1644-3 © Коллектив авторов, 2016 **Предисловие**

В настоящем сборнике опубликованы материалы, представленные на Интернет-конференции «Информационные технологии и право», проведённой в апреле 2016 года кафедрой информатики Саратовской государственной юридической академии в рамках мероприятий, посвященных ее 85-летию . В конференции приняли участие представители 15 вузов России.

Тематика публикуемых материалов достаточно обширна и актуальна. Широко представлены доклады по методам защиты информации в Интернете и корпоративных сетях, защите персональных данных, борьбе с преступлениями в сфере компьютерной информации, противодействию экстремизму и терроризму в сети. Нашли отражение вопросы защиты авторских прав, применения информационных технологий в политологических исследованиях, избирательных кампаниях, криминалистике, судебной экспертизе.

Доклады, размещенные на сайте, вызвали интерес участников конференции, о чем свидетельствует большое количество отзывов и вопросов, поступивших на форум.

Оргкомитет конференции благодарит всех студентов, магистрантов, аспирантов, молодых ученых и их научных руководителей, представивших результаты научных работ на конференцию и принявших участие в их обсуждении на форуме сайта кафедры информатики Саратовской государственной юридической академии.

СОДЕРЖАНИЕ

М.А. Айбазова, А.А. Аргуянова

ФГБОУ ВПО «Северо-Кавказская государственная
гуманитарно-технологическая академия».
Юридический институт

*Научный руководитель: **Н.С. Утехина**, ассистент кафедры социальных, гуманитарных, экономических, правовых и прикладных дисциплин ФГБОУ ВПО «Северо-Кавказская государственная гуманитарнотехнологическая академия»*

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРАВОСОЗНАНИЕ И ПРАВОВУЮ КУЛЬТУРУ

Стремительное развитие информационных технологий привело к совершенствованию компьютерной техники, программного обеспечения, создания автоматизированных систем обработки информации, электронных баз и банков данных, сложнейших аналитических и экспертных систем.

Существенным образом изменяет современные общественные отношения, бурное развитие разнообразных телекоммуникационных сетей, включая глобальную сеть Интернет.

Информационные технологии оказывают существенное влияние на общественные процессы, внедряя достижения информационного прогресса в деятельность не только общества, но и государства. Это приводит к тому, что общественные отношения приобретают электронную форму. В последнее время многие страны, в их число входит и Россия, ставят перед собой задачу перехода к электронным формам управления, которые необходимы в информационном обществе.

Создание новейших разработок в области информационных технологий является важнейшим стратегическим направлением политики государства. Нынешнее состояние государства и права находятся в тяжелой и неясной взаимосвязи с происходящими в стране процессами модернизации, процессами широкого внедрения и использования новейших информационных технологий.

Проблемы взаимосвязи правовой культуры и информационных технологий не раз поднимались в трудах отечественных ученых – правоведов. Они связаны, главным образом с профессиональными аспектами данной правовой категории.

Правовая культура сегодняшнего времени отличается от той, которая была раньше. Меняется сама общественная жизнь, социальные, экономические, политические условия. Проблемы дальнейшего развития культуры, в том числе правовой имеют особую значимость. Таким образом, информационные технологии постепенно становятся важным фактором, влияющим на правовое сознание.

Правосознание – это динамично развивающаяся под воздействием информационного общества система идей, теорий, представлений, чувств, привычек о праве, правовой действительности на основании информации, полученной в большинстве своем посредством информационных технологий, а также ценностных ориентиров, правовых установок, призванных регулировать поведение человека в юридически значимых ситуациях[1].

На основе этих суждений сформулировано определение информационной технологий.

Информационная технология – это основанная на достижениях современной компьютерной техники и средств коммуникации совокупность процессов воздействия на информацию, инструментарий для получения разнообразной информации, а также способ взаимодействия между людьми современного общества, способ совместного приятия решений и рождения новых знаний, создания законодательства, развития правовой системы

[1] *Алексеев С.С.* Общая теория права: учебное пособие для студентов вузов. М., 2010.
[2] *Алешин Л.И.* Информационные технологии: учебное пособие. М., 2011.

государства в целом и способ воздействия на сознание, а, следовательно, и его составляющую правосознания[2].

Благодаря переходу к информационному обществу появились новые возможности, связанные с бурным развитием и модернизацией различных направлений информационных технологий, таких как: Интернет, мобильные технологии, различные специализированные программы, базы и банки данных, аналитические и экспертные системы и т.п.

Информационные технологии для современного человека, носителя традиционного правосознания, становятся основным источником информации о праве и правовой деятельности, которую он получает из справочных правовых систем, официальных сайтов органов государственной власти, специализированных юридических порталов, отдельных юридических Webстраниц и т.п.

Благодаря этой информации выражаются правовые направления, устанавливаются правовые цели и формируется практическая деятельность в правовой сфере.

Человек, имея обширный доступ к различной информации, может быстрее оценить полученные данные и принять наиболее правильное решение, спрогнозировав последствия своих поступков.

Шагом в развитии современной цивилизации является информационное общество, характеризующееся повышением роли информации и знаний в жизни государства, ростом информационно-коммуникационных технологий, образованием глобальной информационной системы, обеспечивающей эффективное информационное взаимодействие людей, которое предоставляет необходимую информацию для удовлетворения их социальных и личностных нужд в информационных продуктах и услугах.

Технологической базой информационного общества являются глобальные телекоммуникационные сети.

Интернет представляет собой крупнейшую в мире телекоммуникационную сеть, которая возникла как средство связи для узкого круга специалистов, но весьма быстро превратилась в массовое явление.

В настоящее время Интернет является международной технологической системой общего пользования, предназначенной для обмена информацией.

Усовершенствование правовой культуры связано с процессом функционирования Интернета как источника правовой информации, образующего взаимную связь между государством, организациями и обществом.

Влияние Интернета на правосознание является присущей частью структуры правовой культуры, как всего общества, так и человека в отдельности.

Процесс формирования концепции правового государства сталкивается с комплексом проблем, связанных с правовой информированностью, правовым сознанием человека, социально-правовой активностью, что является правовой установкой, которая представляет собой механизм активного, деятельностного отражения окружающей действительности.

Интернет как телекоммуникационная сеть общего пользования является эффективным средством реализации творческой роли права и дает возможность более полному использованию гражданами своих демократических прав и свобод[2].

Кроме того, будучи представителем правовой социализации, Интернет обладает потенциальной возможностью воспитывать уважение к закону, развивать правовое мышление, формировать правовую культуру и обеспечивать социально активное поведение в правовой сфере. Информационный обмен через Интернет представляет единство деятельности, общения и познания.

Необходимо также обратить внимание на правовое воспитание подрастающего поколения с использованием информационных технологий.

[2] *Голицына О.Л.* Информационные технологии: Учебник. М., 2013.

Молодежь тратит большую часть своего времени на использование различных компьютерных устройств и глобальных телекоммуникационных сетей, в которые входит сеть Интернет.

В связи с этим информационные технологии предоставляют наиболее продуктивный метод воздействия на формирование сознания молодого поколения, его основной частью – правосознания.

Создание четких установок на правомерное поведение, используя метод, который будет понятен и доступен подрастающему поколению.

Для реализации этого метода нужно подключить специалистов из области информатики, права, психологии и педагогики.

Необходимо создавать и модернизировать специально направленные на правовое воспитание интернет-ресурсы разрабатывать различные обучающие компьютерные программы, воздействующие на все общество, а именно на молодое поколение, которые активно пользуются информационными технологиями.

Студенты-юристы, которые изучают правовые дисциплины в различных учебных заведениях, относятся к особой группе носителей правового сознания. Ее особенность заключается в том, что она стоит на границе между носителями традиционного правосознания и в процессе обучения постепенно переходит в группу носителей профессионального сознания.

В связи с изменением государственно-правового устройства, существенным образом, подверглось изменениям право нашей страны, быстрое развитие общественных отношений в информационной сфере, разработка и совершенствование информационных технологий протекает намного быстрее, чем развитие правовых норм, которые регулируют информационную сферу.

Вследствие этого возникает потребность формирования на правовое сознание студентов, которые правильно будут воспринимать изменения, направленные на создание информационного общества. И это первостепенная задача по формированию правосознания современного юриста.

Провозглашение в Российской Федерации развития информационного общества и, как следствие, начавшийся процесс активного внедрения информационных и телекоммуникационных технологий, являющихся инструментом отражения действительности, оказывает некоторые негативные воздействия на правовую культуру.

Негативная сторона заключается в том, что информационные технологии стали активно использоваться представителями преступного круга для совершения различных преступлений, вовлекая в свою деятельность новых членов современного общества. Чтобы как-то снизить уровень влияния неблагоприятных факторов, вызывающих искажение правосознания, необходимо усилить контроль со стороны государства за распространением общественно-опасной информации в информационных технологиях. Несмотря на то, что государство предприняло попытки усиления контроля над распространением общественно-опасной информации этот вопрос остается актуальным.

Подводя итоги можно сказать, что образование новых общественных отношений, которые возникают во взаимосвязи с информационными технологиями, ведет к улучшению современной правовой культуры.

Выступая источником двухстороннего контакта между обществом и государством, информационные технологии осведомляют общество и деятельность политических и правовых институтов, властных структур о жизни общества и его реакции на их действия.

Информационные технологии выступают как наиболее действенный метод воздействия на формирование правого воспитания молодого поколения.

При внедрении информационных технологий в процесс преподавания юридических дисциплин повышается качество правового образования и уровень правосознания студентов.

Необходимо точно понимать, что являясь отражением реальной жизни, информационные технологии могут оказывать и разрушительное воздействие на правовую культуру.

Разработки и применения информационных технологий, создают подходящие условия для участия граждан в правотворческом процессе, управлении делами государства, наполняют действительно важной и актуальной правовой информацией российское информационное пространство, улучшают психологический настрой в обществе, помогают растить действительно активных граждан своей страны с высоким уровнем правосознания и правовой культуры.

Г.А. Алиева

ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова»

заведующая лабораторией криминалистики и специальной техники, старший преподаватель кафедры уголовного права и процесса

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ВЗЯТОЧНИЧЕСТВА И КОММЕРЧЕСКОГО ПОДКУПА В ЖКХ В СВЕТЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Группа преступлений в сфере ЖКХ, заявленная в теме настоящей статьи, характеризуется тем, что в настоящее время способ их совершения становится все более изощренным: привлекаются несколько посредников; незаконное вознаграждение выступает в качестве «откатов» от полученных бюджетных средств на капитальный ремонт, благоустройство и пр.; выводятся в оффшорные зоны и др. Средствами, благодаря которым реализуются такие схемы, выступают, в том числе, современные информационные технологии.

В связи с этим возникает объективная потребность следователя в использовании знаний сведущих лиц в области информационных технологий. Следственная практика показывает, что зачастую следователи прибегают к помощи специалистов экспертно-криминалистических подразделений МВД России, Института ЦСТ ФСБ России. Совместно с ними к участию привлекаются специалисты отделов документальных проверок и ревизий управлений экономической безопасности и противодействия коррупции управлений внутренних дел МВД России по субъектам РФ. Проведение ими исследований предметов и документов в данном случае имеет важное значение, так как по

современным преступлениям в сфере ЖКХ осуществляются сложные схемы приема - передачи предмета взятки или незаконного вознаграждения при коммерческом подкупе, при этом оформляются большое количество бухгалтерских, финансово-расчетных документов, осуществляется значительное количество банковских операций и пр., что маскирует преступную деятельность под правомерное осуществление должностным лицом или лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий.

Особенно необходимо привлекать специалистов к производству обысков в служебном кабинете, квартире подозреваемого, подсобных помещениях, гаражах, в квартирах его родных и близких лиц, их дачах и др., когда перед следователем стоит задача своевременного обнаружения, фиксации и изъятия объектов на электронных носителях, а также документов, имеющих признаки подделки, подчисток, дописок или травления; незаконно полученных документов; документов с содержанием недостоверных сведений; недействующих документов и т.д. Указанные признаки могут свидетельствовать о совершении должностным лицом или лицом, выполняющим управленческие функции в коммерческой или иной организации в сфере ЖКХ, определенных действий по подготовке, совершению и сокрытию преступления. Наряду с применением научно-технических средств, специалист сообщает следователю ориентирующую информацию об особенностях искомых объектов, которые возможно обнаружить в ходе производства обыска. Обычно, такими сведениями располагают специалисты, принимавшие участие в осмотре места происшествия по уголовному делу о взяточничестве или коммерческом подкупе в ЖКХ, так как у последних имелась возможность проанализировать механизм его совершения и условия следообразования.

При производстве выемки и обысков по уголовным делам рассматриваемой группы преступлений все чаще обнаруживаются объекты, квалифицированное описание и изъятие которых без специалистов не представляется возможным. К

таковым относятся как носители электронной информации [3] (стационарные компьютеры, планшеты, гаджеты, мобильные телефоны, внешние жесткие диски, видеорегистраторы и др.), так и неправомерно списанная уборочная, коммунальная, дорожная техника. Наряду с этим, проведенный автором опрос свидетельствует о том, что при расследовании взяточничества или коммерческого подкупа в ЖКХ 31% респондентов прибегали к помощи специалистов при осмотре документации, изъятой на электронных носителях, 6% – затрудняются ответить на данный вопрос, 53% опрошенных – не привлекали к участию лиц, обладающих специальными знаниями.

В свою очередь, привлечение специалистов помогает следователю определить особенности каждого из указанных объектов, функциональную часть, техническую документацию и т.д., способствует переносу хранящейся на электронных носителях информации на лазерные диски. Кроме того, при производстве данного следственного действия помощь специалиста будет выражаться в отборе объектов, которые будут использованы в качестве образцов для сравнительного исследования при назначении судебных экспертиз (фоноскопических, почерковедческих, технико-криминалистических и др.).

Следует отметить, что подготовка к передаче - получению предмета взятки или незаконного вознаграждения в ЖКХ может осуществляться с использованием информационных технологий (переписка в Интернет-сайтах, использование программ для мгновенного обмена сообщениями и др.). Кроме того, передача денежных средств может осуществляться посредством электронных платежных систем («Яндекс. Деньги», «Деньги@Mail.ru», «Webmoney», «Rapida», «PayPal», «Qiwi» и др.). При указанных обстоятельствах использование специальных знаний при расследовании данной группы преступлений в сфере ЖКХ возрастает.

Помощь специалиста также возможна и после получения заключения эксперта. Учитывая, что заключение эксперта является доказательством по

[3] См.: п. 3.1 ст. 183 Уголовно-процессуального кодекса РФ.

уголовному делу, полученным с использованием специальных знаний, оно представляет определенную сложность во всесторонней оценке для следователя. В связи с этим требуется помощь лица, обладающего соответствующими познаниями. Вместе с тем, результаты проведенного опроса показывают, что лишь 2 % респондентов привлекали специалистов для оценки заключения эксперта по уголовным делам о взяточничестве или коммерческом подкупе в ЖКХ.

Таким образом, подводя итог изложенному, можно сделать вывод о том, что без использования знаний сведущих лиц при расследовании взяточничества и коммерческого подкупа в сфере ЖКХ, следователю сложно разобраться в многоуровневых способах приема - передачи предмета взятки или незаконного вознаграждения при коммерческом подкупе, где преступники все чаще используют современные информационные технологии с целью подготовки и сокрытия следов преступления.

А.О. Анненкова
ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт
*Научный руководитель: **В.Ф. Изотова**, к.ф.-м.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПРАВОВЫЕ ОСНОВЫ БОРЬБЫ СО СПАМОМ

Развитие глобальных коммуникационных сетей привело к росту правонарушений совершаемых с их использованием. Среди них назойливые рекламные рассылки, так называемый спам, занимают не последнее место.

Рассылка рекламы при относительно малых затратах очень эффективна и постепенно превращается в серьезный бизнес. Но спам не так безобиден, как может показаться на первый взгляд. Спамеры, рассылая не запрошенную рекламу, нарушают правила распространения информации и ведения рекламной деятельности, уклоняются от уплаты налогов, что приводит к значительным материальным потерям и потерям рабочего времени.

Спам активно используется для совершения противоправных действий, например для рассылки вредоносных программ, ссылок на подставные сайты, с целью получения логинов и паролей и другой конфиденциальной информации для доступа, например, к банковским счетам. Такой вид мошенничества называется фишинг. По статистике доля спама в российских почтовых отправлениях в июле выросла до 60,98% и продолжала расти до 63,32% в сентябре[4].

В силу трансграничности Интернета спам является глобальной проблемой. По оценкам аналитиков в третьем квартале 2015 года в тройку лидеров среди стран – источников спама вошли: США (15,3%), Вьетнам (8,4%) и Китай (7,2%)». Во втором квартале 2015 Россия занимала второе место Россия (7,8%) доли спама.

[4] *Щербакова Т., Вергелис М., Демидова Н.* Спам и фишинг в третьем квартале 2015. URL: https://securelist.ru/analysis/spam-quarterly/27294/spam-i-fishing-v-tretem-kvartale-2015.

Спамеры в своих рассылках учитывают внимание пользователей к значимым событиям и сезонность интересов. Например, в дни летних каникул и сезон отпусков, рассылают поддельные уведомления от имени известных сервисов бронирования отелей и авиакомпаний, причем в такие письма, как правило, вложены архивы с вредоносными программами.

Эффективным средством технической защиты от спама считается метод автоматической фильтрации на основе черных и серых списков. Способ на основе серых списков основан на том, что почтовый сервер, ссылаясь на техническую ошибку, повторно запрашивает почтовое отправление. Реальный пользователь отправляет письмо еще раз, а спамерская программа нет. По оценкам специалистов только метод серых списков, позволяет отсеивать 90% спама, практически без риска потери «правильных» сообщений. Однако, преступники непрерывно совершенствуют технологии обхода спам-фильтра.

В Российской Федерации основными законами, регулирующими рассылку сообщений, являются Федеральные законы «О рекламе» и «О персональных данных». Федеральный закон «О рекламе», допускает рассылку рекламы «только при условии предварительного согласия абонента или адресата на получение рекламы». «Не допускается использование сетей электросвязи для распространения рекламы с применением… автоматического дозванивания, автоматической рассылки»[5]. Федеральный закон «О персональных данных»[6], определяет, что «обработка персональных данных в целях продвижения товаров, работ, услуг на рынке … допускается только при условии предварительного согласия субъекта персональных данных».

Понятие спама определено законодательно как «телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду

[5] Федеральный закон от 13 марта 2006 г. № 38-ФЗ (ред. от 28 декабря 2013 г.) «О рекламе» // Собрание законодательства РФ. 2006. 20 марта. № 12, ст. 1232.

[6] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изм. и доп., вступ. в силу с 1 сентября 2015 г.)// Собрание законодательства РФ. 2006. 31 июля. № 31, ч. 1, ст. 3451.

указания в нем несуществующего или фальсифицированного адреса отправителя»[7].

Государственный контроль над соблюдением ФЗ «О рекламе» возложен на Федеральную антимонопольную службу, которая не имеет ряда полномочий (работа с персональными данными, ограничение тайны переписки и др.) для решения возложенных на нее задач.

В судебной практике при рассмотрении дел о фишинге применяются следующие статьи: УК статью 272 «Неправомерный доступ к компьютерной информации», статью 273 «Создание, использование и распространение вредоносных компьютерных программ, так же статью 159 (мошенничество), которая подразумевает за собой наказание мошенничество в сфере компьютерной деятельности[9].

И хотя наблюдается рост судебной практики по искам, связанным с противодействием спаму, еще решены не все вопросы по правовому регулированию в этой сфере.

На наш взгляд, для эффективной борьбы со спамом следует законодательно возложить ответственность на заказчика спама за его распространение и разработать механизм оперативного предоставления информации антимонопольным органам операторами сотовой связи. Кроме того, каждый получатель спама, понесший материальный ущерб, должен обращаться в

[7] Постановление Правительства РФ от 10 сентября 2007 г. № 575 (ред. от 19 февраля 2015 г.) «Об утверждении Правил оказания телематических услуг связи» // Собрание законодательства РФ. 2007. 17

правоохранительные органы, поскольку без заявлений граждан у органов нет основания для проведения расследования.

сентября. № 38, ст. 4552.

[9] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) // Собрание законодательства РФ. 1996. 17 июня. № 25, ст. 2954.

А.А. Быкасов

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **П.В. Ересько**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

О ПРОБЛЕМНЫХ ВОПРОСАХ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

На сегодняшний день, передовые технологии внедряются учёными посредством успешных проектов и программ, реализуемых в самых различных сферах современного общества. Инновации, несомненно, способствуют улучшению качества жизни граждан, повышают эффективность труда и производства. Несмотря на все позитивные аспекты научно-технического прогресса, всё большую актуальность приобретает проблема появления видов преступлений, связанных с применением новейших технических средств и технологий. В связи с этим, институт судебно-экспертной деятельности в Российской Федерации выходит на передовые позиции по осуществлению активного противодействия преступности, используя современные технические

и криминалистические средства и методы в раскрытии, расследовании и предупреждении преступлений.

Судебная экспертиза играет важную роль при разрешении вопросов в процессе судопроизводства и как область практической деятельности представляет собой сложную систему разнородных элементов[8], в том числе: нормативного регулирования, статуса и функций субъектов деятельности, системы технических средств, научных основ, методов и методик проведения экспертных исследований. Столь сложная, динамически развивающаяся система не может существовать и развиваться без использования передовых технологий и инноваций. Особое место среди них занимают инновации в сфере информационных технологий. Освоение новейших информационных технологий является необходимостью повышения эффективности решения задач и качества проведения судебно-экспертных исследований. В частности, в сфере применения информации и компьютерных технологий необходима разработка оптимальных условий для удовлетворения информационных потребностей на основе создания и использования информационных ресурсов, оснащения новыми технологиями сбора, обработки и предоставления данных.

Вместе с тем, любой процесс, а именно, использование информационных технологий, не может происходить спонтанно. Он развивается в соответствии с правилами, определенными законами. Считаю необходимым создание эффективной правовой основы для полноценного обращения информации, а также для стимулирования использования новейших информационных технологий при решении задач судебно-экспертной деятельности и повышения эффективности работы экспертов и специалистов. Достижение указанной цели требует координации и согласованности правотворческой деятельности органов власти, её соответствия государственной политики РФ как в сфере совершенствования судебно-экспертной деятельности.

---

[8] *Россинская Е.Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. М., 2005.

Правовая основа информационных технологий находит своё отражение в обширных массивах нормативно-правовых актов и баз методических документов. Источниками юридического регулирования деятельности в сфере вышеуказанных технологий является, прежде всего, основной закон – Конституция РФ. Следом идут международно-правовые нормы, узкоспециализированные законы в сфере информации и информатизации, Указы Президента РФ, Постановления Правительства РФ, акты министерств и ведомств, а также иные нормативно-правовые акты, так или иначе затрагивающие деятельность информационных технологий. Правовые аспекты, регламентирующие использование информационных технологий, относятся к особой, интенсивно развивающейся отрасли современного права, так называемому информационному законодательству.

Согласно статье 71 Конституции, информация и связь находятся в ведении РФ, а статья 29 гласит – каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом[9]. Вопросы работы с информацией также затрагиваются в нормативных правовых актах, посвящённых отдельным сферам правового регулирования: гражданское, административное, уголовное, уголовнопроцессуальное, трудовое, налоговое законодательство РФ.

Если же говорить о законодательстве в области производства судебной экспертизы, сегодня остаётся нерешённым целый комплекс принципиально важных вопросов, связанных с правовыми и организационно-методическими проблемами внедрения и использования компьютерных технологий и вычислительной техники в экспертной практике. Заслуживает внимания точка зрения Е.Р. Россинской: информационное обеспечение судебно-экспертной деятельности законодатель понимает очень узко. Действительно, ФЗ ГСЭД, в частности, статья 9 раскрывает информационное обеспечение деятельности государственных судебно-экспертных учреждений только как возможность по запросам руководителей государственных судебно-экспертных учреждений

[9] Конституция Российской Федерации. М., 2015.

безвозмездного и беспрепятственного получения этими учреждениями образцов или каталогов продукции, технической и технологической документации и других информационных материалов, необходимых для производства судебной экспертизы, а также права ходатайствовать перед субъектом, назначившим экспертизу, о получении по окончании производства по делу предметов – вещественных доказательств для использования в экспертной, научной и учебно-методической деятельности[10].

Е.Р. Россинская считает, что кроме получения продукции, документации и других материалов информационное обеспечение должно подразумевать под собой ещё и информационные технологии, которые способствуют более качественному и эффективному решению экспертных задач. К таким стоит отнести компьютерные технологии, программное обеспечение, электронные ресурсы, базы данных и автоматизированные информационные системы.

Эксперт в своей профессиональной деятельности перерабатывает и использует большой объём сведений в разных областях знаний. Поэтому возникает целесообразность создания систематизированной базы, включающей нормативные документы, специальную литературу, научные труды, учебные пособия и другие источники, используемые при производстве судебных экспертиз. Данный вопрос является актуальным и может найти практическое отражение в разработке и внедрении баз данных и автоматизированных информационных систем, представляющих собой архивы источников сведений, ориентированных на решение задач судебно-экспертной деятельности с последующей их классификацией по видам экспертиз.

Автоматизированные информационные системы создаются с целью оптимизации деятельности и при должном создании правовой основы для полноценного обращения информации, указанные системы, способны значительно повысить эффективность работы эксперта или специалиста. Процесс внедрения и использования современного информационного

[10] Федеральный закон от 31 мая 2001 г. №73-ФЗ «О государственной судебно-экспертной деятельности в РФ» // Российская газета. 2001. 5 июня.

обеспечения и инновационных технологий, по моему мнению, позитивно влияет на работу по проведению подбора и поиска, интересующей эксперта информации. Обширный информационный массив баз данных, без существенных материальных и временных затрат, может использоваться сотрудниками экспертного учреждения, в целях оперативного проведения экспертных исследований.

Институту судебно-экспертной деятельности необходимо идти в ногу со временем и решать задачи, соответствующие духу современного мира, в связи с чем, считаю обязательным восполнять пробелы в законодательном уровне закрепить понятие и содержание информационного обеспечения деятельности государственных судебно-экспертных учреждений.

Я.С. Винокурова

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПОЛИТИЧЕСКАЯ РЕКЛАМА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В нашем современном мире, где развиты информационные технологии и настала новая эпоха – информационного общества, роль СМИ возросла. Это заметно проявляется в политических процессах, как в отдельных странах, так и в мире в целом. Средство массовой информации, выполняя ряд функций таких как: объединение, социализации интересов, критики и контроля, привлечения масс, СМИ имеют возможность влиять на формирование и развитие общественного представления. Поэтому степень влияния политической рекламы и средств массовой информации на политические процессы и на политику, в целом, является актуальным на сегодняшний день. Политическая реклама имеет два принципиальных отличия. Первое: ограниченное время рекламной кампании. Второе: на выборах главная цель – победа над конкурентами. Даже отставание на один голос сведет на нет все усилия рекламистов.

Целью работы является рассмотреть политическую рекламу как неотъемлемую часть в информационных технологиях.

Были поставлены следующие задачи: 1) выяснить, что такое политическая реклама; 2) рассмотреть примеры политической рекламы; 3) выявить влияние информационных технологий в политической рекламе.

Политическая реклама берет свое начало в далеком прошлом. Первые попытки развития в данном направлении было отмечено еще в Древней Греции и Древнем Риме, когда появились так называемые глашатые[11]. В их обязанности входило сообщать народу о положении государства, о войнах, и т.д. Так же глашатые, могли распространять о неприличных моментах из личной жизни конкурентов в политической сфере, об их тщеславии, низких моральных ценностях и др. Примером политической рекламы представленного периода может служить то, что были обнаружены надписи на стене в Помпее, призывающие голосовать за сенатора Марка Публия Фурия.

Что касается сегодняшнего времени, то полный расцвет политической рекламы в нашей стране пришёл с началом демократических выборов, с помощью которых изображали того или иного кандидата, с целью максимального воздействия на мнение и сознание электората.

Теперь хотелось бы разобраться в трактовке, что такое вообще политическая реклама, и в чем заключается её сущность. Политическая реклама – это реклама, направленная на изменение политического поведения общества или его части в условиях политического выбора[12].

У политической рекламы, как у любого другого социального явления, есть ряд задач, которые необходимы для функционирования. Во-первых, это раскрыть содержание политической программы, на которой основывается политический лидер. Во-вторых, необходимо определить содержание представленной политической силы. И наконец, в-третьих, самая важная, на мой взгляд, задача политической рекламы, это помочь не только электорату, но и спонсору выбрать своего кандидата. Что касается цели политической рекламы, то она заключается в привлечении общества в сферу политического

---

[11] Глашатай – в старину: вестник, всенародно объявляющий, возвещающий что-нибудь.

[12] Информационно-справочный портал. URL: http://adindustry.ru/doc/1133 (дата обращения: 05.11.2015).

взаимодействия, в побуждении к делегированию полномочий, в том числе к участию в выборах.

Политическая реклама, также имеет ряд функций, необходимых для политической сферы. Она является неким проводником между электоратом и кандидатами. Политическая реклама сообщает идеи, представления, характер, при этом фиксируя связь между государством и народом. Так она выполняет коммуникативную функцию. Другая не менее важная функция— это информационная, которая заключается в знакомстве электората с существующими партиями и её лидерами, их программами, идеями, с их характерными особенностями, одним словом сообщает необходимую информацию для народа и его выбора. Политической рекламе, как и самой политике свойственна конкуренция, поэтому ей необходимо выполнять и такую функцию как мировоззренческую.

Политическая реклама может быть выражена в разных формах. Неизменной и весьма распространенной формой политической рекламы является плакат. Он относительно недорог в производстве, сочетая визуальный образ и лаконичный текст, легко воспринимается и легко запоминается. Главные требования к политическому плакату те же, что и к коммерческому: броскость, понятность, лаконизм. Многословный текст не позволяет визуально быстро оценить контент плаката, ведь он должен быть охвачен с первого взгляда каждым прохожим, должен быть понят и запечатлен в памяти.

Из печатной политической рекламы самым распространенным видом является, конечно, листовка. В почтовых ящиках избирателей в зарубежных странах чуть ли не каждый день можно найти самые разнообразные политические листовки или «фолдеры» — складные листовки, как правило, многокрасочные, напечатанные на первоклассной бумаге. У нас этот вид политической рекламы тоже весьма распространен. Только качество их в большинстве своем низкое – скучный текст, плохое полиграфическое исполнение на плохой бумаге.

Рекламные щиты и транспаранты. Это прекрасные информационные носители имиджевых характеристик кандидата, так как на них может быть зафиксировано его изображение в наиболее привлекательном виде, соответствующем ценностям и симпатиям конкретного сегмента избирателей: среди семьи, на встрече с избирателями и т.д.

Реклама при помощи сети Интернет, в нашем современном мире только набирает свои обороты.

Проводимый мною опрос среди студентов нашей академии, выявил, что 76,9% опрашиваемых слышали о таком виде рекламы, как политический, а 65,4% респондентов посчитали телевизионную рекламу самой эффективной политической рекламой, так как телевизионная реклама во время важнейших политических событий в стране стала в России не только особой индустрией, но и мощным средством психологического воздействия на население.

Телевизионная реклама сильно потеснила политическую рекламу в газетах, прежде всего за счет динамики визуального образа, который не только имеет цвет и объем, но и находится в движении, что позволяет вниманию дольше фиксироваться на объекте. Безусловно, политическая реклама помогает электорату узнать своего кандидата, так ответили 80,8% опрашиваемых.

Поскольку в Российской Федерации агитацией признаются призывы голосовать за или против кандидата или прийти на выборы, содержание политический рекламы в ходе предвыборной кампании чаще всего использует одну из этих тем. Объем политической рекламы, используемой в ходе предвыборной кампании, ограничен косвенно – кандидат или партия не может потратить на политическую рекламу сумму, превышающую размер избирательного фонда, а размер этого фонда ограничен законодательно. Так же кандидат или список кандидатов (партия) должны уведомить избирательную комиссию о выпуске политической рекламы и предоставить образцы этой рекламы. Содержание политической рекламы, используемой в ходе выборов, определяется стратегией предвыборного штаба. На сегодняшний день самым эффективным инструментом управления как политической организацией в

целом, так и предвыборной кампанией, становятся информационные автоматизированные системы. Они представляют собой совокупность математических методов, технических средств и организационных комплексов, обеспечивающих рациональное управление работой политической структуры в соответствии с заданной целью. Как же использование таких систем повышает эффективность управления избирательной кампании? После принятия решения об участии в выборах, начинается процесс формирования штаба и проектирования предвыборной кампании. В рамках проектирования и управления избирательной кампании решаются следующие задачи: 1) создание, поддержание и развитие структуры управления избирательной кампанией; 2) управление разработкой, утверждение и необходимые корректировки стратегии, тактики и плана-графика кампании; 3) контроль исполнения графика мероприятий; 4) управление разработкой и реализацией спецпроектов; 5) контроль деятельности агитаторов и функционеров и т. д.

Разработка стратегии начинается с исследования предвыборной ситуации, определения конфигурации кампании и заканчивается определением агитационных тем кампании. Большинство данных собирается благодаря социологическим опросам, которыми занимаются социологические службы. Большинство из этих данных без глубокого анализа не представляют большой ценности для управленцев партии. Современные политические организации обладают стандартными программами для обработки данных, полученных в результате социальных опросов. К таким программам можно отнести: HTMLредакторы, например, MacromediaWeb (дизайн и программирование); текстовые редакторы – Microsoft Word (текст); табличные процессоры – Microsoft Excel (обработка числовых данных, статистические и экономические решения); системы управления базами данных: Microsoft Acces (учет ценности, сбор и обработка данных); статистические системы – SPSS, Statistika (статистическая обработка информации); векторные графические редакторы – AdobeIllustrator, CorelDraw (создание графики); растровая графика – Photoshop; 3D моделирование – 3DMax; Flash анимация – AdobeAfterEffects (создание

анимации и видео); создание мультимедиа презентаций – MicrosoftPowerPoint, MacromediaDirector и другие. Благодаря использованию специализированного программного обеспечения, данные об электорате, могут быть представлены с любой степенью детализации и легко проанализированы. Инструментарий, заложенный в автоматизированные системы управления избирательными кампаниями, должен позволять: комплексно анализировать данные о ходе кампании, круглосуточно контролировать ход кампании из любой точки мира через Интернет, прогнозировать результаты выборов и так далее.

Очень важной информацией в процессе разработки стратегии избирательной кампании являются сведения о предыдущих выборах, такие как, например, данные о влиянии проведенных спецпроектов на динамику рейтинга лидера партии и т. д. На сегодняшний день с помощью автоматизированных систем управления неплохо реализованы многие функции штаба предвыборной кампании, повышающие эффективность его работы и облегчающие её. Вот что содержат такие системы: гибкая система коммуникаций и документооборота между всеми сотрудниками; контроль ресурсообеспеченности мероприятий и проектов; обработка статистических данных; предоставление аналитических данных с любой степенью детализации: функционально-стоимостный анализ.

А теперь, переходя к конкретным примерам политической рекламы в России, хотелось бы рассмотреть пример президентских выборов 2012 года, и посмотреть, как и насколько эффективна была осуществлена политическая реклама. Хотелось бы начать с политической кампании Владимира Путина. Что касается его политической рекламы, то хочется отметить его предвыборные ролики, в которых отсутствует сам Путин. Среди тех, кто призывал голосовать, были как общественные деятели, спортсмены, артисты и так далее. Почему выбран был именно такой ход? Могу предположить, что это связано в первую очередь с тем, что людей общественной жизни знают, прислушиваются к их мнению, а это способствует к большому охвату электорального круга. Вовторых, такая реклама направлена на то, чтобы показать людям, насколько и как поддерживают люди культуры, спорта, искусства В.В. Путина. Также второй

ареной размещение политической рекламы Путина, стал сервис YouTube. Там была представлена не только целевая группа (пенсионеры, студенты, военнослужащие и пр.), но были даны обещания в разной сфере жизнедеятельности, были представлены результаты работы за четыре года, что, безусловно, являлось несомненным плюсом для электората. Поэтому рассматривая политическую рекламу В.В. Путина, хочется сказать следующее, что она наполнена прагматизмом, четкостью и лаконичностью, и все это, на мой взгляд, является примером хорошей политической рекламы.

Сравнивая политическую программу Путина с другими кандидатами выборов 2012 года, хотелось бы отметить Михаила Прохорова, который был таким неким Антипутиным, с лозунгом на политической рекламе, «Новый президент – Новая Россия». Анализируя его политическую программу, можно прийти к выводу, что это полная противоположность рекламе В.В. Путина. Вопервых, потому что она построена на юморе, хотя такой ход оправдан, поскольку электорат не старше 35 лет направлен на принятие таких своеобразных идей. Во-вторых, такая реклама выделяет кандидата от других, и добавляет симпатии от тех, кто уже устал от действующих лиц. И можно сделать вывод, что такая политическая реклама направлена на создание идеального образа для электората. Сравнивая политическую рекламу В.В. Путина и М. Прохорова, можно выявить существенные различия. Так реклама первого, в виду своей лаконичности, направлена на достижение нужного результата, путем правдивых обещаний. В то время как реклама второго кандидата не смогла реализовать стратегию пропаганды своих идей.

Другим кандидатом был Г.А. Зюганов, чья политическая реклама была направлена на развитие ассоциаций в сознании человека с символами граждан. Целью такой рекламы было не донести что-то новое, а наоборот обращаться к тем доводам и фактам, которые уже есть в сознании граждан. Видеоролик, который, безусловно, можно считать одним из видов политической рекламы, был снят в стиле голливудских фильмов, где Г. Зюганов был «главным героем блокбастера». Это помогло показать кандидата с новой стороны. Но, анализируя

данную деятельность, могу сказать, что это скорее та политическая реклама, которая будет интересна молодому поколению, нежели людям уже старшего возраста.

Еще одним ярким кандидатом президентских выборов 2012 года, был Владимир Жириновский,. чья политическая реклама является довольно интересной, поскольку проходила в двух разных формах. Первая более жесткая, которая направлена на укрепление русского этноса, справедливого положения в стране. И вторая — мягкая, которая была направлена на тех, кто хотел голосовать больше не за идею данного представителя, а за шанс выразить свое негодование к существующей власти. В политической рекламе
В. Жириновского присутствует запугивание граждан тем, что будет хуже, а с другой стороны, – правильное позиционирование в отношении власти, подстраивание. «Лидер ЛДПР берет за основу лозунги, которые позволяют ему, с одной стороны не сталкиваться с властью, а с другой, – выглядеть оппозиционным кандидатом»[13]. И, на мой взгляд, политическая реклама В. Жириновского полностью соответствует образу самого кандидата, так как показывает не только его идеи и мысли, но и его саму личность в целом.

И наконец, Сергей Миронов, последний представитель, чью политическую рекламу хотелось бы рассмотреть. Реклама данного кандидата была практически незаметна, размещалась в основном только на официальном сайте «Справедливая Россия». Его реклама была направлена на то, чтобы дать понять чиновникам, как живут обычные люди. То есть нагонялся страх и отчаяние о том, как живет простой народ. Поэтому можно сделать вывод, что данная политическая реклама была направлена на тот электоральный круг, который не был доволен деятельностью партии «Единая Россия».

Таким образом, сравнивая политические рекламы выше перечисленных кандидатов, хочется сделать вывод, что более яркой и выразительной рекламой

---

[13] *Саитова Н.Н.* Динамика современной политической рекламы в России на материале президентских выборов в 2012 году // Пробелы в российском законодательстве. 2013. № 2. URL: URL: http://cyberleninka.ru/article/n/dinamika-sovremennoy-politicheskoy-reklamy-v-rossii-na-materiale-prezidentskihvyborov-v-2012-godu (дата обращения: 08.03.2016). [16] Там же.

была реклама В.В. Путина, которая, безусловно, обошла по интенсивности своих конкурентов. Поэтому проводя анализ политической рекламы кандидатов, хотелось бы напомнить итоги президентских выборов России в 2012 году: «В.В. Путин – 63,60%; Г.А. Зюганов – 17,18%; М.Д. Прохоров – 7,98%; В.В. Жириновский – 6,22%; С.М. Миронов – 3,85%»[16]. Поэтому, безусловно, политическая реклама играет важную роль в избирательной кампании нашей страны.

А сейчас бы хотела рассмотреть, как действует политическая реклама в США, и какое влияние оказывает на граждан этой державы. Рассматривая эффективность политической рекламы в США, хотелось бы обраться к президентским выборам 2012 года. На двух ярких кандидатах выявить специфику политической рекламе в США.

Один из кандидатов президентских выборов, Барак Обама, баллотировался на второй срок от демократической партии. Политическая реклама была направлена на его личность, для того, чтобы могли сравнить Обаму с другими выдающимися американскими политиками, например с Джоном Кеннеди. Основной площадкой распространения рекламы, будущий президент выбрал Интернет. Целью такого хода было сплотить американцев снизу, для этого он отказался от масштабных реклам на телевидении, мероприятий, а стал использовать социальные сети для дискуссий. Такие как Facebook, MySpace, YouTube, Twitter и др. Особый вклад в распространении политической рекламы Обамы, внесли интернет-блоги, там, где будущий президент мог общаться со своим электоратом, к тому же простые названия статьи, к примеру «Обама нормальный парень» играли немаловажную роль в избирательной кампании 44го президента США. На YouTube у Барака работал предвыборный канал, где были выложены видеоматериалы, некоторые даже с участием звезд, что непременно послужило росту просмотра данных роликов. На мой взгляд, такой вид политической рекламы, в связи с информационным развитием является достаточно эффективным среди населения. В связи с этим, можно проследить следующую закономерность: в результате распространения данной рекламы на

страничку Барака Обамы в социальной сети Facebook подписывалось ежедневно большое количество людей, и в результате эта цифра дошла до 790 тыс. человек. Сегодня это число намного превышает 35,5 млн. человек. Поэтому обобщая проведенную политическую рекламу Барака Обамы можно сделать вывод о том, что благодаря активному использованию Интернетресурсов, отказ от использования бюджетных средств для предвыборной кампании и привело к такому бурному успеху кампании Обамы и его победе на выборах 2012 года.

Таким образом, политическая реклама имеет ряд специфических особенностей. Одна из основных ее особенностей – это массовость целевой аудитории. Это, в свою очередь, означает, что методы воздействия должны быть таковы, чтобы как можно больше людей восприняло бы информацию наилучшим (для заказчика, конечно) образом. Именно здесь и приходит осознание того, что без психологической науки в целом и без определения понятия восприятия в частности, мы не сможем разобраться в этом вопросе.

Политическая реклама в российских избирательных кампаниях следующая:

1) Сейчас широко используется Интернет, создание сайтов и интернетрекламы программ.

2) Почтовая рассылка – она успешно использовалась ещё в 1991 г.

3) Благотворительные акции и кампании – очень эффективный способ институциональной рекламы.

4) Привлечение людей, которые восхваляют кандидата – «свидетельство».

5) Плакаты и листовки – начали успешно использоваться ещё со времён революции 1917 г.

Политическая реклама нужна, чтобы имя кандидата везде узнавали; чтобы его программа была популярна, и все проблемы обсуждались; был хороший имидж.

Политическая реклама использует эмоционально-психологические методы воздействия на людей. Самый основной инструмент политической рекламы в

избирательной кампании – это возможность манипулировать политическим восприятием человека.

Хотелось обратиться и к проводимому мною опросу. Всего было составлено 5 вопросов, а опрашиваемых составляло 26 человек. Опрос был проведен при помощи Интернета, который помог в короткий срок провести опрос не только среди своей группы, но и среди других факультетов Саратовской государственной юридической академии. И теперь, в виде заключения, хочу представить следующие результаты, к которым я уже обращалась ранее.

На вопрос: «Слышали ли Вы о такой рекламе, как "политическая реклама"?», большинство моих опрошенных ответили, да, и это составило 76,9%. По мнению, студентов нашей академии, самой эффективной политической рекламой является телевизионная реклама, так ответили 65,4%, на втором месте реклама при помощи сети Интернет, что составило 23,1%. Политическая реклама, безусловно, помогает узнать кандидата, и со мной согласилось 80,8%, видимо, поэтому большинство и считают, что политическая реклама в России достаточно развита, так ответили 57,7% опрашиваемых.

Таким образом, рейтинг того или иного кандидата или же партии непременно зависит от эффективности выбранной PR-политики, а также эффективности использования в качестве инструментов её проведения средств массовой информации.

Список использованной литературы и источников

1. *Егорова-Гантман Е., Плешаков К.* Политическая реклама. М.: Центр политического консультирования «Никколо М», 1999.
2. *Лисовский С.Ф.* Политическая реклама. М.: ИВЦ «Маркетинг», 2000.
3. *Жукова Н.А.* Сравнительный анализ роли СМИ в политическом процессе России и США: автореф. … дис. канд. полит. наук. М., 2008. URL: http://pandia.ru/text/79/355/32909.php (дата обращения: 05.11.2015).
4. *Феофанов О.А.* США: Реклама и общество. М.: Мысль, 1974. URL: http://mssdelka.ru/_ld/2/209_b993972a5b50cf3.htm (дата обращения: 20.02.2016).

5. *Гомеров И.Н.* Человек в поле политики: лекция, 2012 http://lib.sale/politologiya_uchebnik/chelovek-pole-politiki.html (дата обращения: 25.02.2016).

6. Интернет-ресурс. Информационно-справочный портал. http://adindustry.ru/doc/1133 (дата обращения: 05.11.2015).

7. Интернет-ресурс. Библифонд. Специфика современной политической рекламы. URL: http://bibliofond.ru/view.aspx?id=659184 (дата обращения: 07.11.2015).

8. Caricatura Napoleonica СПб.: Альфарет, 2012. URL: http://alfaret.ru/item.php?prod=1417&subid=1&catid (дата обращения: 02.02.2016).

9. Идеология России. Политическая реклама. URL: http://newideology.ru/slovar/p/politicheskaya-reklama/ (дата обращения: 15.02.2016).

10. Служба новостей «URA.Ru». URL: http://ura.ru/svrd (дата обращения: 03.03.2016).

11. Выборы депутатов в Госдуму. URL: http://2016-god.com/vybory-deputatovv-gosdumu-v-2016-godu/ (дата обращения: 05.03.2016).

12. *Феофанов О.А.* Реклама. Новые технологии в России. URL: http://alexskaj.ru/rntr/zrnrr.html (дата обращения: 05.03.2016).

13. *Саитова Н.Н.* Динамика современной политической рекламы в России на материале президентских выборов в 2012 году // Пробелы в российском законодательстве. 2013. № 2. URL: http://cyberleninka.ru/article/n/dinamikasovremennoy-politicheskoy-reklamy-v-rossii-na-materiale-prezidentskih-vyborov-v2012-godu (дата обращения: 08.03.2016).

14. Использование политических технологий в предвыборной кампании Барака Обамы в 2012 году. URL: http://www.lawinrussia.ru/node/297868 (дата обращения: 22.03.16).

15. Ансар. РБК. 09. 10.11. URL: http://www.ansar.ru/world/2011/10/09/22570?print (дата обращения: 22.03.16).

16. Результаты президентских выборов в США 2012 года. URL: http://intermediaexpert.ru/2016/01/11/rezultati-prezidentskih-viborov-v-ssha-2012goda/ (дата обращения: 22.03.16).

К.С. Волкова, Ю.В. Терехова

ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» *Научный руководитель:* ***О.А. Иванова****, к.ю.н., доцент кафедры публичного права ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова»*

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И НРАВСТВЕННО-ЭТИЧЕСКИЕ ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ И ИНСТИТУТОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

На современном этапе развития общества, средства массовой информации (далее – СМИ) являются одним из важнейших социальных и политических институтов. СМИ играют важную роль в формировании сознания и мышления людей, выполняют функцию агента социализации человека. СМИ являются мощнейшим фактором воздействия на правотворческую и правоприменительную деятельность государства. Недаром СМИ называют «четвертой ветвью власти».[14] Общественное мнение также является фактором, который может оказать воздействие на правотворчество. Если государство при издании нормативно-правовых актов не будет считаться с общественным мнением, то не сможет эффективно регулировать значимые на определенном этапе общественные отношения, а, следовательно, утратит авторитет и способность управлять. Логично, что наиболее распространенным способом выражения общественного мнения являются СМИ и Интернет, а потому изучение влияния общественного мнения и СМИ в совокупности на правотворческий процесс видится достаточно оправданным и значимым.

С появление прессы (XVII-XVIII вв.) СМИ становятся активными и непоколебимыми участниками политического процесса. Первые президентские дебаты, транслируемые по телевидению, прошли в 1960 году. Сенсационная победа на президентских выборах в США малоизвестного тогда сенатора Джона

[14] *Дегтярев А.А.* Основы политической теории: учебное пособие. М., 2010. С. 239.

Кеннеди над вице-президентом страны Ричардом Никсоном была сразу же зачислена в актив телевидения, транслировавшего дебаты. «Вера во всемогущество телевидения настолько велика, что, по мнению иных политических деятелей, тот, кто контролирует телевидение, контролирует всю страну»[15].

Настоящее время отличается от прошлого: здесь правит техника и товаром выступает информация. Недаром же говорят, что XXI век –век информационных технологий. Информация стала «сырьем», основой для принятия решений, инструментом контроля в политической и в экономической сферах жизни общества. Сегодня информация дает небывалый успех или беспощадно губит, а тот, кто ею владеет, тот владеет миром[16]. Примером этому может служить изобретение информационного оружия, гораздо более сильного, чем оружие массового поражения.

В настоящее время СМИ превращаются в один из важнейших инструментов реализации политического процесса. В современной политической науке СМИ «наградили» такими титулами, как великий арбитр, четвертая ветвь власти – наряду с законодательной, исполнительной и судебной[17].

СМИ должны быть и развиваться независимо как с экономической, так и политической точки зрения. В большинстве индустриально развитых стран СМИ представляют собой частнопредпринимательский институт. Критика СМИ отличается широтой или даже неограниченностью своего объекта, который составляют и президент, и правительство, и суд, и различные направления государственной политики, и сами СМИ. Хотя СМИ не могут применять санкции к нарушителям, их контроль часто более эффективен и даже более строг. Часто стремящиеся «взорвать бомбы» журналисты, раскрывают одновременно коррупцию, должностные злоупотребления, обман избирателей и падение политической морали в коридорах власти.

---

[15] *Горбачёва О.М.* Информационно-манипулятивные технологии в политических процессах современной России (на примере избирательных кампаний): дис. … канд. полит. наук. М., 2004. С. 148.

[16] *Поляков. Ю.М.* Сборник цитат и афоризмов. М., 2010. С. 35.

[17] *Дегтярев А.А.* Основы политической теории: учебное пособие. М., 2010. С. 209.

СМИ представляют собой сложный многогранный институт. Нужно добавить еще одну важнейшую функцию – политической социализации населения. Пресса, радио, телевидение претендуют на выполнение функции «сторожевой собаки общественных интересов», на то, чтобы быть «глазами и ушами общества», предупреждая, например, о спаде в экономике, росте наркомании, преступности и т.д. Для оправдания такого имиджа СМИ должны быть и выглядеть максимально независимыми как с экономической, так и с политической точки зрения.

В настоящее время именно СМИ выступают важнейшей составляющей в системе реализации государственной информационной политики, позволяющей регулировать процессы информационного взаимодействия в различных сферах общественной жизни и государства. Мнения общества становится более действенным регулятором политического процесса. СМИ не только отражают сложившиеся настроения, но и формируют общественное мнение.

Информационная сфера становится одним из важнейших объектов государственного управления. Взаимоотношения власти и СМИ осуществляются пресс-службами, созданными при органах государственной власти. Главной формой информационного взаимоотношения органов власти и СМИ является диалог. СМИ оперативно освещая работу органов власти, выступает посредником между обществом и государством. В настоящее время, когда будущая власть определяется общественностью, деятельности, как средства формирования общественного мнения, становится решающей. Лояльные СМИ становятся для государства одним из факторов долголетия и стабильности[18].

Нормативной основой взаимодействий органов власти и СМИ в форме диалога является: Конституция, Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 (ред. от 30 декабря 2015 г.) «О средствах массовой информации»[19], Федеральный закон от 13 января 1995 г. № 7-ФЗ (ред. от 12 марта 2014 г.) «О

[18] *Леонтьева Л.С.* Государственное управление информационными процессами. Казань, 2008. С. 124.

[19] Рос. газета. 1992. № 32; Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 30.12.2015). [23] Российская газета. 1995. № 9-10.

порядке освещения деятельности органов государственной власти в государственных СМИ»[23].

Так, гарантируется свобода массовой информации, обеспечивается открытость и публичность органов государственной власти пред СМИ, например, пресс-службы федеральных органов государственной власти ведут аудио- и видеозапись всех официальных мероприятий с участием Президента Российской Федерации, заседаний Совета Федерации и Государственной Думы, Правительства Российской Федерации и его Президиума[20]. Стоит принять во внимание тот факт, что многие российские политические деятели являются активными пользователями Интернета и имеют свои блоги в таких социальных сетях, как Twitter, Instagram, Вконтакте. Среди них Дмитрий Рогозин, Сергей Миронов, Дмитрий Медведев, Владимир Жириновский, Борис Грызлов, Татьяна Голикова. Даже органы государственной власти имеют свои официальные «страницы» в социальных сетях: МИД РФ, МЧС РФ, ФАС РФ, Минобороны России.

Не допускается цензура, а именно цензура массовой информации, то есть требование от редакции СМИ со стороны должностных лиц, госорганов, учреждений, организаций или общественных объединений предварительно согласовывать сообщения и материалы, а равно наложение запрета на распространение сообщений и материалов, их отдельных частей, – не допускается[21].

Реализуется стратегия в сфере СМИ, которая решает задачу предупреждения угроз, возникающих в информационном обществе, в частности недопущение распространения запрещенной и противоречащей приоритетам развития России информации. Также задачи обеспечения доступа граждан и

---

[20] Федеральный закон от 13 января 1995 г. № 7 «О порядке освещения деятельности органов государственной власти в государственных СМИ» // Российская газета. 2010. 18 июня.

[21] Закон РФ от 27 декабря 1991 г. № 2124-1 (в ред. от 13 июля 2015 г.) «О средствах массовой информации» // Российская газета. 1991. 28 декабря.

организаций к услугам на основе информационных технологий в частности обеспечения права на информацию[22].

Изучение психологического портрета общества облегчает процесс манипулирования общественным сознанием. Именно манипулирование является одной из основных целей воздействия СМИ. Картина мира после такого воздействия будет уже скорректированной с учётом целей манипуляции[23].

Такую тенденцию можно проследить в следующей ситуации: в столице Франции Париже ночью 14 ноября произошли 6 терактов, погибли 129 человек, около 180 пострадали. В стране был введен режим чрезвычайного положения.

По словам очевидцев, нападавшие заявляли о намерении отомстить за кампанию в Сирии. Пользователи социальных сетей, известные интернетблоггеры мирового уровня, мировые государственные деятели после первых сообщений о терактах в своих интернет-страницах ставят на обложку фразу JesuisParis («Я Париж») или PrayforParis («Молюсь за Париж») делятся картинками с этими словами. Но: почему, когда самолет российской авиакомпании «Когалымавиа», выполнявшего рейс из Египта в СанктПетербург, упал при «еще неизвестных обстоятельствах», когда 224 человека погибли, никто не молился за Санкт-Петербург? Эта ужасная катастрофа стала неким тестом на человечность и отношение к России. Наряду с официальными соболезнованиями, которые приходили со всех концов мира, от руководителей иностранных государств и простых людей в адрес руководства РФ и родственников пассажиров рейса, Запад постарался максимально не заметить трагедию, в результате которой погибло 224 человека. Скупые заметки западных СМИ соседствуют с масштабным освещением Хэллоуина.

Сирийский лидер Башар Асад на наш взгляд, очень достойно и правильно выразил свое мнение на счет сложившийся ситуации в мире. «Безусловно, это страшная трагедия в Париже, но это происходит в Сирии уже 5 лет. Каждый день

---

[22] Распоряжение Правительства РФ от 20 октября 2010 г. «О государственной программе РФ "Информационное общество 2011-2020 годы"» // Российская газета. 2013. 26 июля.

[23] *Кара-Мурза С.* Манипуляция сознанием. М., 2000. С. 48.

там погибают сотни людей. Их взрывают, казнят, насилуют… И в Ливии еще дольше, и в Ираке, и в Афганистане. Жизнь французов ценнее жизни сирийцев, ливийцев, иракцев или афганцев? Что за истерии в соцсетях: флаги, слезы, причитания… Где же вы раньше были со своей вселенской скорбью?
Вот недавно казнили двести детей! Что молчали, причитатели?»[28]. Невыгодные факты составляют малую часть повестки дня, либо вообще о них никто предпочитает не вспоминать.

Почти всегда искаженная информация используется вместе с соответствующим способом подачи. Здесь стоит отметить такие приемы как умолчание, привлечение авторитетного посредника.

Такими примерами изобилует СМИ Украины. Например, умолчание – суть приема в том, что «невыгодная» информация изымается. 2 марта 2014 года, в своем видеообращении к украинскому народу известный политический и государственный деятель Украины, руководитель партии «Всеукраинское объединение „Батькивщина“, на тот момент кандидат в президенты Ю.В. Тимошенко напоминает гражданам Украины: «в 1994 году Украина подписала Будапештский меморандум с Великобританией, США и Россией… и, объявляя войну нам, Путин объявляет ее Великобритании и США». Однако Тимошенко забывает упомянуть, что документ так и не был ратифицирован ни одной из сторон.

Следующий прием – привлечение авторитетного источника, чаще всего привлекаются «народные кумиры». Это видные деятели искусства, культуры, кино, театра и спорта, которых обычный человек смотрит каждый день по телевизору или за которых «болеет» на спортивных соревнованиях. В качестве примера можно привести запущенную украинскими журналистами «утку» – осуждение захвата Крыма актером В. Золотухиным. Так называемый украинскими официальными лицами, «захват» Крыма Россией произошел в марте 2014 года. Журналисты даже не удосужились выяснить, что актер и народный артист РСФСР умер 30 марта 2013 г.

Таким образом, общественное мнение играет значительную роль в развитии жизни и направляет деятельность социальных институтов, в том числе СМИ. Однако, СМИ стараются освещать актуальные для общества проблемы и во многом рассматривают их с точки зрения общественного мнения, можно

[28] Российская газета: интернет издание. URL: http://www.rg.ru/interviews/2061.html (дата обращения: 20.03.2016).

сделать вывод, что не только общественное мнение может направлять деятельность СМИ, но и само общественное мнение формируется под воздействием различных факторов, в частности, СМИ, например, через распространение идеологии и пропаганды.

Сегодня происходит развитие всех сфер общественной жизни общества. Это развитие носит противоречивый характер. Не являются исключением взаимоотношения СМИ и органов власти. Суть конфликта состоит в наличие между СМИ и органами власти разногласий по поводу принимаемых решений и попыток убедить общество в своей правоте. СМИ могут представлять интересы государства либо выражать интересы политических кругов, стремящихся к власти. При этом противостояние может выглядеть не как борьба власти и оппозиции, а как конфликт органов власти и СМИ, которые стремятся к отображению истинной ситуации.

В ходе исследования нами были получены следующие выводы.

1. Российская действительность последнего десятилетия отчетливо показала, что не может быть подлинной демократии в стране без сильного и авторитетного парламента и свободной прессы. Объективная, непредвзятая информация о деятельности российского парламента в СМИ способна сохранить баланс интересов в изменяющейся политической действительности.

2. СМИ стараются освещать актуальные для общества проблемы и во многом рассматривают их с точки зрения общественного мнения. Таким образом, не только общественное мнение может направлять деятельность СМИ, но и общественное мнение формируется под воздействием СМИ, например, через распространение идеологии и пропаганды.

3. СМИ представляют собой сложный многогранный институт, состоящий из множества элементов, информирующих население о происходящих в мире явлениях. Основными функциями СМИ должны быть: сбор и распространение информации; отбор и комментирование информации; формирование общественного мнения; распространение культуры, политическая социализация населения.

4. Государственная власть заинтересована не только в информировании общества о своих правотворческих и правоприменительных действиях, но и в привлечении граждан к участию в правотворческом процессе, общественному контролю за правоприменением. Вовлечение граждан в эти процессы возлагается на институты гражданского общества, в числе которых свободные
СМИ.

5. Нормой взаимоотношений гражданского общества и власти должен стать конструктивный диалог, направленный на решение существующих и предупреждение возникновения новых социальных проблем. В настоящее время именно СМИ выступают важнейшей составляющей в системе реализации государственной информационной политики, позволяющей регулировать процессы информационного взаимодействия в различных сферах общественной жизни и государства.

Д.С. Герцен
ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт
*Научный руководитель: **В.Ф. Изотова**, к.ф.-м.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПРИЗНАНИЕ ИНОСТРАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Бурное развитие информационных коммуникационных технологий в конце двадцатого века, формирование глобального информационного пространства стимулировало международный обмен электронными документами.

Законодательной основой электронного информационного обмена в Российской Федерации стал ряд федеральных законов, в первую очередь ФЗ «Об участии в международном информационном обмене»[24], ФЗ «Об информации, информатизации и защите информации»[25] и ФЗ «Об электронной цифровой подписи»[26]. Трудно переоценить значение данных нормативных актов для вступления России в единое глобальное информационное пространстве.

Закон об информации и информатизации определил ключевые понятия в сфере информационного обмена, в частности информационных ресурсов, заложил основы их правового режима, определил роль государства в развитии информатизации, информационных технологий и защиты информации.

Закон о международном информационном обмене создал условия для эффективного участия России обмене информацией в рамках глобального пространства. Провозгласил в качестве главного приоритета защиту интересов государства и его граждан при международном информационном обмене.

Основой организации эффективного электронного документооборота между государствами стал закон «Об ЭЦП». Было законодательно закреплено

[24] Федеральный закон от 4 июля 1996 г. № 85-ФЗ (ред. от 29 июня 2004 г.) «Об участии в международном информационном обмене»// Собрание законодательства РФ. 1996. 8 июля. № 28, ст. 3347.

[25] Федеральный закон от 20 февраля 1995 г. № 24-ФЗ (ред. от 10 января 2003 г.) «Об информации, информатизации и защите информации» // Собрание законодательства РФ. 1995. 20 февраля. № 8, ст. 609.

[26] Федеральный закон от 10 января 2002 г. № 1-ФЗ (ред. от 8 ноября 2007 г.) «Об электронной цифровой подписи»// Собрание законодательства РФ. 2002. 14 января. № 2, ст. 127.

понятие электронного документа, как документа, «в котором информация представлена в электронно-цифровом виде». Определено условие признания его юридической силы – заверение его электронной цифровой подписью (ЭЦП). Разработаны условия использования ЭЦП, в том числе и в международном информационном обмене.

Но если говорить об обмене электронными документами между государствами разной юрисдикции, то очевидно возникает вопрос доверия иностранной цифровой подписи. Разные государства решают этот вопрос поразному.

Где-то требуется обязательная или добровольная аккредитация в своей юрисдикции иностранных удостоверяющих центров (УЦ), выдающих сертификат ключа подписи. Например, в ЕС признание ЭЦП осуществляется в рамках межгосударственных соглашений. В некоторых случаях резидентный УЦ государства может поручиться за достоверность иностранной ЭЦП. Иногда допускается безоговорочное признание сертификата ключа подписи.

В Федеральном законе «Об ЭЦП» сказано, что сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, признается на территории Российской Федерации в случае выполнения процедур признания юридического значения иностранных документов, установленных законодательством Российской Федерации. Однако данные процедуры в Законе об ЭЦП и других подзаконных актах разработаны не были.

Таким образом, законодательно было определено, что в России признается иностранный сертификат ключа подписи, но разработанная на должном уровне процедура признания так и не появилась. Возможно, этот факт определил низкую эффективность законодательства, регулирующего ЭЦП, которую отмечают некоторые авторы[27]. Что подтверждается слабым распространением ЭЦП: за пять лет с момента принятия закона об электронной цифровой подписи лишь 0,2%

[27] *Кирилловых А.А.* Правовые аспекты механизма электронного взаимодействия в законодательстве об электронной подписи // Адвокат. 2011. № 11.

населения нашей страны имели сертификаты ЭЦП. В то время как в Европе усиленные электронные подписи использовало около 70% населения.

Дело в том, что информационный обмен в странах Евросоюза регулируется Директивой ЕС об электронных подписях 1999/93/ЕС[28][29], в которой прописана вся процедура сертификации иностранных электронных подписей. Данная Директива признает сертификат, выданный провайдером сертификационных услуг стран, не входящих в ЕС, в следующих трех случаях: в случае добровольной аккредитации провайдера в одной из стран ЕС; гарантии провайдера, утвержденного в рамках ЕС; наличия международного соглашения между ЕС и третьими странами.

В качестве основы для национальных законов регулирующих отношения в области использования электронных подписей во многих странах используется типовой закон ЮНСИТРАЛ, в котором признается иностранный сертификат при условии сходного уровня надежности с учетом признанных международных стандартов об электронных подписях.

Формирование единой информационной системы России, активное внедрение технологий электронного государства в деятельность государственных органов и органов муниципального самоуправления в середине первого десятилетия двадцать первого века было призвано повысить эффективность управления государством и оказания государственных услуг населению. Этот процесс потребовал дальнейшего совершенствования законодательства в информационной сфере и принятия нового Федерального закона «Об электронной подписи»[30], который учитывал бы международный опыт в этой сфере.

Федеральный закон «Об электронной подписи» регулирует отношения в области использования электронных подписей при совершении гражданскоправовых сделок, оказании государственных и муниципальных

[28] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUN CIL of 13 December [29] on a Community framework for electronic signatures.

[30] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) «Об электронной подписи» // Собрание законодательства РФ. 2011. 11 апреля. № 15, ст. 2036.

услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Данным законом введены три(?) вида электронных подписей: простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись. Юридическую силу электронному документу придает без дополнительных соглашений только квалифицированная электронная подпись.

Согласно закону в Российской Федерации иностранные электронные подписи, созданные в соответствии с международным стандартом признаются подписями того вида, признакам которого они соответствуют.

Признание иностранных электронных подписей и легализация возможности их использования является, несомненно, одним из важных достоинств Закона об Электронной подписи и открывает большие возможности для развития международного обмена электронными документами на территории Российской Федерации.

Ю.С. Гладилкина, К.Ю. Меркурьева

ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал

*Научный руководитель: **И.А. Кузнецова**, к.ю.н., доцент кафедры гражданско-правовых дисциплин во Владимирском филиале ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»*

ПРАВОВАЯ ИНФОРМАТИЗАЦИЯ КАК ОДИН ИЗ СПОСОБОВ ПОВЫШЕНИЯ УРОВНЯ ПРАВОВОЙ КУЛЬТУРЫ ГРАЖДАН В СОВРЕМЕННОЙ РОССИИ

В наше время одной из актуальных проблем России, как демократического и правового государства является повышение уровня правой культуры граждан и создание единого информационного правового пространства.

Для того чтобы попытаться решить поставленную перед нами проблему (повышение уровня правовой культуры граждан), необходимо как можно точно и четко определить понятие информатизации в целом. В России первым, кто стал применять данный термин, был А.И. Ракитов в 1987 году. Под информатизацией он понимал «процесс, в котором технологические, социальные, политические, экономические и культурные механизмы не просто взаимодействуют, а буквально соединены воедино в целях прогрессивно возрастающего использования информационных технологий для формирования, производства, использования, переработки, распространения и хранения информации»[31].

Под информатизацией, в широком смысле, понимается реализация комплекса мер, направленных на обеспечение полного и своевременного использования достоверных знаний во всех общественно значимых видах человеческой деятельности. В более узком смысле под информатизацией понимается процесс создания, развития и всеобщего применения информационных средств и технологий, обеспечивающих достижение и поддержание уровня информированности всех членов общества, и достаточного для кардинального улучшения качества труда и условий жизни общества[32].

Правовая информатизация – процесс создания оптимальных условий для максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий[33].

Правовая информатизация как важный процесс преследует определенные цели, среди которых основной является формирование системы механизмов, которые посредством правовой информированности граждан, способствует

---

[31] *Шамин Е.А.* Сущность информатизации, ее цели, субъекты и объекты // Е.А. Шамин, И.Г. Генералов, Н.С. Завиваев, А. Д. Черемухин // Вестник НГИЭИ. 2015. № 11. С. 100.

[32] *Линейцева К.С.* Правовая информатизация как средство повышения электорально-правовой культуры // Учёные труды Российской академии адвокатуры и нотариата. 2013. № 1. С. 42.

[33] Указ Президента РФ от 28 июня 1993 г. № 996 «О Концепции правовой информатизации России» // Собрание актов Президента и Правительства РФ. 1993. 5 июля. № 27, ст. 2521.

поднятию уровня правовой культуры и совершенствованию жизни личности, общества и государства.

Роль правовой информатизации велика на современном этапе, постольку, поскольку она пронизывает все сферы деятельности органов государственной власти Российской Федерации, а также внедряется в работу организаций, предприятий и учреждений независимо от их организационно - правовой формы и, не менее важно, имеет место быть среди отдельных граждан, которые в своей повседневной жизни оперируют данной информацией.

Необходимым условием стабильного современного состояния и дальнейших перспектив развития правовой культуры населения выступает высококачественное информационное обеспечение органов государственной власти Российской Федерации. Рассмотрим это с позиций различных органов государственной власти России.

Информатизация деятельности в законодательных органах включает в себя: во-первых, информационное обеспечение всех стадий подготовки законопроектов; во-вторых, автоматизированный контроль за документооборотом; информационное обеспечение процесса обсуждения законопроектов; в-третьих, распространение правовой информации посредством информационно-телекоммуникационной сети.

Что касается исполнительной власти, правовая информатизация проявляется в следующем: обеспечение цивилизованного информационного взаимодействия власти и гражданского общества.

Относительно судебной власти, стоит говорить непосредственно про процесс создания благоприятных условий для доступа к информации, используемой в судопроизводстве, то есть для наилучшего использования баз данных, применяемых в судебной деятельности.

С помощью правовой информатизации происходит массовое утверждение в правосознании граждан чувства уважения к закону и правопорядку, что непосредственно сказывается на повышении уровня их правовой культуры.

Для современной Российской действительности проблема становления и улучшения правовой культуры является актуальной, что объясняется существующим пренебрежением правом, проявляющееся в несоблюдение конституционных прав и свобод граждан; в принятии законов, не соответствующих Конституции РФ; в несоблюдении государственными органами, ведомственными и должностными лицами установленных государством предписаний; в проявлении правового нигилизма, связанного с несовершенством законодательства; в повсеместном проявлении крайних степеней деформации правосознания, выражающееся в криминализации общественных отношений и др.

Для выхода из создавшегося положения необходимо продолжать проведение развития процесса преобразований в стране и практической реализации идей и ценностей современной правовой культуры, дальнейшего улучшения организации, совершенствования форм и методов работы государственного аппарата и правоохранительных органов, строгого соблюдения демократических принципов их деятельности, обеспечения достоверности и доступности выходящей информации; повышение авторитета суда, укрепление гарантий его независимости[34].

Представляется необходимым отметить механизмы правовой информатизации, а именно: с помощью пяти основных каналов (телевидение, Интернет, печатные издания, СМИ, справочно=правовые системы) осуществляется доведение информации до граждан; а особенностью работы этих механизмов является оценка качества частоты обращений и ответов, простоты и доступности информации, достоверности и т.д.

Для повышений уровня правовой культуры, считаем необходимым, решение таких задач, как: во-первых, развитие инфраструктуры правовой информатизации; во-вторых, обеспечение взаимодействия формированием и пользованием информационными ресурсами в Российской Федерации; втретьих,

[34] *Кузнецова В.А., Семенова К.А.* Правовая информатизация как средство повышения правовой культуры // Неделя науки СПБГПУ. СПб., 2014. С. 85.

контроль над информационной безопасностью и обеспечение права на информацию; в-четвертых, обеспечение нужной документацией лицензирования информационных ресурсов и информационных услуг в правовой сфере; в-пятых, создание и обеспечение эффективного функционирования единого информационно-правового пространства для обмена банками правовой информации различных уровней, и наконец, вшестых, создание научно-технической продукции правовой информации на основе новейших информационных технологий.

Исходя из вышесказанного, можно сделать вывод о значимости правовой информатизации для совершенствования уровня правовой культуры граждан в современных условиях. Правовая осведомлённость в свою очередь дает возможность гражданам правильно воспринимать остановку и ориентироваться в существующем положении дел страны, а также это способствует преодолению правового нигилизма, и большей правовой подкованности граждан в области обеспечения и защиты своих прав и свобод.

П.И. Давыдова

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **П.В. Ересько**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ЭЛЕКТРОННЫЕ ДЕНЕЖНЫЕ СИСТЕМЫ

В настоящее время ежедневно используется Интернет для интернетпокупок, где совершаются интернет операции, связанные именно с денежным эквивалентом. Наличные деньги как широко используемый инструмент денежного обращения начинают мало- помалу «сходить на нет». Вместе с развитием науки и техники, развивается возможность проведения денежных расчетов.

ЭПС или электронная платежная система – это система расчетов между финансовыми организациями (коммерческими банками, небанковскими кредитными организациями, инвестиционными организациями), бизнесорганизациями и интернет-пользователями при осуществлении

покупкипродажи товаров и за оказание различных услуг через Интернет. Такая платежная система является разновидностью традиционных денежных расчетов.

Виды платежных систем:

– дебетовые (связанные с электронными чеками и цифровой наличностью); – кредитные (связанные с кредитными карточками).

Функционирование ЭПС является необходимым условием обращения электронных денег.

Прежде чем электронные деньги стали неотъемлемой частью повседневной жизни многих людей, они прошли свое развитие в три этапа. Первым этапом развития электронных денег являются 60-80-е годы 20 века. В этот период происходит внедрение в обращение магнитных кредитных дебетовых карт, а также распространялось использование электронной системы платежей.

Вторым этапом 90-2000-е годы этого же столетия, стало внедрение в обращение смарт-карт или, по-другому, карт, на которых хранится определенная сумма. Большая часть исследователей, проживающих на Западе, рассматривают смарт-карты в качестве одного из элементов электронных денег. В то же время смарт-карты являются одним из инструментов электронных денег, так называемым «продуктом-ключом».

И заключительный этап развития электронной денежной формы проходит в 2000-2010-е годы. Это десятилетие характеризуется появлением внедрения новых видов электронных денег, так называемых «сетевых денег», которые дают возможность проводить платежи в режиме «онлайн» в компьютерных сетях. Благодаря специально разработанному программному обеспечению эти платежи являются возможными.

Разновидности электронных денег: на базе смарт-карт (card-based) и на базе сетей (network-based).

Популярными платежными системами в России и в мире являются: PayPal, E-gold, Perfect Money, WebMoney, Яндекс.Деньги, Qiwi.

К преимуществам электронных денег относят:

–объединяемость и делимость. При осуществлении расчетов отсутствуетпотребность в сдаче.

–хранение является достаточно компактным, то есть не требуетдополнительного места и специальных устройств механической защиты.

–отсутствие нужды в пересчете и доставке. Платежей и храненияэлектронных денег выполняется автоматически.

–минимальные затраты на эмиссию. Нет необходимости в чеканке монет ипечатании банкнот.

–неподверженность износу банкнот может послужить неограниченномусроку службы.

К недостаткам электронных денег относят:

–нерегламентированность едиными законами является риском развитияпроизвола в обращении электронных денег;

–необходимость наличия специальных инструментов осуществленияплатежей и хранения;

–не до конца разработаны безопасные средства хранения и обеспечениезащиты электронных денег от подделок;

–неподготовленность продавцов принимать электронные платежи. Это связано с отсутствием необходимых приборов для проведения этих самых платежей;

–преобразование средств одной электронной платёжной системы в другуюявляется затруднительной;

–государственные гарантии, подтверждающие надежность организации,выпускающей ценные бумаги и электронные деньги, как таковые отсутствуют.

Только при полной защищенности и соблюдении безопасного пользования Интернетом возможно осуществление платежных операций в Интернете.

Пути решения проблемы безопасности, основывающиеся на криптографических и шифровальных системах:

–конфиденциальность – информация должна быть защищена отнесанкционированного доступа как при хранении, так и при передаче. Для постороннего лица, кому информация не предназначена, доступ должен быть закрыт. Конфиденциальность поддается шифрованию;

–аутентификация – в обязательном порядке необходимо отождествлятьотправителя. В этом случае отправленная информация должна подтверждаться электронной цифровой подписью и сертификатом;

–целостность – информация должна быть защищена отнесанкционированной модификации, как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью.

Электронная платежная система – это технология, представляющая собой совокупность методов, договоренностей и средств, которая позволяет совершать операции связанные с электронными деньгами, между сторонами сделки по средствам электронных платежных систем. Очевидно, что скорость распространения электронных платежей зависит не только от развития самих электронных платежных систем, но и от расширения доступа населения к Интернету и грамотности граждан в вопросе электронных платежей. Недоверие со стороны людей, непривычность оплаты услуг, а так же недостаток платежных терминалов в некоторых регионах страны являются главным фактором затруднения развития данной системы.

Г.С. Дунас
ФГБОУ ВО «Саратовская государственная юридическая академия»
*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ДАННЫХ В КРИМИНАЛИСТИЧЕСКИХ ИССЛЕДОВАНИЯХ

В 21 веке резко возрастают темпы развития и использования информационных технологий в различных сферах жизни общества. Сейчас уже речь идет о переходе к построению глобального информационного сообщества с развитой системой информационных телекоммуникаций. Наблюдается также интенсивное внедрение перспективных информационных технологий во все сферы юридической деятельности. При этом значительный объем информационных функций осуществляется правоохранительными органами.

Актуальным является расширение практики использования криминалистических учетов, организованных в автоматизированные информационные поисковые системы, предназначенные для получения сведений, имеющих доказательственное значение, в целях выявления, раскрытия и расследования широкого спектра преступлений (в том числе в сфере компьютерной информации).

Криминалистическая регистрация долгое время называлась уголовной регистрацией, потому что ее основу составлял учет лиц, привлеченных к уголовной ответственности, и преступлений, которые они совершили. Расширение круга учитываемых объектов (а сейчас регистрируются и лица, без вести пропавшие; предметы преступного посягательства; предметы со следами преступления; средства и способы совершения преступлений; следы преступлений) и разработанные криминалистами средства и методы получения указанной информации стали более совершенными. И изменяются они за счет внедрения современных информационных технологий.

Средства совершения компьютерных преступлений классифицируются по различным критериям: по законности происхождения; по созданию; по

техническому содержанию; по технологии использования; по стадии в преступлении.

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Они включают в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, и т.д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеют различное назначение — разрешенные и бесплатно распространяемые программы (например, Opera), вредоносные программы(например, SpyEye, Zeus) и т.д. Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые сами по себе обычно не представляют опасности.

Следственные органы, особенно на первоначальном этапе расследования компьютерных преступлений, редко располагают сведениями о средствах, используемых в преступлении. В отсутствие такой информации важную роль для проведения расследования играет криминалистическая характеристика аналогичных преступлений. Ее практическое значение, проявляющееся в корреляционной взаимосвязи между структурными элементами преступления, дает основания строить следственные версии на основе использования имеющихся неполных данных. В компьютерных преступлениях выбор средств для их совершения обычно зависит от целого ряда факторов: объекта посягательства, принятого на нем режима охраны, применяемых технических и организационных средств охраны, программно-аппаратной защиты информации. Если поводом для возбуждения уголовных дел являются заявления потерпевших, то следствию становится известен объект посягательства. Его исследование может внести ясность на способ совершения преступления или примененные преступником программно-аппаратные средства. Анализ судебно-следственной практики показывает, что относительно простые или, наоборот, высокотехнологичные способы совершения преступлений могут осуществляться

характерными для них программно-аппаратными средствами. А бывает ситуация, когда данные о средствах преступления известны и помогают строить следственные версии о других искомых элементах преступления. Например, конкретные средства совершения преступления могут указывать на применяемый преступниками способ совершения преступления, а также время и место его осуществления.

Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28-й УК РФ, Преступными являются следующие виды деяний: неправомерный доступ к охраняемой законом конфиденциальной компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей стакими программами (ст. 273 УК); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).

Чаще всего компьютерная информация используется для совершения следующих преступлений: нарушение авторских и смежных прав (ст. 146 УК); мошенничество (ст. 159 УК); подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК); изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК); изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК); уклонение от уплаты налогов с организаций (ст. 199 УК). При раскрытии и расследовании данных преступных посягательств необходимо использовать определенные методы, которые относятся к расследованию преступлений в сфере компьютерной информации.

Компьютерная информация – это сведения, обращающиеся в вычислительной среде, закрепленные на носителе в форме, доступной восприятию ЭВМ, или передающиеся по каналам электросвязи посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на внешний носитель памяти.

Средства, которые используются при совершении преступлений в сфере компьютерной ин формации, достаточно разнообразны. Важно также, что с

криминалистических позиций их можно сгруппировывать по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении и др. Это обусловливает необходимость разработки системы криминалистической классификации. В целях повышения эффективности расследования компьютерных преступлений разнообразные средства их совершения следует классифицировать, учитывая их основные особенности

Криминалистическая классификация средств совершения компьютерных преступлений:

– по законности происхождения: законные /незаконные;
– по созданию: готовые /модифицированные /собственной разработки;
– по техническому содержанию: аппаратные /программноаппаратные/программные;
– по технологии использования: без удаленного доступа /с удаленнымдоступом;
– по стадии в преступлении: при подготовке /при совершении /присокрытии /при противодействии следствию.

Для защиты компьютерной информации от несанкционированного доступа используются различные средства защиты. Под средствами защиты компьютерной информации понимаются технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих информацию - средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

При выявлении и расследовании преступлений в сфере компьютерной информации подлежат установлению: факт совершения преступления; непосредственная причина нарушения безопасности компьютерной информации и орудий ее обработки; предмет преступного посягательства; категория компьютерной информации (общего пользования или конфиденциальная); место и время совершения преступления; способ совершения преступления; совершено ли преступление дистанционно извне помещения (по каналам электросвязи и

локальной сети ЭВМ); режим работы с компьютерной информацией, орудиями ее обработки и средствами их защиты; с помощью каких СВТ совершено преступление (тип, вид, модификация, и др.); конкретный терминал или участок сети (абонентский номер, код, шифр), режим их работы и ответственное лицо; имела ли место утечка конфиденциальной информации; размер материального ущерба; личность подозреваемого и основные ее характеристики; совершено ли преступление группой лиц, каковы роль и характер каждого участника преступления; мотив преступления; кто является потерпевшим (физическое или юридическое лицо); кто участвовал в сокрытии преступления и его следов; причины и условия, способствовавшие совершению и сокрытию преступления, что усугубило их проявление – не обусловлено ли это нарушениями нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам.

На сегодня имеется целый ряд организаций, которые занимаются программами для проведения криминалистических исследований в сфере компьютерной информации. Одной из наиболее популярных и востребованных на сей день является лаборатория компьютерной криминалистики и информационной безопасности ЕПОС. Она предлагает специализированные технические и программные средства для проведения исследований в области компьютерной криминалистики.

Отличительной особенностью компании ЕПОС является наличие отдела научно-исследовательских и опытно-конструкторских работ (НИОКР), в функции которого входит разработка специализированных аппаратных и программных средств для съема, восстановления и анализа данных на различных цифровых носителях. Благодаря этому, лаборатория компьютерной криминалистики ЕПОС имеет в распоряжении средства расследования компьютерных происшествий собственной разработки.

Не для кого не будет секретом, что нет одного универсального оборудования, которое бы выполняла все исследования, но и так же не столь

много оригинальных оборудований. Все программно-аппаратные средства либо друг друга заменяют, любо выполняют схожие функции.

ACE Laboratory (ООО НПП «ACE», Россия) – специализированное оборудование и программное обеспечение для ремонта HDD, восстановления данных с поврежденных HDD, копирования информации на HDD.Его можно сравнить с Тайваньской разработкой Decision Group и Российской BelkaSoft которое к тому же проводит мониторинг использования ресурсов Интернет, предотвращает утечки информации.

NRTeam (NAND Recovery Team, (Россия) – программные и аппаратные средства восстановления данных с Flash-накопителей. Самый известный проект лаборатории – ПО «Dumppicker» для логического восстановления информации с Flash-накопителей.

ICS Intelligent Computer Solutions, Inc. (США) – оборудование для высокоскоростного криминалистического сбора данных с жестких дисков. Продукты компании разрабатываются в сотрудничестве с правоохранительными органами США и других стран.

США является наиболее развитой страной по производству программ подобного типа. Можно выделить ряд компаний, которые разрабатывают аппаратные и программные средства.

Tableau. С мая 2010 г. компания входит в состав корпорации «Guidance Software, Inc.» производит средства расследования компьютерных происшествий: устройства копирования, аппаратные блокираторы, аппаратные ускорители и программное обеспечение.

eDEC Digital Forensics (США) – устройства и программы для компьютерной криминалистики, следующие за новейшими веяниями в отрасли. Компания известна своими средствами снятия данных со смартфонов китайского производства.

Barracuda Networks, Inc. (США) – широкий спектр сетевых устройств и облачных услуг по обеспечению безопасности электронной почты и прочих сетевых приложений для организаций всевозможных размеров.

Rapid7 (США) – продукты анализа и обработки рисков информационной безопасности, обладающие широким набором функциональных возможностей для выявления и уменьшения рисков, а также проверки соответствия различным стандартам информационной безопасности.

Addonics (США) – защищенные модульные системы хранения данных, средства шифрования информации на накопителях, дубликаторы и преобразователи интерфейсов. Разрабатываемые компанией технологии рассчитаны на обеспечение максимальной совместимости со всевозможным оборудованием и ОС.

Cellebrite Mobile Synchronization Ltd. (Израиль) – высокопроизводительные решения в области судебно-криминалистических устройств для извлечения, декодирования и анализа данных с телефонов, смартфонов, планшетных и других портативных устройств.

iStorage Limited (Великобритания) – защищенные накопители с прямым вводом пароля и аппаратным шифрованием хранимой информации. Приоритетами компании являются использование новейших технологий и доступные цены.

В Германии на сегодняшний день две лидирующие компании.

X-Ways Software Technology AG (Германия) – криминалистическое ПО. Продукты компании предназначены для расследования компьютерных происшествий, восстановления и глубокого анализа данных, гарантированного удаления информации и Secusmart GmbH (Германия) – аппаратно-программные средства шифрования мобильной связи: звонков, сообщений SMS и электронной почты. Свои продукты компания разрабатывает совместно с Федеральным ведомством безопасности ИТ Германии (BSI) и производителями мобильных телефонов.

Amped Software (Италия) – программное обеспечение для криминалистического исследования цифрового фото- и видеоматериала. Продукты компании применяются экспертами-криминалистами государственных и частных организаций всего мира.

Рассмотрим теперь несколько аппаратов.

Tableau T35es – Аппаратный блокиратор записи Tableau T35es обеспечивает защиту от записи на SATA и PATA (IDE) HDD. Поддержка четырех скоростных хост-интерфейсов позволяет обеспечить быстрый съем данных с использованием любого ПК или ноутбука.

IM Solo-101 Forensic – быстрый и простой в использовании прибор для создания копий и образов SATA и USB HDD при расследовании компьютерных происшествий и инцидентов. Прибор встроен в легкий и компактный ударопрочный кейс, что позволяет использовать его как в условиях лаборатории, так и на выезде.

RoadMASSter-3 X2 Forensic – Портативная криминалистическая лаборатория предназначена для съема, копирования и анализа информации на HDD и других носителях с выездом на место расследования. Обеспечивает работу со всеми современными накопителями с различными интерфейсами

EDEC Tarantula – первое на рынке специализированное решение для криминалистического съема и анализа данных с мобильных телефонов, смартфонов, планшетов китайских производителей. Комплекс обеспечивает логический и физический съем информации, что позволяет извлечь из исследуемого устройства максимум данных.

Tableau TACC1441 – это аппаратный акселератор подбора (взлома) паролей методами полного перебора и перебора по словарю (атаки типа brute force).

В наши дни именно информационные процессы лежат в основе познания и любого действия, являющегося элементом того или иного вида человеческой деятельности, и именно они являются непосредственными объектами математизации и автоматизации. С точки зрения эволюции информационных технологий обеспечение правоохранительной деятельности информацией начало свое развитие в виде формирования и развития системы криминалистических учетов. И в настоящее время практически ни одно уголовное дело не расследуется без информационной поддержки служб,

осуществляющих ведение учетов, осуществляемых в органах внутренних дел Информационно-аналитическими центрами и Экспертными подразделениями.

Говоря о перспективах информационных технологий в криминалистике, следует выделить несколько направлений интересов ученых: организационноправовые проблемы информатизации; вопросы использования персональных данных, проблемы защиты информации имеют важной значение, вопросы информатизации отдельных направлений криминалистики, теоретикометодологические и образовательные проблемы, и изучение зарубежного опыта информатизации.

Список использованной литературы и источников

1. *Аверьянова Т.В.* Судебная экспертиза. Курс общей теории: М.: НОРМА, 2008.
2. *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г. и др.* Криминалистика: учебник. М.: НОРМА, 2008.
3. *Акопов Г.Л.* Правовая информатика: современность и перспективы. М.: Феникс, 2005.
4. *Видонов Л.Г.* Криминалистические характеристики. Справочник следователя. М., 1990.
5. *Толстолуцкий В.Ю.* Использование информационных технологий в раскрытии и расследовании убийств: электронное учебно-методическое пособие. Н.Новгород: Изд-во Нижегородского госуниверситета, 2012.
6. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993). М., 2015.
7. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 02.03.2016) // Российская газета. 2001. 22 декабря.
8. http://www.epos.ua.
9. http://forensictools.com.ua.
10. http://www.yaroslavl.festivalnauki.ru.

В.В. Емелин
ФГБОУ ВО «Саратовская государственная юридическая академия»
*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

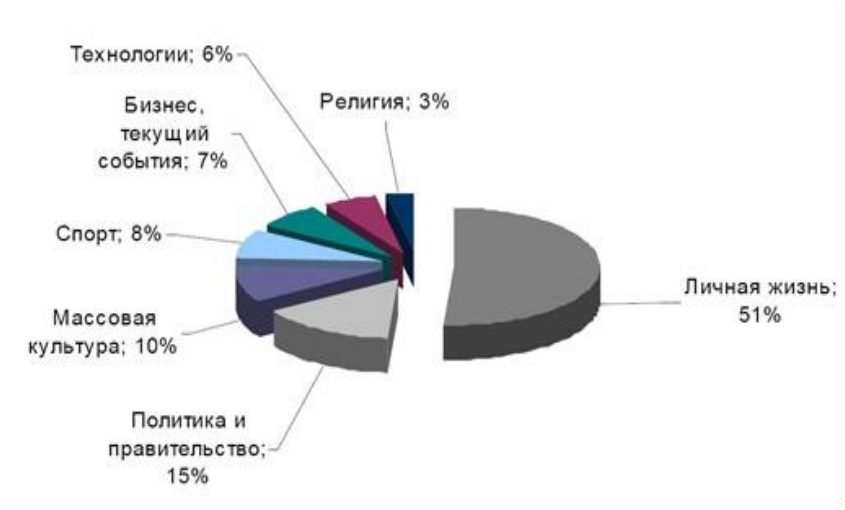
СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ: ПОЛИТИКА В БЛОГАХ

Сегодня многие эксперты исследуют современные политические процессы. Наука дала миру новые способы коммуникаций. Появление глобальной сети Интернет и в дальнейшем блогов и социальных сетей сильно увеличило количество контактов между людьми. Уже большинство населения вовлечено в глобальное информационное пространство. Внедрение новых информационных технологий оказало сильное влияние на процесс деформации Российской политической системы. В демократическом обществе перед властью возникает ряд проблем. Пожалуй, одна из серьезно тормозящих развитие демократии в России – отчужденность масс от политики. Граждане не сильно верят в силу своего голоса и то, что его кто-то услышит. Опросы показывают критически низкий уровень заинтересованности населения в работе местных органов власти и депутатов. Во многом это связано с отсутствием в широком доступе информации об их работе. Современные информационные технологии способствуют демократизации политической сферы России. Блоги, социальные сети позволяют установить более тесный контакт между гражданами и властями. Целью своей работы мы ставим ответить на вопрос: «Насколько успешна политика в блогах?». Соответственно для ответа на поставленный вопрос необходимо сначала выполнить ряд задач: – выявить основные отличия и особенности блогосферы от иных подобных, ее тенденции и проблемы.

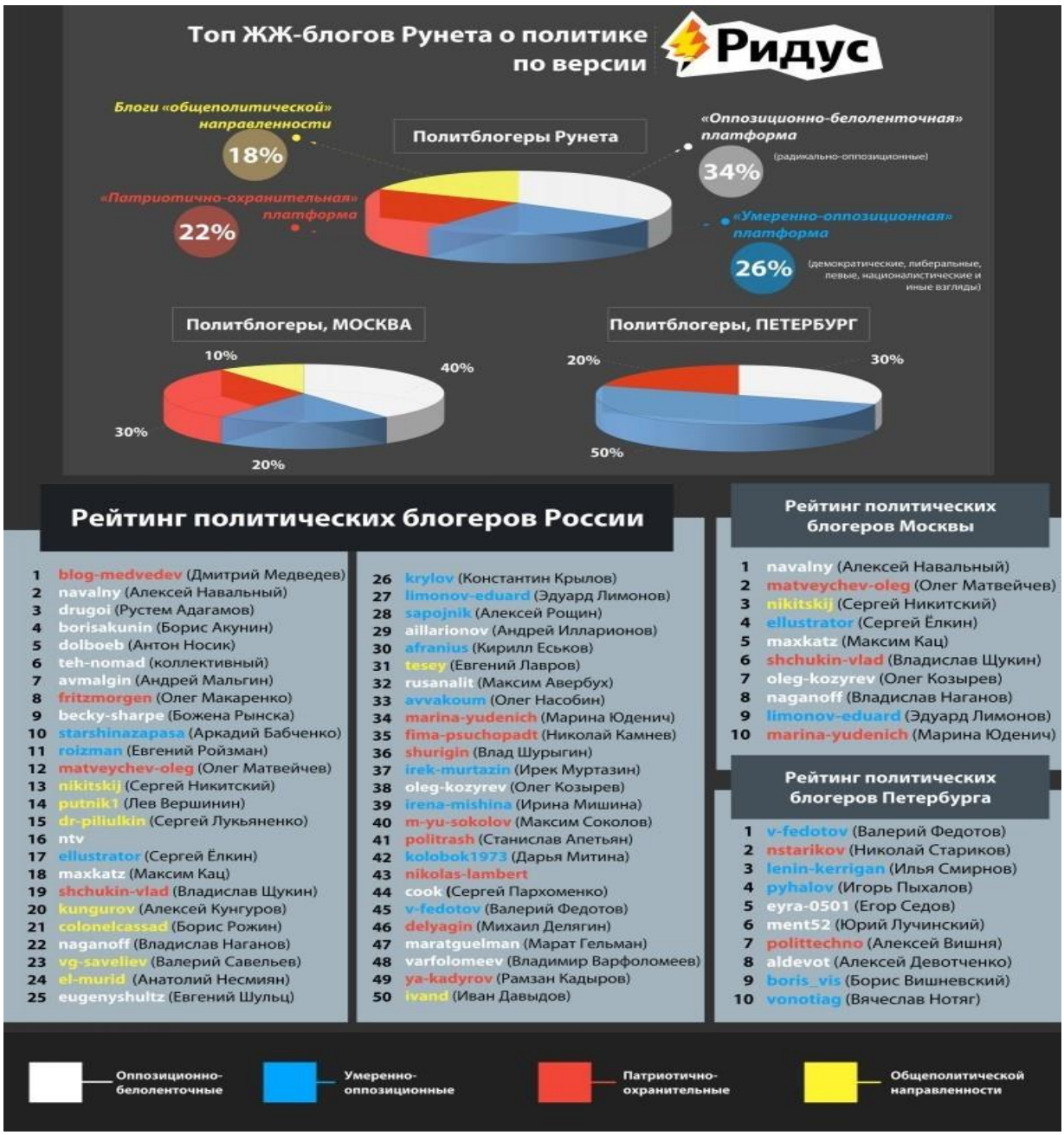
– изучить популярные политические блоги на предмет политическихвоззрений блогеров и их количества.
– рассмотреть политический блог как канал связи власти и общества.
– рассмотреть блог как средства политического пиара.

Политический блог как инструмент политика. Для того чтобы начать исследовать проблему, разберем ключевые понятия. Блог (от английского weblog

– «Интернет-журнал») – персональные заметки, которые публикуются в Интернете в открытом доступе. Это самое простое определение блога и самое первое. С течением времени функции и назначения блогов расширялись, что привело к более комплексному пониманию этого явления. Это не просто дневниковые записи, выстроенные в хронологическом порядке, а уже система коммуникаций производителя информации и ее реципиентов в Интернетпространстве. Широкое распространение блогов началось в 1996 году, но Россию этот бум захлестнул в 2004. Тем не менее, из немногочисленного пока еще числа блогеров, политика занимает интерес лишь относительно небольшого числа пользователей.



Уже не новость, что государственные деятели все чаще заводят собственные блоги в Интернете. Это стало модой среди чиновников после того, как в октябре 2008 года на сайте kremlin.ru Д.А. Медведев завел видеоблог с обращениями к гражданам по актуальным вопросам. В 2010 году Компания Profi Online Research опубликовала результаты опроса российских интернетпользователей на тему их отношения к ведению блогов известными политическими деятелями.



Согласно отчету, 57% отечественных блогеров одобряют ведение политиками собственных дневников и считают такую форму способом обратиться напрямую к должностному лицу с жалобой или просьбой. 21% респондентов считают политические блоги имиджевым ходом, а 11% заявили, что это «хороший способ приобщить россиян пользоваться Интернетом». В то же время 8% опрошенных не одобряют такую деятельность политиков. Среди интересующихся политикой 64% просматривают блог, тогда еще президента РФ

Д.А. Медведева[35]. Для радикальных публичных деятелей блог дает зачастую единственную возможность выступить публично. В остальных случаях открытый диалог с интернет-общественностью вызывает доверие граждан. Сразу стоит отметить, что активно участвуют в блогах уже зрелые опытные люди, это, пожалуй, главное отличие блогов и соц. сетей[36]. Приоритеты блогов – информационная открытость и обратная связь. В теории политически блоггинг имеет ряд преимуществ. Рассмотрим каждое из них.

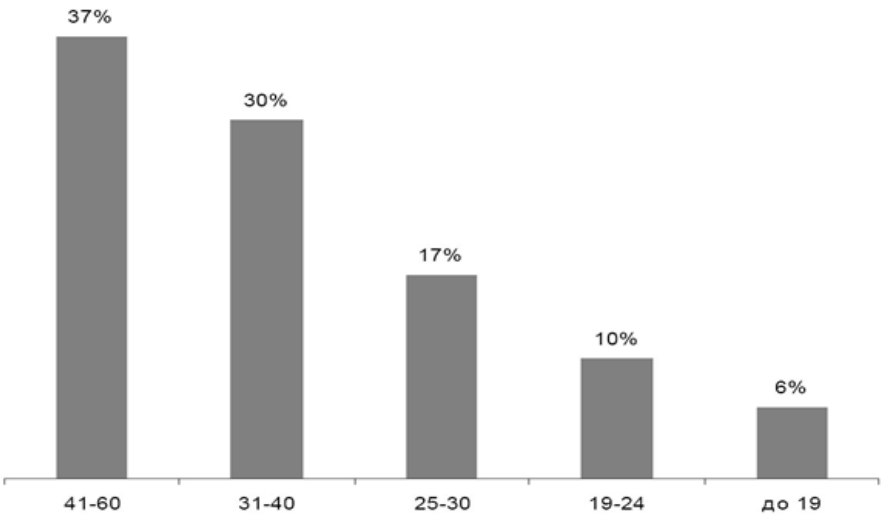
Блог, как политический стартап. Один из плюсов сети то, что начинающий политик может подыскать себе электорат в сети, а именно в собственном блоге. На Западе, это довольно распространенная практика, в России же аудитория очень маленькая, преимущественно зрело возрастная. Основной аудиторией блогов являются преимущественно журналисты, общественники, а также граждане имеющие образование и интерес к политике, и скорее всего они являются авторитетами для своих знакомых. Другими словами, повлияв на это меньшинство, можно привлечь к себе намного больше людей, поэтому блоги не так уж безнадежны. Реально сделать карьеру в блогосфере тяжело и примеров мало, но есть. Просмотрев самые популярные блоги Рунета: Дмитрий Медведев, Адагамов, Рустем Ринатович, Алексей Навальный, и других, я пришел к выводу, что аудитория преимущественно оппозиционно настроенная, поэтому провластному блогу никто не поверит, его не будут читать, или же будут закидывать негативными комментариями, лучшее поле – это критика власти, чиновников, особенно идут посты про коррупционеров, кумовство, внутреннюю политику. Модно в этой среде быть яростным оппозиционером и либералом. Наряду с ростом патриотизма в последние годы, патриотичного толка блоги не так популярны. Реальные примеры стартапа есть: блог Адагамова, Рустема Ринатовича. В блоге он стал размещать переводы интересных статей из норвежских газет, а также собственные небольшие рассказы о своей жизни в

---

[35] *Благовещенский А.* Президентский блог назвали самым популярным среди политических // Российская газета. 2010. 19 октября.

[36] *Горошко Е.И.* Политический блоггинг в глобальной и локальной перспективах // Вестник Одесского национального университета. Социология и политические науки. 2009. Т.14. №3. С. 335-345.

Норвегии. Адагамов размещает у себя в ЖЖ репортажные фотографии зарубежных фотоагентств, таких как Рейтер и Франс Пресс, снабжая их авторскими подписями и комментариями. Еще пример роста Олег Макаренко. В блоге было опубликовано большое число статей по искусству спора, разборы различных риторических приёмов и манипуляций. Значительная часть постов блога посвящена развитию технологий, в том числе роботам и освоению космоса. С 2011 года по настоящее время основная часть содержания блога посвящена политическим темам – информационной войне против России, несистемной оппозиции, противостоянию России и Запада, экономической и моральной деградации Запада, а также важнейшим текущим политическим событиям (белоленточным митингам 2011-2012 гг., Украинскому кризису и другим). Таким образом сделать имя можно только размещая уникальный контент. Сразу писать о политике не удастся. Можно начать с переводом и комментированием иностранных СМИ, политиков, желательно не только с английского, другой вариант, например, развенчивать основные манипуляции, которые используют на выборах или политики. Завоевав популярность можно уже и переходить к конструктивной критике. В блогах преимущественно аудитория взрослая, поэтому материал должен быть ориентирован именно на них.



Блог, как налаживание обратной связи с народом для чиновников. В теории, блок – отличный способ принять жалобы народа, выслушать человека, обсудить тот или иной вопрос со своими избирателями. Но, к сожалению, в России блоги явно не справляются с возложенной на них задачей. На представителей власти

льется огромное количество критики, по большей части грязи. К моему удивлению отсутствует уважение среди читателей блогов к председателю правительства и экс-президенту РФ Дмитрию Анатольевичу Медведеву. В адрес главы исполнительной власти направлены множество оскорблений и неконструктивной критики. Социальная политика вообще больная тема, вызывает исключительно гнев и негатив у пользователей. Даже увеличение МРОТ пользователи восприняли, как попытку увеличить доходы от штрафов, другие осудили, что слишком мало увеличили. На местном уровне: блог Фадеева Владимира – главы Саратовского отделения партии «Родина», пожалуй, один из самых популярных; количество читателей его записей зачастую превышает за тысячу. Вообще, несмотря на доминирование гневных комментариев блог по-прежнему выполняет функцию информирования электората того или иного политика о его работе, мыслях, взглядах на ту или иную проблему. В конце концов, жители области не сильно склонны комментировать и оценивать те или иные записи, поэтому вполне ограничиваются прочтением и формированием своего впечатления.

Блог дает возможность политику узнать мнение людей, позволяет судить об эффективности деятельности чиновника. Блог влияет на формирование повестки дня. Да, в идеале. На практике, как я уже говорил, все полезные предложения и комментарии с вопросами затмят гневные комментарии пользователей, реально найти замечания по существу трудно, единственный плюс – тестировать идеи на людях, заведомо готовых ее отвергнуть, так сказать уровень hard. Если уж там нашлось одобрение, то можно пробовать в массы выносить.

Политический блог разрывает дистанцию между официальным лицом и обычным человеком. Да, в этом определенный плюс, люди явно не чувствуют социальный разрыв и смело высказывают свое мнение. Если в дальнейшем в блоги начнут проникать другие слои населения, то сеть стала бы отличной площадкой для социологических исследований и общению с народом власти. И

снова «но», отсутствие социального статусного барьера приводит к отсутствию уважения друг к другу, то выражается в фактах наличия нецензурной лексики.

Подводя итоги, сразу стоит сказать о наличии больших проблем в отечественной блогосфере. На наш взгляд ключевая проблема – культура общения. Вообще отсутствие манер речи, проявление глубочайшего неуважения друг к другу удивляет, в стране с социалистическим воспитанием, высокой культурой и образованием. Не случайно именно социалистическим, основная аудитория блогов люди опытные, с советским воспитанием и образованием. Молодежь более все-таки предпочитает социальные сети и политикой интересуется мало. Тем не менее, блоги достаточно полезны для политиков и общественных деятелей, они позволяют найти свой электорат, своих единомышленников. Блоги – отличный способ отчитаться о своей работе перед народом (в идеале хорошо бы было всем чиновникам, занимающим важные для общества и государства посты вести свои блоги). Также проблема отечественной блог сферы в идеологической скудности. В Интернет сегодня выходят в основном из-за недоверия СМИ и потерей веры в возможность свободно и без последствий высказывать свое мнение, анонимно это сделать куда проще. Политики не раз предлагали ввести ответственность и убрать анонимность, но в таком случае блоги потеряют свой смысл и действительного доверительного диалога власти и общества не будет. Единственный на наш взгляд выход – пропаганда блогосферы через СМИ: ссылки в репортажах на посты блогеров, если удастся привлечь больше людей с умеренными взглядами, которых большинство, удастся ликвидировать многие недостатки сферы.

Список использованной литературы и источников

1. Самые популярные системы блогов в России. URL: http://whoyougle.ru/texts/russian-blogging-services.
2. *Горошко Е.И.* Политический блоггинг в глобальной и локальной перспективах // Вестник Одесского национального университета.

Социология и политические науки. 2009. Т.14. №3. С. 335-345.
3. *Сандомирский Марк.* Блог как политический старт-ап. URL: http://www.liberty.ru/columns/Psihobloging/Blog-kak-politicheskij-start-ap.
4. *Благовещенский А.* Президентский блог назвали самым популярным среди политических // Российская газета. 2010. 19 октября.
5. Рейтинг блогеров Саратова. URL: https://livedune.ru/city/blogger/%D0% A1% D0%B0%D1%80% D0%B0%D1%82%D0%BE%D0%B2.
6. URL: www.twiter.com.
7. URL: http://www.vzsar.ru/blogs.
8. URL: http://www.livejournal.com.
9. URL: http://s58.radikal.ru/i160/1309/4b/ d611fe378902.jpg.

Ю.С. Изотова
ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт
*Научный руководитель: **П.В. Ересько**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СУДЕБНОЙ ЭКСПЕРТИЗЕ

Если рассматривать судебную экспертизу, как область практической деятельности, она представляет собой сложную систему различных элементов, таких как: статуса и функций субъектов действительности, нормативного регулирования, систему технических средств, научных методов и основ проведения экспертных исследований. Поэтому такая сложная, динамически развивающаяся система не может существовать без использования технических средств.

Информационные технологии сегодня заняли особое место в производстве судебной экспертизы. Поэтому освоение современных информационных технологий, которые позволяют повысить эффективность решения задач в судебной экспертизе, является необходимым для повышения качества подготовки специалистов юридического профиля.

Судебная экспертиза – это процессуальное действие, которое состоит из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, ремесла, искусства, и которые поставлены перед экспертом судом, судьей, следователем, в целях установления обстоятельств подлежащих доказыванию по конкретному делу.

В российском законодательстве этот термин закрепили только уголовнопроцессуальные кодексы 1922 и 1923 годов, отказавшись от термина «сведущие лица», принятого судебными уставами Российской империи и ввели термин «эксперт».

Сегодня в практике расследования преступлений используется как математический аппарат, так и вычислительные устройства. Кроме того,

математический аппарат и средства вычислительной техники используются в различном их сочетании.

Для судебно-автотехнических экспертиз разработаны программы, которые помогают рассчитывать скорость движения транспорта, возможность предотвратить наезд на пешехода, выяснить причину столкновения и т.д. Полученные сведения и данные вводятся в электронно-вычислительную машину, которая после выдает результаты в виде заключения. Затем эксперт оценивает и заверяет своей подписью. Это делает выводы экспертизы более надежными и точными, а также увеличивает скорость производства экспертизы.

В последнее время персональные компьютеры нашли применение в экспертных исследованиях, которые проводятся при расследовании различных преступлений.

С их помощью многие экспертные задачи решаются быстрее, точнее и надежнее, чем другими методами.

Существует три основных пути применения ПК в судебной экспертизе:

1. Математизация отдельных звеньев экспертного исследования.
2. Полная автоматизация исследования вещественных доказательств.
3. Создание диалоговых систем (в узком смысле используются в различных автоматизированных системах обработки информации и управления).

Первыми начали активно применять компьютеры эксперты-почерковеды: для дифференциации исследуемых объектов, близких по характеристикам движений;

Затем компьютеры стали использовать для выделения и оценки количественных признаков в экспертизе фотопортретов, совершенствования реконструкции лица по черепу и так далее.

В судебно-автотехнической экспертизе появились компьютеризированные методики моделирования и анализа механизма ДТП.

В судебно-вокалографичксих и судебно-электроакустических экспертизах ПК используются для исследования речевых сигналов и идентификации звукозаписывающих устройств.

В судебно-баллистической экспертизе они помогают отождествить огнестрельное оружие по стреляным пулям, а в трасологической – идентифицировать орудие по его следам.

В криминалистической экспертизе веществ и материалов ПК нашли применение для количественной обработки результатов рентгенофазового, спектрального и лазерного анализов при исследовании частиц лакокрасочных покрытий транспортных средств.

Так, удается значительно сократить время анализов, повысить их эффективность и точность.

Сегодня разработано и успешно применяются на практике множество методик экспертных исследований, которые основаны на использовании компьютерных программ.

Так, разработаны программные комплексы автоматизированного решения экспертных задач.

К таким компьютерным программам относятся:

– «Кортик». Используется в экспертизе холодного оружия.

– «Эврика». Используется в пожарно-технических экспертизах.

– «Балэкс» в баллистике.

– «Наркоэкс» в исследовании наркотических средств и многиедругие.

Персональные компьютеры не только уточняют и ускоряют экспертную деятельность. Если посмотреть с другой стороны, то, и одна методика, которая основана на использовании компьютеров, не охватывает всего процесса решения экспертной задачи. Их использование объективизирует ту или иную операцию, которая может относиться к самому процессу познания, так и к оценке полученных результатов.

Поэтому использование компьютерных технологий ни в коем случае не исключает использование качественного подхода к объекту познания.

С учетом всего сказанного становится очевидной важность проблемы определения границ, задач и условий использования компьютеров в сфере судебно-экспертной деятельности.

Список использованной литературы и источников

1. Федеральный закон от 31 мая 2001 г. №73-ФЗ «О государственной судебно-экспертной деятельности в РФ» // Российская газета. 2001. 5 июня.
2. *Бурцева Е.В.* Новые информационные технологии в судебной экспертизе: учебное пособие / Э.В. Сысоев, А.В. Селезнев, И.П. Рак, Е.В. Бурцева. Тамбов: Изд-во Тамбовского государственного технического университета, 2006.
3. *Гаврилов О.А.* Курс правовой информатики: Учебник для вузов. М.: НОРМА, 2008.
4. Компьютерные технологии в юридической деятельности / Крылов В.С. [и др.]; под ред. Н.С. Полевого, В.С. Крылова. М., 2001.
5. Криминалистика: Учебник для вузов / Аверьянова Т.В. [и др.]; под ред. Р.С. Белкина. М.: НОРМА, 2004.
6. Проблемы информационного и математического обеспечения экспертных исследований в целях решения задач судебной экспертизы. / Н.С. Полевой [и др.]; под ред. Н.С. Полевого. М., 2000.

А.К. Кичигина, И.В. Свиридова

Национальный исследовательский университет
«Белгородский государственный университет»

Научные руководители:

***Е.М. Маматов**, к.т.н., заместитель директора по учебной работе Института инженерных технологий и естественных наук, доцент кафедры прикладной информатики и информационных технологий НИУ «Белгородский государственный университет»,*

С.В. Игрунова *к.с.н., доцент, доцент кафедры информационных систем*
НИУ «Белгородский государственный университет»
А.Г. Жихарев, *к.т.н., доцент, доцент кафедры информационных систем*
НИУ «Белгородский государственный университет»

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ «КИНОТЕАТРА» С ИСПОЛЬЗОВАНИЕМ JAVASCRIPT, PHP И MYSQL

Роль «всемирной паутины» в жизни людей с каждым годом приобретает все большее значение. Старые «классические» приложения все больше получают распространение в виде онлайновых версий доступных из любой точки земли, где есть подключение к сети Интернет.

Рассмотрим разработку приложения всемирной паутины, которое будет хранитель информацию не только о зрителях, но так же и информацию о свободных местах на сеансы, информацию о текущем фильме, жанре этого фильма, возрастные ограничения на просмотр фильма.

На основании Российского законодательства предложено создать базу данных не только хранящую информацию о зрителях, пришедших на сеанс (в настоящее время введены возрастные ограничения на просмотр тех или иных фильмов), но так же и информацию о свободных местах на сеансы, информацию о текущем фильме, жанре этого фильма, возрастные ограничения на просмотр фильма.

Актуальность данной работы обеспечивается изучением технологии и внедрение в сайт ограничений российского законодательства, которые невозможно оценить без практических работ с предоставленным ими инструментарием. Разрабатываемое веб-приложение должно обеспечивать некоторый вариант автоматизации работы кинотеатра.

Кинотеатр – это общественное здание или его часть, оборудованные для публичной демонстрации кинофильмов. В ходе работы кинотеатра клиентам (зрителям) должна предоставляться информация о фильмах, находящихся в прокате. Но так же должна предоставляться информация касающаяся: стоимости билета на сеанс, свободных мест в кинозале, времени сеанса. Кассир предлагает

свободные места в зале, а клиент (зритель) вправе выбрать наиболее подходящее ему.

Кассир при покупке билета на фильм категории 18+ должен попросить у посетителя паспорт для того, чтобы зафиксировать продажу билета на данный фильм. В базу данных он будет вносить такие поля как: фамилия, имя, отчество, возраст. Данное нововведение позволит ужесточить продажу билетов тем лицам, у которых возраст не соответствует возрастному ограничению фильма.

Данные сгруппированы в разрабатываемой системе следующем образом: репертуар фильмов на сегодня (номер фильма, название фильма, дата показа фильма, время показа фильма); сведения о зрителях (номер зрителя, Фамилия Имя Отчество зрителя, возраст); данные в кассе (номер кассы, номер фильма, номер зрителя).

В разрабатываемой системе имеется возможность ведения данных: организация таблиц для задания режима работы кинотеатра и ссылок на них, ввод и редактирование данных в таблицах.

Конкретный вид и содержание концептуальной модели базы данных определяется выбранным для этого формальным аппаратом. Обычно для построения модели базы данных используют нотации, подобные ERдиаграммам.

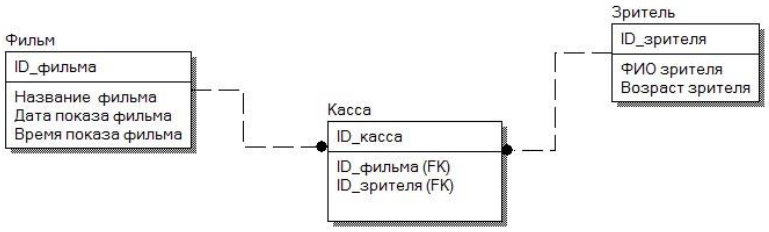


Рисунок 1. Концептуальная модель базы данных

Из рисунка 1, видно, что центральным элементом базы данных предполагается информация о кассе кинотеатра. Таблица билетов и сеансов кинотеатра предполагает последующую сортировку и вывод пользователю конкретной информации.

Между хранилищем базы данных и пользователем должна быть обеспечена связь, реализующая ряд операций над вводом, проверкой, сохранением, поиском и редактированием данных. Данная связь в конечном итоге будет предоставлять набор функциональных возможностей сайта о билетах и сеансах в кинотеатре.

В настоящее время программисту предоставлен очень широкий инструментарий для разработки веб-приложения. Это касается не только серверной части, где существует множество коммерческих решений, но и проектов с открытым исходным кодом. Помимо широкого выбора компонент для сервера, значительное развитие получила и клиентская часть, в которой выбор возможностей в плане производителей очень широк. Исходя из этого инструментом реализации web-приложения стали такие инструменты, как: HTML, CSS, JavaScript, PHP. Для наглядного отображения модулей приложения и связей между этими модулями, была разработана модульная схема приложения.

На рисунке 2 представлена модульная схема приложения.

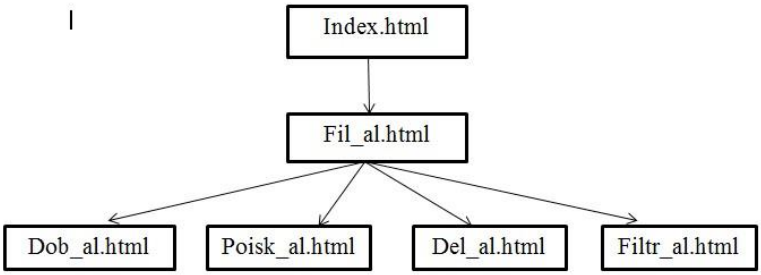


Рисунок 2. Модульная схема приложения

В таблице указано назначение каждого из модулей приложения.

Номер модуля	Название модуля	Описание модуля
1	Index.html	Главная страница сайта
2	Fil_al.html	
3	Dob_al.html	Страница добавления записей в таблицу «Зрители»
4	Poisk_al.html	Страница поиска по таблице «Зрители»

5	Del_al.html	Страница удаления записи в таблице «Зрители»
6	Filtr_al.html	Страница фильтрации по таблице «Зрители»

Пользовательский интерфейс представлен в виде страниц. Главная страница имеет расширение .html и является статической. Она представляет собой «визитную карточку», приветствующую посетителя. В навигационном меню, расположенном в левой части главной страницы расположены ссылки на основные интерфейсы подсистем Web-приложения. На страницах подсистем, также имеется навигационное меню, позволяющее перемещаться между подсистемами, а также вернуться на главную страницу.

На рисунке 3 представлен скриншот главной страницы сайта

Рисунок 3. Главная страница web-приложения

На рисунке 4 представлен скриншот страниц вывода данных из таблицы «Зрители».

Рисунок 4. Информация из страницы «Зрители»

Были рассмотрены такие аспекты как время, дата проведения сеанса и номер зала. Было разработано стабильное web-приложение для учета содержания сеансов и некоторой информации о них, такой как время проведения сеанса, дата проведения сеанса, номер зала.

С помощью данного приложения можно получить информацию о фильмах и сеансах и так же посетители этого web-ресурса смогут отправить администратору сайта и кинотеатра сообщение об ошибке во времени проведения сеанса, или же забронировать билет на тот или иной фильм через Интернет.

В итоге было достигнуто следующее: проанализирована предметная область и выбраны инструментальные средства web-приложения; спроектировано web-приложение; разработано web-приложение; протестировано созданное web-приложение.

Список использованной литературы и источников

1. *МакКоннел Стив.* Совершенный код. СПб.: Питер, 2005.
2. Принципы работы современного ателье одежды. URL: http://bigfashion.ru/odejda/principy-raboty-sovremennogo-atele-odezhdy.html.
3. *Дейт К.Дж.* Введение в системы баз данных. 8-е изд. М.: Вильямс, 2006.

А.В. Кохтов
ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт
*Научный руководитель: **П.В. Ересько**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

АНОНИМАЙЗЕРЫ ИЛИ «ДА Я ТЕБЯ ПО IP ВЫЧИСЛЮ»

В нынешних реалиях жизни в Интернете серьезно встает вопрос о конфиденциальности и защите своего присутствия на определенных ресурсах, и не важно, в каких целях вам это нужно, для удовлетворения ли собственной прихоти или же для поддержания анонимности личности, необходимой в следственных действиях. К одному из множества способов относят программы анонимайзеры.

Анонимайзер – изначально средство для скрытия информации о компьютере или пользователе в сети от удаленного сервера[37].

Клиентское ПО может подключаться к анонимайзеру как к прокси-серверу или, например, как веб-сайту (веб-прокси). На сегодняшний день веб-прокси наиболее популярны, так как не требуют каких-либо дополнительных настроек или программного обеспечения.

Работает веб-анонимайзер по следующему алгоритму:

– Пользователь заходит на веб-сайт, предоставляющий услугу анонимайзера.

– Вводит в адресную строку адрес веб-страницы, которую пользовательжелает посетить анонимно.

– Анонимайзер загружает эту страницу себе, обрабатывает ее и передаетпользователю от своего имени (имени сервера-анонимайзера)

Сфера использования анонимайзеров сегодня сместилась от обеспечения конфиденциальности информации о пользователе в сторону предоставления доступа к запрещенным в локальной сети веб-сайтам[42].

---

[37] URL: https://ru.wikipedia.org (дата обращения: 20.03.2016).
[42] URL: https://lurkmore.to (дата обращения: 20.03.2016).

Необходимо отметить, что использование анонимайзера не только не обеспечивает конфиденциальности передаваемых данных между пользователем и целевым веб-сервером, но и является дополнительным звеном возможности утечки персональной информации. При работе через анонимайзер нежелательно использовать значимые учетные записи, так как они могут быть легко скомпрометированы на сервере-анонимайзере.

При необходимости использовать анонимайзер рекомендуется избирать те, что уже зарекомендовали себя как более-менее надежные и работают уже на протяжении нескольких лет. Также необходимо отметить, что на 1 мая 2015 г. пользователям Рунета активно бесплатно предлагаются плагиныанонимайзеры для основных используемых браузеров. Практически пользователь, используя данные плагины, открывает свою личную информацию. Большинство запросов могут перехватываться через список IPадресов анонимайзеров, которые не особо скрываются. Таким образом, можно провести мониторинг, обработку статистики, обработать информацию. При содействии местных провайдеров очень легко определить местоположение якобы спрятавшихся - по MAC адресам. MAC адреса можно изменить только при наличии спецаппаратуры или старых сетевых или материнских плат с такой возможностью. Более новые варианты связи отслеживаются с такой же легкостью. Лучшим простым вариантом пока является «HTTPS://ddd.ddd.ddd.ddd», что тоже отслеживается, но не читается[38].

Но проще всего будет рассказать об анонимайзерах и о том, зачем они вообще нужны на конкретном примере.

Tor (сокр. От англ. The Onion Router) - свободное и открытое программное обеспечение для реализации второго поколения луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в

[38] Хамелеон – Анонимайзер. URL: cameleo.ru (дата обращения: 20.12.2015).

зашифрованном виде. Написана преимущественно на языках программирования C, C++ и Python.

С помощью Tor пользователи могут сохранять Анонимность В Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счет использования распределенной сети серверов-узлов. Технология Tor также обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только Приватность В Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом.

Tor оперирует сетевыми уровнями onion-маршрутизаторов, позволяя обеспечивать анонимные исходящие соединения и анонимные скрытые службы.

Социальные работники пользуются Tor при общении с учетом тонкой социальной специфики в чатах и веб-форумах для жертв насилия, конфликтов, беженцев, а также для людей с физическими или психическими отклонениями.

Это так же может быть полезным, например, для сбора данных о личности для судебно-психологических экспертиз.

В конце хотелось бы сказать, что анонимайзеры как таковые в основном используются для криминальной деятельности в Интернете, но у любой монеты две стороны. И раз уж (как выяснилось) личность, что скрыта за десятью маршрутами, всё-таки можно обнаружить, это дает возможность полиции и другим спец. службам находить и обезвреживать преступников.

Из всего этого можно сделать вывод, что программы-анонимайзеры очень полезны, как для обычного пользователя, так и в различных структурах, где личность, что скрыта за тем или иным никнеймом (ником) должна оставаться покрытой завесой тайны.

И.С. Кошелева

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ИСПОЛЬЗОВАНИЕ SMS-ГОЛОСОВАНИЯ В РАМКАХ ГОСУДАРСТВЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ «ВЫБОРЫ»

Целью работы является рассмотрение Государственной автоматизированной системы «Выборы», а именно sms-голосования.

Задачи:

– проследить, как работает технология sms-голосования;

– выявить достоинства и недостатки данной системы;

– выявить отношение избирателей к данной технологии.

На современном этапе совершенствования российской государственности происходит формирование элементов правового государства. На этой почве возникает проблема порядка образования правовой основы государственной власти и выстраивания избирательной системы, которые решила новая российская Конституция 1993 года. По Конституции РФ народ является единственным источником власти в стране, который осуществляет ее непосредственно, а так же через органы государственной власти и органы местного самоуправления[39].

Признаком демократического государства является выборность органов государственной власти и наличие прав у населения избирать и быть избранным. От того насколько данная система демократична, зависит в какой степени демократичности будут избираемые органы государственной власти и местного самоуправления.

С развитием избирательной системы совершенствуется и ее технологическая база, а прежде всего автоматизация избирательных процессов при подготовке и проведении выборов.

Число выборов с каждым разом возрастает, они становятся разнообразнее, и возникает потребность в чистых независимых выборах, которые могли бы контролировать избиратели и СМИ. При этом необходимо учитывать

[39] Конституция Российской Федерации. М., 2015.

особенности страны и что организация разного уровня выборов может проходить в один день.

Создание в соответствии с Указом Президента Российской Федерации от 18 августа 1995 г. Государственной автоматизированной системы Российской Федерации «Выборы» (ГАС «Выборы») разрешили организационные и технологические задачи.

ГАС «Выборы» — уникальная, мощнейшая информационнотелекоммуникационная система, охватывающая всю территорию России, самые удаленные районы и поселения[40]. Разработка и внедрение автоматизированных технологий происходит с учетом взаимосвязанного характера правовых, организационных и научно-технических аспектов.

Автоматизированная система является субъектом избирательного права. Функционирование ГАС «Выборы» регулируется федеральными законами, указами Президента Российской Федерации, нормативными правовыми документами ЦИК России.

Хотелось бы остановиться на такой возможности системы ГАС «Выборы», как электронное голосование по средствам мобильной связи.

Следует подробнее рассмотреть, как работает эта технология. Дистанционное электронное голосование может осуществляться по Интернету или по мобильным телефонам. Оно не требует от избирателя личного присутствия на избирательном участке в день выборов. Основным элементом системы дистанционного электронного голосования с использованием средств мобильной связи является программное обеспечение, разрабатываемое центром программных разработок компании «Интеллект Телеком».

Цель развития электронного голосования – снижение уровня вероятности искажения или подтасовки результатов за счет уменьшения влияния, на весь

---

[40] См.: Государственная автоматизированная система Российской Федерации «Выборы». URL: http://www.skachatreferat.ru/referaty/Государственная-Автоматизированная-Система-Российской-ФедерацииВыборы/77506.html (дата обращения: 18.03.2016).

процесс так называемого «человеческого фактора». Также возможно снижение воздействия на избирателя местного административного ресурса.

Но, к сожалению, все не так просто как кажется на первый взгляд. В действительности избирательный процесс, регламентируемый законодательством, накладывает массу условий.

Голосовать имеют право только те, кто достиг совершеннолетнего возраста и считается дееспособным. Никто не может голосовать дважды. Кроме того, голосование должно быть анонимным и достаточно открытым для наблюдения и, в случае чего, перепроверки результата. Все это требует включения в разработку системы электронного голосования таких параметров, как идентификация пользователя (гражданина), обезличивание собранных голосов, защита информации и т.п.

Самым важным в разработке системы электронного голосования является информационная безопасность. Возникает ряд вопросов: как будет подтверждена личность избирателя? Какими средствами можно предотвратить ложное голосование, то есть не допустить голосования от другого имени? Наконец, самый востребованный вопрос: как избиратель может проверить, что он получил доступ именно к сайту избирательной комиссии, а не к мошенническому ресурсу? Ответить на эти вопросы может позволить система электронной цифровой подписи, которая работает по принципу «открытого» и «закрытого» ключей. Электронные ключи (цифровые подписи), как серверу избирательного участка, так избирателю, могут выдаваться уполномоченным агентством (в российском случае – это система центров, созданных Федеральным агентством по информационным технологиям). Доступ к сайту избирательной комиссии для голосования граждан осуществляется при помощи «открытого» ключа. Результат голосования шифруется "закрытым" ключом и отправляется на сервер.

А за анонимность голосования ответственность несет провайдер. При проведении электронных выборов следует учитывать то, чтобы связь конкретного бюллетеня с определенным избирателем не прослеживалась. В

привычных для нас выборах мы убеждаемся в этом, исходя из того нет ли наших данных на бюллетени. С применением схем электронного голосования избиратели уже не смогут самостоятельно убедиться, что информация, позволяющая идентифицировать их личность, не была прикреплена к бюллетеню при отправке на сервер голосования. Для обеспечения анонимности используются серверы деперсонификации[41], стирающие эту информацию. Для многих людей, не знакомых с принципами работы системы, это будет вопрос веры. Да и в целом, доверие к электронным средствам голосования – одна из актуальнейших проблем.

Опрос при помощи мобильных технологий предусматривает использование специальной программы, но загружаться она будет на личный мобильный телефон избирателя. В настоящее время это осуществляет оператор избирательной комиссии. Небольшое Java-приложение для голосования загружается в телефон в заблокированном состоянии. Для разблокировки требуется сделать запрос на участие в дистанционных выборах.

После снятия блокировки на экране телефона отображается электронный бюллетень, гражданин может выразить свое мнение через SMS, которое будет защищено и отправлено приложением. Через SMS-шлюз результат голосования будет доставлен на сервер. Для того, что бы не произошло повторного голосования одним и тем же человеком или использования чужой SIM-карты, каждый избиратель получает уникальный код, действие которого производится однократно. Далее приходит оповещение об удалении приложения.

По данному способу голосования было высказано немало мнений. Так, Геннадий Иванович Райков, член ЦИК России и руководитель рабочей группы по изучению и разработке процедур электронного голосования избирателей, отзывался о данном способе: «Использование мобильного телефона оказалось наиболее защищенным с технической точки зрения и наиболее удобным. Одним из нареканий в адрес разработчиков данного метода были мелкий шрифт и

[41] Деперсонификация (лат. de persona лат. facere – делать) – отношение к другим людям таким образом, будто они являются неким безликим, бездушным предметом.

маленький размер бюллетеня. Мы достаточно быстро решили эту техническую задачу»[42].

В июне 2009 года благодаря SMS-голосованию был проведен опрос участников первого тульского молодежного образовательного форума «СЕЛИСТАРТ 2009». В августе в пределах Всероссийского молодежного образовательного форума "Селигер – 2009" также проводился эксперимент по использованию электронного голосования по средствам мобильного телефона. В данном способе применялась услуга подвижной радиосвязи стандарта GSM по передаче коротких текстовых сообщений /SMS/ и сеть Интернет как средство обмена информацией.

Для проведения электронного голосования с использованием средств мобильной связи была выработана специальная технология и методика, учитывающая специфику данного вида электронного голосования.

Каждый участник эксперимента получал PIN-код и инструкцию на бумажном носителе. Используя ее, он самостоятельно или с помощью консультанта загружал специальное программное обеспечение для электронного голосования на свой телефон.

После этого участник голосования мог (с 14.00 до 17.00 часов по местному времени) в любом месте запустить установленное программное обеспечение и, введя полученный PIN-код, приступить к процедуре голосования. При этом на экране мобильного телефона отображался список кандидатов, и участник голосования мог сделать соответствующий выбор. Информация о выборе шифровалась и отправлялась через SMS-шлюз на сервер хранения данных о результатах электронного голосования.

Если участник голосования не имел мобильного телефона, существовала возможность взять мобильный телефон у консультанта, с установленным программным обеспечением, проголосовать.

---

[42] «Электронный опрос избирателей в Единый день голосования 11 октября 2009 года». Интервью с членом ЦИК России Геннадием Райковым. URL: http://www.cikrf.ru/about/board/int/raikov/int_raykov_240909.html (дата обращения: 18.03.2016).

Как исключение, дополнительно для охвата всех участников Форума был предусмотрен режим голосования путем ручного набора текстового сообщения SMS определенного формата и отправки его на короткий номер.

В электронном голосовании приняло участие 1086 человек, ошибок с использование программного обеспечения так же не нашлось.

В целом, голосование прошло успешно и вызвало большой интерес у участников, которые отмечали удобство и быстроту процесса электронного голосования.

Последний масштабный эксперимент по проведению электронного опроса в России прошел в 2010 году, который проводился в Ленинградской области, а именно Кингисеппском городском поселении. Эксперимент прошел во время выборов депутатов Совета депутатов Кингисеппского городского поселения Кингисеппского муниципального района второго созыва. В рамках эксперимента голосование проводилось с использованием мобильного телефона. В ходе эксперимента проводился социологический опрос, который показал, что большинство граждан довольны электронным опросом (87% избирателей, принявших участие в эксперименте). Но каждый второй сомневается в достоверности его результатов[43].

В рамках данной темы мной был проведен электронный социологический опрос на сайте http://www.survio.com/ru/. Респондентами явились студенты из различных городов России, в возрасте 18-22, в количестве 29 человек. Опрос проводился с целью узнать, знает ли молодежь о такой технологии как SMSголосование. Данные опроса показали следующее.

Об электронных выборах слышало 75,9 % опрошенных. На вопрос о том, голосовали ли Вы по средствам SMS-голосования положительно ответило 34,5% опрошенных, а больше половины, что составило 58,6% не пользовалось данной услугой. Вопрос об удобности данной технологии у молодежи не вызвал сомнений, так удобной системой SMS-голосование считают 55,2% от общего

[43] Электронное голосование: возможности, технологии, вопросы. URL: http://www.gosbook.ru/node/11002 (дата обращения: 20.12.2015).

числа опрошенных, что, как мы видим, составляет больше половины. Актуальным вопросом стал вопрос о доверии данной технологии, так у 48,2% опрошенных, данная система вызывает доверие, а не доверяют этой системе 40,7% избирателей, а так же затруднились ответить 11,1% опрошенных. Из этого можно сделать вывод, что, действительно, как уже отмечалось выше, вопрос о доверии данной системы остается открытым.

На основе вышеизложенной информации, хотелось бы выделить достоинства и недостатки SMS-голосования.

Прежде всего, к достоинству данной системы стоит отнести экономии бюджета. Так же электронное голосование позволит гражданам отдавать свои голоса независимо от их местонахождения. Ведь случается так, что избиратель не может во время проведения выборов находиться на своем избирательном участке. В перспективе считается, что такое голосование повысит явку избирателей, в том числе молодежи.

Но, к большому сожалению, данная система не уникальна и имеет свои недочеты. Во-первых, мобильные телефоны не всегда используются теми, на кого они зарегистрированы. Во-вторых, для использования и установки данного программного обеспечения нужен подходящий сотовый телефон, который данную программу будет поддерживать и запускать. В-третьих, к недостаткам можно отнести и мелкий шрифт SMS-сообщения, который, для пожилых людей является достаточно отрицательным фактором.

В заключении хотелось бы сказать, что использование такой системы, несомненно, повысит явку избирателей в день выборов, приведет к росту активности молодежи. Ведь для того, чтобы представительная власть была эффективной и легитимной, необходимо создать все условия для ее успешного формирования. А здесь без новых технологий не обойтись.

Список использованной литературы и источников

1. Федеральный закон от 10 января 2003 г. № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации "Выборы"». Доступ из справ.-правовой системы «КонсультантПлюс».

2. Федеральный закон от 12 июня 2002 г. № 67-ФЗ (ред. от 28 декабря 2013 г.) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». Доступ из справ.правовой системы «КонсультантПлюс».

3. Официальный сайт Центральной избирательной комиссии Российской Федерации. URL: http://www.cikrf.ru/ (дата обращения: 25.03.2016).

4. Журнал Intelligent Enterprise. Спецвыпуск: ГАС «Выборы». URL: https://docviewer.yandex.ru/?url=http%3A%2F%2Fwww.cikrf.ru%2Fgas%2Fintelligent.pdf&name=intelligent.pdf&lang=ru&c=56f974067b59 (дата обращения: 20.03.2016).

5. *Баранова Е.* Электронное голосование // Интернет-журнал по широкополосным сетям и мультимедийным технологиям. URL: http://www.telemultimedia.ru/art.php?id=37 (дата обращения: 02.03.2016).

6. *Вешняков А.А.* Международно-правовой и зарубежный опыт применения электронных средств голосования при проведении выборов // Международное публичное и частное право. 2006. (дата обращения: 05.03.2016).

7. Тестирование технологии дистанционного электронного голосования с использованием средств мобильной связи в молодежной аудитории // Отчет по результатам исследования ЦИК России, М., 2009. С. 18-24, 33. URL: http://gosbook.ru/node/28330 (дата обращения: 25.03.2016).

8. Отчет по результатам исследования ЦИК России // Сайт Центральной избирательной комиссии Российской Федерации. URL: www . cikrf . ru / exp _ cik / test _ dist .pdf. (дата обращения: 25.03.2016).

Г.Д. Кузахметова

ФГБОУ ВО «Саратовская государственная юридическая академия»

Научный руководитель: ***Е.В. Варламова****, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

КОНТЕНТ-АНАЛИЗ С ПОМОЩЬЮ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПОЛИТОЛОГИИ

(на примере анализа Посланий Президента РФ)

Способность работать с содержанием текстов является значимым аспектом информационной и коммуникативной компетентностей современного специалиста. Существует множество методов анализа текстовых массивов, например, контент-анализ, дискурс-анализ, экспертная оценка текста и др. Тем не менее, наиболее популярным методом является метод контент-анализа.

Контент-анализ позволяет выявить официальную позицию власти и наиболее полно отразить политику власти в отношении субъектов общества (в своих Посланиях Президент обращается не только к Федеральному собранию, но к народу в целом). Хорошим подспорьем при проведении контент-анализа является машинный способ обработки теста. Актуальность данной темы обусловлена следующими факторами:

– обращение к специальному ПО позволяет автоматизировать некоторыеэтапы при проведении контент-анализа.

– при этом сокращаются сроки исполнения работы без потери качестваисследования.

– при проведении контент-анализа с помощью специального ПОснижается вероятность ошибки при кодировке текста.

– систематизация Посланий Президента РФ необходима гражданамдля выявления эффективности выполнения руководством страны ранее поставленных задач.

Целью данной работы является проведение контент-анализа Посланий Президента РФ Федеральному Собранию (2012-2014) с помощью специального программного обеспечения.

Отличительная черта контент-анализа заключается не только в «объективности» и «систематичности», а в самом количественном характере

метода. Контент-анализ предполагает числовую обработку компонентов текста, с последующим выявлением структурных закономерностей.

Мангейм и Рич в своей книге «Политология. Методы исследования» определяют контент-анализ как «систематическую числовую обработку, оценку и интерпретацию формы и содержания информационного источника[44]».

Для начала хотелось бы рассмотреть **TextAnalyzer v1.00**, которая позволяет выявить подробные характеристики текста. Она позволяет определить общее количество символов, букв, цифр, пробелов, предлогов и местоимений, а также выявить частотность употребления слов. Соблюдая законы хронологии, необходимо начать с анализа Послания 2012 года.

Послание Президента РФ Федеральному Собранию 2012 года представляет собой 29 листов напечатанного текста или видеоряд продолжительностью 83 минуты. Оно было озвучено 12 декабря 2012 года в Москве[45].

Табл. 1. Подробные характеристики Послания Президента России Федеральному Собранию 2012 г.

Всего символов	68134
Всего пробелов	9105
Символов без пробелов	59029
Всего строк	163
Всего букв	56496
Всего русских букв	56439
Всего латинских букв	21
Всего цифр	185
Всего запятых	1046
Всего точек	572
Остальных символов	730
Всего символов с предлогами	9300
Всего разных слов	3593
Всего предлогов и местоимений	2036

[44] *Мангейм Дж.Б., Рич Р.К. и др.* Политология: методы исследования. М., 1997.

[45] Послание Президента РФ Федеральному собранию от 12 декабря 2012 г. URL: http://kremlin.ru/events/president/transcripts/messages/17118 (дата обращения: 30.03.2016).

Следующее Послание было озвучено 12 декабря 2013 года в Москве. Данное Послание Президента РФ представляет собой 27 страниц печатного текста или видеоряд продолжительностью 71 минута[46].

Табл. 2. Подробные характеристики Послания Президента России Федеральному Собранию 2013 г.

Всего символов	57863
Всего пробелов	7459
Символов без пробелов	50404
Всего строк	182
Всего букв	48395
Всего русских букв	48348
Всего латинских букв	5
Всего цифр	116
Всего запятых	752
Всего точек	505
Остальных символов	636
Всего символов с предлогами	7656
Всего разных слов	3220
Всего предлогов и местоимений	1632

Послание Президента РФ Федеральному Собранию, озвученное в 2014 году в Москве, представляет собой 24 страницы печатного текста или видеоряд продолжительностью 70 минут[47].

Табл. 3. Подробные характеристики Послания Президента России Федеральному Собранию 2014г.

Всего символов	52414
Всего пробелов	6940
Символов без пробелов	45474
Всего строк	148
Всего букв	43472
Всего русских букв	43452
Всего латинских букв	0
Всего цифр	172
Всего запятых	789

[46] Послание Президента РФ Федеральному собранию от 12 декабря 2013 г. URL: http://kremlin.ru/events/president/transcripts/messages/19825 (дата обращения: 30.03.2016).

[47] Послание Президента РФ Федеральному собранию от 4 декабря 2014 г. URL: http://kremlin.ru/events/president/transcripts/messages/47173 (дата обращения: 30.03.2016).

Всего точек	431
Остальных символов	610
Всего символов с предлогами	7111
Всего разных слов	2952
Всего предлогов и местоимений	1673

Самое актуальное послание Президента РФ было озвучено относительно недавно – 3 декабря 2015 года в Москве. Оно представляет собой 25 страниц печатного текста или видеоряд продолжительностью 60 минут[48].

Табл. 4. Подробные характеристики Послания Президента России Федеральному Собранию 2015 г.

Всего символов	46340
Всего пробелов	6052
Символов без пробелов	40288
Всего строк	137
Всего букв	38508
Всего русских букв	38484
Всего латинских букв	0
Всего цифр	133
Всего запятых	725
Всего точек	410
Остальных символов	512
Всего символов с предлогами	6229
Всего разных слов	2791
Всего предлогов и местоимений	1349

Проведению контент-анализа помогает хорошо известная большинству пользователей ПК программа - Microsoft Office Word. В данном случае нас интересует функция «найти и заменить». Отмечу, что это «полуавтоматизированный» этап, так как для начала исследователю необходимо прочитать текстовый массив и выявить единицы счета в общем виде (обычно это слово или словосочетание). В данном случае единицами анализа выступили такие слова, как: экономика, Россия, общество, граждане\гражданин, суверенитет и т.д. После чего исследователь вызывает диалоговое окно «найти и

[48] Послание Президента РФ Федеральному собранию от 3 декабря 2015 г. URL: http://kremlin.ru/events/president/news/50864 (дата обращения: 30.03.2016).

заменить» и вписывает нужную единицу анализа. Важным является следующий момент: необходимо опустить падежное окончание, т.к. это позволит точно определить количество употребления той или иной единицы.).

После того, как исследователь определил область поиска слова как «Найти в основном документе» и просмотрел контекст употребления, можно вписать количество употребления данной единицы счета в сводную таблицу и переходить к следующей единице анализа.

С помощью MS Word на выходе получились следующие таблицы:

Послание Президента РФ Федеральному Собранию 2012 г.

Табл. 4. Частотность употребления категорий: внутренняя политика и внешняя политика.

Внутренняя политика		Внешняя политика	
Страна	46	Международный	6
Нация/национальный	30	Диалог	2
Россия	56	Безопасность	6
Суверенитет	5	СНГ	6
Развитие	39	Геополитическая востребованность России	1

Табл. 5. Частотность употребления категорий: социальная сфера и экономика.

Социальная сфера		Экономика	
Социальная сфера	8	Бюджет	13
Здравоохранение	2	Экономика	18
Демография	7	Налоги	15
Граждане	22	Бизнес	17
Общество	20	Эффективность\ный	10

Табл. 6. Частотность употребления категории духовная сфера.

Духовная сфера	
Патриотизм	6
Культура	20
Возможность	19
Образование	18

Спорт	16

Послание Президента РФ Федеральному Собранию 2013 г.

Табл. 7. Частотность употребления категорий: внутренняя политика и внешняя политика.

Внутренняя политика		Внешняя политика	
Нация	0	Украина	3
Россия	32	Международный	8
Суверенитет	1	Санкции	0
Стабильность	5	Терроризм	1
Развитие	45	Диалог	0
Конституция	13	СНГ	5
Муниципалитет/Внутренние органы самоуправления	15	Сирия	4
Страна	37	Иранская ядерная программа	4
		Безопасность	5

Табл. 8. Частотность употребления категорий: социальная сфера и экономика.

Социальная сфера		Экономика	
Социальная сфера	3	Инфраструктура	8
Здравоохранение	8	Экономика	13
Демография	5	Налоги	10
Граждане	21	Бизнес	15
Безработица	0	Инфляция	0
Работа	33	Бюджет	11
Общество	8	Эффективность\ный	8

Табл. 9.Частотность употребления категории духовная сфера.

Духовная сфера	
Свобода	0
Равноправие	1
Патриотизм	1
Культура	10
Возможность	14
Перспектива	5
Образование	20
Спорт	7

Послание Президента РФ Федеральному Собранию 2014 г.

Табл. 10. Частотность употребления категорий: внутренняя политика и внешняя политика.

Внутренняя политика		Внешняя политика	
Страна	10	Крым/крымский	11
Нация	5	Украина	16
Россия	50	Международный	7
Суверенитет	7	Санкции	4
Стабильность	4	Терроризм	6
Развитие	23	Диалог	6
Импортозамещение	4	Безопасность	9

Табл. 11. Частотность употребления категорий: социальная сфера и экономика.

Социальная сфера		Экономика	
Социальная сфера	10	Бюджет	7
Здравоохранение	4	Экономика	13
Демография	3	Налоги	8
Граждане	16	Бизнес	11
Безработица	0	Инфляция	4
Работа	23	Ослабление рубля	4
Общество	3	Капитал	5
		Эффективность\ный	10

Табл. 12. Частотность употребления категории духовная сфера.

Духовная сфера	
Свобода	8
Равноправие	7
Патриотизм	3
Культура	4
Возможность	5
Перспектива	5
Олимпиада	2
Образование	14
Спорт	9

Послание Президента РФ Федеральному Собранию 2015 г.

Табл. 13. Частотность употребления категорий: внутренняя политика и внешняя политика.

Внутренняя политика		Внешняя политика	
Страна	25	Турция/турецкий	7

Нация	10	Украина	0
Россия	54	Международный	6
Суверенитет	0	Санкции	0
Стабильность	2	Терроризм	31
Развитие	20	Сирия	8
Импортозамещение	4		

Табл. 14. Частотность употребления категорий: социальная сфера и экономика.

Социальная сфера		Экономика	
Социальная сфера	8	Бюджет	9
Здравоохранение	5	Экономика	22
Демография	6	Налоги	6
Граждане/нин	19	Бизнес	14
Работа	23	Капитал	9
Общество	17	Эффективность\ный	7

Табл. 15. Частотность употребления категории духовная сфера.

Духовная сфера	
Свобода	11
Патриотизм	1
Культура	3
Возможность	12
Перспектива	2
Образование	9
Спорт	2

Несмотря на то, что программа была разработана с целью создания текстов, а не их анализа, проведение контент-анализа в MS Word возможно при соблюдении некоторых нюансов.

После выделения категориальных групп, необходимо составить таблицы отношений (их ещё называют таблицами позиций), которые помогут прийти к объективным выводам при сравнительном контент-анализе. В данных таблицах употребление каждого слова оценивается по 3 критериям: положительный (+), негативный (-) или нейтральный (0) контекст. Построение таблиц позиций позволяет оценить категорию в контексте её употребления и подвести итоги при сравнительном контент-анализе.

Следует отметить и другие программы, которые позволяют провести качественный контент-анализ. К таковым относятся: Hamlet II 3.0, Vaal-mini, Tropes V8.4.

Основная идея Hamlet II 3.0 заключается в поиске частоты употребления слов в определенных текстовых массивах. Данную программу отличает лаконичность, в ней можно разобраться интуитивно, не обладая английским языком. Во всплывающем окне выводится само слово, количество употреблений и процентное соотношение.

Vaal-mini позволяет определить эмоциональный окрас как всего текста, так и отдельного слова. Нужно просто загрузить в программу текстовый массив в формате txt и выбрать интересующий анализ текста. Это наиболее известная программа, позволяющая проводить фоносемантический контент-анализ текста и слов на русском и украинских языках.

Что касается Tropes V8.4, то данное ПО также, как и предыдущие, осуществляет анализ текста. Характерной особенностью данной программы является визуализация проведенного анализа. Подсчитываются все части речи имена существительные, прилагательные, глаголы, наречия, предлоги и союзы. Также можно выбрать интересующее нас слово и посмотреть, какие иные категории с ним используются чаще всего.

Таким образом, мы видим, что существует очень обширный спектр программ для проведения контент-анализа. Это говорит о том, что данный анализ весьма актуален и пользователи заинтересованы в качественном ПО для исследований такого рода.

1. Контент-анализ занимает одну из ключевых позиций среди современных методов исследования политических текстов.

2. Контент-анализ позволяет проследить направленность текста и выявить ключевые позиции автора текста.

3. Благодаря контент-анализу Посланий Президента РФ Федеральному Собранию, удается перейти к абстрактной модели содержания текста, что позволяет выявить приоритетные направления развития страны.

Рассмотренные выше ПО, позволили прийти к следующим качественным выводам:

1. Центральной категорией в Послании Президента РФ Федеральному Собранию является «внутренняя политика», так как она включает фундаментальные вопросы, связанные с политическими и социальноэкономическими сферами жизни общества.

2. В рассмотренных Посланиях Президента РФ Федеральному Собранию за 2012-2015 гг. наблюдается тенденция смещения акцентов: если в Посланиях 2012-2013 гг. приоритет был отдан внутренней политике, то в 2014-2015 первенством обладает внешняя.

3. Послания В.В. Путина характеризуются широким функционалом, где всякого рода политические инициативы получают свое отражение в перечне поручений по реализации Послания Президента Федеральному Собранию.

Список использованной литературы и источников

1. Конституция Российской Федерации: по состоянию на 2015 год. С комментариями юристов. М.: Эксмо, 2015.
2. *Мангейм Дж.Б., Рич Р.К. и др.* Политология: методы исследования. М., 1997.
3. Послание Президента РФ Федеральному собранию от 12 декабря 2012 г. URL: http://kremlin.ru/events/president/transcripts/messages/17118 (дата обращения: 30.03.2016).
4. Послание Президента РФ Федеральному собранию от 12 декабря 2013 г. URL: http://kremlin.ru/events/president/transcripts/messages/19825 (дата обращения: 30.03.2016).
5. Послание Президента РФ Федеральному собранию от 4 декабря 2014 г. URL: http://kremlin.ru/events/president/transcripts/messages/47173 (дата обращения: 30.03.2016).
6. Послание Президента РФ Федеральному собранию от 3 декабря 2015 г. URL: http://kremlin.ru/events/president/news/50864 (дата обращения: 30.03.2016).

7. Ссылка для скачивания ПО Vaal-mini http://www.vaal.ru/prog/free.php.
8. Ссылка для скачивания ПО Hamlet II 3.0 URL: http://apb.newmdsx.com/hamlet2.html.
9. Ссылка для скачивания ПО Tropes V8.4. URL: http://www.semanticknowledge.com/download.htm.
10. Ссылка для скачивания ПО TextAnalyzer v1.00. URL: http://www.textanalyzer.ru.

Е.А. Кульгускина
ФГБОУ ВО «Саратовская государственная юридическая академия»
*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ВИДЫ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И СФЕРЫ ИХ ПРИМЕНЕНИЯ

Вследствие популярности использования информационных технологий во всех сферах жизни нашего общества управление процессами в организациях не является исключением из общего правила. Отдельное значение в этой сфере принимают системы электронного документооборота, которые предназначены для концентрации и автоматизации процедур взаимодействия между сотрудниками. Употребление указанных систем гарантирует эффективное управление документами организации и результативную работу сотрудников. Для организации электронного документооборота требуется использование электронной цифровой подписи, которая, также может потребоваться для выполнения различных торговых операций в онлайн режиме и сдачи отчетности в государственные органы. Именно поэтому обширное изучение электронной цифровой подписи, её видов и сфер применения является наиболее важным и актуальным аспектом на сегодняшний день.

Согласно ФЗ «Об электронной подписи», электронная подпись информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[49].

Электронная цифровая подпись в своём, более обыденном представлении, представляет собой некую совокупность данных, связанных с другими данными, которые помогают понять авторство и единство последних. По другому говоря, она позволяет установить, кто подписал тот или иной документ, и подвергался

[49] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) «Об электронной подписи» // Российская газета. 2011. 8 апреля.

ли изменению документ после подписания. Под документом здесь понимаются любые цифровые данные.

Механизм подписания по своей сути является шифрованием (точнее, криптопреобразованием) по определенному алгоритму на определенном ключе, причём любая уникальная комбинация исходных данных и ключа дает на выходе уникальный массив данных (подпись). Проверка подписи при этом представляет собой повторное её вычисление и сравнение с имеющейся на стороне проверяющего. Таким образом, если подпись неверна, то либо используется неверный ключ, либо документ не тот. Если с последним случаем всё понятно, то первый помогает нам определить авторство документа только при условии, что ключ однозначно принадлежит подписывающему и только ему.[50]

Видами электронных подписей, представляются простая электронная подпись и усиленная электронная подпись. Отличают усиленную неквалифицированную электронную подпись и усиленную квалифицированную электронную подпись.

1. Простой электронной подписью обозначается электронная подпись, которая путём употребления кодов, паролей или иных средств указывает на факт формирования электронной подписи обусловленным лицом.

2. Неквалифицированной электронной подписью обозначается электронная подпись, которая:

1) принята в результате криптографического изменения информации с применением ключа электронной подписи;

2) допускает определить лицо, подписавшее электронный документ;

3) дозволяет установить факт внесения изменений в электронный документ после момента его подписания;

4) реализуется с применением средств электронной подписи.

[50] *Рудин С.* Кратко об электронной цифровой подписи, ключах и сертификатах. URL: http://ecmjournal.ru/card.aspx?ContentID=4582659.

3. Квалифицированной электронной подписью признаётся электронная подпись, которая отвечает абсолютно всем признакам неквалифицированной электронной подписи и следующим факультативным признакам:

1) ключ проверки электронной подписи отмечен в квалифицированном сертификате;

2) для образования и проверки электронной подписи применяются средства электронной подписи.[51]

Функционирование УЦ осуществляется с целью совершенствования процесса официального электронного опубликования нормативно-правовых актов с использованием развитой квалифицированной электронной подписи.

Назначение удостоверяющего центра:

1. обеспечение сторон официального электронного опубликования нормативно-правовых актов развитой квалифицированной электронной подписью;

2. обеспечение сохранения единства и достоверности правовых актов в электронном виде;

3. обеспечение аутентификации сторон официального электронного опубликования правовых актов.

Услуги УЦ:

1. формирование сертификатов ключей проверки электронных подписей, ключей электронной подписи с гарантией сохранения в тайне ключа электронной подписи и выдача таких сертификатов по обращению участника;
2. экстрадиция сертификатов ключей проверки электронных подписей в форме документов на бумажных носителях и в форме электронных документов с информацией об их действии;

[51] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) «Об электронной подписи» // Российская газета. 2011. 8 апреля.

3. передача в электронной форме копий сертификатов ключей проверки электронных подписей лиц, внесенных в реестр сертификатов ключей проверки электронных подписей;
4. определение сроков действия сертификатов ключей проверки электронных подписей;
5. отмена, приостановление и возобновление действия сертификатов ключей проверки подписей;
6. ведение реестра выданных и отозванных сертификатов ключей проверки электронных подписей;
7. контроль за уникальностью открытых ключей проверки электронной подписи в реестре сертификатов ключей подписей;
8. осуществление подтверждения действительности электронной подписи уполномоченного лица УЦ в выданных им сертификатах ключей подписей[52].

В удостоверяющем центре используется лицензионное программное обеспечение, средства криптографической защиты информации и средства защиты от несанкционированного доступа, имеющие сертификаты ФСБ и ФСТЭК, что позволяет максимально полно предоставлять необходимый и широкий комплекс услуг.

Квалифицированная электронная подпись объявляется действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении приведенных ниже условий:

1) квалифицированный сертификат произведен и передан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа или на день проверки

[52] См. Регламент удостоверяющего центра ФСО России (утв. ФСО России 30 июня 2014 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

действительности указанного сертификата, если момент подписания электронного документа не определен;

3) существует положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка производится с применением средств электронной подписи, получивших подтверждение соответствия требованиям, с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) квалифицированная электронная подпись применяется с учетом ограничений, которые содержатся в квалифицированном сертификате лица, подписывающего электронный документ[53].

Исходя из этого, следует, что согласно 63-ФЗ «Об электронной подписи», позволяет Государственному удостоверяющему центру ФСО РФ выдавать квалифицированные электронные подписи.

Принципами употребления электронной подписи становятся:

1) право участников электронного взаимодействия применять электронную подпись различного вида по своему усмотрению;

2) допустимость применения участниками электронного взаимодействия по своему усмотрению различной информационной технологии и технических средств, применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для

[53] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) «Об электронной подписи» // Российская газета. 2011. 8 апреля. [59] Там же.

автоматического создания и автоматической проверки электронных подписей в информационной системе[59].

Для устройства и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны применяться средства электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

2. При создании электронной подписи средства электронной подписи должны:

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана.

3) При проверке электронной подписи средства электронной подписи должны:

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

4) Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

5) Требования частей 2 и 3 настоящей статьи не применяются к средствам электронной подписи, используемым для автоматического создания и автоматической проверки электронных подписей в информационной системе[54].

Процедура подачи заявки на создание сертификата ключа проверки электронной подписи:

Регистрация пользователя удостоверяющего центра на изготовление сертификата ключа проверки электронной подписи осуществляется на основании направляемого в удостоверяющий центр заявления на создание ключей электронной подписи и сертификата ключа проверки электронной подписи. Обязательным условием для получения ключа электронной подписи и сертификата ключа проверки электронной подписи является предъявление

[54] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) «Об электронной подписи» // Российская газета. 2011. 8 апреля.

пользователем удостоверяющего центра паспорта гражданина Российской Федерации и наличие ключевого USB-носителя с защищенной независимой памятью не менее 32 Кб (типа Rutoken или eToken). Для получения ключа электронной подписи и сертификата ключа проверки электронной подписи пользователь лично прибывает в Удостоверяющий центр соответствующего региона РФ[55].

По прибытии регистрируемого лица в удостоверяющий центр ему предоставляются на подпись два экземпляра сертификата ключа проверки электронной подписи на бланках удостоверяющего центра, которые пользователь удостоверяющего центра подписывает собственноручной подписью. Первый экземпляр сертификата ключа проверки электронной подписи на бланке выдается пользователю удостоверяющего центра, а второй экземпляр остается в УЦ. Пользователю удостоверяющего центра выдается комплект документов, включающий в себя:

1. ключ электронной подписи и сертификат ключа проверки электронной подписи, размещенные на ключевом USB-носителе;
2. первый экземпляр сертификата ключа проверки электронной подписи на бланке удостоверяющего центра.

В случае невозможности личного прибытия пользователя удостоверяющего центра ключ электронной подписи и сертификат ключа проверки электронной подписи могут быть выданы доверенному лицу пользователя удостоверяющего центра по доверенности.

По прибытии доверенного лица в удостоверяющий центр его идентификация осуществляется, путем сличения данных, указанных в доверенности пользователя удостоверяющего центра, с его паспортными данными.

Обязательным условием для выдачи (получения) сертификата ключа проверки электронной подписи является предъявление доверенным лицом документа, удостоверяющего его личность, и доверенности на получение

[55] Получение электронной подписи. URL: http://www.iecp.ru/ep/individual.

сертификата ключа подписи. Предъявленный документ, удостоверяющий личность доверенного лица, должен соответствовать документу, указанному в доверенности.

Сферы применения электронной цифровой подписи:

1. Электронный документооборот. Простая электронная подпись рассчитана для документооборота, предоставляет подтвердить авторство, но не обеспечивает неизменность документа после его подписания и не гарантирует юридическую ценность. Простая электронная подпись используется для приобретения доступа к возможностям Единого портала государственных слуг. Технология ЭП открыто применяется в системах электронного документооборота довольно разностороннего предназначения: внешнего и внутреннего обмена, организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и т.д. Это обусловлено важной чертой электронной подписи – она может быть применима как подобие собственноручной подписи или печати на бумажном носителе. Во внутреннем документообороте ЭП употребляется, как способ визирования и установления электронных носителей в пределах внутренних процедур. Например, во время согласования договора директор подписывает его ЭП, что значит, что договор утвержден и может быть передан в исполнение. При построении межкорпоративного документооборота наличие ЭП является абсолютно, весомым условием обмена, потому что является гарантом юридической силы. Только в таком случае электронный документ имеет право быть признан подлинным и применяться в качестве доказательства в судебных разбирательствах. Подписанный усиленной электронной подписью документ также может длительное время храниться в цифровом архиве, сохраняя при этом свою легитимность.

2. Электронные торги. Неквалифицированная электронная подпись помогает понять автора подписанного документа и подтвердить неизменность содержащейся в нем информации. В неквалифицированную электронную подпись положены основы криптографического алгоритма, которые

обеспечивают защиту документов. Такая подпись применима для внутреннего документооборота, а также для отправки электронных документов из одной компании в другую. Во втором случае, стороны обязаны заключить между собой соглашение, устанавливающие правила использования и признания электронных подписей. Неквалифицированная электронная подпись также подходит для участия в электронных торгах. Электронные торги идут на специфических участках (сайтах). Электронная подпись требуется поставщикам на государственных и коммерческих участках. ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Помимо всего, заключенные контракты принимают юридическую силу только при его подписании обеими сторонами[56].

3. Электронная отчетность для контролирующих органов.

Квалифицированная электронная подпись содержит все признаки неквалифицированной, но она может быть получена только в удостоверяющем центре, аккредитованном Минкомсвязи России. Программное обеспечение, необходимое для работы с КЭП, должно быть сертифицировано Федеральной службой безопасности. Вследствие этого, квалифицированная электронная подпись наделяет документы юридической силой и отвечает всем условиям о защите конфиденциальной информацию. КЭП употребляется для сдачи отчетности в контролирующие органы государственной власти и для участия в электронных торгах. Большинство компаний, однозначно, уже оценили и одобрили удобство сдачи отчетности в электронном виде. Современный путь к сдаче отчетности через Интернет состоит в том, что клиент имеет возможность выбрать любой практичный для себя способ: отдельное ПО, продукты семейства 1С, порталы ФНС, ФСС. Основная база данной услуги – это сертификат электронной подписи, который обязан быть предоставлен проверенным удостоверяющим центром, метод же отправки не имеет практически

[56] Федеральный закон от 5 апреля 2013 г. № 44-ФЗ (ред. от 9 марта 1916 г.) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Российская газета. 2013. 12 апреля.

определяющего значения. Такая подпись необходима для придания документам юридической силы.

4. Государственные услуги. Всякий гражданин Российской Федерации имеет право получить электронную подпись для получения госуслуг. Посредством ЭП гражданин может заверять документы и заявления, отправляемые затем в различные ведомства в электронном виде, а так же принимать подписанные письма и уведомления о том, что обращение получено на рассмотрение от надлежащих органов государственной власти. Пользователь имеет основание подписать электронной подписью заявление, которое будет отправлено в орган исполнительной власти (при готовности органа исполнительной власти принимать заявления, подписанные электронной подписью). При осуществлении представленного механизма применяются отечественные стандарты ЭП (ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) и используются сертифицированные в системе сертификации ФСБ России средства криптографической защиты информации, такие как «Aladdin e-Token ГОСТ» и «КриптоПроCSP», что позволяет считать такую подпись усиленной квалифицированной электронной подписью.

Вводимая на территории РФ универсальная электронная карта должна содержать так называемое федеральное электронное приложение, которое, по сути, является усиленной квалифицированной электронной подписью. Универсальная электронная карта (УЭК) – пластиковая карта, представляющая собой уникальное идентификационное средство гражданина. Основное предназначение УЭК - дистанционный заказ, оплата и получение государственных услуг. В идеале карта заменяет множество документов, в том числе медицинский полис и страховое пенсионное свидетельство, объединяя идентификационную карту, электронный кошелёк с привязкой к банковскому счету, электронную подпись и даже проездной билет[57].

[57] См. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Российская газета. 2010. 30 июля.

5. Документооборот с физическими лицами. Необходимо понять, что данная сфера применения ЭП довольно, своеобразна и ныне крайне редко используема, но всё же, возможна. Посредством ЭП заверять документы и иные носители могут физические лица. Вследствие этой возможности удаленные работники на основании договоров оказания услуг, например, могут выставлять акты приемки-сдачи работ в электронном виде.

Так же можно привести в пример использование электронной подписи в Арбитражном суде РФ. Так, при появлении различных споров между организациями в качестве доказательства в суде могут быть употреблены электронные документы. Согласно Арбитражному процессуальному кодексу РФ, полученные посредством факсимильной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам[58].

Таким образом, в заключение хочется сказать, что совершенствование и развитие, а также обширное применение информационных и коммуникационных технологий является основополагающей тенденцией мирового развития и научно-технической революции последних десятилетий.

На сегодняшний день, субъекты предпринимательской деятельности связаны с помощью электронного документооборота, как между собой, так и с конечными потребителями и органами государственной власти.

Задача преобразования российского законодательства в связи с переходом к предприимчивому применению электронного документооборота определена на государственном уровне. Правовым базисом регулирования электронной цифровой подписи как средства для придания юридической силы электронным документам является Федеральный закон «Об электронной цифровой подписи».

[58] Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ // Российская газета. 2002. 27 июля.

Ю.И. Кутенков

ФГАОУ ВПО «Дальневосточный федеральный университет»

*Научный руководитель: **В.И. Курилов**, д.ю.н., профессор кафедры трудового и экологического права, проректор по международным отношениям, директор юридической школы ФГАОУ ВПО «Дальневосточный федеральный университет»*

ПРАВОВОЕ ПОНЯТИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА В ТРУДОВОМ ПРАВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Актуальность заявленной темы настоящей работы в данный период времени обуславливается постепенным объективным появлением и дальнейшим стремительным развитием в Российской Федерации информационных телекоммуникационных технологий и компьютерной техники. В связи с их повсеместным использованием и распространением практически во всех сферах жизнедеятельности страны и российского общества постоянно ускоряется информатизация общества. Наблюдается постепенный объективный переход Российской Федерации и всего населения страны к информационному обществу. Электронный документооборот в трудовых правоотношениях между работником и работодателем становится реальностью.

Вместе с тем, указанные процессы не свидетельствуют и не влекут снятие существующих проблем в названной сфере. Объективная динамика общественных отношений в информационной сфере обуславливает появление новых проблем. К числу названных проблем относятся, в частности, проблемы правового понятия персональных данных работника. Неопределенность правового понятия персональных данных работника, его правовых признаков при отсутствии специализированных дефинитивных норм влечет противоречия правотворческой, правореализационной и правоприменительной, в том числе судебной деятельности, и существенно затрудняет поддержание необходимого баланса интересов личности, работника, работодателя, общества и государства в информационной сфере. В этих условиях анализ правовой категории персональных данных работника играет существенную роль в совершенствовании действующего нормативного правового материала в

трудоправовой сфере, обеспечивающем его соответствие реалиям современного времени.

Настоящая статья посвящена исследованию объективно формируемого в российском трудовом праве правового понятия персональных данных работника. Результатом указанной работы явилась выработка дефиниции указанного правового явления для ее включения в основной источник трудового права России – Трудовой кодекс Российской Федерации. В процессе достижения названной цели объективно потребовалась необходимость обращения к признакам персональных данных работника.

О признаках персональных данных работника прямо не упоминает ни Трудовой кодекс Российской Федерации (далее – ТК РФ)[59], ни Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ)[60]. Признаки персональных данных работника можно вывести путем логического анализа соответствующих положений данных нормативных правовых актов. По нашему мнению, признаками персональных данных работника являются следующие:

–конфиденциальность (секретность). В силу статьи 88 ТК РФ лица, получающие персональные данные работника, обязаны соблюдать режим *секретности (конфиденциальности*). Кроме того, данный признак раскрывается в статье 7 Закона № 152-ФЗ[61];

[59] Трудовой кодекс Российской Федерации // Собр. законодательства Рос. Федерации. 2002. № 1, ч. 1, ст. 3.

[60] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. 2006. 31 июля. № 31, ч. 1, ст. 3451.

[61] В соответствии с указанной статьей под конфиденциальностью персональных данных понимается то, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

–документированность[62] и официальность[63]. В ТК РФ названный признак подтверждают положения абз. 3 ст.89 ТК РФ, в соответствии с которым работники имеют право на свободный бесплатный *доступ* к своим персональным данным, включая право на получение *копий* любой *записи*, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом; абз.5 ст.89 ТК РФ, в соответствии с которым работники имеют право на *доступ* к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору. Подтверждением данного признака являются также положения п. 1 ст. 1[64]; п. 8 ст. 3[65]; п. 10 ст. 3, ст. 13[66]; п. 7 ст. 5[67]; п. 1 ст. 8[68]; пп. 5 п. 2 ст. 19 Закона № 152-ФЗ[75]. По нашему мнению, персональные данные работника могут содержаться только на материальном и (или) электронном носителе. В противном случае отпадает необходимость в их трудо-правовой охране и защите, поскольку визуально они нигде не будут зафиксированы и, следовательно, не будут обладают объективным, предметным характером, а просто будут представлять собой мнение о том или ином лице, клевету и т.п.;

---

[62] Под документированностью персональных данных работника мы понимаем их создание путем фиксации на материальном и (или) электронном носителе, а не в сознании и памяти людей. Указание на электронный носитель имеет важное значение в связи с введением в ТК РФ главы 49.1 «Особенности регулирования труда дистанционных работников» (Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 22 марта 2013 г. // Собр. законодательства Рос. Федерации. 2013. № 14, ст. 1668.), предусматривающей возможность обмена электронными документами между некоторыми субъектами трудового правая. См. напр.: ст. 312.1, 312.2 ТК РФ.

[63] В свою очередь под официальностью персональных данных работника нами понимается их документированность, материализацию, объективизацию (создание в объективной, телесной форме) овеществленность определенным лицом, как физическим, в том числе должностным, так и юридическим, в связи с тем, что персональные данные работника не могут взяться ни откуда. Источником их документированности всегда является определенное лицо.

[64] В котором говорится о поиске персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных и (или) доступ к таким персональным данным.

[65] В котором говорится об уничтожении материальных носителей персональных данных.

[66] В которых говорится об информационной системе персональных данных, представляющей собой совокупность содержащихся в базах данных персональных данных.

[67] В соответствии с которым хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных.

[68] В котором говорится об общедоступных источниках персональных данных (о справочниках, адресных книгах как формах выражения общедоступных источников персональных данных). [75] В котором говорится об учете машинных носителей персональных данных.

–достоверность. Данный признак обуславливает предыдущий признак иозначает, что документированности определенным лицом подлежат только достоверные и правдивые персональные данные о конкретном физическом лице;

- возможность представления другим лицам. Указанный признак обуславливает признак конфиденциальности (секретности) и документированной официальности;

–принадлежность конкретному физическому лицу (конкретномуработнику, как субъекту персональных данных). Данный признак вытекает из п. 1 ст. 3 Закона № 152-ФЗ [69] . Из указанной нормы права следует, что субъектом персональных данных не может быть юридическое лицо. Справедливой точки зрения придерживается проф. Ю.Г Просвирин, говоря о том, что понятие «персональная информация (данные)» обладает двумя признаками: во-первых, она должна относиться к конкретному человеку (в нашем случае к конкретному работнику), что позволило бы идентифицировать его прямо или косвенно. Вовторых, с учетом требования действующего законодательства такая информация должна быть зафиксирована на материальном носителе[70].

–объективность и субъективный характер установления[71]. Ранее в статье 85 ТК РФ при определении персональных данных работника прямо упоминалось о необходимости информации работодателю. Иными словами, в определении персональных данных содержался субъективный признак (необходимость работодателю). По нашему мнению, при определении персональных данных работника необходимо исходить именно из их объективного признака, объективного характера персональных данных, а именно их принадлежности к лично-профессиональным и деловым качествам работника.

[69] В соответствии с названным пунктом персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

[70] *Просвирин Ю.Г.* Защита персональных данных // Вестник ВГУ. Серия: Право. 2008. № 2. С. 175.

[71] Признак субъективного характера установления не следует путать с признаком официальности. В последнем случае речь идет о первоначальном создании конкретных персональных данных конкретного субъекта персональных данных, а не их закрепление в общем виде в документах, принимаемых государственными органами и работодателем.

По мнению некоторых авторов, категория «персональные данные» в значительной степени носит субъективный характер, и физическое лицо вправе самостоятельно относить к их числу те или иные сведения[72]; это подтверждается открытостью перечня персональных данных, установленного Законом № 152. По нашему мнению, данный подход не относится и не может быть применен к персональным данным работника, так как персональными данными работника является не любая информация, и соответственно, применительно не к любой информации работник может установить соответствующий режим защиты как со стороны государства, так и со стороны работодателя.

Однако, необходимо отметить, что при определении персональных данных работника все-таки может присутствовать субъективный признак[80] в их установлении. Указанный субъективный признак *в узком смысле* проявляется при установлении работодателем перечня персональных данных работника в локальных актах. При этом, по нашему мнению, данный субъективный признак персональных данных работника не может прикрывать собой их объективности, а именно их необходимости для непосредственного осуществления работником трудовой деятельности, связанности с выполнением конкретной трудовой функции и трудовыми обязанностями работника. Связанность персональных данных работника, указанных в названных документах работодателя, со спецификой деятельности работодателя и трудовой функцией работника необходима для того, чтобы избежать ряд негативных последствий и не допустить желание работодателя связать с трудовыми отношениями какую угодно информацию о работнике. Однако, если рассматривать субъективный признак *в широком смысле*, как проявление деятельности компетентных органов законодательной и исполнительной власти по субъективной объективизации государственной воли в правовые акты, то субъективный признак персональных данных работника является их неотъемлемым признаком;

---

[72] *Кучеренко А.В.* Этапы и тенденции нормативно-правового регулирования оборота персональных данных в Российской Федерации // Информационное право. 2009. № 4. С. 32-36. [80] В широком или узком смысле.

–прямая или косвенная идентификация (персонификация) с помощьюперсональных данных конкретного физического лица (конкретного работника, как субъекта трудового права) и, соответственно, их прямое или косвенное отношение к конкретному физическому лицу (конкретному работнику, как субъекту персональных данных). Необходимо отметить, что ни один правовой акт не говорит о том, что собой представляют прямые и косвенные персональные данные, и, соответственно, о прямом или косвенном определении (идентификации, персонификации) с их помощью конкретного физического лица, а также об их прямом или косвенном отношении к конкретному физическому лицу,

Как отмечают некоторые авторы, персональные данные представляют собой средство идентификации конкретного человека, т.е. выделяют его из множества на основе комплекса достоверно установленных идентификационных признаков[73]. Персонификация личности представляет собой необходимый и исходный элемент ее социализации в государстве, является важнейшей предпосылкой для включения личности в социальные контакты и создает юридическую платформу для реализации ее право- и дееспособности[74]. Персональные данные есть необходимый элемент социализации индивида. Они представляют собой его своеобразную визитную карточку в обществе и являются юридической основой для реализации его право- и дееспособности[75].

Говоря о признаке прямой или косвенной идентификации конкретного физического лица необходимо отметить, что данный признак также закреплен в определении персональных данных, содержащемся в ст.3 Закона № 152-ФЗ[76].
Из данного определения следует, что персональными данными является информация, относящаяся: к прямо или косвенно определенному и к прямо или косвенно определяемому физическому лицу.

---

[73] *Бугель Н.В., Никулин А.В.* Защита персональных данных как объект организационно-правового регулирования // Вестник Санкт-Петербургского университета МВД России. 2012. № 2. С. 231.

[74] *Петрыкина Н.И.* Правовое регулирование оборота персональных данных. Теория и практика. М., 2011.

[75] *Просвирин Ю.Г.* Указ. соч.

[76] Согласно которому персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

При этом указанное определение персональных данных не дает ответа на вопрос, с помощью кого и чего в современном правовом российском государстве достоверно устанавливается прямо или косвенно определенное, или определяемое конкретное физическое лицо. С помощью персональных данных? С помощью экстрасенсорных способностей? С помощью устного диалога с иным физическим лицом?

Необходимо отметить, что прямое или косвенное установление конкретного физического лица возможно при устном разговоре, диалоге с иным субъектом. Однако данный диалог и его результат, по своему существу, не являются персональными данными конкретного физического лица в силу вышеназванных признаков. Более того, возникают сомнения относительно абсолютной правдивости устного диалога. При устном разговоре правовая персонификация конкретного физического лица невозможна.

По нашему мнению, к прямым персональным данным человека, как гражданина Российской Федерации относятся данные, которые должны иметься у любого гражданина Российской Федерации, к примеру, данные, содержащиеся в паспорте[77] или ином документе, удостоверяющем личность (свидетельство о рождении (для лиц, не достигших 14-летнего возраста) [78], временное удостоверение личности гражданина РФ [79]. Следовательно, с их помощью возможна именно прямая идентификация (персонификация) конкретного физического лица. Все иные персональные данные относятся к числу косвенных.

---

[77] Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации : постановление Правительства РФ от 8 июля 1997 № 828 // Собр. законодательства Рос. Федерации. 1997. № 28. Ст. 3444. В соответствии с данным постановлением паспорт гражданина Российской Федерации является основным документом, удостоверяющим личность гражданина Российской Федерации на территории Российской Федерации. Паспорт обязаны иметь все граждане Российской Федерации, достигшие 14-летнего возраста и проживающие на территории Российской Федерации (п.1); Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации. См.: указ Президента РФ от 13 марта 1997 г. № 232 // Собр. законодательства Рос. Федерации. 1997. № 11. Ст. 1301.

[78] Приказ Минюста России «Об утверждении форм бланков свидетельств о государственной регистрации актов гражданского состояния» от 25 июня 2014 г. № 142 // Российская газета. 2014. № 157.

[79] Приказ ФМС России «Об утверждении Административного регламента Федеральной миграционной службы по предоставлению государственной услуги по выдаче и замене паспорта гражданина Российской Федерации, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации» от 30 ноября 2012 г. № 391 // Российская газета. 2013. № 122.

Соответственно, признак косвенной идентификации (персонификации) с их помощью конкретного физического лица позволяет охватить случаи, когда информация не включает имя лица, однако, учитывая определенный способ ее организации, можно при желании установить и имя субъекта информации. Например, информация, включающая в себя наименование и место окончания высшего учебного учреждения, название специальности, квалификации, стаж работы, настоящее место работы в совокупности дает возможность косвенным путем идентифицировать конкретного работника.

Таким образом, по нашему мнению, определенное или определяемое конкретное физическое лицо устанавливается прямо или косвенно с помощью, соответственно, прямых или косвенных персональных данных, с помощью информации, о которой как раз и говорится в определении персональных данных, указанном в Законе № 152-ФЗ.

Таким образом, из содержащегося в ст.3 Закона № 152-ФЗ определения персональных данных следует, что персональными данными является прямая или косвенная информация, относящаяся: к прямо или косвенно уже определенному с помощью нее (уже известному ранее) конкретному физическому лицу; к прямо или косвенно еще определяемому с помощью нее в данный момент времени (еще не известному ранее) конкретному физическому лицу.

Кроме этого, возникают следующие вопросы, можно ли прямо или косвенно определить в настоящий период времени уже известное для конкретного субъекта на данный период времени физическое лицо; можно ли прямо или косвенно не определить неизвестное физическое лицо? Ни один правовой акт не дает ответа на данные вопросы. Указанные вопросы, по нашему мнению, являются изначально неправильными в силу того, что определить (идентифицировать, персонифицировать) уже известное для конкретного субъекта физическое лицо априори ни прямо, ни косвенно невозможно, а вот установить принадлежность (отношение) соответствующих персональных данных именно указанному физическому лицу, вполне вероятно. В данном

случае прямые и косвенные персональные данные характеризуют именно принадлежность их конкретному физическому лицу, а не его определенность (идентификацию, персонификацию).

Таким образом, персональные данные не являются предметом определения (идентификации, персонификации) в данный период времени известного для конкретного субъекта физического лица, ибо могут быть им только в отношении неизвестного в данный период времени для конкретного субъекта физического лица. По нашему мнению, прямо или косвенно можно определить неизвестное для конкретного субъекта в данный период времени физическое лицо.

Однако многие могут сказать, что физическое лицо может быть определенно, известно для конкретного субъекта внешне. Однако внешняя известность не означает достоверную определенность указанного физического лица. Более того, сама визуальная не фиксированная внешность не является персональными данными физического лица, в отличии, к примеру, от фото на паспорте. Таким образом, внешняя известность не означает определенность указанного физического лица для конкретного субъекта, следовательно, внешняя известность не означает известность с правовой точки зрения конкретного физического лица. С юридической точки зрения данное физическое лицо является неизвестным для конкретного субъекта.

Определенное физическое лицо уже известно и было определенно конкретным субъектом ранее, будучи еще не известным с помощью как раз прямых или косвенных персональных данных, а неизвестное лицо, как раз и определяется конкретным субъектом на основании также прямых или косвенных персональных данных. Относительно уже определенного ранее физического лица необходимо отметить, что в данном случае не возникает вопрос о способе (прямом или косвенном) его определении. В данном случае на первый план выходит природа именно самих персональных данных (прямые или косвенные), а не способ определения с их помощью конкретного физического лица. В свою очередь для определения неизвестного ранее физического лица (субъекта персональных данных) на первый план выходит именно способ определения

(прямой или косвенный) данного физического лица, а не природа самих персональных данных.

С учетом изложенного, по нашему мнению, *персональные данные работника* можно определить, как любую зафиксированную на материальном носителе компетентным или уполномоченным органом или лицом прямую или косвенную конфиденциальную достоверную информацию, относящуюся к прямо или косвенно уже определенному с помощью нее для конкретного субъекта или соответственно, к прямо или косвенному определяемому с помощью нее в данный момент времени для конкретного субъекта конкретному работнику и характеризующую последнего с лично-деловой и профессиональной стороны в зависимости от выполняемой работником трудовой функции и специфики деятельности работодателя, за исключением случаев, прямо указанных в законе.

Из вышеизложенного следует, что включение указанного определения в российское трудовое законодательство, постепенно повысит эффективность норм, регламентирующих трудовую правовую охрану и защиту персональных данных работника в сфере труда.

М.И. Липанов, Т.Т. Конов

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПРОБЛЕМЫ РАСПРОСТРАНЕНИЯ РЕЛИГИОЗНОГО ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Сегодня проблема распространения религиозного экстремизма явно обозначена и для Российской Федерации. Об этом говорит большое внимание, уделяемое ей со стороны руководства страны в течении последних лет. Так, в ст. 37 Указа Президента Российской Федерации от 12 мая 2009 года «О Стратегии национальной безопасности Российской Федерации до 2020 года»[80]отмечается,

[80] Стратегия национальной безопасности Российской Федерации до 2020 года // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/99.html (дата обращения: 17.05.2015).

что основными источниками угроз национальной безопасности в сфере государственной и общественной безопасности является экстремистская деятельности националистических, религиозных, этнических и иных организаций и структур направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, что, безусловно, является тревожным знаком для всех без исключения граждан нашей страны.

Данные статистической отчетности показывают, что имеет место распространение религиозного экстремизма по территории РФ, причем количество преступлений экстремистской направленности ежегодно увеличивается. По данным доклада генпрокурора РФ Совету федерации от 28 апреля 2014 года[81] за последние десять лет в Российской Федерации произошел значительный рост преступлений экстремистской направленности (в 2004 году – 130, в 2013 – 896). Подобный «скачок» экстремизма, в том числе и религиозного, связан с широким развитием сети Интернет, где, как правило, и происходит вербовка новых кадров. Таким образом, молодежь, гуляющая по просторам сети Интернет, в первую очередь становится жертвами преступных намерений.

Что же на самом деле является «религиозным экстремизмом». На законодательном уровне Российской Федерации не дается чёткого разъяснения данного понятия что, безусловно, является пробелом, поэтому следует обратиться к определениям данного понятия и аспектам проявления религиозного экстремизма.

Так, Баглушкин Е.Г. понимает под «религиозным экстремизмом» – отрицание системы традиционных для общества религиозных ценностей и догматических устоев, а также агрессивную пропаганду идей противоречащих им[82].

---

[81] Генпрокурор: в РФ растет число регистрируемых экстремистских преступлений // ТАСС. Информационное Агенство России. URL: http://tass.ru/obschestvo/1153518 (дата обращения: 17.05.2015).

[82] *Баглушкин Е.Г.* Нетрадиционные религии в современной России: морфологический анализ. М., 1999. С. 172.

Сергун Е.П. в одной из своих работ дает немного иное определение этому явлению. По его мнению, «религиозным экстремизмом» можно считать активную приверженность к экстремистской идеологии, прямым или косвенным мировоззренческим источником (стимулом) которой выступают исторически-сложившиеся и современные нормы религиозного и оккультного характера, разработанные сектантами или иными основателями [83].

Очень распространена среди исследователей точка зрения Яворского М.А. относительно данного понятия. Он считает, что «религиозный экстремизм» есть крайняя форма реализации радикальной идеологии, выражающейся в осуществимых по мотивам религиозной нетерпимости противоправных деяний лиц или групп, приверженцев определенного вероучения, а также в публичных призывах к совершению таковых деяний по отношению к лицам и социальным группам, не разделяющим взгляды и убеждения экстремистов[84].

Как видно выше, понятие «религиозного экстремизма» в научных кругах толкуется по-разному, поэтому, чтобы избежать различного рода казусов, необходимы более полные разработки данного понятия с целью закрепления на законодательном уровне.

На наш взгляд, наиболее преуспел в этом плане Кокорев В.Г. Под «религиозным экстремизмом» он понимает совершение общественно опасных противоправных деяний по религиозным мотивам, выражающееся в крайней форме реализации радикальной религиозной идеологии, направленной на разжигание нетерпимого отношения к представителям других конфессий, либо проявляющееся в противоборстве в рамках одной конфессии[85].

Следует отметить, что часть экспертов призывают не употреблять термин «религиозный экстремизм», предлагая заменить его термином «религиознополитический экстремизм» или «экстремизм на религиозной почве»

---

[83] *Сергун Е.П.* Соотношение понятий «религиозный экстремизм» и «религиозный фундаментализм» // Правовая культура. 2012. № 2. С. 99.

[84] *Яворский М.А.* Причины и условия проявления религиозного экстремизма в современной России // Юридический мир. 2008. № 11. С. 22-24.

[85] *Кокорев В.Г.* Понятие и признаки религиозного экстремизма // Социально-экономические явления и процессы. 2014. № 5. С. 94.

так как за всяким религиозным явлением, в том числе религиозным экстремизмом, стоят политические, экономические или военные интересы, поэтому чистого религиозного экстремизма не существует [86]. Впервые это понятие «религиознополитический экстремизм» употреблено Н.П. Адриановым в 1981 году[87].

Такое разграничение, безусловно, имеет право на существование. Религиозно-политический экстремизм зачастую ставит перед собой цель изменить существующий государственный строй, нарушить суверенитет и территориальную целостность государства, а также навязать в качестве государственной идеологии определенное религиозное учение, утвердить власть определенной конфессии на территории всей страны или ее части с применением противозаконных методов и средств. В свою очередь религиозный экстремизм не преследует политических целей и главным образом проявляется в религии[88].

Существуют и иные разграничения религиозного экстремизма в научных кругах, однако целью данной статьи является рассмотрение этого явления в его первоначальном варианте.

Размещаемые в Интернете материалы экстремистского характера часто достаточно сложно отличить от материалов, направленных на распространение религиозных идеи исключительно мирного характера. Как утверждает В.Д. Лаза, в религии нет экстремизма, так как отстаивание своей веры является одним из основных положений многих конфессий [89]. Поэтому, необходимо иметь наглядные критерии для распознавания материала экстремистского характера.

Ознакомившись с имеющейся литературой по данной проблеме, мы поставили перед собой цель выявить эти критерии. В целом, большинство исследователей данной проблемы практически одинаково выделяют их, однако,

---

[86] *Биккинн Э.И.* Религиозный экстремизм в структуре преступлений, совершаемых на религиозной основе // Гуманитарные и социальные науки. 2011. № 5. С. 146.

[87] *Андрианов Н.П.* Советский образ жизни и атеистическое воспитание. М., 1981. С. 94.

[88] *Старосельцева М.М., Пелюх Е.И.* Религиозный экстремизм: интерпретация понятия? // Вестник Белгородского Юридического Института МВД России. 2012. № 2. С. 60.

[89] *Лаза В.Д.* Корни и Профилактика религиозного экстремизма // Вестник Пятигорского государственного лингвистического университета. 2008. № 2. С. 290-291.

на наш взгляд, именно Абдулганеевым Р. Ф. критерии сформулированы наиболее полно и четко, и мы их здесь приводим[90]:

1. отвержение общепринятых социальных ценностей. Общество придерживающееся их признается заблудшим, а его идеалы греховными;
2. пропаганда идеологии непринятия норм существующего общественного порядка через призывы к отказу от соблюдения мирских запретов и стремлению исключительно к беспрекословному подчинению идеологическим догмам экстремистского объединения;
3. враждебное отношение к традиционным конфессиям и их представителям, стремление к противостоянию с ними;
4. отказ от принятия и соблюдения правовых норм государства и формирования собственного правового пространства основанного только на мнимых теологических представлениях и духовных канонах;
5. противопоставление экстремистского религиозного объединения существующим институтам государственной власти. Признание их нелегитимными и призвания своих последователей к невыполнению их требований;
6. продвижение идеологии непримиримой борьбы со всякого рода инакомыслием и посягательством на истинность учения деструктивного религиозного объединения;
7. требование чистоты – резкое деление мира на «чистый» и «нечистый», «хороший» и «плохой»;
8. наличие эмоциональных способов воздействия на человека, с целью принудить к противоправным действиям.

Распространение названных критериев в сети Интернет под тем или иным предлогом, в том или ином виде является одной из наиболее опасных угроз. В целях предотвращения данных угроз Минюстом разрешается блокировка опасных сайтов. Однако подобная блокировка сайтов не дает полных гарантий

[90] *Абдулганеев Р.Р.* Деструктивные культуры и тоталитарные секты как источник распространения религиозного экстремизма // Юридическая наука. 2012. № 1. С. 77-78.

недоступности в дальнейшем использовать запрещенные ресурсы, так как существует множество различных способов обхода такой блокировки, коими активно пользуется молодежь.

Самым распространенным методам преодоления интернет-запретов являются использование анонимайзеров или VPN технологий. Анонимайзер – это программа или сервис, позволяющая пользователю скрыть от владельцев сайтов информацию о своем местоположении, а от операторов сети то, какие ресурсы данный пользователь посещает. Информация от пользователя к ресурсу и обратно передается по случайной цепочке узлов, восстановить целостность которой практически невозможно [91] . Проблема распространённости программного обеспечения такого типа и его широкого применения обсуждается не первый год. Еще в 2013 году Общественным советом при ФСБ России были предложены поправки в федеральный закон «Об информации, информационных технологиях и защите информации», в которых вводится ответственность за создания подобных сервисов и блокировка уже имеющихся анонимайзеров[92]. Однако, результаты такой инициативы на данный момент не наблюдается, в то время как в Белоруссии уже с 19 февраля 2015 года данный запрет вступил в силу[93].

VPN (или Виртуальная Частная Сеть) является самым стабильным способом обхода блокировок. Весь трафик пользователя шифруется и перенаправляется через внешний сервер – как правило, в другой стране. В данном случае, ввести запрет на частные сети практически не представляется возможным, так как они крайне важны для работы бизнеса. Такой запрет сильно ударит по коммерческим компаниям и потребует радикальных изменений в сетевой структуре

---

[91] Как подготовиться к новой атаке на интернет? // Meduza Project URL: https://meduza.io/cards/kakpodgotovitsya-k-novoy-atake-na-internet (дата обращения: 17.05.2015).

[92] Силовики предлагают запретить ПО, скрывающее пользователя в Сети // Известия URL: http://izvestia.ru/news/551271 (дата обращения: 17.05.2015).

[93] Постановление оперативно-аналитического центра при президенте республики Беларусь 19 февраля 2015 г. № 6/8 // Национальный правовой интернет-портал республики Беларусь URL: http://www.pravo.by/main.aspx?guid=12551&p0=T21503059&p1=1&p5=0 (дата обращения: 18.05.2015).

организации, что потребует от законодателя принятия множества специальных мер[94].

Таким образом, в результате предпринятого исследования выявлены следующие проблемы в сфере борьбы с религиозными и религиознополитическими экстремистскими объединениями на просторах сети Интернет:

1. отсутствие определения «религиозного экстремизма» на законодательном уровне, что дает возможность злоумышленникам трактовать его «в свое удобство»;
2. существование путей обхода блокировки запрещённых Минюстом ресурсов, что как минимум, делает такие запреты малодейственными.

Если первая проблема, на наш взгляд, в перспективе может быть полностью разрешена путем внесения поправок Государственной Думой в Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» [95] , то решение второй проблемы в настоящее время не представляется возможным из-за широкого использования VPN сетей коммерческими компаниями.

Список использованной литературы и источников

1. Стратегия национальной безопасности Российской Федерации до 2020 года // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/99.html (дата обращения: 17.05.2015).
2. Генпрокурор: в РФ растет число регистрируемых экстремистских преступлений // ТАСС. Информационное Агентство России URL: http://tass.ru/obschestvo/1153518 (дата обращения: 17.05.2015).
3. *Баглушкин Е.Г.* Нетрадиционные религии в современной России: морфологический анализ. М., 1999.
4. *Сергун Е.П.* Соотношение понятий «религиозный экстремизм» и

[94] Как подготовиться к новой атаке на интернет? // Meduza Project URL: https://meduza.io/cards/kakpodgotovitsya-k-novoy-atake-na-internet (дата обращения: 17.05.2015).

[95] Федеральный закон от 25 июля 2002 г. № 114-ФЗ (ред. от 31 декабря 2014 г.) «О противодействии экстремистской деятельности» // Российская газета. 2002. 30 июля.

«религиозный фундаментализм» // Правовая культура. 2012. № 2.

5. *Яворский М.А.* Причины и условия проявления религиозного экстремизма в современной России // Юридический мир. 2008. №11.

6. *Кокорев В.Г.* Понятие и признаки религиозного экстремизма // Социально-экономические явления и процессы. 2014. № 5.

7. *Биккинн Э.И.* Религиозный экстремизм в структуре преступлений, совершаемых на религиозной основе // Гуманитарные и социальные науки. 2011. № 5.

8. *Андрианов Н.П.* Советский образ жизни и атеистическое воспитание. М., 1981.

9. *Старосельцева М.М., Пелюх Е.И.* Религиозный экстремизм: интерпретация понятия? // Вестник Белгородского Юридического Института МВД России. 2012. № 2.

10. *Лаза В.Д.* Корни и Профилактика религиозного экстремизма // Вестник Пятигорского государственного лингвистического университета. 2008. № 2.

11. *Абдулганеев Р.Р.* Деструктивные культуры и тоталитарные секты как источник распространения религиозного экстремизма // Юридическая наука. 2012. № 1.

12. Как подготовиться к новой атаке на интернет? // Meduza Project URL: https://meduza.io/cards/kak-podgotovitsya-k-novoy-atake-na-internet (дата обращения: 17.05.2015).

13. Силовики предлагают запретить ПО, скрывающее пользователя в Сети // Известия. URL: http://izvestia.ru/news/551271 (дата обращения: 17.05.2015).

14. Постановление оперативно-аналитического центра при президенте республики Беларусь 19 февраля 2015 г. № 6/8 // Национальный правовой интернет-портал республики Беларусь URL: http://www.pravo.by/main.aspx?guid=12551&p0=T21503059&p1=1&p5=0 (дата обращения: 18.05.2015). 15. Федеральный закон от 25 июля 2002 г. № 114-ФЗ (ред. от 31 декабря 2014 г.) «О противодействии экстремистской деятельности» // Российская газета. 2002. 30 июля.

Б.М. Малахиров

ФГБОУ ВО «Уральский государственный юридический университет»

*Научный руководитель: **П.У. Кузнецов**, д.ю.н., профессор, заведующий кафедрой информационного права ФГБОУ ВО «Уральский государственный юридический университет»*

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО КОДЕКСА РФ

Право имеет двуединую природу: с одной стороны оно является показателем общего уровня развитости государства, а с другой стороны, призвано обеспечить это развитие. Общество не стоит на месте, оно постоянно развивается, а с ускоряющимися в геометрической прогрессии темпами научнотехнического прогресса, с внедрением информационных технологий в повседневную жизнь, право должно «гнаться» за эволюцией общества. И обеспечение этого процесса возложено не только на совершенствование правовых средств, методов правового регулирования, но и на систематизацию, формирование адекватных моделей систематизированных актов. Итак, кодификация – это важнейший шаг в совершенствовании системы права, производимая, в конечном счете, в целях соответствия норм права потребностям общества.

1. Отсутствие единой государственной политики

Информационное право, несмотря на недавнее возникновение, характеризуется наличием значительного массива нормативного материала: с 1990 г. принято около 1300 нормативно-правовых актов, так или иначе регулирующих отношения по поводу информации. Более того, данные законы и подзаконные акты подвергались неоднократным изменениям. Это свидетельствует не о полном, всестороннем и исчерпывающем правовом воздействии на отношения в информационной сфере, а об отсутствии единой рационально организованной программности информационного законотворчества. За неимением четкого представления о направленности

многие акты принимаются в связи с определенными конкретными событиями или особыми задачами в деятельности государства[96].

Подобная деятельность приводит как к нарушению системности отрасли: слабая связь актов и норм, их дублирование, несогласованность, а порой и противоречивость, так и их содержательным промахам: пробелы в правовом регулировании, декларативность, недостаточность механизмов реализации. Бессистемные попытки решить названные проблемы не имеют позитивного результата в силу того, что способ устранения недостатков должен быть адекватен сущности проблемы. Казуальное, выборочное решение проблемы ситуативного нормоустановления ведет к противоположным целям, в случае нарушения системности невозможно применение принципа «клин клином».

Сложность процесса определяет большой объем подготовительной работы для принятия кодифицированного акта: необходимо создание научно обоснованной концепции. Как отмечает выдающийся правовед Люблинский, «кодификация представляет вид законодательства, оплодотворенный юридической наукой, создающий новое право»[97]. В этом смысле позитивное влияние науки должно выражаться не только в формировании доктрины, но и оперативном реагировании на постоянно развивающиеся общественные отношения, что крайне актуально для отрасли информационного права.

Важен также следующий момент: законодательство не лишено субъективного фактора в смысле нарушения баланса интересов. Поэтому высокая обобщенность основополагающих положений может явиться фактором лоббизма. Действенным решением проблемы может стать предварительная конкретизация принципов соответствующей отрасли права до уровня программы правовой политики. В частности, ряд специалистов в свое время предлагал предварить принятие Лесного кодекса РФ разработкой и утверждением

---

[96] *Алексеев С.С.* Общая теория права. Т. 2. М., 1981. С. 251.

[97] Цит. по кн.: Теоретические вопросы систематизации советского законодательства / Под ред. С.Н. Братусь. М., 1962. С. 11.

Национальной лесной политики, основанной на балансе интересов разных лесных отраслей и страны в целом[98].

Кодифицированный акт, в сущности, не может и не должен регулировать все входящие в отрасль отношения, но избранную предметную область – полно, едино, юридически и логически цельно, внутренне согласованно. Данные суждения справедливы и по отношению к информационному законодательству, поэтому задача Информационного кодекса (далее – ИК) - дать основные принципы, требования к законодательству и закрепить исходные позиции для дальнейшего продвижения юридической основы развития информационного общества[107].

Целесообразность разработки ИК напрямую зависит от решения следующего вопроса: сможет ли он эффективно действовать в условиях отсутствия государственной политики в области информационного законодательства? В устоявшихся веками отраслях, вроде уголовного, гражданского права, для соответствия правового регулирования объективным потребностям регулярно издаются акты концептуального характера. Например, реформирование современного гражданского законодательства основывается на подобного рода документах (на данный момент действует Концепция развития гражданского законодательства Российской Федерации (одобрена Советом при Президенте РФ по кодификации и совершенствованию гражданского законодательства 7 октября 2009 г.)[108].

Во-первых, правовое регулирование призвано содействовать зарождению и дальнейшему развитию общественных отношений[109]. Именно нормы права непосредственно воздействуют на поведение людей, а не концепции, доктрины и программы. Последние направляют деятельность государственного аппарата, в том числе его законодательные органы, тем самым лишь опосредованно воздействуя. Исходя из понимания информационного общества как общества

[98] *Зорькин В.Д.* Концептуальные основы кодификации российского законодательства. Тезисы доклада на Международных правовых чтениях им. М.М. Сперанского «Кодификация российского законодательства» (Санкт-Петербург, 1 октября 2010 г.) // Конституционный суд РФ. Официальный сайт. URL:

гражданского, социального, демократического и правового, следует, что общественная инициатива, в частности в правотворческой деятельности,

http://www.ksrf.ru/ru/News/Speech/Pages/ViewItem.aspx?ParamId=38.

[107] Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М., 2014. С. 25.

[108] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ7 февраля 2008 г. № Пр-212) // Российская газета. 2008. 16 февраля. № 34.

[109] *Алексеев С.С.* Механизм правового регулирования в социалистическом государстве. М., 1966. С. 10.

должна быть учтена, поэтому уместно положить в основу ИК неофициальную научную концепцию.

Во-вторых, возможность руководствоваться основным комплексным документом – Стратегией развития информационного общества в Российской Федерации[99] (далее – Стратегия). Ее целью является повышение качества жизни граждан путем формирования информационного общества, которое характеризуется высокоразвитой информационной культурой, инфраструктурой и массовой информатизацией, широким доступом населения к информационным ресурсам, рынком информационных продуктов и приоритетным развитием информационного сектора экономики[100]. Отношения, возникающие на таком уровне развития общества, составляют предмет информационного права. Очевидно, что российское общество еще не в полной мере соответствует такому состоянию, но как уже отмечалось, правовое воздействие способствует социальному прогрессу.

Таким образом, отсутствие политики в рассматриваемой области с неизбежностью не приведет к «мертворожденному» акту. Первостепенным требованием к проекту ИК должно быть его научное обоснование, поскольку речь идет о такой специфической отрасли, то к разработке концепции должны быть привлечены не только правоведы, но и представители иных наук. Будучи результатом системного научного исследования, кодекс будет способен

[99] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) // Российская газета. 2008. 16 февраля. № 34.

[100] Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. П.У. Кузнецова. М., 2013. С. 160.

выполнять функцию направляющего вектора развития информационного законодательства.

2. Предмет Информационного кодекса

Фактором, определяющим предмет кодекса, является его значение для отрасли: он может быть основополагающим, базовым актом для всей отрасли или может содержать нормы отдельных(ого) институтов(а). На данный момент существует концепция ИК, разработанная ИГП РАН и предполагающая полипредметную модель акта.[101]

Согласно данной концепции, ИК должен выступить единым, генеральным актом в отрасли информационного права, отражая ее систему, поэтому кодекс должен также состоять из двух частей: общей и особенной. В определении содержания общей части все еще относительно ясно – в ней определяется предмет регулирования, его цели и задачи, место кодекса в системе законодательства, даются дефиниции основных понятий, закрепляются принципы, основные субъекты информационных отношений и их правовой статус.

Стоит отметить, что Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ на данный момент, в сущности, выполняет роль общей части и довольно успешно. Имеется обширная практика применения названного закона, его основные положения довольно стабильны, но он регулярно дополняется новыми нормами, что свидетельствует о необходимости определенной реструктуризации информационного законодательства.

Однако в науке информационного права отсутствует единая позиция относительно состава Особенной части. Для определения предмета регулирования Информационного кодекса важно провести «водораздел» между институтами, которые целесообразно отнести к информационным, и теми, которые логичнее отнести к иным отраслям и подотраслям права. Наиболее

[101] Выступление проф. Бачило И.Л. на Ученом совете ИГП РАН. Официальный сайт ИГП РАН. URL: http://www.igpran.ru/news/3415/.

чистыми относительно отрасли информационного права являются такие, как институт доступа к информации, институт обеспечения информационной безопасности, институт трансграничной передачи информации, киберпреступности, информационных конфликтов, информации, институт информационных ресурсов, институт информационных технологий[102].

Включению в кодекс подлежат, бесспорно, признаваемые институты: информации, информационных ресурсов, информационных технологий, передачи информации (в том числе трансграничной), доступа к информации, обеспечения информационной безопасности и информационных конфликтов. Именно их наиболее целесообразно положить в Особенную часть, в том числе с точки зрения определенности предмета и практического удобства поиска норм в конкретном акте.

Однако не стоит забывать о важнейшем качестве информационного права – его комплексности. Существуют отношения, находящиеся под «перекрестным» регулированием ИП и других отраслей и отношения, в которых информационный элемент является вспомогательным. Нельзя, забывать, что определенные группы норм попросту нельзя «вырвать» из их родной отрасли (например, уголовная и административная ответственность). Таким образом, кодекс должен быть широко и полипредметным и, соответственно, охватывать довольно широкий круг отношений в информационной сфере.

Концепция полипредметного ИК имеет альтернативу. Е.С. Андрющенко предлагает сконцентрироваться на одном предмете - информации: «если создавать кодекс с одним предметом, то есть шансы сделать его более цельным, чем, если пытаться решить в одном Кодексе несколько вопросов. Также, что немаловажно, Кодекс, охватывающий только один предмет, будет более понятным его пользователям»[103]. Такой подход не лишен смысла, например, в другой комплексной отрасли, экологическом праве, действуют

---

[102] Концепция Информационного кодекса Российской Федерации / под ред. И.Л. Бачило. М., 2014. С. .2529.

[103] Там же. С. 162.

кодифицированные акты, сосредоточенные на одном объекте: водный и лесной. В данной отрасли также обсуждалась возможность создания единого кодекса, но в виду того, что «получится громоздкий закон, содержащий и впитывающий тысячи статей природоресурсного законодательства, который превзойдет по объему четыре части ГК РФ; пользоваться им будет достаточно затруднительно, а изменяться он будет ежемесячно»[104]. В некоторой мере этого можно избежать за счет технико-юридических средств, в частности лаконичности формулировок, экономичного изложения норм и грамотным подходом к архитектуре кодекса.

Нам представляется, что такая модель кодекса менее предпочтительна, так как кодификация информационного законодательства производится не только в целях устранения проблем системности (слабая связь актов и норм, их дублирование, несогласованность, а порой и противоречивость), но и для восполнения пробелов правового регулирования (отсутствуют базовые законы «О праве на информацию», «О базах данных», «О реестровой информации, «Об электронных системах», «Об электронном документе» и другие)[105]. В случае концентрации на одном объекте результат не будет в полной мере оправдывать потраченные на его формирование средства и может породить новые противоречия в нормативной базе отрасли.

Разработка «с нуля» новых норм в рамках ИК, устанавливающих понятия вышеназванных объектов права, принципы, правовой статус субъектов и общее содержание подобных правоотношений, будет более целесообразна, нежели принимать их в рамках отдельных правовых актов с точки зрения рационализации огромного количества нормативных актов и опять же, организации их системности. Начальный этап кодификации как таковой, состоящий в анализе массива норм и мониторинге их реализации, исключительно сложен как в смысле объема, так и содержания. Поэтому формирование новых норм, определения их в места в структуре кодекса, создавая дополнительную нагрузку, может стать фактором снижения качества

[104] *Боголюбов С.А.* Проблемы и задачи Экологического кодекса // Экологическое право. 2010. № 6. С. 15.
[105] *Кузнецов П.У.* Основы информационного права: учебник для бакалавров. М., 2014. С. 205.

конечного результата. Данное суждение подтверждает тезис о первостепенности определения предмета Кодекса, важности здравой оценки возможностей законодателя по проведению кодификации в таком виде и о невозможности осуществления кодификации без активного деятельного участия научного общества.

На основании вышесказанного следует важнейший вывод о том, что кодекс не потерпит в разработке и принятии спешки и непродуманности. Промахи в определении предмета и структуры кодекса, с большой долей вероятности, приведут к прямо противоположным целям принятия акта. В процессе предметных обсуждений на уровне государственной власти можно достичь необходимого результата – привлечения экспертов в области информационного права и других специальных научных дисциплин.

Теоретические наработки концепции ИК послужат катализатором в принятии генерального акта. Грамотно разработанный кодекс, безусловно, поможет решить важные проблемы правового регулирования в информационной сфере. Однако до тех пор, пока действующее законодательство будет справляться с воздействием на информационные отношения, пусть и с оговорками, как таковая острая потребность в кодификации не будет иметь места. А существующий механизм регулирования справляется, соответственно, в ближайшем будущем не приходится говорить о законотворческой инициативе.

А.О. Мамонов

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ВОЗМОЖНОСТЬ ОРГАНИЗАЦИИ ЛОКАЛЬНЫХ СЕТЕЙ С КРИПТОЗАЩИТОЙ ПОСРЕДСТВОМ VPN СЕТИ

В современном мире значительное место в жизни людей занимает обработка информации посредством использования компьютера и сети Интернет. Для организаций компьютер играет большую роль при передаче и обмене информацией. Для удобства в какой-то организации можно организовать документооборот информацию через сеть Интернет, это облегчает работу организации, потому что можно получить документ за считанные секунды. С целью реализации локальной корпоративной сети могут использоваться VPN сети.

VPN (англ. Virtual Private Network- виртуальная частная сеть) – логическая сеть, создаваемая поверх другой сети. Коммуникации в данной сети осуществляются по публичным сетям с использованием обычных протоколов, но за счёт шифрования создаются закрытые от посторонних каналы обмена информацией. VPN позволяет объединить, например, несколько кабинетов в академии в единую сеть с использованием для связи между ними неподконтрольных каналов. VPN обладает многими свойствами выделенной линии, однако развертывается она в пределах общедоступной сети, например Интернет. Посредством туннелирования пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель-получатель данных» устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого. Основными компонентами туннеля являются: инициатор, маршрутизируемая сеть, туннельный коммутатор, один или несколько туннельных терминаторов.

Сам по себе принцип работы VPN не противоречит основным сетевым технологиям и протоколам. Тем не менее, принципиально новым моментом является пересылка пакетов через безопасный туннель, организованный в пределах общедоступной сети. Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации. Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения. Организацию виртуальной частной сети можно сравнить с прокладкой кабеля через глобальную сеть. Как правило, непосредственное соединение между удаленным пользователем и оконечным устройством туннеля устанавливается по протоколу PPP. Наиболее распространенный метод создания туннелей VPN - инкапсуляция сетевых протоколов (IP, IPX, AppleTalk и т.д.) в PPP и последующая инкапсуляция образованных пакетов в протокол туннелирования. Обычно в качестве последнего выступает IP или ATM и Frame Relay. Такой подход называется туннелированием второго уровня, поскольку «пассажиром» здесь является протокол именно второго уровня. Альтернативный подход - инкапсуляция пакетов сетевого протокола непосредственно в протокол туннелирования (например, VTP) называется туннелированием третьего уровня. Независимо от того, какие протоколы используются или какие цели преследуются при организации туннеля, основная методика остается практически неизменной. Обычно один протокол используется для установления соединения с удаленным узлом, а другой – для инкапсуляции данных и служебной информации с целью передачи через туннель.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит

инкапсулированное соединение (Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя, либо при установке соединения с другой защищённой сетью, сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь и удаленная сеть наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

Для авторизации клиентов выполняется проверка подлинности. При VPNподключениях возможными являются три формы проверки подлинности: на уровне пользователя по протоколу PPP; на уровне компьютера по протоколу IKE; проверка подлинности источника данных и обеспечение целостности данных

При проверке подлинности первого типа выполняется: для установления VPN-подключения VPN-сервер выполняет проверку подлинности клиента, пытающегося установить подключение и проверяет, имеет ли клиент требуемую авторизацию. При взаимной проверке подлинности VPN-клиент также выполняет проверку подлинности VPN-сервера.

Второй тип проверки является самым безопасным. Для установления сопоставления безопасности клиент и сервер используют протокол IKE для обмена предварительным ключом. В обоих случая VPN-клиент и VPN-сервер выполняют взаимную проверку подлинности на уровне компьютера.

При выполнении проверки третьего типа чтобы убедиться в том, что источником отправленных данных является другая сторона VPN-подключения и что данные переданы в неизменном виде, используют контрольные суммы шифрования. Контрольная сумма имеет ключ шифрования, который известен только отправителю и получателю.

Реализация корпоративной сети посредством VPN-сети осуществляется с использованием криптографических протоколов. Протокол – это

последовательность шагов, которые используют две и более сторон для совместного решения задачи. Последовательность имеет строгий порядок, пропуск шагов исключается. Критерии составления протоколов вполне определенны:

–все участники протокола должны принимать правила добровольно, безпринуждения;

–каждый участник, который использует протокол, должен быть заранееоповещен от правилах работы;

–протокол должен быть толкован однозначно, а все правила были четкиеи лаконичные;

–все возможные реакции участников должны быть заранее описаны впротоколе.

Криптографический протокол – это протокол с использованием криптографического алгоритма. При данном типе протокола участники не могут узнать или сделать больше, чем предусмотрено протоколом. Криптографические протоколы несут на себе следующие функции: проверку подлинности источника данных; проверку подлинности сторон; предотвращение утечки информации; неизменность данных

Криптографические протоколы классифицируют по следующим параметрам: по числу участников: двусторонний, трёхсторонний, многосторонний; по числу транспортируемых сообщений: интерактивный (одновременный обмен), не интерактивный (одновременно идет отправка только в одну сторону).

Самым оптимальным является подход классификации по целевому назначению. При выполнении одной функции криптографические протоколы классифицируются на следующие виды.

1. Протокол идентификации/аутентификации участников: односторонняя (обычно клиент доказывает свою подлинность серверу), двусторонняя (взаимная, применяется для взаимной аутентификации участников и для обмена ключом сессии)

2. Протокол распределения ключей. Главная функция в криптографической системе, так как стойкость такой системы зависит от ключа.

3. Протокол привязки к биту – протокол с 2 участниками, где отправитель передает бит данных так, что реализуются два условия: после передачи бита, отправитель не может изменить его значения, получатель не может сам определить значение бита и раскрывает его после реализации отправителем схемы раскрытия.

4. Протокол подбрасывания – протокол разрешает двум не доверяющим друг другу участникам сгенерировать общий случайны бит.

5. Протокол групповой подписи – подразумевает одновременное участие всех участников группы для формирования подписи. Отсутствие хотя одного участника не позволяет создать подпись.

6. Примитивный криптографический протокол — это протокол, не имеющий самостоятельного прикладного значения, но реализуется как основной компонент при создании прикладных криптографических протоколов.

7. Прикладной криптографический протокол – нужен для решения практических задач с помощью сервисов безопасности, они могут решать сразу несколько задач.

Примером вида криптографических протоколов является протоколы с арбитражем. У арбитра нет личной заинтересованности в достижении тех или иных целей, преследуемых участниками протокола, и он не выступает на стороне одного из них. Участники протокола принимают на веру все, что скажет арбитр, и беспрекословно следуют всем его рекомендациям.

Одним из примеров протокола с арбитражем является адвокат. Но попытки перенести протоколы с адвокатом в качестве арбитра из повседневной жизни в компьютерные сети наталкиваются на существенные препятствия:

– легко довериться адвокату, про которого известно, что у негонезапятнанная репутация и с которым можно установить личный контакт.

Однако если два участника протокола не доверяют друг другу, арбитр, не облаченный в телесную оболочку и существующий где-то в недрах компьютерной сети, вряд ли будет пользоваться у них большим доверием.

– расценки на услуги, оказываемые адвокатом, известны. Кто и какимобразом будет оплачивать аналогичные услуги арбитра в компьютерной сети?

– введение арбитра в любой протокол увеличивает время, затрачиваемоена реализацию этого протокола.

– поскольку арбитр контролирует каждый шаг протокола, его участиев очень сложных протоколах может стать узким местом при реализации таких протоколов. Соответствующее увеличение числа арбитров позволяет избавиться от данного узкого места, однако одновременно увеличиваются и расходы на реализацию протокола.

В силу того, что все участники протокола должны пользоваться услугами одного и того же арбитра, действия злоумышленника, который решит нанести им ущерб, будут направлены, в первую очередь, против этого арбитра. Следовательно, арбитр представляет собой слабое звено в цепи участников любого протокола с арбитражем.

Несмотря на отмеченные препятствия, протоколы с арбитражем находят широкое применение на практике.

Итак, задачами криптографических протоколов являются: обеспечение различных режимов аутентификации; генерация, распределение и согласование криптографических ключей; защита взаимодействий участников; разделение ответственности между участниками.

Криптографические протоколы очень часто подвергаются атакам. При пассивной атаке взломщик не участвует в протоколе, он только следит за протоколом и пытается раздобыть ценную информацию. При активной атаке взломщик пытается изменить протокол к собственной выгоде. Существует атака по словарю. Она позволяет сравнивать краденный зашифрованный файл паролей с приготовленным файлом зашифрованных вероятных паролей, отыскивая

совпадения. Затруднить атаку по словарю можно использованием случайных строк, которые вступают во взаимодействие с паролями перед их обработкой функцией. Защита от атак с повторной отсылкой сообщений заключается в том, что операции шифрования и цифровой подписи должны различаться. Для этого нужно использовать разные ключи для каждой операции, либо использовать разные алгоритмы в каждой операции, либо наложение меток, либо создание цифровых подписей с применением хешфункций.

Способами противодействия атакам с воспроизведением сообщений являются использование порядковых номеров сообщений, меток даты/времени, уникальных запросов (оказий) и ответов, содержащих корректное значение оказии. Включив текущее время в криптографические протоколы, мы мешаем злоумышленнику пересылать старые сообщения под видом новых.

Но успешная атака на систему часов (перевод часов назад или вперед, остановка часов) приводит к отправке сообщений с неправильной даты/времени, что может иметь большие последствия. Помешать атаке на систему часов можно, связывая между собой метки даты/времени всех сообщений.

При организации VPN-сети для обеспечения документооборота в какойнибудь компании следует соблюдать законы о служебной тайне, коммерческой, врачебной и т.д. В самой организации или компании должны быть предприняты меры по обеспечению защиты информации от несанкционированного доступа. Они включают: организационные, технические меры. Разграничение и соблюдение прав доступа, а также автоматический мониторинг обмена информацией между компьютера в сети, который позволит при утечке информации определить, между какими компьютера был проведён обмен особо защищаемой информацией. Законодательные меры защиты информации представлены такими правовыми документами, как, например: Закон РФ от 21 июля 1993 г. № 5485-1 (ред. от 8 марта 2015 г.) «О государственной тайне», Федеральный закон от 29 июля 2004 г. № 98-ФЗ (ред. от 12 марта 2014 г.) «О коммерческой тайне».

В статье 10 в ФЗ «О коммерческой тайне» говорится об определённых мерах, которые необходимы для защиты информации. Например, организация должна: определить перечень документов, которые составляют коммерческую тайну; ограничить доступ к этой информации; вести учёт лиц, которые получили информацию; регулировать отношения по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и другие.

Также государство накладывает на получателей тайной информации определённые условия, которые закреплены ст. 14 ФЗ «О коммерческой тайне». Например: Органы государственной власти, иные государственные органы, органы местного самоуправления обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями. При несоблюдении охраны тайной информации физические и юридические лица, организации несут ответственность в соответствии с законодательством Российской Федерации.

Таким образом, сегодня возможно создать корпоративную сеть поверх внешней сети Интернет посредством VPN, и криптографические протоколы вкупе с законодательными мерами могут обеспечить должный уровень защиты информационного обмена.

Список использованной литературы и источников

1. https://ru.wikipedia.org/wiki/ (дата обращения: 12.03.2016).
2. *Денисова Т.Б.* Криптографические протоколы: задачник. Самара, 2006.
3. Основные виды криптографических протоколов http://infoprotect.net/varia/kriptograficheskie_protokolyi (дата обращения: 12.03.2016).
4. Основные понятия криптографии. URL: http://www.intuit.ru/studies/ courses/691/547/lecture/12371?page=4 (дата обращения: 12.03.2016).

5. http://pro-spo.ru/network-tech/4304-chto-takoe-vpn-ili-kak-zashhitit-set (дата обращения: 11.03.2016).
6. https://ru.wikipedia.org/wiki/VPN(дата обращения: 11.03.2016).
7. https://technet.microsoft.com/ru-ru/library/cc731954(v=ws.10).aspx (дата обращения: 11.03.2016).
8. https://offliner.ru/vpn/ (дата обращения: 12.03.2016).

Л.Р. Мингазова
ФГАОУ ВО «Казанский (Приволжский) федеральный университет»
*Научный руководитель: **О.Н. Низамиева**, к.ю.н., доцент кафедры гражданского и предпринимательского права КФУ*
ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

ПРОБЛЕМА РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ PRODUCT PLACEMENT НА YOUTUBE

Почти каждому представителю современной молодежи хорошо известен такой интернет-ресурс, как YouTube. Если в России индустрия блогинга только набирает обороты, то в США, Великобритании и Канаде блогеры в возрасте от 13 до 29 лет уже зарабатывают тысячи долларов за свои видео, активно сотрудничают с известными брендами и набирают миллионы просмотров и подписчиков.

Люди чаще всего обращаются к советам блогеров, рассчитывая на максимально честные и справедливые отзывы. Однако все не так просто, как кажется. Чем популярнее блогер, тем больше у него шансов заработать на своем канале. Популярным блогерам часто поступают коммерческие предложения от известных брендов.

К сожалению, не все рекламодатели и блогеры в равной степени добросовестны при использовании рекламы на YouTube. Часть блогеров не скрывает того, что видео спонсировано, и это, в свою очередь является «маячком» для зрителя. Иные блогеры чаще используют маркетинговый прием под названием «product placement».

Данный термин не имеет нормативного закрепления ни в Федеральном

Законе «О рекламе», ни в каком-либо другом нормативно-правом акте в отечественной системе права. В Директиве Европейского Парламента и Совета Европейского Союза об аудиовизуальных медиа-услугах под product placement понимается «любая форма аудиовизуальных коммерческих сообщений, суть которого во включении или ссылке на продукт, услугу или торговую марку таким образом, что она становится частью программы, в обмен на платеж или по схожим соображениям»[106].

В соответствии с положениями п. 9 ст. 2 Федерального Закона от 13 марта 2006 г. № 38-ФЗ «О рекламе» действие данного закона не распространяется на «упоминания о товаре, средствах его индивидуализации, об изготовителе или о продавце товара, которые органично интегрированы в произведения науки, литературы или искусства и сами по себе не являются сведениями рекламного характера». Product placement – это особая форма рекламы, особенно распространенная на интернет-ресурсе YouTube.

Следует разграничивать понятия «скрытая реклама» и «product placement». В положении п. 9 ст. 5 ФЗ «О рекламе» под скрытой рекламой понимается реклама, «которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами»[107].

С одной стороны, product placement является ненавязчивой квазирекламой. С другой стороны, зритель, попадет под неосознанное воздействие по причине того, что блогер говорит о том или ином товаре или услуге исключительно, как рядовой потребитель, а не субъект рекламы.

Следует отметить, что product placement направлен на повышение лояльности к торговой марке. Кроме того, немаловажно учитывать и моральный аспект product placement. Он не осмысливается зрителем критически. Так,

---

[106] Директива Европейского Парламента и Совета Европейского Союза «О координации некоторых законодательных, регламентарных и административных положений, действующих в Государствах-членах ЕС, относительно оказания аудиовизуальных медиа-услуг (директива об аудиовизуальных медиа-услугах)». 2010/13/ЕС от 10 марта 2010 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[107] Федеральный закон от 13 марта 2006 г. №38-ФЗ (в ред. от 8 марта 2015 г.) «О рекламе». Доступ из справ.-правовой системы «КонсультантПлюс».

блогер, рассказывающий зрителю о любимых косметических продуктах, не вызывает такой агрессии, какую может вызывать обычная реклама. Однако нередко подобные рекомендации оплачиваются компаниейрекламодателем. Мы считаем, это вводит зрителей в заблуждение. Однако зритель с каждым годом становится все более зорким и учится замечать product placement. Поэтому с каждым разом блогерам становится все труднее «обелиться» перед зрителями. Многие блогеры указывают в информации под видео, что оно не спонсировано. На наш взгляд, это хорошая практика.

Таким образом, в современное законодательство о рекламе необходимости внести изменения, а именно:

1) урегулировать размещение рекламы на YouTube, т.к. сейчас данный интернет-ресурс становится также обширной площадкой для рекламодателей;

2) ввести в российское законодательство понятие product placement,т.к. отрицать наличие данного явления уже невозможно, а оно, в силу своего быстрого развития, нуждается в правовом регулировании.

3) прописать в ФЗ «О рекламе» обязанность блогеров и их партнеровсообщать зрителю о том, что данное видео спонсировано.

Е.А. Модина

ФГБОУ ВО «Владимирский государственный университет
имени А.Г. и Н.Г. Столетовых» Юридический институт

*Научный руководитель: **Д.Н. Мешков**, к.ю.н., доцент кафедры финансового права и таможенной деятельности ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых»*

К ВОПРОСУ ОБ ОТМЕНЕ ТРУДОВЫХ КНИЖЕК И ВВЕДЕНИИ ИХ ЭЛЕКТРОННОГО АНАЛОГА

Информационные технологии, постоянно развиваясь, проникают во все сферы жизни общества. Сегодня невозможно представить жизнь без технических достижений. Сфера трудовых отношений не исключение.

Вопрос об отмене трудовых книжек возник довольно давно. Еще в 2006 году выдвигалась подобная инициатива. Однако она так и не была реализована. Ведь, что представляет собой трудовая книжка?

В соответствии со статьей 66 Трудового кодекса Российской Федерации[108](далее – ТК РФ) трудовая книжка установленного образца является основным документом о трудовой деятельности и трудовом стаже работника. Трудовая книжка – своего рода паспорт трудовых свершений. Данный документ впервые появился в Англии, позднее - в годы Великой Французской революции – во Франции.

В России первые трудовые книжки появились в октябре 1918 года после издания Советом народных комиссаров Декрета о трудовых книжках для нетрудящихся. В этом документе говорилось, что поскольку труд является обязанностью граждан республики, то вместо паспортов и других удостоверений личности теперь будут использоваться трудовые книжки.

В советское время введение трудовых книжек преследовало несколько целей: во-первых, упорядочить систему назначения пенсий, во-вторых, укрепить трудовую дисциплину.

Таким образом, трудовая книжка – это документ, благодаря которому работодатель может узнать в каких организациях и в какое время специалист официально работал, каковы причины увольнения, и этот документ не представляет для работодателей каких-либо трудностей.

Однако в настоящее время многие считают, что трудовая книжка – это пережиток прошлого, который утратил свой первоначальный смысл. В частности, в августе 2011 года официальный представитель Министерства здравоохранения и социального развития объявил о подготовленных поправках в трудовое законодательство, связанных с отменой трудовой книжки и о грядущем внесении соответствующего законопроекта на рассмотрение в Государственную Думу.

Планируемая отмена трудовых книжек, по мнению сторонников реформы в Министерстве здравоохранения и социального развития РФ и профильном

[108] Трудовой кодекс Российской Федерации. М., 2015. С. 43.

комитете Государственной Думы, имеет следующие положительные моменты для работодателей:

– во-первых, освобождение от оформления целого ряда документов, чтостановится возможным в связи с переходом на электронный документооборот, межведомственный обмен данными;

– во-вторых, снятие дополнительной нагрузки с работников кадровых служб пооформлению трудовых книжек и выдаче их заверенных копий, по ведению книг учета движения трудовых книжек и т. п.;

– в-третьих, отпадение необходимости обеспечивать надежную охрануупраздняемых документов;

– в-четвертых, исчезновение риска предоставления работником нелегальнокупленной трудовой книжки с ложными сведениями;

– в-пятых, работники иногородних представительств организации не будутвынуждены неделями ждать пересылки трудовых книжек в результате увольнения.

В то же время с отменой трудовых книжек возникнет немало проблем, среди которых можно выделить следующие:

– Пенсионный фонд РФ не сможет обеспечить получение работодателямисправок для последующего трудоустройства работников.

– работодатель, который желает проверить сведения из резюме, будетвынужден звонить в организации, в которых ранее был трудоустроен работник. Это означает, что кадровым службам крупных организаций придется постоянно отвечать на обращения со стороны новых работодателей.

– организация – прежний работодатель – может быть ликвидирована, а, следовательно, работник будет не в состоянии предоставить рекомендательное письмо.

– один из главных минусов – сотрудники отдела кадров не смогут рассчитыватьстаж для оплаты больничного листа.

– работник будет вынужден до достижения им пенсионного возраста ипрекращения трудовой деятельности хранить все трудовые договоры, которые он когда-либо заключал.

Однако в рамках предложений по модернизации трудовой книжки предлагается введение ее электронной версии, то есть в качестве альтернативы бумажной трудовой книжки будет использоваться электронная трудовая книжка. Об этом заявила заместитель председателя правительства РФ Ольга Голодец.

Электронная трудовая книжка – это аналог трудовой книжки на бумажном носителе, используемый в качестве регистрационного документа у работодателя и в Государственных учреждениях – Центрах занятости населения (ОГУ ЦЗН) для первичной регистрации, перерегистрации и поиска работы в информационной системе ОГУ ЦЗН.

Стоит отметить, что по результатам опроса, проведенного Исследовательским центом портала «Superjob.ru»[109], идею введения электронных трудовых книжек поддерживает 39 % экономически активных россиян и 40 % работодателей, выявляя в этом новшестве немало плюсов, а именно:

1 – страховка на случай утери бумажного документа;

2 – защита от недобросовестных работодателей;

3 – как уже отмечалось ранее, облегчение работы отдела кадров ибухгалтерии;

4 – контроль над отчислениями компаний во внебюджетные фонды идругие положительные моменты.

Среди молодых людей в возрасте до 24 лет доля одобряющих возможное введение электронных трудовых книжек составляет 42 %, а респонденты в возрасте старше 45 лет относятся к этой идее с осторожностью (одобрение – 37 %).

[109] URL: http://www.superjob.ru/community/life/68388 (дата обращения: 28.03.2016).

Однако противников введения электронных трудовых книжек тоже немало – 35 % среди экономически активного населения России и 40 % среди работодателей. Аргументируя свою позицию, они заявляют:

1 – о недостаточной защите электронных архивов от взлома;

2 – о слабом оснащении многих предприятий современной компьютернойтехникой и технологиями;

3 – о дополнительных финансовых расходах, которые потребуются нанововведения.

Кроме того, по мнению граждан: «Достаточно одного вируса, чтобы уничтожить целую базу и, как следствие, весь трудовой стаж».

Таким образом, по нашему мнению, к введению электронной трудовой книжки нужно подойти с осторожностью. Несомненно, что в связи со стремительным развитием информационных технологий, этот шаг представляется закономерным. Однако следует учесть, что это не единовременный и трудоемкий процесс, который потребует немало финансовых и трудовых затрат. Для того чтобы полностью отказаться от бумажных трудовых книжек, нужно учесть все плюсы и минусы, возможность наступления негативных последствий, а также модернизировать технические ресурсы и обеспечить надежную систему безопасности персональных данных работников.

Кроме того, потребуется ряд новелл в законодательство, а именно:

1. внести изменения в статью 65 ТК РФ, давая право работодателю требовать рекомендательные письма с прежних мест работы;

2. пересмотреть положения законодательства, касающиеся работы по совместительству (ст. ст. 60.1, 282 – 288 ТК РФ);

3. уточнить порядок подтверждения трудового стажа для ПФРФ;

4. изменить процедуру выдачи загранпаспортов и виз, предусматривающих предоставление копии трудовой книжки и ряд иных нововведений[110].

Только тогда, взвесив все «за» и «против», можно с уверенностью ответить на вопрос: Нужна ли нам электронная трудовая книжка?

Список использованной литературы и источников

1. Трудовой кодекс РФ от 30 декабря 2001 г. №197-ФЗ // Собрание законодательства РФ. 7 января 2002 г. № 1. Ч. 1. Ст. 3.
2. Постановление Правительства РФ от 16 апреля 2003 г. №225 «О трудовых книжках» // Собрание законодательства РФ. 2003. 21 апр. № 16. Ст. 1539.
3. Трудовые книжки уже не актуальны. Пресс-конференция заместителя министра здравоохранения и социального развития РФ Александра Сафонова. 4 августа 2011 года // Информационный портал Интерфакс. URL: http://www.interfax.ru/txt.asp?id=202211 (дата обращения: 28.03.2016).
4. Административный регламент ФМС по предоставлению государственной услуги по оформлению и выдаче паспортов гражданина РФ, удостоверяющих личность гражданина РФ за пределами территории РФ и по исполнению государственной функции ее учета, утвержденный Приказом ФМС от 3 февраля 2010 г. №26 // Российская газета. 2010. 5 марта. №5125.
5. *Филипова И. А.* Трудовые книжки и последствия их возможной отмены. // Вестник Нижегородского университета им. Н.И. Лобачевского. 2012. № 3.С. 295–300.

[110] Административный регламент ФМС по предоставлению государственной услуги по оформлению и выдаче паспортов гражданина РФ, удостоверяющих личность гражданина РФ за пределами территории РФ и по исполнению государственной функции ее учета, утвержденный приказом ФМС от 3 февраля 2010 г. №26 // Российская газета. № 5125. 2010. 5 марта. № 5125.

6. *Баркевич М. М., Харчева И. В.* Отмена трудовой книжки // Современные наукоемкие технологии. 2013. №10. С.219–221.

К.О. Моисеев

ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»

*Научные руководители: **С.С. Гельбух**, к.ф.-м.н., доцент кафедры информационные системы и технологии, начальник Управления информатизации и телекоммуникаций ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»; Е.А. Новикова, старший преподаватель кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ЗАЩИТА УНИВЕРСИТЕТСКОЙ СЕТИ С ПОМОЩЬЮ СТАТИСТИЧЕСКОЙ МОДЕЛИ ТРАФИКА ЗАПРОСОВ WEB-ШЛЮЗА

Стремительный прогресс телекоммуникационных средств и информационных технологий, общедоступность и востребованность программного обеспечения за последние двадцать лет привели к распространению различных информационных систем повсеместно.

Современные информационные системы могут объединять разнотипные аппаратные ресурсы, программные системы, и, конечно, пользователей разного уровня. Масштабные характеристики таких систем постоянно растут.

По мере расширения объёма и видов сетевых услуг, приобретают всё большую актуальность проблемы обеспечения защиты сетевых служб от преднамеренного воздействия с целью нарушения обслуживания (Dos-атак).

Задачи, направленные на оптимизацию процессов обнаружения нежелательного трафика, в последнее время, набирают всё большую популярность. Важнейшим фактором является то, как быстро система отреагирует на подозрительный трафик.

В наши дни существует огромное количество типов атак на сети предприятий и университетов. Некоторые рассчитаны на удар по уязвимостям операционной системы, некоторые по уязвимостям любого установленного программного обеспечения, а некоторые по уязвимостям топологии сети и сетевой инфраструктуре.

Киберпреступники всегда совершенствуют свои методы атаки, результатом их атак может оказаться несанкционированный доступ к конфиденциальной

информации, выведение всей системы из строя, а также её захват с возможностью использовать для совершения новых атак на другие сети.

Необходимо понимать, какого типа сетевые атаки смогут угрожать университетской сети, для того чтобы обеспечить её защищённость.

Основные типы сетевых атак на сеть можно классифицировать:

По характеру воздействия – на активные и пассивные атаки.

Активная атака стремится ослабить работу частей системы или всей системы. Этого можно достигнуть, например, с помощью изменения конфигурации системы или логики работы сетевых соединений и сервисов.

Пассивная атака реализует угрозу раскрытия путем прослушивания каналов связи и не оказывает при этом воздействия на функционирование системы.

По расположению источника - на внутренние, сетевые и межсетевые атаки.

При внутренней атаке источник расположен в одном домене с атакуемым объектом и может прослушивать абсолютно все сетевые пакеты объекта.

Во время сетевой атаки источник находится в одной IP-сети с атакуемым объектом, но сеть может быть сегментирована коммутатором, вследствие чего атакующий может прослушивать только широковещательные пакеты объекта.

В случае межсетевой атаки источник и объект расположены в разных IPсетях, разделенных либо маршрутизатором, либо межсетевым экраном.

Все типы атак характеризуются свойственным только им сценариями обмена сетевыми пакетами, и существует реальная возможность формализовать сценарии сетевого трафика для каждого типа атак. Поэтому можно без разработки сложных интеллектуальных систем на основе набора типовых признаков выявить факт проведения сетевой атаки какого-либо типа, что существенно снижает временные затраты.[111]

На сегодняшний день для общества обретает всё наибольшую значимость информационная составляющая, и, в результате чего, защита информации

[111] *Сенеенков П.* Киберпреступность. М., 2011.

приобретает всё большее значение. Для её обеспечения создаётся качественная и полная, по своему охвату, нормативно-правовая база.

В нынешней законодательной системе рассмотрены все виды информации: от общедоступной информации и заканчивая гостайной. Для всех типов защищаемых данных устанавливаются конкретные меры гражданско-правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил ее защиты, указанные в соответствующих нормативно-правовых актах. Данная детализация позволяет обеспечивать на правовом уровне максимальную степень защиты информации[112].

В системах, которые направлены на обнаружение сетевых атак основную роль играют применяемые методы анализа поступающей информации. От этого зависит эффективность работы всей системы.

Первоначально в таких системах, которые были написаны ещё в начале восьмидесятых, использовались статистические методы. На сегодняшний день к статистическому анализу добавились новые методики, начиная с экспертных систем и нечеткой логики и заканчивая использованием нейронных сетей[113].

Статистические параметры в рамках некоторой адекватной модели трафика могут использоваться в качестве сигнатуры состояния системы сервисклиент, их изменения могут служить индикатором изменения состояния этой системы, в том числе угрожающего воздействия на систему со стороны клиента.

Главным преимуществом статистического метода является применение зарекомендовавшего себя аппарата математической статистики и адаптация математического аппарата к поведению субъекта.

Статистические методы исследования предполагают количественный анализ трафика. Системы защиты, основанные на таких методах, выполняют мониторинг поведения системы и ведут контроль значения характеристических

---

[112] *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002.

[113] *Лукацкий А.* Обнаружение атак. СПб., 2008.

величин. Любое отклонение величины от эталона будет считаться несанкционированной деятельностью.

Особенность таких систем – они способны обнаружить принципиально новые типы атак. Статистические методы достаточно универсальны, т.к. для проведения анализа трафика не требуется знаний о возможных атаках и используемых ими уязвимостях.

Использования статистических параметров временных рядов в качестве индикатора изменения состояния системы позволит на ранних этапах выявить DOS-атаку.

Для повышения защищённости университетской сети стоит задача по разработке системы обнаружения атак за счёт статистического анализа трафика.

В исследовании проводился мониторинг сервера университетской сети ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.».

Было реализовано приложение, используемое для сбора, хранения, обработки и анализа информации о состоянии сети и сетевой нагрузке в реальном времени. Приложение применяется системными администраторами для принятия необходимых мер, направленных на защиту сети от Dos-атаки.

Программа основана на анализе временных рядов. Реализована процедура, позволяющая автоматически обнаружить подозрительные (т.е. которые аномально отклоняются от тренда) значения. В основе процедуры лежит представление о ряде как о сумме тренда и случайной составляющей. Соответственно, выброс – это точка, находящаяся от предполагаемой линии тренда слишком далеко.[114]

Для того чтобы построить модель временных рядов используют экспериментальную информацию (информацию, полученную в реально функционирующей сети).

[114] Статистический анализ и мониторинг научно-образовательных интернет-сетей / И.С. Енюков, И.В. Ретинская, А.К. Скуратов; под. ред. А.Н.Тихонова. М., 2004.

Статистические модели сетей в виде временных рядов более достоверны, т.к. основаны на большом множестве экспериментальных данных и, соответственно, наиболее информативны для анализа состояния сети.

Необходимо понимать, что сетевая безопасность – это эволюционный процесс. Не существует продуктов, которые способны предоставить университету или предприятию «полную безопасность». Надежность защиты сети обычно достигается сочетанием различных продуктов и услуг, а также грамотной политикой безопасности и ее соблюдением всеми сотрудниками организации.

Сейчас в Интернете можно найти большое число обучающих материалов и готовых программных продуктов, которые позволяют реализовать несанкционированный доступ к компьютерным сетям. Многие статьи написаны на доступном языке и дополнены подробными инструкциями по реализации сетевых атак. Проблема не в наличие данных материалов в свободном доступе, а в слабости современных технологий по защите сетей.

Если безопасность сети будет нарушена, то юридическая ответственность в результате может повлечь за собой значительные расходы и уголовное наказание. Поэтому проблема защиты компьютерной сети в последнее время является наиболее актуальной и ей уделено огромное внимание.

Н.И. Новикова

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **В.К. Федоров**, к.т.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Развитие информационных технологий, их вторжение в среду человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё больше актуальными – и параллельно более сложными. Технологии обработки информации непрерывно совершенствуются, а совместно с ними меняются и практические методы обеспечения информационной безопасности.

На самом деле, совершенных способов защиты не найдено, во многом успех при построении механизмов безопасности для существующей системы будет зависеть от её индивидуальных особенностей, учёт которых плохо подаётся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа.

На сегодняшний день информационная сфера – не просто одна из главных сфер международной работы, но и объект столкновения интересов. Страны с развитой информационной инфраструктурой, определяя некие технологические стандарты и предлагая потребителям свои ресурсы, создают условия формирования и осуществления деятельности информационных инфраструктур в других странах, оказывают воздействие на развитие их информационной сферы. Поэтому в более промышленно развитых странах при формировании национальной политики почетное место получают развитие средств защиты и обеспечение безопасности информационной сферы[115].

Концентрация данных в компьютерных системах вынуждает наращивать усилия по её защите. Национальная безопасность, тайна государственного масштаба и пр. - все эти юридические аспекты требуют усиления контроля над информацией в коммерческих и государственных организациях.

В настоящие дни общество эффективно развиваться и совершенствовать свои внутренние механизмы может только в условиях правового государства, которое основывается на неукоснительном соблюдении законодательных норм. Роль права в жизни информационного общества становится определяющей, все его члены должны исполнять нормы законов и разрешать возникающие споры цивилизованным способом на основе законодательства[116].

Современные методы изменения, переработки, хранения и передачи информации создают благоприятную сред для появление информационных

---

[115] *Цирлов В.Л.* Основы информационной безопасности автоматизированных систем. краткий курс М., 2008.

[116] Правовое обеспечение информационной безопасности: учебное пособие для студентов высших учебных заведений / С.Я. Казанцев, О.Э. Згадзай, Р.М. Оболенский и др.; под ред. С.Я. Казанцева. М., 2007.

угроз, которые связаны с вероятностью раскрытия, утери и изменения данной информации. Вследствие этого обеспечение информационной безопасности – это наиболее важное, определяющее направление развития информационных технологий.

Непосредственными исполнителями злокачественного действия, которое негативно воздействует на информацию, могут выступать:

– люди;

– технические устройства;

– модели, алгоритмы, программы;– технологические схемы обработки; – внешняя среда.

Существуют следующие предпосылки, или причины появления угроз:

– объективные (количественная или качественная недостаточностьэлементов системы) - не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы; – субъективные - непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации[117].

Опасность вмешательства в информационные ресурсы в овладении личной информации, конфиденциальной информации, которая в последствии может быть использована против ее первоначального обладателя и нанесение ему вреда.

Осуществление угроз информационной безопасности может быть произведено:

---

[117] *Сёмкин С.Н, Беляков Э.В., Гребенев С.В., Козачок В.И.* Основы организованного обеспечения информационной безопасности объектов информатизации. М., 2005.

– через агентурные источники в органах коммерческих структур,государственного управления, имеющих возможность получения конфиденциальной информации;

– путём подкупа лиц, работающих на предприятии или в структурах,непосредственно связанных с его деятельностью;

– путём перехвата информации, циркулирующей в средствах и системахсвязи и вычислительной техники, с помощью технических средств разведки и программно-математических воздействий на неё в процессе обработки и хранения;

– путём подслушивания переговоров, ведущихся в служебных помещениях, автотранспорте, в квартирах и на дачах;

– через переговорные процессы с зарубежными или отечественнымифирмами, используя неосторожное обращение с информацией.

– через «инициативников» из числа сотрудников, которые хотят улучшитьсвоё благосостояние с помощью «заработка» денег или проявляют инициативу по другим материальным или моральным причинам. Основы информационной безопасности.

Способы и методы защиты информационных ресурсов

Параллельно развитию методов изменения и переработки информации, развиваются и способы ее защиты. Если ранее эта проблема была не столь явной и распространенной, то сейчас ставится вопрос о нарушение национальной безопасности через информационные ресурсы. Проблема имеет два комплексных решения.

К первому относится охрана конфиденциальности государственных сведений, которая обеспечит невозможность взлома и несанкционированного доступа. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (коммерческая тайна, партийная тайна и т. д.).

Ко второму направлению относится защита от информации, которая в последнее время приобретает международный масштаб и стратегический характер. При этом выделяют три основных направления защиты от так называемого информационного оружия (воздействия):

– на технические системы и средства;

– общество;

– психику человека.

– конфиденциальности.

Сервисы сетевой безопасности представляют собой механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях.

1. *Инженерно-технические методы* ставят своей целью обеспечение защиты информации от утечки по техническим каналам - например, за счёт перехвата электромагнитного излучения или речевой информации.
2. *Правовые и организационные методы* защиты информации создают нормативную базу для организации различного рода деятельности, связанной с обеспечением информационной безопасности.
3. *Теоретические методы* обеспечения информационной безопасности, в свою очередь, решают две основных задачи. Первая из них - это формализация разного рода процессов, связанных с обеспечением информационной безопасности. Так, например, формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе - а значит, гарантировать выполнение требуемых свойств безопасности. Отсюда непосредственно вытекает вторая задача – строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищённости. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.

Процесс информатизации касается практически всех сфер человеческой деятельности. С появлением новых информационных технологий информация начинает являться необходимым атрибутом обеспечения деятельности государств, юридических лиц, общественных объединений и граждан. От качества и достоверности информации, от её оперативности передачи зависят многие решения, принимаемые на самых разных уровнях - от глав государств до рядового гражданина.

Обеспечение информационной безопасности – одна из ведущих задач, стоящих перед государствами, ведь информационная среда – очень сложный механизм, который обеспечивает стабильное функционирование электронного оборудования, программного обеспечения и пр.

Для того чтобы успешно справляться с поставленной задачей необходимо действовать на законодательном, программно-техническом, организационном и идеологическом уровне. Лишь комплексное решение проблемы приведет к желаемому результату и обеспечению должного уровня защиты информационных ресурсов.

В.С. Подсеваткин, А.М. Самойлов

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПРИ РАБОТЕ НА КОМПЬЮТЕРЕ И ВОЗМОЖНЫЕ СРЕДСТВА ЗАЩИТЫ

В современном мире роль персональных компьютеров при обработке, передаче и хранении информации неуклонно растет. Это связанно и с новым взглядом на информацию, которая приобретает новый статус - экономический, в обществе развивается информационное право, информация переходит в категорию защищаемых и охраняемых объектов. В связи с этим важным моментом при работе с информацией на персональных компьютерах, является знание и исследование возможных каналов утечки информации.

Рассмотрим понятия, связанные с утечкой информации. Хранение информации представляет собой поддержание исходной информации в виде, обеспечивающем выдачу данных по запросам пользователей в необходимые или установленные сроки. Утечка информации на уровне принятой терминологии представляет собой несанкционированный доступ.

Несанкционированный доступ – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к данной информации. Несанкционированным доступом в отдельных случаях называют также получение лицом, имеющим право на доступ к информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Развитие компьютерной техники и информационных технологий позволяет работать на компьютерах как независимо друг от друга, так и взаимодействуя с другими компьютерами по компьютерным сетям, причем последние могут быть локальными и глобальными. С учетом названного перечень участков, где могут находиться подлежащие защите данные, может быть представлен следующими элементами:

– оперативная и постоянная память ПК;

– съемные магнитные, магнитооптические, лазерные и другие носителиинформации;

– внешние устройства хранения информации коллективного доступа (RAID-массивы, файловые серверы и т.п.);

– экраны устройств отображения (дисплеи, мониторы, консоли);

– память устройств ввода/вывода (принтеров, графопостроителей,сканеров);

▪ память управляющих устройств и линии связи, образующие каналы сопряжения компьютерных сетей.

Существует несколько причин и каналов утечки важной информации, в основном это:

– ошибки конфигурации (прав доступа, файерволов, ограничений намассовость запросов к базам данных);

– слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам в отсутствии сотрудников);

– электромагнитные каналы;

– сетевая разведка;

– оптические каналы (утечка изображения);

– инсайдерские каналы утечки информации;

– злоупотребление служебными полномочиями (воровство резервныхкопий, копирование информации на внешние носители при праве доступа к информации);

– использование клавиатурных шпионов, вирусов и троянов накомпьютерах сотрудников для имперсонализации.

Раскроем каждый и названных каналов подробнее.

1. Наиболее популярной причиной утечки информации среди ошибок конфигурации на данный момент является именно ограничение на массовость запросов к базам данных (DoS – атака):

DoS – хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой. Целью большинства атак является либо несанкционированный доступ в систему, либо получение прав администратора, либо другие неправомерные действия пользователя, такие как подмена документов и кража конфиденциальной информации. Вариантов проведения такой атаки множество. Самыми популярными являются наводнение (flood) сети пакетами различных протоколов (например, ICMP, UDP или TCP), в результате которого почти все вычислительные и сетевые ресурсы уходят на создание бесполезных ICMP-ответов или TCP-сессий. DoS и DDoS-атаки позволяют

довести до отказа практически любую систему, не оставляя юридически значимых улик.

2. Если у пользователя стоит лёгкий пароль, то украсть его для хакеров очень просто. В современном мире существует большое множество программ для подбора паролей к учётным записям (PasswordCracker, PasswareKitEnterprise, MultiPasswordRecovery). Злоумышленнику будет достаточно знать только ваш логин. Чаще всего такому взлому подвергаются учётные записи на различных сайтах, в которых может хранится личная информация. Иногда злоумышленнику даже не нужно подбирать пароль, т.к. владелец ПК, например в офисе, может оставить свой компьютер включённым и отойти от рабочего места, что даёт другому человеку сесть за стол и воспользоваться компьютером в полной мере.

3. Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки. Данный канал утечки наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым средствам связи и при общении с другими людьми с помощью ПК. Для перехвата побочных электромагнитных излучений ТСПИ (Технические средства передачи информации) “противником” могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Как правило, полагается, что ТСР ПЭМИН располагаются за пределами контролируемой зоны объекта. Для перехвата информации, обрабатываемой ТСПИ, также возможно использование электронных устройств перехвата информации (закладных устройств), скрытно внедряемых в технические средства и системы. Они представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается в специальное запоминающее устройство, а уже затем по команде управления

передается по радиоканалу. Наиболее вероятна установка закладных устройств в ТСПИ иностранного производства.

4. Под сетевой разведкой подразумевается сбор информации о сети с помощью общедоступных данных и приложений. При подготовки атаки против какой либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов доменных сетевых имён – DNS, эхо-тестирования и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены.

Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. Далее, он получает доступ к файлам, которые находятся на ПК.

5. В оптическом канале получение информации возможно путем: визуального наблюдения, фото-видеосъемки, использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

Наиболее опасным каналом утечки является дисплей, так как с точки зрения защиты информации он является самым слабым звеном в компьютерной системе. Это обусловлено принципами работы видеоадаптера, состоящего из специализированных схем для генерирования электрических сигналов управления оборудования, которое обеспечивает генерацию изображения. Кроме того, в существующих программах удаленного доступа имеется функция записи экрана дисплея по расписанию в отдельный файл.

6. Инсайдер – член какой-либо группы людей, имеющей доступ к информации, недоступной широкой общественности. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями.

7. Сознательные действия сотрудников, обусловленные инициативным сотрудничеством с другой фирмой; продажей информации за взятку, под угрозой шантажа, в виде мести; переход на другую фирму на более высокую оплату

8. Компьютерный вирус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Как правило, целью вируса является нарушение работы программноаппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т.п. Вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы. Они могут распространятся через Интернет (в случае скачивания файла, в нём может находится вирус), через локальные сети, через съёмные носители. Существует разновидность вирусов, которая называется «Программа-шпион». Она собирает информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли). Поэтому, злоумышленники получают полный контроль над личной информацией человека

Каналами распространения вирусов могут быть: дискеты, флешнакопители, электронная почта, системы обмена мгновенными сообщениями, веб-страницы, Интернет и др. При использовании флеш-накопителей и дискет опасность представлял размещаемый на них с целью заражения файл autorun.inf. Но, начиная с Windows 7, возможность автозапуска файлов с переносных носителей отключена. Вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу для рассылки самого себя дальше. В системах мгновенного обмена сообщениями распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами. Заражение через страницы Интернета реализуется посредством размещенных на них скриптов и ActiveX-компонентов.

Сетевое заражение могут осуществлять черви, они используют так называемые уязвимости в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Если на компьютере стоит слабая защита, то данные пользователя могут подвергнуться взлому, результатом которого могут быть следующие последствия: утечка персональных данных, коммерческой тайны, служебной переписки, государственной тайны, полное либо частичное лишение работоспособности системы безопасности компании.

Чтобы компьютер не подвергся атаке со стороны злоумышленников, данные на компьютере нужно держать в защите. Существуют различные способы, которые помогут сделать это: шифрование данных, использование надёжных паролей, защита Wi-Fi доступа, установка антивирусных программ

Шифрование данных можно произвести всего один раз, например с помощью программы TrueCrypt. Шифрование нужно делать для того, чтобы никто не смог смотреть ваши файлы, войти в систему, кроме вас самих.

Использование надежных паролей затрудняет доступ к информации. Надежные пароли представляют собой сложную комбинацию цифр, букв, символов, длиной не менее 8 символов, причем с использованием прописных и строчных символов различных алфавитов (русского и английского). Желательно записывать свои пароли на отдельный лист и хранить в надёжном месте. Не следует хранить пароли в блокноте на компьютере, т.к. существует множество вирусов, которые могут просматривать файлы на вашем ПК.
Сообщать свой пароль никому не следует..

Попадание вируса на компьютер чревато неприятными последствиями. Лучше сразу поставить надёжный антивирус и держать его постоянно включённым. При работе в сети Интернет постоянное включение антивируса является необходимостью.

У хакеров имеется множество средств и способов, чтобы обойти защищенные сети и шифрование. Они ежедневно крадут номера кредитных карт,

банковские счета и сведения о персональных данных. Поэтому при работе на ПК необходимо предпринимать всевозможные меры защиты информации, как программно-аппаратные, так и организационные.

В РФ в целях защиты информации от неправомерного доступа введены и действуют и законодательные меры защиты. В УК РФ предусмотрены статьи в целях предотвращения неправомерного доступа к информации, это статья 137 «Нарушение неприкосновенности частной жизни», статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», статья 272 «Неправомерный доступ к компьютерной информации», статья 273 «Создание, использование и распространение вредоносных компьютерных программ», статья 274.«Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Список использованной литературы и источников

1. *Загинайлов Ю.Н* Теория информационной безопасности и методология защиты информации. URL: http://window.edu.ru/resource/984/71984 (дата обращения: 18.03.2016).
2. *Хорев А.А.* Технические каналы утечки информации. http://www.analitika.info/kanalutechki.php (дата обращения: 18.03.2016).
3. *Артамонов В.А., Артамонова Е.В*. Каналы утечки информации. URL: http://media.professionaly.ru/processor/topics/original/2013/09/24/utechki-kanal.pdf (дата обращения 18.03.2016).
4. Правовая охрана интеллектуальной собственности: учебное пособие. М., 1999. URL: http://ftemk.mpei.ac.ru/ip/IPTextBook/05/5-4/5-4.htm (дата обращения 18.03.2016).

Д.А. Рыбакова
ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал
*Научный руководитель: **Е.А. Лачина**, к.ю.н., заведующая кафедрой гражданско-правовых дисциплин ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал*

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ: ОТЕЧЕСТВЕННЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

XXI век – век бурного развития техники, экономики, промышленности, энергетики, науки, информационных технологий, век развития глобальных связей и обмена информацией по всему земному шару. Уже практически не осталось места, куда бы не пришел Интернет.

Глобализация затрагивает все сферы жизни общества – не только производство или торговлю, общемировое сотрудничество необходимо также и в политике, в разрешении дипломатических и вооруженных конфликтов, в разрешении иных споров, которые в большинстве случаев разрешаются в судебном порядке.

С ростом объема информации, которую получает общество в период такого взаимопроникновения наций и культур, стремления к интеграции, темп жизни убыстряется. Именно поэтому сейчас так много говорят об оптимизации всех институтов общественной жизни, в том числе и деятельности судебных инстанций.

В 2012 г., по итогам проведения VIII Всероссийского съезда судей, были подведены некоторые итоги деятельности судов, а также намечены перспективы развития. Так, в постановлении съезда «О состоянии судебной системы РФ и основных направлениях ее развития» от 19 декабря 2012 г. отмечено, что ежегодно количество рассматриваемых судами дел возрастает, а, следовательно, увеличивается нагрузка на судей и аппарат суда.

Так, арбитражными судами за 4 года (2008-2011) рассмотрено 5,8 млн. дел по экономическим спорам и иных дел, подведомственных системе арбитражных

судов, причём наибольший рост количества рассмотренных дел пришёлся на 2008 и 2009 годы, когда в отдельных регионах их количество увеличилось в 5 раз. К 2012 году количество дел практически вернулось к прежнему периоду (в арбитражных судах первой инстанции в 2008 году – свыше 1,4 млн. дел; в 2011 – более 1,7 млн. дел). Возрастала и судебная нагрузка: в 2008–2011 годах в среднем по системе она составляла около 50 дел в месяц, а по некоторым судам превышала 100 дел в месяц, тогда как научно обоснованные нормы составляют ежемесячно 15–20 дел[118].

Судами общей юрисдикции, включая военные суды и мировых судей, ежегодно рассматривалось (по всем инстанциям) дел и материалов: в порядке уголовного судопроизводства – около 4,5 млн., в порядке гражданского судопроизводства – свыше 14,5 млн., в порядке, установленном КоАП РФ, – более 5,5 млн. В среднем на одного судью общей юрисдикции приходилось 76 дел и материалов в месяц; наибольшее количество приходилось на мировых судей.[141]

В связи с этим возникает острая необходимость в оптимизации деятельности суда, снижении нагрузки на судей, без потерь в эффективности рассмотрении дел, достижении истины, а также без подрыва авторитета суда в разрешении конфликтов.

Участники VIII Всероссийского съезда судей основными причинами снижения эффективности деятельности судов назвали нарушение сроков рассмотрения дел, например, часто встречаются случаи ненадлежащего извещения лиц, участвующих в деле, о времени и месте судебного заседания; возникают трудности с формированием коллегии присяжных заседателей; ненадлежащим образом исполняются судебные акты о приводе лиц по уголовным делам и делам об административных правонарушениях; недопустимо долго производятся судебные экспертизы. Процессуальные законы не содержат эффективных механизмов защиты от искусственного затягивания сроков

[118] Постановление VIII Всероссийского съезда судей от 19 декабря 2012 г. «О состоянии судебной системы РФ и основных направлениях ее развития». URL: http://www.ssrf.ru/page/9085/detail. [141] Там же.

рассмотрения дел, действенных санкций за неисполнение процессуальных обязанностей и злоупотребление участниками судопроизводства процессуальными правами[119].

Полагаем, что наиболее оптимальным способом разрешения подобных ситуаций является внедрение информационно-коммуникационных технологий в деятельность судов, создание так называемого «электронного правосудия».

Законодательное закрепления понятия «электронное правосудие» на данный момент отсутствует. Воспользуемся наиболее, на наш взгляд, емким определением, данным Е.С. Дружинкиным: «Электронное правосудие – это способ осуществления правосудия, основанный на использовании информационных технологий»[120].

С.В. Романенкова в своей работе на тему электронного правосудия в правоприменительной практике зарубежных стран дала, на наш взгляд, точное понятие термина «электронное правосудие», рассмотрев его в широком и узком смыслах.

Так, в широком смысле под электронным правосудием можно понимать совокупность различных автоматизированных и информационных систем – сервисов, предоставляющих средства для публикации судебных актов, ведения электронного дела и доступа сторон к материалам электронного дела. Вышеуказанные средства позволяют вывести на совершенно иной качественный уровень взаимодействия суда, участников процесса и иных заинтересованных лиц. В то же время все эти сервисы носят прикладной, вспомогательный характер, не изменяя способов ведения судебного процесса. В узком смысле электронное правосудие – это возможность суда и иных участников судебного процесса осуществлять предусмотренные нормативными правовыми актами действия, непосредственно влияющие на начало и ход судебного процесса (например, такие действия, как подача в суд документов в электронной форме

[119] Постановление VIII Всероссийского съезда судей от 19 декабря 2012 г. «О состоянии судебной системы РФ и основных направлениях ее развития». URL: http://www.ssrf.ru/page/9085/detail.

[120] *Дружинкин Е.С.* Электронное правосудие в России: некоторые итоги и перспективы развития // Вопросы экономики и права. 2013. № 11. С. 35.

или участие в судебном заседании посредством системы видеоконференцсвязи)[121].

Принципами функционирования электронного правосудия являются открытость, обеспечение права на доступ к информации о деятельности судов, транспарентность (от английского слова transparent – прозрачный).

Реализация данных принципов – важная веха в укреплении основных демократических институтов общества, поэтому Правительством Российской Федерации принята целевая программа «Развитие судебной системы России на 2013-2020 годы»[122], принят Федеральный закон от 22 декабря 2008 г. № 262ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Программе «Развитие судебной системы России на 2013-2020 годы» предшествовала аналогичная ей, рассчитанная на 2007-2012 годы, в которой процесс внедрения информационно-коммуникационных технологий в деятельность судов по отправлению правосудия именуется «системой электронного обеспечения правосудия», т.е. учитывались лишь чисто технические процессы, не затрагивая самого процесса отправления правосудия.

В процессе реализации данной программы нашли свое отражение такие элементы «Электронного правосудия» как фиксация судебных заседаний при помощи средств цифровой записи и возможность ознакомления с текстами судебных решений и материалами всеми желающими, а также с информацией о деятельности судов. В Программе же до 2020 года понятие «Система электронного обеспечения правосудия» уже отсутствует, но появляются такие понятия как «электронное правосудие» и «электронное судопроизводство». Если первое понятие четко разъяснено не было, то второе раскрыто следующим образом: «Под электронным судопроизводством понимается упрощение

---

[121] *Романенкова С.В*. Понятие электронного правосудия, его генезис и внедрение в правоприменительную практику зарубежных стран // Арбитражный и гражданский процесс. 2013. № 4. С. 47.

[122] Постановление Правительства РФ от 27 декабря 2012 г. № 1406 «О федеральной целевой программе "Развитие судебной системы России на 2013 - 2020 годы"» // Собрание законодательства РФ. 2013. № 1, ст. 13.

процедур подачи в суд исковых заявлений, жалоб в электронном виде, получения копий документов и ознакомления с материалами дела.

Указанные акты также направлены на формирование самостоятельной и независимой судебной власти как одной из ветвей государственной власти, на повышение эффективности и качества правосудия, достижение открытости и прозрачности судебной системы, независимости судей, самостоятельности судов, приведение норм отечественного законодательства в соответствие с нормами международного права.

Кроме того, в развитии судебной системы Российской Федерации в целом и электронного правосудия в частности учитывается международный опыт. К примеру, в основу национального законодательства России в сфере развития судебной системы легли базовые рекомендации Комитета министров Совета Европы CM/Rec (2009)1 государствам-участникам Совета Европы по электронной демократии (приняты Комитетом министров 18. Февраля 2009 г. на 1049 собрании заместителей министров).

Внедрение электронных средств в судопроизводство способно вывести его на более высокий уровень развития, создать условия для системного управления движением дела, включающего определение режима прохождения дела в суде от его возбуждения до вынесения решения, ведение графика управления делом, контроль за продвижением дела, обеспечение эффективной связи с представителями сторон, непрерывную оценку работы системы, автоматизацию процесса управления делом, что, в конечном счете, повысит эффективность правосудия[123].

Л.А. Прокудина и Дж.С. Сосил (цитата приведена выше) отмечают, безусловно, важную практическую значимость электронного правосудия, однако немаловажным остается и другие его преимущества:

– открытость и доступность информации о деятельности судов,

[123] *Прокудина Л.А., Сосил Дж.С.* Система управления движением дела – фактор повышения эффективности отправления правосудия // Вестник ВАС РФ. 2003. № 10. С. 160.

– достоверность информации и деятельности судов и своевременностьее предоставления,

– свобода поиска, получения, передачи и распространения информациио деятельности судов любым законным способом,

– соблюдение прав граждан на неприкосновенность частной жизни,личную и семейную тайну, защиту их чести, достоинства и деловой репутации, права организаций на защиту их деловой репутации,

– соблюдение прав и законных интересов участников судебного процессапри предоставлении информации о деятельности судов,

– невмешательство в осуществление правосудия при предоставлениинформации о деятельности судов.

Необходимо также отметить высокую значимость внедрения информационных технологий в деятельность судов для правоприменителейцивилистов. В этой сложной области права как нигде важно своевременное и полное обеспечение юриста информацией о ходе дела, а также о состоянии практики рассмотрения дел судами. Нередко возникают спорные вопросы при трактовании той или иной правовой нормы, разрешить которые способно только решение суда по аналогичному вопросу. Понимая это, законодатель установил необходимость публикации всех решений суда, за исключением случаев, предусмотренных законодательством Российской Федерации и за некоторыми изъятиями, как то даты, персональные данные участников, взысканные суммы.

Подведем некоторые итоги деятельности по внедрению механизмов электронного правосудия в деятельность российских судов. Здесь сразу необходимо отметить, что процесс этот идет далеко не равномерно: арбитражные суды всех уровней достигли гораздо большего уровня информатизации, нежели суды общей юрисдикции.

Наибольших успехов в применении информационных технологий достиг Верховный суд Российской Федерации. В 2004 году началось создание государственной автоматизированной системы «Правосудие» для

автоматизации деятельности Верховного суда. Также в 2004 году была создана автоматизированная система «Судебное делопроизводство и статистика», которая затем вошла в ГАС «Правосудие». На данный момент ГАС «Правосудие» работает во всех судах общей юрисдикции, однако на практике нередки случаи ее сбоев, например, часто в ней нельзя осуществить поиск участка мирового судьи по субъекту Российской Федерации, городу проживания и улице, дому, где зарегистрирован гражданин.

Кроме того, в Верховном суде создана и действует система технической фиксации судебных процессов для протоколирования судебных заседаний, система «Судебное делопроизводство» (служит для хранения, учета и анализа судебных дел) и «Электронный банк судебных решений» (создана для обеспечения деятельности судей и их помощников, открыта и для общего доступа).

В Верховном суде совершенствуются возможности видеоконференцсвязи.

Все суды общей юрисдикции и мировые суды субъектов РФ на данный момент имеют сайты в сети Интернет для обеспечения свободного доступа граждан и организаций к информации о деятельности судов.

На сайтах должна быть размещена:

– общая информация о суде;

– информация, связанная с рассмотрением дела в суде;

– сведения о регистрационных номерах дел, находящихся в суде,их наименовании, предмете спора, о движении дела, о результатах рассмотрения дел, тексты решений, сведения об обжаловании;

– информация о времени и порядке приема граждан;– контактная информация для справок.

Вся перечисленная информация имеется на сайтах судов общей юрисдикции, сведения выкладываются своевременно, тексты судебных актов чаще всего имеются в свободном доступе. Сайты являются большим подспорьем в деятельности практикующего юриста. Именно благодаря своевременному

размещению информации можно вовремя узнать, к примеру, дату и время судебного заседания и начать подготовку к слушанию.

С сайтами мировых судов субъектов РФ дело обстоит несколько хуже. Здесь менее внимательно следят за ведением дела, информация поступает не всегда верная и вовремя, тексты судебных актов не выкладываются, затруднен поиск конкретного дела из-за частых перебоев в работе сайта.

Еще одной важной вехой развития электронного правосудия в судах общей юрисдикции стало использование мобильной связи для извещения участников судопроизводства о дате и месте проведения судебного заседания посредством СМС-сообщений в случае согласия участников на такое оповещение. Допустимость данного метода оповещения была подтверждена Постановлением Пленума Верховного суда РФ от 09.02.2012 № 3 «О внесении изменений в некоторые постановления Пленума Верховного суда Российской Федерации»[124].

В случае согласия лица, участвующего в процессе, на извещение посредством СМС-сообщений, у него отбирается расписка, в которой указываются контактные данные лица, а также его процессуальное положение. Факт отправки и доставки СМС-сообщения фиксируется. Конечно, данная практика позволяет существенно сэкономить денежные средства, а также время сотрудников аппарата суда, а участникам производства оперативно получать информацию. Так должно быть в идеале, однако на практике не все так однозначно. Часто встречаются технические ошибки при наборе СМССообщения, ошибки лица, отвечающего за отправку сообщений в аппарате суда либо сбои в работе сайта, через который происходит отправка СМССообщений, и уточнять информацию, все же, приходится в аппарате суда.

В настоящее время многие кабинеты судей общей юрисдикции имеют возможность проведения заседаний с использованием видеоконференцсвязи, растет использование аудиозаписи судебного заседания.

---

[124] Постановление Пленума Верховного суда РФ от 9 февраля 2012 г. № 3 «О внесении изменений в некоторые постановления Пленума Верховного суда Российской Федерации» // Российская газета. 2012. № 5708.

Арбитражные суды сделали большой шаг вперед в процессе информатизации и продолжают развиваться в этом направлении. В 2010 году был принят Федеральный закон № 228-ФЗ «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» [125], который открыл возможность подачи исковых заявлений, заявлений и жалоб в электронной форме (например, подача в электронной форме искового заявления, отзыва на исковое заявления, заявления об отмене решения третейского суда, заявлений о выдаче исполнительного листа на принудительное исполнение решения третейского суда, заявлений о приведения в исполнение решения иностранного суда и иностранного арбитражного решения, апелляционной и кассационной жалобы, заявлений о пересмотре в порядке надзора, заявлений о пересмотре судебного акта по вновь открывшимся обстоятельствам и т.д.), в нем регламентировано использование видеоконферецсвязи, введено обязательное протоколирование судебного заседания с использованием аудиозаписи, извещение о процессе с использованием сайтов судов либо по электронной почте.

Тут следует отметить, что участники процесса считаются извещенными надлежащим образом, если к началу судебного заседания суд располагает сведениями о получении адресатом копии определения о принятии искового заявления или заявления к производству и возбуждении производства или иными доказательствами получения лицами, участвующими в деле, информации о начавшемся судебном процессе. В дальнейшем же все сведения о движении дела публикуются на сайте соответствующего арбитражного суда, а участники производства самостоятельно принимают меры к получению информации и несут риск наступления неблагоприятных последствий в результате непринятия мер по получению указанных сведений.

С 2008 года арбитражные суды начали использовать автоматическую систему распределения дел между судьями. Эта система позволяет избежать

[125] Федеральный закон № 228-ФЗ от 27 июля 2010 г. «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» // Собрание законодательства РФ. 2010. № 31, ст. 4197.

попадания спора к судье, который может иметь склонность к одной из сторон, что должно исключить коррупционную составляющую. Но не все так прозрачно: сотрудники аппарата суда свободно могут поменять в ней данные по различным причинам.

В Арбитражном суде Владимирской области также действуют системы автоматизированного судопроизводства. Официальный сайт Арбитражного суда дает ясное представление о деятельности суда, открывает доступ к следующим сервисам:

1. В «Банке решений арбитражных судов» размещены данные обо всех судебных делах и документах, тексты решений и иных процессуальных документов. Здесь можно произвести поиск по следующим критериям:
   - наименование стороны;
   - категория спора;
   - вид спора;
   - номер дела;
   - текст документа;
   - суд, рассматривающий дело;– период поиска.
2. На сайте суда размещена информация о персонале суда, кратко сообщаются данные судьи, его контактный телефон, данные о помощнике судьи.
3. «Картотека арбитражных дел» позволяет получать сведения о поданных заявлениях, жалобах, ходатайствах, текущем статусе дела и др.

Карточка дела содержит следующие данные:

- текущий статус дела и его рассмотрение в судебных инстанциях;
- наименование сторон, участвующих в деле;
- суды, в которых рассмотрено дело;
- судьи, принимавшие участие в рассмотрении дела;– судебные акты.

Практически по любому арбитражному делу можно найти информацию в карточке дела. В ней можно просмотреть судебные акты в формате PDF, скачать и распечатать их.

4. В «Календаре судебных заседаний» можно увидеть расписание предстоящих судебных заседаний.

5. Сервис «Электронный страж» позволяет получать информацию по выбранному делу на адрес электронной почты. Страж позволит оформить 40 подписок. На электронную почту подписавшегося будут поступать сообщения о движении дела, поступлении новых документов. Для оформления подписки необходимо пройти регистрацию и выбрать функцию в Карточке дела «Отслеживать дело».

6. Система видеоконференцсвязи позволяет проводить видеоконференции как между судами, так и с участниками процесса, что позволяет существенно снизить затраты, к примеру, на проезд к месту проведения заседания.

7. Создана система подачи исковых заявлений, заявлений, жалоб в электронном виде, отслеживать их прохождение в суде. 8. На сайте представлена статистическая информация о суде.

9. В Арбитражном суде Владимирской области используется автоматическая информационно-справочная служба.

Из приведенной выше информации мы можем сделать однозначный вывод – первые шаги в создании электронного правосудия в нашей стране были сделаны, однако необходимо двигаться дальше. Тут не лишним было бы обратиться к практике зарубежных стран.

Наиболее развитой является электронная система в судах Сингапура. Подробное исследование опыта этой станы было сделано В.И. Решетняком в работе «Электронное правосудие в гражданском процессе Сингапура» [126] . Остановимся на некоторых важных моментах.

В сингапурских судах с 1997 года применяется программа подачи и вручения документов в судебном процессе. Сначала эта система применялась в добровольном порядке, впоследствии она стала обязательной для всех гражданских дел. В 2011 году была внедрена интегрированная электронная

[126] *Решетняк В.И.* Электронное правосудие в гражданском процессе Сингапура // Российский юридический журнал. 2012. № 2. С. 75─80.

система для управления всеми документами и оптимизации документооборота в суде. Любой электронный документ, поступивший в суд, проверяется на соответствие требованиям процессуального законодательства, а затем отправляется на обработку и приобщается к нужному делу. Весь процесс автоматизирован, что позволяет говорить о ведении электронного дела в суде. Это позволяет значительно экономить время на рассмотрение документа и рабочее время сотрудников аппарата суда. Хранятся все документы также в электронном виде, бумажных архивов в Сингапуре нет.

Следует отметить, что доступ к этой системе дается только после регистрации, приобретения необходимого оборудования и соответствующего программного обеспечения (при регистрации выдается смарт-карта с цифровым сертификатом).

Похожая система действует в Соединенных Штатах Америки. Под электронным правосудием в США понимают доступ к суду с помощью современных информационно-коммуникационных технологий, получение информации о судебных делах, поиск документов и другой информации.

В США действует система управления делами/электронный архив дел, т.е. в Америке также, как в Сингапуре используется электронный документооборот. Граждане имеют открытый доступ к судебным материалам, однако предоставление документов осуществляется на платной основе. Кроме публичной системы доступа к электронным делам, существуют еще и частные, где собрано больше материалов, стоимость доступа к которым существенно больше.

В США, так же, как в Сингапуре, подача документов в электронном формате является обязательной.

Таким образом, в США реализованы такие элементы электронного правосудия как ведение электронного дела, подача документов посредством сети Интернет и публикация информации о судебных делах посредством сети Интернет.

Германия стала одной из первых стран, применяющих информационные технологии в отправлении правосудия. Начатый еще 80-х гг. прошлого столетия процесс перехода на автоматизированное приказное производство был завершен в 2007 году, когда к системе присоединились земли Тюрингия и Саксония.

В гражданском процессе Германии используется термин «электронная коммуникация». В сущности, это – то же самое, что и электронный документооборот. В 2005 году был принят закон «об использовании электронных форм коммуникации в судопроизводстве. В качестве основной цели его принятия было названо введение полностью электронной коммуникации и системы документооборота между участниками судопроизводства[127].

В Англии «электронное правосудие» означает возможность свидетелю с разрешения суда давать показания с использованием видеоконференцсвязи, разрешение стороне давать показания из-за границы, как посредством видео, так и телефонной связи. Также существует возможность электронной подачи документов, инициации процесса и выполнение последующих процессуальных действий в электронной форме в некоторых суда Высокого суда в Англии.

В Финляндии существует возможность подачи заявлений и обращений в суд в электронной форме, управления электронным делом, использования видеоконференцсвязи, аудио- и видеозаписи судебного заседания, отслеживания дела и составления графика заседаний в календаре судебных заседаний. Сторонам также могут направляться по электронной почте процессуальные документы (решения суда, заочные решения, образцы мирового соглашения).

При этом использование новых технологий позволяет ускорить рассмотрение и разрешение дел; улучшить качество судебных услуг; снизить расходы на судопроизводство и временные затраты работников суда; повысить прозрачность правосудия; достигнуть качественно нового уровня доступности

[127] *Брановицкий К.Л.* Информационные технологии в гражданском процессе Германии (сравнительноправовой анализ). М., 2010. С. 6.

правосудия за счет того, что отправка и ознакомление с необходимыми документами могут осуществляться семь дней в неделю и 24 часа в сутки[128].

В Италии в электронное правосудие входят:

– Электронное заполнение исковых документов;

– Виртуальные консультации по исковым документам и судебнымрешениям;

– Электронные запросы и предоставление электронных копий;

– Возможность использования определенного электронного адреса, накоторый пользователи могут получать информацию из канцелярии суда.

Завершая приведенный краткий обзор зарубежного опыта, можем сделать вывод о том, как же понимают в мире электронное правосудие и какие его базисные используются практически повсеместно.

Итак, электронное правосудие основывается на:

1. Ведении судебного процесса через Интернет (под этим понимается как возможность подачи заявлений, так и ведение заседаний посредством видеоконференцсвязи).
2. Внедрении электронного документооборота, позволяющего участникам процесса обмениваться юридически важными документами в электронной форме.
3. Фиксации судебных заседаний путем аудио- и видеозаписи.
4. Внедрении системы публикации судебных актов.
5. Широком использовании оборудования, позволяющего исследовать доказательства, представленные в электронной форме.

Как видно из выделенных элементов «электронного правосудия», их отличительной чертой является именно использование информационнокоммуникационных технологий при рассмотрении дел в суде и закреплении юридически значимой информации в электронной форме[152].

---

[128] *Хиетанен А.* Электронный суд и электронные правовые коммуникации в Финляндии // Использование новых информационных технологий в арбитражном процессе и при осуществлении нотариальной

Анализ отечественной и зарубежной практики внедрения информационных технологий в процесс судопроизводства в полной мере показал важность таких процессов. Мы не раз упоминали об эффективности

деятельности: материалы междунар. семинара (7-8 сентября 2006 г., Екатеринбург). М., 2007. С. 37-38.

[152] *Мошков Е.А.* Содержание электронного правосудия в России и зарубежных странах // Проблемы права. 2015. № 4. С. 145.

электронного производства, его экономичности и эргономичности. Говорилось и об удобстве доступа к важным процессуальным документам, простоте доступа в зал судебных заседаний посредством видеосвязи.

Наша страна во многом переняла опыт зарубежных коллег в сфере электронного правосудия, однако четко оно не отлажено, встречаются пробелы, причем нередко. Это, в первую очередь, касается судов общей юрисдикции и мировых судов. Опыт внедрения информационно-коммуникационных технологий в деятельность арбитражных судов гораздо более эффективен.

Практика показал (вспомним опыт Сингапура и США), что установление обязательного электронного документооборота способствует более быстрому прогрессу в указанной сфере.

В России арбитражные суды уже начали принимать исковые заявления и жалобы в электронном виде, однако эта функция не пользуется большим спросом. Объем документов, которые необходимо заверить и отсканировать в нужный формат подчас очень велик, при этом мы привыкли действовать «по старинке», не доверяя полезным новшествам.

Поскольку арбитражные суды в нашей стране активнее используют информационные технологии, предлагаем начать реформирование именно с них.

В сфере внедрения электронного документооборота мы предлагаем:

1. Ввести в Арбитражный процессуальный кодекс РФ норму, закрепляющую постепенный переход на электронный документооборот между судом и участниками процесса.
2. Установить переходный период длительностью в пять лет.
3. Во время переходного периода поэтапно вводить обязанность участников процесса направлять документы в суд в электронной форме.

4. Разработать новый регламент подачи электронных заявлений, ходатайств, жалоб и прочих процессуальных документов.

5. Установить возможность управления электронным делом как публичную, так и для ограниченного круга лиц путем выдачи сертификата либо электронного ключа при открытии нового дела.

6. Оснастить арбитражные суды необходимым оборудованием.

Список использованной литературы и источников

1. Федеральный закон № 228-ФЗ от 27 июля 2010 г. «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации» // Собрание законодательства РФ. 2010. № 31, ст. 4197.

2. Постановление Правительства РФ от 27 декабря 2012 г. № 1406 «О федеральной целевой программе "Развитие судебной системы России на 2013 – 2020 годы"» // Собрание законодательства РФ. 2013. № 1, ст. 13.

3. Постановление Пленума Верховного суда Российской Федерации от 9 февраля 2012 г. № 3 «О внесении изменений в некоторые постановления Пленума Верховного суда Российской Федерации» // Российская газета. 2012.

№ 5708.

4. Постановление VIII Всероссийского съезда судей от 19 декабря 2012 г. «О состоянии судебной системы РФ и основных направлениях ее развития». URL: http://www.ssrf.ru/page/9085/detail.

5. *Брановицкий К.Л.* Информационные технологии в гражданском процессе Германии (сравнительно-правовой анализ). М.: Волтерс Клувер, 2010.

6. *Дружинкин Е.С.* Электронное правосудие в России: некоторые итоги и перспективы развития // Вопросы экономики и права. 2013. № 11.

7. *Мошков Е.А.* Содержание электронного правосудия в России и зарубежных странах // Проблемы права. 2015. № 4.

8. *Прокудина Л.А., Сосил Дж.С.* Система управления движением дела – фактор повышения эффективности отправления правосудия // Вестник ВАС РФ. 2003. № 10.

9. *Романенкова С.В*. Понятие электронного правосудия, его генезис и внедрение в правоприменительную практику зарубежных стран // Арбитражный и гражданский процесс. 2013. № 4.

10. *Решетняк В.И.* Электронное правосудие в гражданском процессе Сингапура // Российский юридический журнал. 2012. № 2.

11. *Хиетанен А.* Электронный суд и электронные правовые коммуникации в Финляндии // использование новых информационных технологий в арбитражном процессе и при осуществлении нотариальной деятельности: материалы междунар. семинара (7-8 сентября 2006 г., Екатеринбург). М., 2007.

Г.И. Садыйкова

ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

*Научный руководитель: **Ф.З. Кадырова**, к.п.н., доцент кафедры мониторинга, экспертизы, оценки качества образования, заведующая лабораторией естественно-математических дисциплин мониторинга, экспертизы, оценки качества образования ГАОУ ДПО «Институт развития образования Республики Татарстан»*

ПЕРЕДАЧА КОЛЛЕКТОРСКИМ АГЕНТСТВАМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ БАНКОВСКУЮ ТАЙНУ

Согласно действующему законодательству, банк гарантирует своим клиентам тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте (п.1 ст. 857 ГК РФ[129], статья 26 ФЗ «О банках и банковской деятельности» [130]). Однако на практике бывают случаи, когда довольно затруднительно определить грань нарушения и соблюдения банковской тайны: например, при передаче данных о клиенте коллекторским агентствам. На данный момент этот вопрос довольно спорным образом урегулирован в законодательстве, что позволяет коллекторским агентствам беспрепятственно осуществлять свою деятельность, зачастую используя неправовые методы взыскания задолженностей.

В первую очередь, следует отметить, что коллекторские агентства – это коммерческие организации, не являющиеся субъектами банковской сферы, а их деятельность не подлежит государственному лицензированию. Основными формами сотрудничества с банками являются заключение агентского договора (ст. 779 ГК РФ) или уступка права требования (цессия) (гл. 24 ГК РФ). В первом случае коллекторское агентство выступает в качестве посредника, то есть третьего лица, а во втором случае банк фактически продает свое право взыскания задолженности и передает коллектору все сведения и документы, имеющие значение для осуществления этой деятельности.

---

[129] Гражданский кодекс Российской Федерации. Часть вторая от 26 января1996 г. № 14-ФЗ (в ред. от 29 июня 2015 г.). М., 2015. С. 310.

[130] Федеральный закон «О защите прав потребителей» от 7 февраля 1992 г. №2300-1 (в ред. от 5 мая 2014 г.). М., 2015. С. 32.

Можно обозначить некоторые спорные вопросы о деятельности банков по передаче данных о должниках коллекторским агентствам:

1. **Имеет ли банк право на передачу информации, составляющей банковскую тайну, коллекторским агентствам?**

Из Информационного письма Президиума ВАС РФ от 30 октября 2007 г. № 120 следует, что уступка требований, вытекающих из кредитного договора, не нарушает нормативных положений о банковской тайне. Поскольку, вопервых, требование возврата кредита, выданного физическому лицу по кредитному договору, не относится к числу требований, неразрывно связанных с личностью кредитора. Во-вторых, потому что коллекторское агентство несет установленную законом ответственность за разглашение банковской тайны[131].

Однако из разъяснений Роспотребнадзора следует, что в данном случае имеет место ущемление прав клиентов на банковскую тайну, Роспотребнадзор помимо того, ссылается на п. 1 ст. 16 Закона о защите прав потребителей, устанавливающий недействительность условий договора, ущемляющих права потребителя по сравнению с правилами, закрепленными в российском законодательстве в области защиты прав потребителей[132].

2. **Законна ли передача прав кредитора (банка) по взысканию задолженности не кредитной организации?**

В отношении юридических лиц Высший Арбитражный суд разъясняет данный вопрос следующим образом: поскольку действующее законодательство не содержит предписания о возможности реализации прав кредитора по кредитному договору только кредитной организацией, следовательно, передача такого права не субъекту банковской деятельности не противоречит закону.

В отношении физических лиц, несмотря на положения Информационного Письма № 120, ВАС РФ придерживается другой позиции, указывая, что такие

[131] Информационное письмо Президиума ВАС РФ от 30 октября 2007 г. № 120 «Обзор практики применения арбитражными судами положений главы 24 Гражданского кодекса Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

[132] Письмо Роспотребнадзора от 23 августа 2011 г. № 01/10790-1-32. Доступ из. справ.-правовой системы «КонсультантПлюс».

условия договора нарушают права потребителей финансовых услуг и являются недействительными, поскольку по смыслу статьи 819 ГК РФ денежные средства в кредит может предоставить только банк или иная кредитная организация (имеющая соответствующую лицензию), следовательно, право требования может быть передано лишь субъектам банковской сферы"[133].

Роспотребнадзор придерживается идентичной позиции, ссылается на отсутствие разрешительного порядка осуществления подобных действий и в связи с этим на противоречие положениям статьи 388 ГК РФ[134].

3. **Каким образом должно быть оформлено согласие клиента?**

Согласно положениям Гражданского Кодекса не допускается уступка права требования без согласия должника, если личность кредитора имеет существенное значение для должника (п. 2 ст. 388 ГК РФ). Как известно, на практике в кредитный договор всегда включается условие о согласии передачи информации, составляющей банковскую тайну, третьим лицам.

Роспотребнадзор полагает, что при разрешении подобных споров, судам общей юрисдикции необходимо в каждом случае достоверно устанавливать факт действительного наличия добровольного волеизъявления заемщика на включение в кредитный договор условия о возможности уступки требования третьему лицу, не равноценному банку (иной кредитной организации) по объему прав и обязанностей в рамках лицензируемого вида деятельности, осуществляемой первоначальным кредитором. При этом указывается что, такое условие в любом случае является оспоримым, и к нему могут применяться правовые последствия по статье 167 и 178 ГК РФ. К тому же включение в договор условий, ущемляющих права потребителя и доказанный в этой связи факт нарушения прав может являться достаточным условием для предъявления и удовлетворения иска о компенсации потребителю морального вреда (пункт 45 Постановления).

---

[133] Постановление ФАС Северо-Западного округа от 28 апреля 2010 г. по делу N А56-60582/2009.

[134] Письмо Роспотребнадзора от 2 ноября 2011 № 01/13941-1-32 «Об отдельных аспектах правоприменительной практики по привлечению банков к административной ответственности за нарушение законодательства о защите прав потребителей». Доступ из справ.-правовой системы «КонсультантПлюс».

Анализ практики арбитражных судов показал, что в основном суды придерживаются позиции Роспотребнадзора. Как отмечают суды, согласно закону о персональных данных гражданин должен иметь возможность принять самостоятельное решение, дать согласие на передачу персональных данных третьим лицам или отказать. При этом такое согласие должно включать в себя необходимые реквизиты, в частности, кому именно могут быть переданы сведения о персональных данных, какая именно информация о заемщике станет известна третьим лицам, срок действия такого согласия, порядок его отзыва и др.[135]

Суды отмечают, что банки, как правило, используют типовые договоры присоединения, которые не содержат подобной информации, а специальное заявление о согласии на обработку и передачу персональных данных третьим лицам потребителем не заполняется. В связи с этим, по мнению судов, названное условие договора фактически является обязательным и не представляет право выбора. В случае его исключения, договор заключен с гражданином не будет, что нарушает права потребителя и противоречит принципу свободы договора[136].

Главная проблема заключается в том, что все участники соответствующих правоотношений вынуждены руководствоваться крайне разрозненными положениями гражданского и банковского законодательства, нормами в области защиты прав потребителей, которые изначально принимались без учета данного рынка услуг и не позволяют сегодня однозначно и комплексно его регулировать. Судебная практика также различна в зависимости от субъекта РФ.

Как отмечалось на заседании коллегии Генеральный Прокуратуры РФ коллекторские агентства зачастую допускают многочисленные нарушения законодательства, которые в ряде случаев имеют признаки преступлений. Нередко выявляются факты угроз жизни и здоровью граждан, их запугивания, незаконного проникновения в жилище, распространения порочащих их

[135] Постановление Шестого арбитражного апелляционного суда от 17 октября 2012 г. № 06АП-4042/12.

[136] Постановление Конституционного Суда РФ от 23 февраля 1999 г. № 4-П. Доступ из справ.-правовой системы «КонсультантПлюс».

сведений. Повсеместно ими не соблюдаются требования законодательства о персональных данных, обработка и разглашение которых осуществляются без согласия граждан.

К тому же согласно статистике, случаи регистрации правоохранительными органами сообщений о преступных посягательствах «коллекторов» получают все более широкое распространение. За период 2013 год – первое полугодие 2015 г. их число превысило 21,6 тыс. При этом в 2014 году по сравнению с предыдущим годом оно увеличилось с 6,3 тыс. до 8,7 тыс., а в первом полугодии 2015 г. составило 6,6 тыс.[137]

Поскольку гражданин является экономически слабой стороной и нуждается в особой защите своих прав, то необходимо внести некоторые ограничения для банков по передаче персональных данных клиентов третьим лицам. Например, ввести запрет передачи информации о клиентах коллекторским агентствам без наличия отдельно оформленного соглашения, поскольку наличие пункта в кредитном договоре зачастую является обязательным и не выражает в полной мере согласие клиента с возможными последующими действиями банка. К тому же многие специалисты отмечают, что коллекторская деятельность нуждается в лицензировании, стандартизации и в ведении государственного реестра. На данный момент в Государственную Думу внесен законопроект «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату долгов», однако в нем также не регулируются правила передачи банковской тайны коллекторским агентствам. Можно сделать вывод, что действующее законодательство нуждается в восполнении пробелов по регулированию данных отношений.

Список использованной литературы и источников

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации. Часть вторая от 26 января 1996 г. № 14-ФЗ. М: Проспект, 2015.

[137] http://genproc.gov.ru/smi/news/genproc/news-999695/ от 16.12.2015.

2. Информационное письмо Президиума ВАС РФ от 30 октября 2007 г. № 120 «Обзор практики применения арбитражными судами положений главы 24 Гражданского кодекса Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

3. Письмо Роспотребнадзора от 23 августа 2011 г. № 01/10790-1-32. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Письмо Роспотребнадзора от 2 ноября 2011 г. № 01/13941-1-32 «Об отдельных аспектах правоприменительной практики по привлечению банков к административной ответственности за нарушение законодательства о защите прав потребителей». Доступ из справ.-правовой системы «КонсультантПлюс».

5. Федеральный Закон «О защите прав потребителей» от 7 февраля 1992 г. № 2300-1 (ред. от 5 мая 2014 г.). М: Эксмо, 2015.

Судебная практика

6. Постановление Конституционного Суда РФ от 23 февраля 1999 г. № 4-П. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Постановление ФАС Северо-Западного округа от 28 апреля 2010 г. по делу № А56-60582/2009.

8. Постановление Шестого арбитражного апелляционного суда от 17 октября 2012 г. № 06АП-4042/12.

А.О. Сдобникова

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **В.Ф. Изотова**, к.ф.-м.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ФИШИНГ – ИНТЕРНЕТ-МОШЕННИЧЕСТВО С БАНКОВСКИМИ РЕКВИЗИТАМИ. ВОЗМОЖНОСТЬ ПРОТИВОДЕЙСТВИЯ

Развитие глобальных сетей привело к возникновению новых видов мошенничества, например фишинга (от английского fishing — рыбная ловля, выуживание). Фишеры обманным путем стремятся получить доступ к

конфиденциальным данным пользователя: банковским реквизитам, логинам и паролям для совершения мошеннических действий через Интернет.

Мошенники пытаются вывести пользователя на поддельный сайт или страницу – похожие на реальные страницы и сайты, им используемые. Применяя специальные психологические приёмы, фишеры побуждают пользователя ввести на поддельной странице свой логин и пароль, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Рассылка ссылок на ложные сайты достигается путём массовых рассылок электронных писем от имени популярных брендов, например, от имени банков, а также личных сообщений внутри различных сервисов, например, социальных сетей.

Фишинг может быть: почтовым (с использованием рассылки электронных сообщений), онлайновым (с использованием копирования страниц онлайнбанкинга самых известных банков) и комбинированным.

При комбинированном фишинге мошенники создают поддельный сайт банка. Письменно рекомендуют от имени банка ознакомиться с новыми привлекательными банковскими продуктами. При этом они предлагают пользователю перебросить средства со своего счета на депозит, якобы открытый для него банком. Получив, таким образом, доступ к счету жертвы, мошенники переводят деньги с него на свои счета.

В России фишинг широко распространен, с его помощью осуществляется около 70% всех несанкционированных операций с применением платежных карт. Так только в 2015 по данным Центробанка от действий кибермошенников банки и их клиенты потеряли более 3,5 млрд. рублей.

В Российской Федерации предусмотрена уголовная ответственность за кибермошенничество. В судебной практике для наказания фишеров используют статью 272 «Неправомерный доступ к компьютерной информации», статью 273 «Создание, использование и распространение вредоносных компьютерных программ» в главе 28 УК, так же статью 159 (мошенничество), которая

подразумевает за собой наказание вымогательство и мошенничество в сфере компьютерной деятельности[138].

Однако, зачастую наказания мошенников несоизмеримы с масштабом их преступлений. Так Чертановский суд Москвы приговорил к условным срокам хакеров Дмитрия и Евгения Попелышей, похитивших 13 млн. руб. у клиентов банка «ВТБ 24» [139] и оставил условный приговор фишерам без изменения, несмотря на протест прокуратуры[140].

В связи с этим, законодатели предлагают ужесточить наказание за кибермошенничество дополнить главу 28 УК РФ, посвященную преступлениям в сфере компьютерной информации, новой статьей, определяющей ответственность за фишинг. предполагающей наказание до четырех лет лишения свободы и крупный штраф[141].

В настоящее время разработан целый ряд специальных компьютерных программ, которые позволяют пользователю самостоятельно контролировать веб-доступ, блокировать нежелательные или опасные веб-сайты. Кроме того почтовые службы перед доставкой к пользователю обрабатывают электронные письма с помощью специальных спам-фильтров. Функцией «Антифишинг», обладают все современные браузеры, они информируют пользователей о подозрительных сайтах. Поэтому важно постоянно устанавливать обновления браузера. Нужно использовать современные антивирусные программы, поскольку все они обладают функцией предупреждения и блокировки перехода на сомнительные порталы.

При этом сам пользователь должен быть внимательным к тому, где и какую конфиденциальную информацию он вводит. Не следует переходить по

---

[138] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 30 декабря 2015 г.) // Собрание законодательства РФ. 1996. 17 июня. № 25, ст. 2954.

[139] Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга. URL: http://ria.ru/incidents/20121221/915789715.html (дата обращения: 12.03.2016).

[140] Владислав Мещеряков Россия: Хакеры, укравшие миллионы, остались на свободе. URL: http://www.cnews.ru/news/top/rossiya_hakeryukravshie_millionyostalis (дата обращения: 12.03.2016).

[141] В Госдуме предложили ввести уголовное наказание за фишинговые сайты. URL: http://www.interfax.ru/russia/472734 (дата обращения: 12.03.2016).

сомнительным и не проверенным ссылкам. Необходимо обращать внимание на адресную строку и адрес, ведь адрес http://facebook.sait.com – только похож на адрес социальной сети, но на самом деле это ссылка на фишинговую страницу сайта sait.com. Если получено письмо из банка, то для проверки подлинности информации следует позвонить непосредственно в банк.

Обычно порталы делают массовую рассылку о попытке взлома пользовательских аккаунтов и о том, что пользователи могут получить письмо с мошеннической ссылкой. Если же логин и пароль все-таки введен на ресурсе злоумышленников, то в кратчайшие сроки необходимо зайти на настоящий сайт и изменить пароль, логин и конфиденциальную информацию, а о попытке фишинга сообщить в службу поддержки ресурса.

А.О. Соловьев

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **В.Ф. Изотова**, к.ф.-м.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ВОЗМОЖНОСТЬ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ВРЕДОНОСНОЙ ИНФОРМАЦИИ В ГЛУБОКОМ ИНТЕРНЕТЕ

Понятие глубокий Интернет (DeepWeb) не имеет четкого значения. В широком смысле это словосочетание обозначает информацию, скрытую от индексации поисковыми системами, и включает закрытые сообщества и форумы, запрещенные к индексации отдельные страницы сайтов, базы данных, а также зашифрованные сети для анонимного серфинга (под последними чаще всего понимаются TOR и i2p). В более узком смысле глубокий Интернет – это псевдодоменные пространства, созданные при помощи зашифрованных соединений, обеспечивающие анонимность пользователя, благодаря сокрытию выданного ему провайдером IP адреса[142].

[142] *Пьерлуиджи Паганини* Хорошее и плохое в Deep Web // URL: http://hrazvedka.ru/guru/xoroshee-i-ploxoev-deep-web.html (дата обращения: 10.12.2015).

Индексирование в поисковых системах (веб-индексирование) – это процесс добавления сведений (о сайте) роботом поисковой машины в базу данных, впоследствии использующуюся для поиска информации на проиндексированных сайтах. Индексировать сайты глубокого Интернета невозможно, поскольку эти сайты находятся в специальной псевдодоменной зоне .onion. Из обычного Интернета они не открываются. а только из запущенного и подключенного к сети специального браузера Tor.

TOR (TheOnionRouter, что дословно переводится как луковый маршрутизатор) – свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Благодаря браузеру Tor имеется возможность скрыть свою личность как при использовании Интернет ресурсов и размещения различных материалов, так и при отправке электронных писем[143].

Высокий уровень защищенности достигается за счет того, что данные отправляются по зашифрованным каналам. Компьютеры, являющиеся узлами, через которые проходит информация, зачастую принадлежат обычным пользователям. Именно это и определяет их разбросанность по странам. В любой момент можно проложить новый маршрут пересылки данных, если в старом возникли сомнения. Единственный момент, когда можно произвести перехват данных – это в тот момент, когда они поступают к провайдеру.

Для того, что бы начать поиск по глубокой сети нужно найти сборник сайтов. Существуют также и поисковые системы, специально разработанные для поиска по сети tor, но чаще всего они не находят нужный контент. Одним из самых больших каталогов ссылок в глубокой сети является TheHiddenWiki. В ней содержится множество ссылок на сайты, форумы, онлайн-магазины, соцсети.

[143] Немного о Tor и русскоязычном .onion-пространстве 22 сентября 2014. URL: http://habrahabr.ru/post/237673/ (дата обращения: 10.12.2015).

Некоторые из них содержит противозаконные материалы. К примеру, сайты террористических группировок, запрещенных в РФ. Или предоставляют противозаконные услуги, такие как продажа оружия, наркотиков и т.д. Также в глубокой сети есть используется валюта для расчета-Bitcoin. Её в основном используют в преступных махинациях и при покупке все того же оружия и наркотиков. Для захода на большинство сайтов требуется регистрация, что усложняет их контроль со стороны правоохранительных органов, поиска покупателя и продавца.

Главная причина, по которой невозможности правовое регулирование глубокой сети это её децентрализованность. Не существует единых серверов, на которых расположена информация с сайтов. Поэтому, не возможно заблокировать доступ к ним, удалить информацию. Еще одной причиной является анонимность пользователей данной сети. Все их действия не возможно отследить, так как данные проходят через несколько серверов тора, прежде чем попадут во внешний мир через выходной сервер, а все данные, проходящие через сервера, шифруются.

На данный момент не существуют эффективных технических способов борьбы с глубокой сетью, одним из способов является отслеживание данных на выходе от клиента, когда она только поступает к провайдеру. Но данный способ затруднителен в применения в виду огромного количества данных ежесекундно поступающих к провайдеру и годится лишь в единичных случаях, когда нужно отследить конкретного пользователя. Следующим витком борьбы с глубоким Интернетом стал DPI (анализ трафика). Но пользователи глубокой сети издали версию Tor с маскировкой трафика, что провалило эффективное использование данного метода.

Правоведы отмечают большие проблемы правового регулирования Интернета. М.А Лапина., и Б.С. Николаенко признают, что «информационная функция государства по обеспечению безопасности информации, содержащейся в сети Интернет, не может быть в полной мере реализована силами, методами и

средствами, предлагаемыми российским законодательством и подзаконными актами[144].

Возможность защиты государственных интересов в сети ученые видят в международном сотрудничестве и жестком регулировании глобального информационного пространства. В тоже время приходится учитывать, что зашифрованные каналы связи используются для обмена важной государственной информацией и, что через глубокий Интернет осуществляется контроль за деятельностью криминальных сообществ.

Ю.С. Стребкова

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБРАБОТКЕ СОЦИОЛОГИЧЕСКИХ ОПРОСОВ

Информационные технологии (ИТ) – совокупность приемов и способов, производственных и программно-технологических средств и объединенных в технологическую цепочку, которая обеспечивает сбор, хранение, обработку, вывод и распространение информации, особенно в крупных организациях и компаниях[145].

На сегодняшний день современное человечество не представляет свою жизнь без компьютера. Без его использования не обходится и современные социальные науки. С помощью современных программ возможно выполнение самые различных процедур статистической обработки, начиная с простой группировки результатов опроса по критериям и до приближения зависимостей по точечным экспериментальным данным. Значительная часть методов математической статистики сложна для ручных расчетов, а автоматизация расчетов значительно облегчает работу исследователя.

---

[144] *Лапина М.А., Николаенко Б.С.* Информационная функция государства в сети Интернет // Информационное право. 2013. № 4. С. 11-15.

[145] *Гаврилов М.В.* Информатика и информационные технологии М., 2006. С. 528.

Одной из сфер применения информационных технологий при обработке социологических опросов является *автоматизация проведения опросов*. В настоящее время значительная часть опросов проводится при помощи сайтов. По сравнению с обычным анкетированием это дает ряд преимуществ, но самое основное – это отсутствие человека, который задает вопросы. Это создает ощущение большей защищенности ответов от постороннего глаза и, следовательно, повышает желание респондентов сообщать о себе больше сведений. Одним из относительно новых методов социологических опросов сегодня является SMS-опрос.

Отмечу еще одну сфера применения – *компьютерное моделирование*. В ряде случаев исследователи при изучении социальных процессов прибегают к такому методу как имитационное моделирование или ситуационное моделирование. Это такой метод исследования, при котором изучаемый социальный процесс заменяется моделью, которая точно описывает реальную ситуацию. По результатам данного исследования можно получить достоверные данные.

Приведу конкретный пример математической модели поведения в политике. Это модель гонки вооружений – модель Льюиса Ф. Ричардсона[146]. В 1918 году он вернулся с первой мировой войны и был потрясен размерами увиденных им разрушениями и насилия. Он был преисполнен решимости применить свои математические способности и знания к изучению феномена войны. Гонка вооружений, по его мнению, также является динамическим процессом и может быть представлена с помощью математической модели. Модель учитывала действие трех факторов: наличие военной угрозы между государствами, существующее бремя расходов, наличие прошлых обид. Такое рассуждение сводится к двум уравнениям:

$$X_{t+1}=kY_t–aX_t+g,$$

[146] *Мангейм Дж.Б., Рич Р.К.* Политология. Методы исследования: Пер. с англ. / Предисл. А.К. Соколова. М., 1997. С. 482.

$$Y_{t+1}=mX_t–bY_t+b,$$

где:

- X_t и Y_t – уровень вооружения в момент времени t;
- X_{t+1} и Y_{t+1} – в момент времени $t+1$;
- коэффициенты k, t, a, b – величины положительные, g и h – отрицательные либо положительные в зависимости от того, насколько враждебно или дружелюбно настроены государства X и Y;
- kY_t и mX_t – величина угрозы, так как чем больше эти числа, тем больше количество вооружений у противной стороны;
- aX_t и bY_t – величина расходов, так как за счет этих членов снижается уровень вооружений в следующем году;
- g и h – величина прошлой обиды, которая в рамках данной модели считается неизменной.

Особенность модели Ричардсона заключается в возможности прогнозировать будущее, и Ричардсон надеялся, что если политики смогут предсказывать приближение войны, то они смогут научиться предотвращать ее. К началу 70-х годов модель была испробована уже много раз на самых разных вариантах гонки вооружений. Модель работала, но ведь любая гонка вооружений имеет сложный комплекс причин, при изучении которых ни одна искусственно созданная модель охватить не может. Однако модель Ричардсона эффективна в случаях краткосрочных прогнозов. Касается ли это противостояния между НАТО и Организацией Варшавского Договора, ближневосточного конфликта или трагической 30-летней войны в ЮгоВосточной Азии, модель Ричардсона гонки вооружений всякий раз адекватно отражает основные особенности конкретного варианта гонки вооружений.

Существует несколько подходов к имитационному моделированию: системная динамика, дискретно-событийное моделирование и агентное моделирование. Исторически важнейшей моделью, существенно популяризовавшей системную динамику, является модель динамики городов

Дж. Форрестера[147]. В 1960-х гг. Форрестер построил динамическую модель типичного американского города. В качестве подсистем он выделил население, жилой фонд и предприятия. Население было поделено на не полностью занятых, занятых и менеджеров, жилой фонд – на дешевый, доходный и сверхдоходный, предприятия – на новые, зрелые и пришедшие в упадок. Была построена сложная модель с многочисленными прямыми и обратными связями между этими полученными подсистемами. За счет такой модели появилась возможность прогнозировать развитие городов. Несмотря на неактуальность модели для значительной части современных городов, модель не утратила своего исторического значения.

Такой метод как статистическая обработка данных можно рассмотреть на конкретном примере. Это пресс-конференция В.В. Путина 18 декабря 2014 года. Все данные взяты с фонда «Общественное мнение». Респондентам был предложен ряд вопросов:

1) первый вопрос: знаете ли вы, что-то слышали или слышите сейчас впервые об этом событии? Данные анализируются за 4 года: с 2006 по 2014. Большая часть респондентов знали об этом событии, но за исключением 2013 года; 2) второй вопрос: Вы лично видели или не видели (слышали или не слышали) прямую трансляцию или репортажи о пресс-конференции, проведенной В. Путиным 18 декабря? И если видели (слышали), то вам понравилось или не понравилось, как он отвечал на вопросы журналистов? Большей части респондентов понравилась речь президента, но в отличии опять-таки от 2013 года;

3) третий вопрос: Как вам кажется, в ходе этой пресс-конференции В. Путин отвечал на вопросы искренне или неискренне? Большая часть респондентов считает, что президент искренне отвечал на вопросы.

Судя по полученным данным можно сделать следующие выводы:

1) Пресс-конференция Президента в 2014 году стала более популярной по сравнению с 2013 годом и почти достигла уровня 2006 и 2007 годов. Уровень

[147] *Форрестер Дж.* Динамика развития города. М., 1974.

тех, кто не слышал и не знал о пресс-конференции в 2014 году заметно снижается.

2) Уровень тех, кто не слышал и не смотрел прямую трансляцию с течением лет растет. Количество тех, кому понравилась речь президента в 2014 году выросла, по сравнению с 2013, до уровня 2007 года.

3) Количество тех, кто считает, что Президент отвечает на вопросы неискренне к 2014 году снижается, а тех респондентов, кто считает что искренне – значительно растет.

Таким образом, внесение информационных технологий в практическую деятельность несет глобальные последствия, как для самих исследований, так и для исследователя. Исходя из этого нужно говорить о всё более растущей компьютеризации и машинизации процессов анализа вычислений, представление итогов в виде графиков, таблиц, схем и т.д. Поэтому повышается уровень скорости, а самое главное качества проводимых исследований, происходит разработка всё более новых видов опросов, а также модернизация уже существующих. В общем, растет уровень технологичности процесса.

Список использованной литературы и источников

1. *Гаврилов М.В.* Информатика и информационные технологии. М.: Гардарики, 2006.
2. *Кузнецова И.О., Григорьев Е.С., Фёдоров В.К.* Правила проведения конкретных социологических исследований. Саратов: Изд-во ГОУ ВПО «Саратовская государственная академия права», 2011.
3. *Латкин А.* Технологии, которые изменили мир. М.: «Манн, Иванов и Фербер», 2013.
4. *Мангейм Дж.Б., Рич Р.К.* Политология. Методы исследования: Пер. с англ. / Предисл. А.К. Соколова. М.: Издательство «Весь Мир», 1997.
5. *Форрестер Дж.* Динамика развития города. М.: Прогресс, 1974.
6. URL: http://fom.ru.
7. URL: https://ru.wikipedia.org.

К.А. Суханов

Национальный исследовательский университет «Высшая школа экономики» *Научный руководитель: **Б.А. Геренрот**, к.ю.н., доцент кафедры теории и истории права факультета права НИУ «Высшая школа экономики»*

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ДОМЕННЫХ ИМЕН И ТОВАРНЫХ ЗНАКОВ

На сегодняшний день в Российской Федерации отсутствует правовое регулирование отношений, связанных с использованием доменных имен. При регистрации доменного имени не происходит процедуры сравнения с зарегистрированными средствами индивидуализации. Это, в свою очередь, порождает весьма серьезную проблему для правообладателей таких обозначений – доменное имя может быть сходно до степени смешения с товарным знаком. Важно также учитывать, что лицо, зарегистрировавшее доменное имя, может действовать как добросовестно, так и недобросовестно.

Очевидно, на практике чаще встречаются случаи недобросовестного поведения лиц, которое проявляется в регистрации ими доменных имен, сходных до степени смешения или попросту идентичных товарным знакам. Такое явление называется киберсвоттингом. Законодательство Российской Федерации не дает определения этому понятию. Однако определение содержится в некоторых зарубежных источниках, например, в Законе США о защите потребителей от киберсквоттинга 1999 г.[148] В соответствии с данным актом, киберсквоттинг сводится к недобросовестности намерений в отношении владельца товарного знака, а также к регистрации, осуществлению сделок по возмездному отчуждению доменного имени или использованию доменного имени, идентичного или сходного до степени смешения с товарным знаком. Соответственно, под киберсквоттингом следует понимать деятельность лица (киберсквоттера), направленную на недобросовестное использование товарного знака или иного обозначения в схожем с ним до степени смешения доменном

[148] Anticybersquatting Consumer Protection Act (ACPA) // 15 U.S.C. § 1125 (d).

имени с целью получения прибыли от выкупа правообладателем такого обозначения.

С развитием электронной коммерции киберсквоттинг также стал популярным и в Российской Федерации, но в меньших масштабах чем в США, где, например, в 1999 г. доменное имя business.com было продано киберсквоттером за 7 500 000 $[149]. В Америке также весьма радикально решают проблему кражи домена: в 2011 г. к 5 годам тюремного заключения приговорили Даниэля Гонкальвеса за то, что он совершил кражу с последующей продажей доменного имени P2P.com интернет-предпринимателя Марка Островски[150].

В России с тем чтобы не допустить киберсквоттинг и защитить права обладателя товарного знака 11.12.2002 г. были внесены изменения в действовавший тогда Закон «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров»[151]. Поправки закрепили приоритет товарного знака над доменным именем, и, таким образом, использование товарного знака без разрешения правообладателя стало нарушением.

Одним из известных доменных споров в российской судебной практике, является спор международной компании «Истман Кодак Компани» (истец) с российским индивидуальным предпринимателем (ответчик). Согласно материалам дела, ответчик использовал в доменном имени обозначение «Kodak», сходное до степени смешения с товарным знаком правообладателяистца. Ввиду того что между сторонами не был заключен лицензионный договор об использовании товарного знака предусмотренным законом способом, суд пришел к выводу, что ответчик был не вправе регистрировать домен с таким обозначением. Поэтому ему было запрещено использовать обозначение, схожее с товарным знаком[152].

---

[149] Официальный сайт проекта компании RU-CENTER info.nic.ru. URL: http://info.nic.ru/node/3744 (дата обращения: 23.03.2016).

[150] Тюрьма за кражу домена. URL: http://info.nic.ru/node/3744 (дата обращения: 23.03.2016).

[151] Федеральный закон от 11 декабря 2002 г. № 166-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» // Собрание законодательства РФ. 2002. 16 дек. № 50, ст. 4927.

[152] См.: Постановление ФАС Московского округа от 6 сентября 2001 г. № КГ-А40/4822-01. Доступ из справ.-правовой системы «КонсультантПлюс».

Однако недобросовестность действий возможна и со стороны лица, которое регистрирует товарный знак со схожим до степени смешения или идентичным обозначением доменным именем, зачастую известным в сети Интернет. Такой вид нарушения называется обратным захватом домена. В качестве примера можно привести спор между ООО «Медиа-сервис-2000» (истец), и ООО «Комбатс» (ответчик)[153]. Ответчиком были зарегистрированы доменные имена combats.ru и kombats.ru. Позже истец зарегистрировал исключительные права на товарные знаки с аналогичными названиями. Суд первый инстанции иск удовлетворил, т.к. проведенная Федеральным институтом промышленной собственности экспертиза подтвердила использование ООО «Комбатс» доменных имен, сходных до степени смешения с товарными знаками истца. Поэтому ответчик по решению суда был обязан передать спорные домены истцу, а также выплатить денежную компенсацию в размере 2 млн. руб. В апелляционной инстанции стороны пришли к мировому соглашению, по условиям которого истец отказался от исковых требований, а ответчик обязался выплатить вознаграждение по договору отчуждения исключительных прав на товарные знаки.

Поэтому в условиях приоритетности товарных знаков, лицу, добросовестно использующему доменное имя и не нарушающего права других лиц такой регистрацией, рекомендуется также зарегистрировать товарный знак с аналогичным обозначением, чтобы избежать в будущем судебных споров, а также вероятного выкупа обозначения.

Следует заметить, что приоритет товарного знака в гражданском законодательстве Российской Федерации существовал не всегда. С введением в действие ч. 4 Гражданского кодекса Российской Федерации (далее – ГК РФ) стал действовать иной принцип – принцип старшинства прав, в соответствии с которым право признается за тем лицом, доменный знак или товарное имя которого было зарегистрировано раньше. Кроме того, согласно п. 9 ст. 1483 ГК

[153] См.: *Михеева Е.* Товарный знак и доменное имя // Корпоративный юрист. 2006. № 3. С. 18.

РФ не могли быть зарегистрированы в качестве товарных знаков обозначения, тождественные доменному имени, права на которые возникли ранее даты приоритета регистрируемого товарного знака[154]. Таким образом, администратор доменного имени мог оспорить на основании ст. 1512 ГК РФ (в ред. от 01.12.2007) предоставление правовой охраны товарному знаку и признать регистрацию такового недействительной. Однако в 2010 г. поправками, внесенными в ч. 4 ГК РФ, из п. 9 ст. 1483 ГК РФ было исключено указание на доменное имя[155]. Таким образом, законодатель вновь установил приоритет товарных знаков над доменными именами.

Кроме того, за несколько лет до этого, российским законодателем была предпринята попытка урегулировать отношения, связанные с использованием доменных имен. В Проекте ч. 4 ГК РФ (далее – Проект) была выделена гл. 76 «Право на доменное имя»[156]. В соответствии с Проектом доменное имя являлось одним из результатов интеллектуальной деятельности, а, следовательно, и объектом интеллектуальной собственности. В связи с чем, лицо, обладающее исключительным правом на доменное имя, могло рассчитывать на правовую охрану, аналогичную средствам индивидуализации. Также в Проекте были определены положения, устанавливающие регистрацию, порядок пользования и прекращения исключительного права на доменное имя, а также сроки действия такого права.

Однако изменения, которые предусматривались Проектом, не были приняты. Во многом статьи из §5 гл. 76 «Право на доменное имя» были схожи с положениями §2 «Право на товарный знак и право на знак обслуживания» и в большинстве своем дублировали их. Также причины отказа от принятия объяснил Комитет Государственной Думы РФ по экономической политике,

---

[154] Федеральный закон от 18 декабря 2006 г. № 231-ФЗ (в ред. от 24 июля 2007 г.) «О введении в действие части четвертой Гражданского кодекса Российской Федерации» (утратил силу) // Собрание законодательства РФ. 2006. 25 дек. № 52, ч. 1, ст. 5497.

[155] Федеральный закон от 4 октября 2010 г. № 259-ФЗ «О внесении изменений в часть четвертую Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 2010. 11 октября. № 41, ч. 2, ст. 5188.

[156] Проект № 323423-4 Гражданского кодекса Российской Федерации (части четвертой) (ред., принятая ГД ФС РФ в первом чтении 20 сентября 2006 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

предпринимательству и туризму. Он посчитал, что введение норм, регулирующих использование доменного имени «будет блокировать регистрацию товарных знаков» ввиду того, что ни в Российской Федерации, ни в зарубежных странах на тот момент не было определено место доменного имени в системе объектов интеллектуальной собственности[157].

В научной среде также критично относятся к отсутствию регулирования отношений, связанных с использованием доменных имен. Так, А.Г. Серго отмечает ошибочность доминирования товарных знаков над доменными именами, это, по его мнению, является причиной роста судебных споров[158]. Действительно, на практике нередко случается, когда добросовестный администратор доменного имени вынужден по решению суда передать права администрирования правообладателю товарного знака. Поэтому существующий приоритет во многом подрывает развитие экономической деятельности в сети Интернет.

В связи с этим правовое регулирование данной области нуждается в доработке, прежде всего, необходимо определить правовой статус доменного имени, не ограничиваясь лишь закреплением его определения в законе, установить[159]. Данные меры во многом бы способствовали как развитию предпринимательства в сети Интернет, так и ограничению распространения киберсквоттинга и обратного захвата доменов.

Г.С. Ткаченко

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

---

[157] Заключение Комитета по экономической политике, предпринимательству и туризму на проект № 323423-4 части четвертой Гражданского кодекса Российской Федерации. С. 8. URL: http://asozd2.duma.gov.ru/arhiv/a_dz_4.nsf/ByID/D07BB5890376674AC32571EF003B1FC3/$File/3АКЛ3234234.RTF?OpenElement (дата обращения: 21.03.2016).

[158] *Серго А.Г.* Правовой режим доменных имен и его развитие в гражданском праве: дис. … докт. юрид. наук. М., 2011. С. 18.

[159] См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 10 января 2016 г.) // Собрание законодательства РФ. 2006. 31 июля. № 31, ч. 1, ст. 3448.

ВЕРОЯТНОСТНЫЕ МЕТОДЫ В ПОЛИТОЛОГИИ

В политологии, также, как и в других областях человеческой деятельности, постоянно приходится иметь дело с событиями, которые невозможно точно предсказать. Так, например, процент голосов за того или иного кандидата может существенно изменяться, от ряда многих факторов, которые учесть практически нереально. Поэтому при организации выборов и непосредственно самого голосования приходится прогнозировать исход деятельности на основе какого-либо опыта, либо интуиции. Одной из главных задач в теории вероятностей является задача определения количественной меры возможного появления события. Вероятность – степень возможности наступления некоторого события. Когда основания для того, чтобы какое-нибудь возможное событие произошло в действительности, перевешивают противоположные основания, то это событие называют вероятным, в противном случае – маловероятным или невероятным. Вероятность и, естественно, невероятность события, может быть различной, в зависимости от перевеса положительных оснований над отрицательными, и наоборот. Поэтому часто вероятность оценивается на качественном уровне, особенно в тех случаях, когда более или менее точная количественная оценка невозможна или крайне затруднительна. Возможны различные варианты «уровней» вероятности.

Исследование вероятности с математической точки зрения составляет особую дисциплину – теорию вероятностей. Теория вероятностей[160] – раздел математики, изучающий закономерности случайных явлений: случайные события, случайные величины, их свойства и операции над ними. Теория вероятностей исследует закономерности, которым подчинены случайные события и случайные величины. Событием является констатация факта, в результате наблюдения или опыта. Наблюдением или опытом называют реализацию каких-либо условий, в которых событие может состояться. Опыт означает, что упомянутый комплекс обстоятельств создан сознательно. В ходе

[160] URL: https://ru.wikipedia.org/wiki/Теория_вероятностей.

наблюдения сам наблюдающий комплекс этих условий не создает и не влияет на него. Все события, за которыми люди наблюдают или сами создают их, делятся на:

– достоверные события;

– невозможные события;

– случайные события.

Достоверные события наступят всегда, если для этого создан определенный комплекс обстоятельств. Например, если депутат будет работать на благо народа, то он будет иметь успех среди граждан. Также можно наблюдать достоверное событие, если в урне для бюллетеней будут находится только голоса за кандидата А, то при подсчете голосов он, бесспорно, одержит победу на выборах.

Невозможные события, при создании комплекса определенных условий, не наступают. Здесь, наоборот, если в урне не будет бюллетеней за кандидата А, он не выиграет. Случайные события могут наступить, а могут и не наступить, в зависимости от реализации определенного комплекса условий. Например, курс доллара завтра может подняться или же опуститься. Также, и кандидат в депутаты может победить на выборах, а может и проиграть. Ожидаемая частота наступления случайных событий тесно связана с понятием вероятности. Закономерности наступления и не наступления случайных событий исследует теория вероятностей.

Также событие может наступить и не наступить, в зависимости от полученной информации о нем, например, сведений будет недостаточно, если комплекс нужных условий реализован лишь один раз. Если комплекс условий реализован много раз, то появляются известные закономерности. Например, никогда невозможно узнать заранее, принесет ли успех тот или иной законопроект в государстве, но если проанализировать ход истории и подобные проекты в других странах, то можно на основе этих данных сделать выводы и принять решение. Знание закономерностей, которым подчинены случайные события, позволяет делать прогнозы о том, когда эти события наступят. Например, как уже ранее отмечено, заранее нельзя предусмотреть результат

выборов в президенты, но если большинство граждан уже много лет симпатизирует одному из депутатов, то можно предусмотреть его победу. Ошибка может быть небольшой. Существует также множество задач, которые мы сможем решить только с помощью формул, так, например, в городе работают три избирательных пункта. В первом пункте приема бюллетеней есть 5 урн, во втором пункте – 3, а в третьем - 7. Каждый человек может проголосовать за одного из двух кандидатов, за кандидата ***А*** или ***Б***. Найдите вероятность того, что из урны будет извлечен бюллетень за кандидата ***А***. К этой же задаче прописано условие такого вида:

Голоса:

1) 5 урн - *А*-6 голосов, *Б*-3 голоса;
2) 3 урны - *А*-10 голосов, *Б*-1;
3) 7 урн - *А*-0 голосов, *Б*-10;

Первым делом мы вводим *Н*-гипотезы и представим, что:

H_1 – любой голос из пункта 1

H_2 – любой голос из пункта 2

H_3 – любой голос из пункта 3

А – голос за кандидата *А*

Существует формула полной вероятности: $P(A)=P(H_1)P(A/H_1)+P(H_2)P(A/H_2)+P(H_3)P(A/H_3)$, в нее мы подставим значения: $P(H_1)=1/3$, $P(H_2)=1/5$, $P(H_3)=7/15$, чтобы их найти мы обратимся к условию задачи. Если сложить урны, то получается 15, значит в одном пункте $5/15=1/3$, во втором получается $3/15=1/5$, а в третьем $7/15$. Теперь найдем другие значения: $P(A/H_1) = 2/3$, $P(A/H_2) = 10/11$, $P(A/H_3) = 0$. Как находить:

1) 30 голосов за кандидата *А*, 15 голосов за кандидата *Б*: $30/45=2/3$;
2) 30 голосов за кандидата *А*, 3 голоса за кандидата *Б*: $30/33=10/11$; 3) 0 голосов за кандидата *А*, значит вероятность равна 0.

После этого подставляем значения в формулу полной вероятности: $P(A)=1/3\cdot2/3+1/5\cdot10/11+7/15\cdot0=40/99$ или $40{,}4\%$.

Задачи на теорию вероятности встречаются в различных сферах жизни. Например, в выборах участвуют 4 кандидата. Кандидат *А*, кандидат *Б*, кандидат *В*, кандидат *Г*. Найдите вероятность того, что в выборах победит кандидат *В*. Так как, всего 4 кандидата, значит вероятность того что победит один из них равна *¼*. Еще одна задача: Сколько существует способов составления в случайном порядке списка из *7* кандидатов для выбора на руководящую должность? Так как порядок случаен, то количество способов равно числу перестановок из 7 человек: $P = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ (способов). Факториал числа [161] – это произведение натуральных чисел от *1* до *n* (включая данное число).

Методы теории вероятностей широко используются в различных отраслях естествознания, физике, астрономии, экономике, политологии и во многих других теоретических и практических науках. Теория вероятностей широко используется в планировании и организации производства, анализе качества продукции, анализе технологических процессов, статистике населения, биологии и других отраслях. Предназначение теории вероятности в политологии состоит в осуществлении прогнозов политических ситуаций и политической динамики, а также в получении количественных оценок политических и экономических рисков при принятии политических решений. Политология – наука о политике, то есть об особой сфере жизнедеятельности людей, связанной с властными отношениями, с государственно-политической организацией общества, политическими институтами, принципами, нормами, действие которых призвано обеспечить функционирование общества, взаимоотношения между людьми, обществом и государством. Политология изучает, прежде всего, политическую сферу жизнедеятельности людей: политические отношения, структуру, политические институты, политических лидеров и их поведение и т.д. Следовательно, объектом исследования политологии является сама, непосредственно, политическая сфера общества, как независящая от исследователя объективная реальность. В качестве предмета конкретного

[161] URL: http://ru.math.wikia.com.

политического исследования мы можем выбрать любой аспект политической сферы общества, например, политическую культуру граждан или политические институты. Итак, предметом политологии являются закономерности функционирования политической системы, политические лидеры, политические партии, процессы, конфликты, политические институты и отношения и т.д. Одной из важных функций политологии является прогностическая – это разработка вероятного знания относительно развития процессов в политической сфере. Какая вероятность победить того или иного кандидата на выборах? Какие изменения будет вносить в жизнь людей принятый той или иной нормативно-правовой акт? И какие последствия он будет нести в будущем? Любое политическое решение должно быть спрогнозировано, и именно поэтому в политологии очень широко применяется теория вероятности.

Политическое прогнозирование представляет собой исследования научного характера, применяемые к процессам и явлениям в политике. Посредством изучения определяются перспективы развития каких-либо событий в указанной сфере. Для наиболее точной оценки шансов на успех и вероятных политических стратегий применяемое прогнозирование должно опираться на аналитические аспекты методологии. Основной задачей предвидения считается способность предположить ход развития события с высоким уровнем вероятности. Следует отметить, что во всех видах деятельности возможно несоответствие результатов первоначальным намерениям. Однако, по мнению специалистов, именно в политике это явление приравнено к закономерному. Именно в этой сфере отмечается частое и очень далекое расхождение между запланированными целями и результатом их осуществления.

Таким образом, рассмотрев применение теории вероятности в политологии, можно утверждать, что возникновение данной теории не было случайным явлением в науке, а было вызвано необходимостью дальнейшего развития человека и общества.

Список использованной литературы и источников

1. *Гмурман В.Е.* Теория вероятностей и математическая статистика. М., 2007.
2. *Самойленко Н.И., Кузнецов А.И., Костенко А.Б.* Теория вероятностей и математическая статистика. Харьков, 2009.
3. *Ересько П.В., Изотова В.Ф., Сенина (Варламова) Е.В.* Информатика и математика (справочник для гуманитариев): учебное пособие. Саратов, 2010.
4. *Купин В.Н.* Политология. СПб., 2006.
5. URL: http://forexaw.com.
6. URL: https://ru.wikipedia.org.
7. URL: http://nsportal.ru.

П.А. Томникова

ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал

*Научный руководитель: **Е.А. Лачина**, к.ю.н., заведующая кафедрой гражданско-правовых дисциплин ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал*

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРАВ НА СЛУЖЕБНЫЕ ИЗОБРЕТЕНИЯ В СОВРЕМЕННОМ ГРАЖДАНСКОМ ПРАВЕ

В связи с социально-экономическими преобразованиями в стране центральное место в правовом регулировании занимают вопросы собственности. Вместе с этим в настоящее время одной из приоритетных задач государства является эффективная инновационная политика и политика реиндустриализации, направленная на развитие научно-технической сферы для повышения конкурентоспособности отечественных разработок на мировом рынке, стратегии импортозамещения и увеличения экспорта наукоемкой продукции, который непременно затрагивает вопросы интеллектуальной деятельности. Для перехода к такой новой модели экономики ключевое значение приобретает стимулирование создания результатов интеллектуальной деятельности и актуализация ее эффективного управления, что включает себя в первую очередь эффективное правовое регулирование возникновения, осуществления и защиты прав на эти результаты.

В результате этого мы видим тесную взаимосвязь проблем урегулирования гражданско-правовых отношений относительно имущественных и связанных с ними личных неимущественных прав на объекты интеллектуальной (промышленной) собственности. К ним относятся исключительные права на использование этих объектов, поэтому представляется актуальным решение вопроса о принадлежности этих прав, определение оснований получения этих прав, защите, в частности, для изобретений, полезных моделей и промышленных образцов, созданных в условиях служебной деятельности, а также правовое

регулирование взаимоотношений между создателями служебных результатов интеллектуальной деятельности и их правообладателями – работодателями.

На сегодняшний день достаточное количество результатов интеллектуальной деятельности носят служебный характер, т.е. они создаются в связи с выполнением работником своих трудовых обязанностей или конкретного задания работодателя. Это можно объяснить тем, что для коммерциализации объектов промышленной собственности необходимо большое количество финансовых, технологических, технических средств, которые могут быть сосредоточены в крупных хозяйственных субъектах. При этом коммерциализация осуществляется, как правило, не авторами, а иными лица, приобретающие на основании закона исключительные права на данные результаты интеллектуальной деятельности. Регулирование правоотношений между работником и работодателем, связанных с созданием технического результата интеллектуальной деятельности и последующим использованием объектов промышленной собственности в настоящий момент несовершенно и содержит достаточное количество пробелов, а вместе с тем и вопросов, в связи с чем, права и обязанности сторон довольно часто нарушаются и не соблюдаются, что приводит к возникновению споров. Одним из основных таких вопросов, является выплата авторского вознаграждения, что сопряжено с определенными правовыми проблемами. Нормы, регулирующие отношения, связанные со служебными результатами интеллектуальной деятельности, содержатся в различных главах части четвертой ГК РФ, начиная с главы 69 («Общие положения»).

Наибольший интерес среди служебных результатов интеллектуальной деятельности вызывают служебные *объекты патентных прав*, а именно изобретения, полезные модели и промышленные образцы, которые чаще всего выступают в роли объектов промышленной собственности и поэтому требуют наиболее полного и комплексного исследования.

Понятие «служебный результат интеллектуальной деятельности» возникло

в рамках патентного права. На сегодняшний день Гражданский кодекс РФ [162] выделяет как минимум семь понятий результатов интеллектуальной деятельности (далее по тексту - РИД), носящих статус служебных и имеющих разные формулировки и основания возникновения. В частности: - ст. 1295 ГК РФ относит к служебным РИД: - произведения науки, литературы или искусства, созданные в пределах, установленных для работника (автора) трудовых обязанностей; - ст. 1320 признает служебным исполнение, созданное в порядке выполнения служебного задания; - ст. 1370 наделяет изобретение, полезную модель, промышленный образец статусом служебных, при условии, что они созданы работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя; - аналогичные условия предусмотрены в ст. 1430 для признания служебным селекционного достижения; в ст. 1461 - для служебной топологии.

Правовой режим служебных результатов интеллектуальной деятельности (РИД) намного более сложен и существенно отличается от так называемых «свободных» или не служебных. Они в первую отличаются степенью урегулированности взаимоотношений между субъектами права, которые в свою очередь могут быть многоаспектными, а также содержанием правовых норм и их расположением. Это должно позволить правомерно разрешить притязания на один и тот же объект патентных прав работодателя, работника, а в некоторых случаях и третьих лиц, обеспечивая баланс экономических интересов.

По мнению российских и зарубежных специалистов «при создании служебных изобретений важным аспектом является обеспечение баланса интересов участников правоотношений в связи со служебными изобретениями: для работника – посредством стимулирования к созданию служебных изобретений через систему льгот, поощрений и пр.; для работодателя – право

[162] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (в ред. 30 декабря 2015 г. № 431-ФЗ) // Собр. законодательства Рос. Федерации. 2006. № 52, ч. 1, ст. 5496. С. 14803– 14949.

использовать изобретение, созданное работником в порядке выполнения им своих трудовых функций»[163].

Правовое регулирование служебных результатов интеллектуальной деятельности (РИД) осуществляется на основании главы 72 «Патентное право» Гражданского кодекса РФ, в частности, согласно норме пункта 1 статьи 1370 ГК РФ «изобретение, полезная модель или промышленный образец, созданные работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, признаются соответственно служебным изобретением, служебной полезной моделью или служебным промышленным образцом»[164]. При этом служебный результат интеллектуальной деятельности характеризуется наличием трудовых отношений между работником и работодателем. Другими словами, в период создания служебного РИД работник и работодатель должны состоять в правоотношениях, вытекающих из трудового договора, т.е. правовым основанием для создания служебного результата являются первоначально трудовые отношения, а уже основанием для возникновения гражданских прав и обязанностей (в том числе и интеллектуальных прав) на служебный РИД является факт его непосредственного создания (подпункт 5 пункта 1 статьи 8 Гражданского кодекса РФ).

В настоящее время «концепция служебного изобретательства в Российской Федерации состоит в том, что факт создания служебного изобретения влечет за собой возникновение у работодателя правомочие на такое изобретение, судьбу которого он вправе определить по своему усмотрению»[165]. Вот почему особенно важно определить момент создания служебного РИД, поскольку неправильное решение может повлечь автоматически изменение правового режима объекта патентных прав и, следовательно, повлиять на права и обязанности как

---

[163] *Крупко С.И.* Институт служебных изобретений. Новеллы и проблемы правового регулирования // Интеллектуальная собственность в России и ЕС: правовые проблемы. Сборник статей. М., 2008. С. 133.

[164] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (в ред. 30 декабря 2015 г. № 431-ФЗ) // Собр. законодательства Рос. Федерации. 2006. № 52, ч. 1, ст. 5496. С. 14803– 14949.

[165] *Гаврилов Э.П., Еременко В.И.* Комментарий к части четвертой Гражданского кодекса Российской Федерации (постатейный). М., 2009. С. 306.

работника, так и работодателя (заказчика). Согласно ст. 1363 ГК РФ «Исключительное право на изобретение, полезную модель, промышленный образец и удостоверяющий это право патент действуют при условии соблюдения требований, установленных настоящим Кодексом, с даты подачи заявки на выдачу патента в федеральный орган исполнительной власти по интеллектуальной собственности или в случае выделения заявки (пункт 4 статьи 1381) с даты подачи первоначальной заявки»[166]. И как отмечает С.И. Крупко, «момент создания изобретения не совпадает и всегда предшествует моменту возникновения исключительных прав на него и моменту, с которого начинается патентная охрана изобретения. Появление исключительных прав на изобретение обусловлено актом признания со стороны государства, в котором испрашивается правовая охрана»[167]. Следует полностью согласиться с позицией С.А. Казьминой, которая справедливо замечает, что «изобретение не создается в одночасье, а существуют фазы жизненного цикла, связанные с его созданием (создание изобретения, формулировка изобретения, подача заявки на изобретение). При этом фаза создания может быть сильно растянута по времени. Поэтому в случае, если фаза создания РИД приходится на период оформления отношений с работодателем, то вопрос о правообладателе технического решения решается просто в соответствии с положениями Гражданского кодекса. Но в том случае, когда одна из фаз приходится на период либо еще не оформленных отношений с работодателем, либо уже прекративших с ним отношений, либо оформленных отношений уже с новым работодателем, то вопрос усложняется и может перейти в стадию судебного рассмотрения»[168].

На сегодня во избежание конфликтов на многих российских предприятиях и организациях действует практика, согласно которой между работником и работодателем оформляется дополнительное соглашение в качестве

---

[166] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (в ред. 30 декабря 2015 г. № 431-ФЗ) // Собр. законодательства Рос. Федерации. 2006. № 52, ч. 1, ст. 5496. С. 14803– 14949.

[167] *Крупко С.И.* Материально-правовые аспекты изобретений работников // Хозяйство и право. 2011. № 8. С. 16-18.

[168] *Казьмина С.А.* Служебные изобретения: конфликт и баланс интересов (Система правовой охраны изобретений на предприятии). М., 2010. С. 49-50.

неотъемлемой части трудового договора, либо гражданско-правовой договор, либо должностная инструкция работника, из которой следует, что создание новых технических решений, способных к правовой охране в качестве объектов патентного права, в определенной технической области непосредственно входит в круг обязанностей работника, или должно существовать должным образом оформленное задание на разработку, не противоречащее должностной инструкции работника, устанавливающее, в частности, кому из сторон трудового договора будут принадлежать права на патентоспособный результат интеллектуальной деятельности, созданный работником, условия, порядок создания и использования созданных РИД, размер и порядок выплат компенсаций или вознаграждений авторам. Согласно новой редакции статьи 1370 ГК РФ (изменения в части четвертой ГК РФ в редакции федерального закона от 12.03.2014 № 35-ФЗ, вступившие в действие с 01.10.2014,), положения о служебных результатах интеллектуальной деятельности следует включать только в индивидуальные договоры, т.е. либо в трудовые, либо в гражданскоправовые договора. Ранее, положения о служебных РИД могли включаться и в коллективные договора (ст.40 Трудового кодекса РФ). Как отмечал В. Дозорцев, «условия об изобретении могут быть как предметом трудового договора, так и предметом гражданско-правового договора, а право на получение патента имеет гражданско-правовую природу»[169]. Так как защита интеллектуальных прав осуществляется посредством гражданско-правовых норм, предусмотренных в ст. ст. 1248, 1252, п. 2 ст. 1370 ГК РФ, то в любом случае, куда бы ни были включены данные положения, они сохраняют свой гражданско-правовой характер, а взаимоотношения между работником и работодателем принимают смешанных характер как трудовых, так и гражданско-правовых.

«Законодательное закрепление договора между работодателем и работником в качестве основания перехода права на получение патента и

[169] *Дозорцев В.А.* Интеллектуальные права. Понятие. Система. Задачи кодификации: Сборник статей. М., 2005. С. 294, 303.

исключительных прав на изобретение от работника к работодателю в большей степени отвечает интересам автора. При таком подходе работодатель вынужден заблаговременно до момента создания служебного изобретения урегулировать с работником условия распределения исключительных прав на служебное изобретение, условия его использования, размер и порядок выплаты вознаграждения и компенсаций. Предварительные договоренности между работодателем и работником способствуют правовой определенности и снижают риск возникновения споров, в том числе относительно квалификации изобретения работника как служебного».[170] Договор, в частности, должен содержать обязательство работника письменно информировать работодателя о каждом созданном в ходе работы патентоспособном результате интеллектуальной деятельности (п. 4 ст. 1370 ГК РФ). Представляется, что данное обязательство создано в интересах обеих сторон трудового или гражданско-правового договора, чтобы избежать в дальнейшем споров, связанных с защитой патентных прав. В данном уведомлении работник должен указать, использовались ли им денежные, технические или иные материальные средства работодателя/заказчика, в рамках каких работ, задания было создано техническое решение для последующего решения вопроса в соответствии с п. 5 ст. 1370 ГК РФ. «При отсутствии в договоре между работодателем и работником соглашения об ином (пункт 3 настоящей статьи) работник должен письменно уведомить работодателя о создании в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя такого результата, в отношении которого возможна правовая охрана».[171] Бывают ситуации, когда работник-автор умышленно скрывает факт создания патентоспособного изобретения, либо неверно истолковывает статус созданного технического решения как «не служебного», то «в случае ненадлежащего исполнения автором обязанности по уведомлению работодателя о создании служебного изобретения

[170] *Крупко С.И.* Материально-правовые аспекты изобретений работников // Хозяйство и право. 2011. № 8. С. 16-18.

[171] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (в ред. 30 декабря 2015 г. № 431-ФЗ) // Собр. законодательства Рос. Федерации. 2006. № 52, ч. 1, ст. 5496. С. 14803– 14949.

работодатель вправе обратиться в суд в защиту своих прав с иском об установлении патентообладателя, если патент еще не выдан, а если патент выдан – с иском о признании патента недействительным»[172].

Более существенная проблема возникает в случае решения работником уступить право на получение патента третьему лицу. Сразу возникает вопрос о нарушении имущественного права работодателя (право на использование). Не будут ли нарушены условия трудового договора, в которых могут содержаться дополнительные условия, в частности, о неразглашении служебной (коммерческой) информации? Логично также предположить, что в случае уступки патента работником третьему лицу, работодатель получает прямого конкурента в лице патентообладателя, что негативно может сказаться на работодателе. Либо ситуация, когда патентообладатель (иное лицо) предоставляет такое право использования на правах лицензии работодателю, кто и каким образом будет выплачивать автору РИД вознаграждение за использование? Патентообладатель, на наш взгляд, в такой ситуации вправе обратиться в суд с требованием к работнику возместить убытки в связи с упущенной выгодой (ст.15 ГК РФ) от права на использование РИД в собственном производстве. Во-вторых, законодатель в случае такого перехода права на получение патента к работнику не применяет к нему определения «не служебного», не относит прямо к так называемым «свободным» (как, например, в случае с п.5 ст.1371) и в случае с использованием работодателем РИД в своем производстве четко указывает на сохранение за ним служебного характера – «… работодатель в течение срока действия патента имеет право использования *служебного изобретения, служебной полезной модели или служебного промышленного образца* в собственном производстве на условиях простой (неисключительной) лицензии с выплатой патентообладателю вознаграждения…»[173]. Т.е., можно предположить, что даже при возвращении

[172] *Крупко С.И.* Материально-правовые аспекты изобретений работников // Хозяйство и право. 2011. № 8. С. 16-18.

[173] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ (в ред. 30 декабря 2015 г. № 431-ФЗ) // Собр. законодательства Рос. Федерации. 2006. № 52, ч. 1, ст. 5496. С. 14803– 14949.

работнику-автору прав на получение патента на РИД, он не утрачивает своего служебного характера и поэтому полноправно и полностью своими исключительными правами на него работник как патентообладатель без одобрения работодателя не может. В чем весь и казус данной ситуации. Таким образом, несовершенство современного законодательства в данном вопросе может не только негативно сказаться на балансе интересов всех участников данных правоотношений, но и ущемить в правах работодателя.

В связи с этим, законодателю в п.4 ст.1370 ГК РФ предлагается внести ясность в случай, касающийся перехода прав на получение патента к работнику, а именно статуса результата интеллектуальной деятельности к категории «свободного», т.е. не служебного, либо законодательно ограничить объем исключительных прав работника в пользу работодателя.

Предлагается сформулировать второй абзац п. 4 ст. 1370, по аналогии со статьей 1371 ГК РФ, следующим образом: «Если работодатель в течение четырех месяцев со дня уведомления его работником не подаст заявку на выдачу патента на соответствующие служебное изобретение, служебную полезную модель или служебный промышленный образец в федеральный орган исполнительной власти по интеллектуальной собственности, не передаст право на получение патента на служебное изобретение, служебную полезную модель или служебный промышленный образец другому лицу или ***письменно не уведомит*** работника о сохранении информации о соответствующем результате интеллектуальной деятельности в тайне, право на получение патента на такие изобретение, полезную модель или промышленный образец возвращается работнику *либо передается указанному работником третьему лицу*.

В случае, когда право на получение патента возвращено работнику, работодатель в течение срока действия патента имеет право использования служебного изобретения, служебной полезной модели или служебного промышленного образца в собственном производстве на условиях простой (неисключительной) лицензии с выплатой патентообладателю вознаграждения,

размер, условия и порядок выплаты которого определяются договором между работником и работодателем, а в случае спора – судом.

В случае, когда право на получение патента передано указанному работником третьему лицу, работодатель вправе по своему выбору потребовать с работника возмещение убытков в связи с упущенной выгодой, либо имеет право в течение срока действия патента использовать служебное изобретение, служебную полезную модель или служебный промышленный образец в собственном производстве на условиях ***безвозмездной*** *простой (неисключительной) лицензии с патентообладателем с выплатой* ***работнику вознаграждения за использование****, размер, условия и порядок выплаты которого определяются договором между работником и работодателем, а в случае спора – судом».*

Предполагается, что такая формулировка должна соблюсти баланс интересов всех участников данных правоотношений.

Е.А. Трифонова
ФГБОУ ВО «Саратовская государственная юридическая академия»
*Научный руководитель: **Т.Н. Романченко**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ПЕРЕДАЧА ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ И ВОЗМОЖНОСТИ ОБЕСПЕЧЕНИЯ ЕЕ БЕЗОПАСНОСТИ

На наш взгляд, одной из актуальных проблем современности является обеспечение безопасности информации. Многие знают (либо слышали) об Эдварде Сноудене, бывшем сотруднике АНБ, раскрывшем факт всеобъемлющего слежения в 60 странах за более чем миллиардом человек правительствами 35 стран.

Во время службы в ЦРУ он под дипломатическим прикрытием был направлен в Женеву. В круг его обязанностей входило обеспечение безопасности компьютерных сетей. По словам самого Эдварда, работа в Швейцарии открыла ему глаза на то, что он является особым звеном в спецслужбах США, приносящим людям больше вреда, чем пользы. В 2009 году программист уволился из ЦРУ и начал работать в сотрудничающих с АНБ консалтинговых компаниях, выполнял обязанности внешнего подрядчика. Работа здесь в большей степени разочаровала Сноудена в деятельности Агентства национальной безопасности США, избавив от иллюзий о правомерных действиях правительства в отношении всего мира. Молодой идеалист Сноуден отмечает, что рассекретить неправомерные действия АНБ и ЦРУ он хотел еще в 2008 году, но понадеялся, что с приходом к власти Барака Обамы ситуация в секретных службах США изменится. Вскоре для программиста стало очевидным, что новый президент США продолжает политику своих предшественников и не намерен препятствовать подобной деятельности. По его словам, тогда он впервые задумался о разглашении служебных тайн, но не сделал этого потому, что большинство секретов ЦРУ – про людей, а не про машины и системы.

Приняв решение действовать в январе 2013 года, он связался с прессой посредством кодированных e-mail сообщений, при этом не раскрывал своего имени, но сообщил, что обладает важной секретной информацией. Сноуден писал, что со временем его личность раскроется, но до тех пор просил не делать длинных цитат из его сообщений, из опасения быть идентифицированным посредством семантического анализа.

Сноуден раскрыл информацию о программе PRISM, включающей в себя массовую слежку за переговорами американцев и иностранных граждан посредством телефона и Интернета. По его утверждениям, PRISM дает возможность Агентству просматривать фотографии, видео, отслеживать пересылаемые файлы, просматривать электронную почту, прослушивать голосовые и видеочаты, узнавать другие подробности из социальных сетей. В программе PRISM принимают участие Microsoft (Hotmail), Google (Gmail), Yahoo!, Facebook, Skype, YouTube, Apple и Paltalk. Широкой общественности о существовании программы стало известно 6 июня 2013 года, когда отрывки из секретной презентации о PRISM были опубликованы в газетах «Washington Post» и «The Guardian». Директор Национальной разведки США Джеймс Клеппер подтвердил существование PRISM и заявил, что программа работает в соответствии с законом об иностранной разведке, недавно пересмотренным Конгрессом США. Также Сноуден разгласил сведения о существовании британской программы слежения Tempora и сообщил, что из-за интегрированного программного обеспечения, позволяющего следить за пользователем, не пользуется iPhone. Сноуден предпочитает обычный мобильный телефон вместо современных смартфонов.

Деятельность PRISM и Tempora по сбору и хранению информации, полученной в результате прослушки звонков, перехвата сообщений, является незаконной, как в соответствии с законодательством Российской Федерации, так и с международным. Таким образом, налицо непосредственное нарушение конституционных прав граждан, так как в соответствии со ст. 23 Конституции

Российской Федерации каждый гражданин имеет право на тайну переписки, телефонных разговоров, почтовых и иных сообщений.

17 июня со ссылкой на данные Сноудена газета «The Guardian» сообщила, что спецслужбы Великобритании осуществляли мониторинг компьютеров, перехватывали телефонные звонки иностранных политиков и чиновников, участвовавших в саммите Большой двадцатки в Лондоне в 2009 году. Секретную работу проводили Центр правительственной связи Великобритании и Агентства национальной безопасности США. Также британские спецслужбы во время саммита перехватывали телефонные переговоры президента России Дмитрия Медведева.

Именно такая версия событий была нам представлена, можно однако сомневаться в ее реальности, ведь скачать данные подобного объема без ведома ЦРУ – практически невозможно. Отсюда вывод о том, что их позволили скачать и существует возможность того, что последующие события – спланированный спектакль. Но факт остается фактом – пользователи смартфонов подвержены опасности, которая исходит именно от спецслужб. Безусловно, информация о том, что телефоны прослушиваются, не нова, а задача в том, чтобы минимизировать риск утечки личной информации. В интервью программе BBC «Панорама» Сноуден сообщил, что британская GCHQ[174] может использовать эксплойт[175], который позволяет подслушивать разговоры и получать доступ к передаваемым и хранящимся данным, без ведома пользователя дистанционно управлять смартфоном: включать и выключать его, производить звукозапись (не только во время разговора), фотои видеосъёмку, определять местоположение телефона.

Какие же устройства наиболее безопасны для их владельцев? В настоящее время существует множество корпораций, производящих технические средства

[174] GCHQ – Government Communications Headquarters, спецслужба Великобритании ответственная за ведение радиоэлектронной разведки и обеспечение защиты информации органов правительства и армии.

[175] Эксплойт, эксплоит — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования.

передачи информации. С точки зрения безопасности на уровне корпорации ОС от Apple имеет ряд преимуществ перед Android. iOS имеет в своем арсенале мощные средства для централизованного управления девайсами, такие как профили конфигурации, возможность удаленного полного сброса и встроенная поддержка сторонних MDM-решений. Android в чистом виде таких возможностей не имеет. Для интеграции с MDM-системами[176] на Android необходимо предварительно устанавливать специальное ПО. Стоит отдельно отметить, что компания Samsung ушла далеко вперед в вопросах корпоративной безопасности по сравнению с другими производителями девайсов на Android. Речь идет о программе SAFE (Samsung For Enterprise) и надстройке KNOX, которая представляет собой хорошо защищенный контейнер для всех рабочих активностей пользователей с поддержкой сторонних MDM-систем. Таким образом, все аппараты от Samsung, работающие на Android 4.3 и выше, полностью соответствуют принципам защищенного бизнеса. Тем не менее, Apple имеет гораздо меньшую линейку продуктов, нежели производители Android-девайсов, поэтому ей не составляет труда обеспечить поддержку систем корпоративной безопасности для всех своих смартфонов, планшетов и актуальных версий ОС. В категории наиболее безопасной для использования на уровне компаний операционной системы победителем выходит iOS.

Безопасная последовательность загрузки, подпись кода и функции обеспечения безопасности в процессе выполнения помогают следить за тем, чтобы на устройстве запускались только надежные программы и фрагменты кода. В iOS также реализованы дополнительные функции шифрования и защиты данных для обеспечения безопасности данных пользователей даже в случае компрометации других частей системы безопасности (например, на устройстве с несанкционированными модификациями). В каждом устройстве с iOS имеется специализированный криптографический модуль, который встроен непосредственно между флэш-памятью и основной системной памятью для

[176] MDM – Master Data Management, система управления, применяющаяся для согласования данных различных информационных систем и создания целостного представления об учетных записях.

повышения эффективности шифрования файлов. В мобильных устройствах решающее значение имеют скорость и энергоэффективность.

Криптографические операции требуют значительных ресурсов и могут снижать время работы от аккумулятора или производительность устройства, если при разработке и реализации не уделить этим аспектам должного внимания. Уникальный идентификатор устройства (UID) и идентификатор группы устройств (GID) – это 256-битные ключи, вшитые (UID) или скомпилированные (GID) в процессор программ и Secure Enclave[177] на этапе производства. Ни одна программа или микропрограмма не может прочитать их напрямую; им доступны только результаты операций шифрования и дешифрования. Кроме того, эти ключи могут быть использованы только специализированным модулем Secure Enclave. Идентификаторы UID являются уникальными для каждого устройства и не регистрируются компанией Apple или ее поставщиками. Идентификаторы GID являются общими для всех процессоров одного класса устройств (например, всех устройств с процессором Apple A8) и используются для некритических по отношению к безопасности задач, таких как доставка системного программного обеспечения во время установки и восстановления. Интеграция этих ключей в микросхему предотвращает их подделку или обход и гарантирует, что они будут доступны только специальному модулю. UID обеспечивает возможность криптографической привязки данных к конкретному устройству. Например, UID входит в иерархию ключей, используемых для защиты файловой системы, поэтому при физическом перемещении микросхем памяти из одного устройства в другое файлы будут недоступны. UID не связан ни с каким другим идентификатором устройства. За исключением UID и GID, все остальные криптографические ключи создаются системным генератором случайных чисел с использованием алгоритма. Для генерирования ключей внутри Secure Enclave

[177] Secure Enclave – технология безопасности для защиты данных паролей и отпечатков.

используется аппаратный генератор истинно случайных чисел: в его основе лежат нескольких кольцевых генераторов.

Помимо функций аппаратного шифрования, встроенных в устройства iOS, Apple использует специальную технологию для более надежной защиты данных, хранящихся во флэш-памяти на устройстве. Технология защиты данных позволяет устройству реагировать на обычные события, такие как поступление телефонного вызова, а также обеспечивает более высокий уровень шифрования данных пользователей. Основные системные программы, такие как Сообщения, Почта, Календарь, Контакты, Фото и Медиа данные, используют технологию защиты данных по умолчанию, а программы сторонних разработчиков, установленные в iOS 7 или более поздней версии, получают ее автоматически. Защита данных осуществляется путем построения и контроля иерархии ключей и основана на технологиях аппаратного шифрования, встроенных в каждое устройство iOS. Защита данных организована на уровне файлов: каждому файлу назначается один из классов защиты, а доступность определяется разблокированием ключей класса.

Эдвард Сноуден считает, что не только корпорация Apple имеет ключи к личным данным, которые хранятся в телефонах iPhone.

«ФБР говорит, у Apple имеются «эксклюзивные технологические средства» для разблокирования этого телефона. При всём уважении это чушь,» – сказал Сноуден в рамках видеомоста, посвящённого теме демократии и развитию гражданского общества. Его слова приводит Sputnik.

Напомним, 1 марта судья нью-йоркского района Бруклин Джеймс Оренштейн поддержал корпорацию Apple и освободил её от оказания технической помощи американским властям в части взлома смартфонов iPhone. Речь идёт не о телефоне террориста из Сан-Бернардино Сайеда Фарука, а о другом устройстве, фигурировавшем в деле о наркотиках.

Apple уже находится в состоянии судебной тяжбы с ФБР, которое потребовало у компании взломать телефон исламиста Фарука. Доказывая, почему это необходимо сделать, федералы заявили, что на гаджете может

храниться информация, которая способна помочь выявить других экстремистов и предотвратить возможные теракты.

Однако производитель «айфона» назвал требование ФБР создать механизмы для отключения защиты смартфона нарушением сразу двух поправок Конституции США (особенности прецедентного права).

По мере развития дела Apple против ФБР всплывали разные подробности, которые способны были обеспечить дополнительными доводами как одну сторону конфликта, так и другую. Например, как сообщает агентство Reuters, один неназванный осужденный поведал, почему преступники все более активно переходят на iPhone.

По его словам, представители криминального мира активно используют новые технологии шифрования Apple, поскольку они надежно защищают разговоры и переписку, не позволяя властям взламывать конфиденциальные данные. Однако самое забавное состоит в том, что эти слова, которые сегодня используются как свидетельство в суде, были получены полицией в результате перехвата телефонного разговора преступника.

Настаивая на необходимости создания бэкдора [178] для извлечения необходимых данных из устройств на базе iOS, правоохранительные органы ссылаются на тот факт, что преступники более активно пользуются iPhone вместо привычных «одноразовых» телефонов, которые часто можно увидеть в криминальных боевиках. Вместо того, чтобы покупать дюжину подобных телефонов, злоумышленники просто устанавливают на iPhone зашифрованные мессенджеры и общаются в них.

Нельзя не согласиться с разумностью этих конкретных доводов обвинения, ведь надежное шифрование в плохих руках может стать инструментом для беззакония. Однако с другой стороны, если в плохие руки попадет гипотетический бэкдор для iOS, последствия могут оказаться еще страшней. На данный момент дело закрыто, поскольку спецслужбы нашли другой способ

[178] Бэкдор – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить тайный доступ к данным или удалённому управлению компьютером.

получить доступ к информации на Iphone террориста, однако это не исключает возможности того, что в результате совершения новых преступлений опасный прецедент все же появится.

Таким образом, мы понимаем, что в настоящее время масштаб развития систем передачи и хранения информации впечатляет, однако велик риск утечки конфиденциальной информации, принадлежащей именно гражданским лицам. С особой осторожностью стоит подходить к выбору технического средства, вопервых. А во-вторых, несмотря на все обещания производителя о защите данных, важно фильтровать ту информацию, которую вы планируете передать либо сохранить на своем гаджете.

Список использованной литературы и источников

1. Конституция Российской Федерации. М., 2015.
2. Обзор безопасности iOS, 2015 Apple Inc.- Cupertino.
3. *Кучерена А.* Время спрута. М., 2015.
4. РИА Новости – http://ria.ru.
5. 24СМИ Новости – http://24smi.org.
6. 3Dnews – http://www.3dnews.ru.
7. http://appleinsider.ru.
8. http://www.securitylab.ru.

А.А. Хананова

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **В.Ф. Изотова**, к.ф.-м.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работа органов государственной власти и органов местного самоуправления базируется на большом количестве самой разнообразной информации, которая содержится на бумажных и электронных носителях и требует особого

административно-правового регулирования, а также установления специальных мер юридической ответственности за различные правонарушения в этой сфере.

Информация играет важную роль в жизнедеятельности общества. Как отмечает Н.Н. Лебедева, «...доступная в электронном виде информация может способствовать развитию открытого информационного взаимодействия между государством и общественностью, обеспечению открытости и прозрачности процедур разработки и принятия государственных решений, реализации права граждан на доступ к информации о деятельности органов власти»

Информация может носить как социально полезный характер, так и представлять угрозу безопасности личности общества и государства. Поэтому особую актуальность приобрели проблемы информационной безопасности. Доктрина информационной безопасности определяет, что под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность – это состояние защищенности личности, общества и государства в информационной сфере, которая позволяет обеспечить всех заинтересованных субъектов необходимым объемом социально полезной информацией, также обеспечить права доступа всех заинтересованных субъектов необходимым объемом информации.

Информационная безопасность обеспечивается нормами международного, конституционного и уголовного права. Особое место в системе правовых средств обеспечения информационной безопасности занимают административно-правовые средства. Предписания КоАП РФ занимают важное место в системе административно-правовых средств обеспечения информационной безопасности по целому ряду направлений. В отличие от уголовной ответственности административная ответственность не влечет судимости, отличается меньшей тяжестью наказания и более коротким сроком давности.

Административной ответственности в области связи и информатизации посвящена глава 13 КоАП РФ. Статьи этой главы условно можно разделить на

две группы. Статьи с 13.1 по 13.10 КоАП РФ посвящены регулированию отношений в области технической эксплуатации средств связи. В них определяется ответственность за самовольное проектирование, строительство, подключение к сети, использование не сертифицированных средств, не обеспечение охраны линий связи, предоставление не сертифицированных услуг и т.д. Статьи, начиная со 13.11, предусматривают ответственность за нарушения в сфере сбора, хранения, использования или распространения информации разного вида информации, нарушения правил защиты информации непредоставления первичных статистических данных, хранения, комплектования, учета или использования архивных документов и т.д.

Анализ вышеперечисленных составов позволяет говорить о разнообразии административных правонарушений, объектом посягательства которых является информация. Трудно не согласиться с И.Л. Бачило в том, что «...сложность отнесения некоторых составов к области информационных правонарушений связана с тем, что они являются пограничными и касаются не только информации, но и той области отношений, где информация работает и является предметом отношений».

М.В. Ханцис

Санкт-Петербургский юридический институт (филиал)
ФГКОУ ВО «Академия Генеральной прокуратуры Российской Федерации»

*Научный руководитель: **Л.А. Чернышева**, к.ю.н., доцент кафедры гражданскоправовых дисциплин Санкт-Петербургский юридический институт (филиал)*
ФГКОУ ВО «Академия Генеральной прокуратуры Российской Федерации»

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, РАЗМЕЩЕННЫХ В СЕТИ «ИНТЕРНЕТ»

В современном мире весьма разнообразна работа с персональными данными человека. Стремительно развивающаяся технологическая составляющая нашей жизни увеличивает уязвимость информации, являющейся сведениями о частной жизни человека, в частности в процессе трудовой деятельности.

Конституция Российской Федерации закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну (ст. 23). Сбор,

хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24).[179]

Персональные данные, согласно ст. 3 Федерального Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее ФЗ «О персональных данных»), это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Федеральным законом от 7 мая 2013 г. № 99-ФЗ была признана утратившей силу ст. 85 ТК РФ, в которой законодатель раскрывал понятие «персональных данных работника». Теперь же определение, приведённое в ФЗ «О персональных данных» применимо и к трудовым правоотношениям. Также необходимо учитывать, что конкретного перечня сведений, представляющих собой персональные данные, не приведено ни в ФЗ «О персональных данных», ни в Трудовом Кодексе Российской Федерации.

Поэтому на практике к таким данным относят все те сведения, основываясь на которые можно идентифицировать работника[180] (например, ФИО; дата и место рождения; адрес (место регистрации) и т.д.). Указанная информация чаще всего содержится в таких документах, как анкета, автобиография, личная карточка, трудовая книжка, копия документа, удостоверяющего личность работника и т.д.

Одна из актуальных проблем работы с персональными данными работника состоит в том, из каких источников получается такая информация, как и для каких целей используются сведения о сотруднике со стороны работодателя и третьих лиц.

Как уже отмечалось ранее, в настоящее время активно распространяются технологические новшества, к которым можно отнести социальные сети. Сложно представить себе человека, который не слышал никогда про Facebook, Вконтакте, Одноклассники и прочие Интернет-сервисы. В связи с широким распространением такого вида общения, в Сети публикуются различные

---

[179] *Паламарчук А.В.* Надзор за исполнением законодательства о персональных данных в сети Интернет // Законность. 2010. № 12. С. 3–5.

[180] *Сергеева А.* Персональные данные работника // Учреждения физической культуры и спорта: бухгалтерский учет и налогообложение. 2015. № 6. Доступ из справ.-правовой системы «КонсультантПлюс».

подробности о частной жизни людей, которыми, как представляется, не все хотели бы делиться со своим работодателем.

Известны случаи, когда работодатели «мониторят» личные страницы в социальных сетях, как своих настоящих сотрудников, так и кандидатов на вакантные должности. Согласно опросам, у 43% американских работодателей ухудшилось мнение о кандидате, 19% работодателей заявили об изменении в лучшую сторону мнения о потенциальном сотруднике [181]. Но такой опрос демонстрирует положение дел за рубежом. А как дела обстоят на Российском рынке труда? Большинство работодателей признаются, что просматривали страницы соискателей, но, чаще всего, размещённая там информация не отражает профессиональных навыков кандидатов на должность. Некоторые из работодателей признают такой метод сбора данных неэтичным и неэффективным[182].

Определяя законность таких действий работодателя, следует учитывать, что согласно ч. 3 ст. 86 Трудового Кодекса РФ, все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие, также работодателем должно быть сообщено для каких целей осуществляется сбор информации и из каких источников планируется получение сведений.

С другой стороны, не будет ли аргументом в пользу работодателя тот факт, что работник/соискатель разместил свои персональные данные (фамилию, имя, отчество, фотографию и т.п.) в сети Интернет, так называемом общедоступном источнике? Законодателем установлено в ч. 1 ст. 8 ФЗ «О персональных данных», что в общедоступные источники персональные данные могут попадать исключительно с письменного согласия субъекта таких персональных данных. Как все понимают, получить такое письменное согласие в рамках Интернета

---

[181] *Авшалумова Р.* Facebook вредит карьере // Ведомости. 2014. 15 мая. № 3589. URL: https://www.vedomosti.ru/newspaper/articles/2014/05/15/facebook-vredit-karere (дата обращения: 31.03.2016).

[182] *Авшалумова Р.* Facebook вредит карьере // Ведомости. 2014. 15 мая. № 3589. URL: https://www.vedomosti.ru/newspaper/articles/2014/05/15/facebook-vredit-karere (дата обращения: 31.03.2016).

невозможно. Соответственно, признание опубликованных на личной странице в Интернете данных человека общедоступными не соответствует букве закона.

Исходя из выше сказанного, работодатель, планирующий проверять публикации кандидата на должность в Интернете, обязан предупредить о такой проверке и получить письменное согласие на обработку персональных данных (ч. 1 ст. 24 Конституции РФ, п. 8 ст. 86 ТК РФ, п. 1 ч. 1 ст. 6, ч. 1 ст. 9 ФЗ «О персональных данных»).

Вместе с тем, широко известны случаи увольнения сотрудников, опубликовавших записи, вызвавшие широкий общественный резонанс. Например, увольнение стюардессы авиакомпании «Аэрофлот», опубликовавшей в одном из своих аккаунтов в социальной сети, издевательскую запись о крушении самолёта в Индонезии в мае 2012 года. Или увольнение другой бортпроводницы. Девушка выложила в Интернет фотографию, на которой жестами «демонстрировала» свое отношение к клиентам авиакомпании, находившимся в тот момент на борту самолёта. Если не рассматривать ситуацию с морально-этической стороны, а с правовой точки зрения, то законных оснований для увольнения за публикации в Интернете не предусмотрено. Однако многие компании используют в качестве «основания» для расторжения трудового договора с «провинившимся» сотрудником соглашение сторон, предусмотренное п. 1 ст. 77 ТК РФ, как было в приведенных случаях.

С государственными служащими дело обстоит несколько иначе. Например, увольнение федерального судьи Улан-Удэ за выложенные в социальную сеть фотографии, на которых женщина была запечатлена «в обнимку» с бутылками спиртных напитков. Комиссией по этике такое поведение было признано как несоблюдение профессиональной этики, в связи с чем и был расторгнут трудовой договор с судьей. Увольнение замминистра экономического развития было связано с его публикациями, критикующими политику государственных органов в сфере пенсионных накоплений, в личном профайле в Интернете. Такими действиями чиновник нарушил запрет на публичные высказывания в адрес

деятельности госорганов, предусмотренный законом «О государственной гражданской службе РФ».

За рубежом также происходят увольнения за публикации в социальных сетях. Например, в одной немецкой компании был уволен сотрудник за снимок, на котором этот работник нёс свою супругу на руках. Руководству компании не понравился тот факт, что этот молодой человек уже несколько месяцев «находился на больничном» с диагнозом межпозвонковая грыжа. Правда, сотрудник обжаловал действия работодателя в суде, который обязал компанию выплатить уволенному работнику выходное пособие. Однако не всегда суд встает на сторону работника. Британским судом по трудовым спорам было признано законным увольнение работника одного из магазинов Apple. В корпоративных правилах прописано, что сотрудники не имеют права высказывать своё отрицательное отношение к компании и производимой продукции. Данное правило и было нарушено опубликованием в социальной сети негативного отзыва о компании.

На данный момент очень проблематично проследить тенденции судебных решений по вопросу законности увольнения за активность в социальных сетях не только в России, но и за границей.

По мнению М.С. Журавлева, проблемы контроля работодателя за работником и границы частной и «рабочей» жизни сотрудника следует решать путем «поиска баланса двух групп интересов и легального закрепления границ вмешательства работодателя в частную жизнь своих сотрудников», «выработки определённых принципов взаимодействия работодателя и работников при осуществлении производственного контроля за последним»[183].

Подводя итог сказанному, следует отметить, что:

во-первых, при обработке персональных данных работников или соискателей работодатель в первую очередь должен заручиться письменным, однозначным, осознанным разрешением работников – субъектов персональных

[183] *Журавлев М.С.* Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2013. № 4. С. 35-38.

данных; во-вторых, следует законодательно закрепить перечень сведений, составляющий персональные данные работника. Также, на взгляд авторов, следует восстановить ст. 85 Трудового Кодекса Российской Федерации, с легальным определением персональных данных работника.

в-третьих, мониторинг аккаунтов в социальных сетях не представляет законных оснований для работодателя в вопросах увольнения работника или отказа в приеме на работу соискателя.

Т.В. Чеботарева

ФГБОУ ВО «Саратовская государственная юридическая академия» *Научный руководитель: **А.Е. Федюнин**, д.ю.н., профессор кафедры уголовного процесса ФГБОУ ВО «Саратовская государственная юридическая академия»*

ИНТЕРНЕТ БЕЗОПАСНОСТЬ НЕСОВЕРШЕННОЛЕТНИХ: МИФ ИЛИ РЕАЛЬНОСТЬ

В Интернете несовершеннолетних подстерегает много опасностей. Находясь в виртуальном пространстве, дети неизбежно сталкиваются с целым комплексом киберугроз, среди которых можно отметить вредоносное программное обеспечение, интернет-мошенничество, оскорбление и преследование (кибербулинг), контакты с нежелательными людьми, угроза со стороны интернет – хулиганов, ловушки, расставляемые мошенниками для получения частной информации, нежелательные для просмотра или использования материалы и другие. Но, конечно же, наиболее опасной среди них по своим социальным последствиям, выступает угроза для ребенка стать жертвой преступления против половой неприкосновенности.

В интерактивном мире дети могут быть также беззащитны, как и в реальном. Необходимо сделать все возможное, чтобы несовершеннолетние могли пользоваться телекоммуникационными сетями в безопасном для их физического и психического развития режиме.

К сожалению, за последние годы количество преступлений против половой неприкосновенности несовершеннолетних возросло. И это проблема не только России, но и всех стран мира в целом. Преступления такого рода имеют высокий уровень латентности, это обусловлено тем, что рассматриваемая группа

преступлений затрагивает интересы семьи, интимной жизни человека. Зачастую сами родители детей, потерпевших от сексуальных посягательств, не обращаются с заявлениями в правоохранительные органы, так как боятся «позорящей огласки». Следует учитывать и беззащитность малолетних потерпевших по рассматриваемой категории преступлений, их запуганность.

Преступления против половой неприкосновенности несовершеннолетних, совершаемые с использованием телекоммуникационных технологий, представляют собой серьезную опасность. Сеть Интернет становится все более востребованной и популярной среди детей и подростков. Растет количество времени, проводимого несовершеннолетними в Сети, увеличивается интенсивность ее использования. Нахождение в онлайн становится вполне привычным, обыденным способом существования, легко сочетающимся с традиционной офлайн реальностью. Согласно данным исследования «Дети России онлайн», проведенного Фондом развития Интернет и факультетом психологии МГУ имени М.В. Ломоносова в 2010 г. в 11 регионах России, средний возраст начала пользования сетью Интернет составляет 10 лет, а в Москве и Санкт-Петербурге – 9 лет.[184] Практически 70 % российских детей выходят в Интернет каждый день или почти каждый день. Четверть опрошенных российских детей проводит в Интернете от 7 до 14 часов в неделю, каждый шестой - от 14 до 21 часа. Каждый пятый ребенок проводит в Интернете больше 21 часа в неделю, то есть больше 3 часов в день. Одно из наиболее востребованных направлений использования Интернета – это социальные сети, которые дают возможность детям общаться и обмениваться информацией со своими друзьями.

В нашей стране более 75 % детей имеют профиль в социальных сетях, при этом почти треть имеет больше одного профиля в разных сетях. Лидером популярности среди сетей является сеть «ВКонтакте» – 89 %, далее следуют

---

[184] *Смирнов А.А.* Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет // Актуальные вопросы публичного права. 2012. № 11. URL: http://kizilov-inc.ru/sites/default/files/gm_articles/viktim_0.pdf (дата обращения: 06.11.2015).

Одноклассники – 16 %, Facebook – 4 %, My space – 2 % и другие социальные сети. Почти каждый пятый (19 %) российский ребенок имеет более 100 друзей в социальных сетях.

В зарубежных странах для обозначения действий совершеннолетнего лица, направленных на установление в Интернете доверительного контакта с ребенком с целью склонить его к вступлению в сексуальную связь, используется термин «кибергруминг» или «онлайн груминг» (cybergrooming / onlinegrooming). Им охватываются как действия, преследующие цель получения педофилом сексуального удовлетворения, так и действия, направленные на вовлечение ребенка в коммерческую сексуальную эксплуатацию. На одном из тематических российских сайтов по интернетбезопасности «Дети онлайн» в разделе «коммуникационные риски» описан типичный механизм груминга: «Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече»[185]. Кибергруминг согласно европейским стандартам рассматривается как уголовное преступление.

В Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г. в разделе материальное уголовное право включен специальный состав преступления ст. 23 «Приставание к детям с сексуальными целями» (Solicitation of children for sexual purposes). В российском уголовном законодательстве подобный состав преступления отсутствует, а описанные действия (кибергруминг) могут быть квалифицированы как приготовление к совершению преступлений, предусмотренных ст. 131-135 УК РФ, а также ст. 127.1, 240, 242.2 УК РФ.

[185] Коммуникационные риски // Линия помощи «Дети онлайн». URL: http://detionline.com/helpline/risks (дата обращения: 06.11.2015).

Анализ российской уголовной статистики показывает высокий рост числа преступлений против половой неприкосновенности несовершеннолетних. За последние годы в России значительно увеличилось число преступлений, связанных со сбытом материалов с порнографическими изображениями несовершеннолетних. По данным МВД России, количество сайтов с детской порнографией увеличилось почти на треть, а количество интернет материалов с детской порнографией увеличилось в 25 раз.[186]

Однако, установить долю указанных преступлений, совершаемых с использованием Интернета, в настоящее время невозможно, так как статистикой они из общего массива зарегистрированных преступлений не выделяются. Рассматриваемая категория преступности в силу ее относительной новизны является недостаточно изученной. Российское уголовное и уголовнопроцессуальное законодательство значительно отстает от мировых тенденций в борьбе с преступлениями против половой неприкосновенности несовершеннолетних, совершаемых через сеть Интернет, как в законодательном, так и в практическом отношении.

В век информационных технологий зачастую при расследовании преступлений против половой неприкосновенности малолетних не обойтись без использования специальных знаний и техник в сфере телекоммуникационных систем. Например, при расследовании преступлений, связанных с изготовлением и распространением детской порнографии необходимо применение специальных знаний в сфере компьютерных систем и информационных технологий. Рассматриваемая категория преступлений, имеет множество уголовно-процессуальных особенностей от момента первоначальной проверки сообщения о преступлении вплоть до направления уголовного дела в суд. Во-первых, потому что речь идет о несовершеннолетних потерпевших, во-вторых, при расследовании посягательств на несовершеннолетних через Интернет правоохранительные органы сталкиваются с относительно новым для нашей

[186] Госдума ратифицировала международные договоры о защите детей // ИА РИА-новости. URL: https://ria.ru/politics/20130426/934746783.html (дата обращения: 05.11.2015).

страны видом кибер преступлений. Доказывание по данной категории преступлений порой бывает весьма затруднительно, в случае если нет очевидных фактов и бесспорных доказательств вины подозреваемого, а такими могут быть показания самого потерпевшего, очевидцев и свидетелей, разного рода вещественные доказательства.

Выявление преступлений данной категории составляет особую сложность. После исследования правоохранительными органами Интернет-материалов (фотографии, видео) порнографического содержания с участием несовершеннолетних, становится очевидно, что налицо преступление против половой неприкосновенности несовершеннолетних. Однако практически невозможно установить ни сведения о потерпевших лицах и преступниках, ни место совершения преступления. Эти обстоятельства служат серьезным препятствием для выявления таких преступлений, для постановки их на учет и уголовного преследования виновных[211].

Важнейшее значение в выявлении неочевидных преступлений против половой неприкосновенности несовершеннолетних, когда нет явного насилия, имеют результаты оперативно-розыскной деятельности. Одним из самых эффективных оперативно-розыскных мероприятий является оперативное внедрение, когда оперативный сотрудник, например, устраивается на работу в организацию, где было совершено насилие над ребенком. Для выявления преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет, лицо, проводящее оперативнорозыскные мероприятия, может зарегистрироваться в социальных сетях под видом малолетнего для знакомства с потенциальным педофилом.

На стадии возбуждения уголовного дела возникают серьезные проблемы, связанные с квалификацией совершенного преступления, с организацией и производством первоначальных следственных действий, собиранием, проверкой и оценкой доказательств, вследствие недопонимания схем организации преступления и знания, какую именно значимую для уголовного дела информацию можно получить.

Интернет лидирует в «сексуальном просвещении» подрастающего поколения. К сожалению, далеко не все родители достаточно осведомлены о существующих рисках в Интернете и способах защиты от них и зачастую недооценивают проблему. В силу существующего «цифрового разрыва» между родителями и детьми, детский мир Интернета не только мало знаком взрослым, но еще нередко и недоступен им. Практически невозможно обычными

[211] *Трунова Е.В.* Проблемы выявления и учета преступлений против половой неприкосновенности несовершеннолетних // Молодежный научный форум: Гуманитарные науки: электр. сб. ст. по материалам XIII студ. междунар. заочной науч.-практ. конф. 2014. № 6. URL: http://nauchforum.ru/node/3762 (дата обращения: 06.11.2015).

средствами оградить ребенка от посещения нежелательных сайтов (а сайтов, «охотящихся» за детьми, в сети достаточно). Но есть ряд обязательных правил поведения в Интернет, которые нужно напоминать ребенку постоянно. Для этого необходимо повсеместное просвещение несовершеннолетних и их родителей о правилах безопасного пользования телекоммуникационными сетями посредством СМИ, печатных изданий, тематических уроков в учебных заведениях. Также необходимы слаженные профессиональные действия правоохранительных органов в своевременном выявлении, расследовании, а главное, предупреждении подобных преступлений.

Список использованной литературы и источников

1. *Смирнов А.А.* Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет // Актуальные вопросы публичного права. 2012. № 11. URL: http://kizilov-inc.ru/sites/default/files/gm_articles/viktim_0.pdf.

2. Коммуникационные риски // Линия помощи «Дети онлайн». URL: http://detionline.com/helpline/risks.

3. Госдума ратифицировала международные договоры о защите детей // ИА РИА-новости. URL: https://ria.ru/politics/20130426/934746783.html.

4. *Трунова Е.В.* Проблемы выявления и учета преступлений против половой неприкосновенности несовершеннолетних // Молодежный научный

форум: Гуманитарные науки: электр. сб. ст. по материалам XIII студ. междунар. заочной науч.-практ. конф. 2014. № 6. URL: http://nauchforum.ru/node/3762.

С.С. Челноков

ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал

*Научный руководитель: **А.И. Быба**, ведущий специалист отдела по обеспечению работы высшей школы государственного управления, руководитель областной Правовой школы по профилактике экстремизма среди молодежи Владимирской области, преподаватель кафедры правового обеспечения государственного и муниципального управления ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» Владимирский филиал*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭКСТРЕМИСТСКИМИ ГРУППИРОВКАМИ

Приход террористов в Сеть или, как некоторые называют, «миграция», произошла около пятнадцати лет назад, когда сам Интернет еще не предусматривал высоких скоростей и таких широких возможностей. Уже с 11 сентября 2001 года терроризм перерастает в глобальную проблему человечества, становится ясно, что использование новых технологий ведет к более изощренным актам насилия, исходящим от преступных группировок. Становится возможным планировать атаки более тщательно, используя картографические сервисы и возможности анонимизации онлайн.

Экстремизм и терроризм сегодня вполне можно рассматривать в контексте общемировых политических реалий, непосредственно влияющих на осуществление мировой политики.

Целями деятельности террористов в сети Интернет являются: реклама своей деятельности, пропаганда террористической идеологии, запугивание и дезинформация, вербовка в террористические организации, поддержка взаимодействия внутри террористической организации и противодействие пропаганде противника.

Интернет сегодня – это универсальное средство общения и обмена информацией между людьми, находящимися в любой точке планеты,

несомненными преимуществами которого являются возможность широкого охвата аудитории; высокая скорость и лавинообразный характер распространения информации; возможность для анонимного ведения противоправной деятельности. Однако последнее десятилетие отмечено такой угрозообразующей тенденцией, как ориентация террористических организаций на Интернет-пространство, где уже сегодня насчитывается до 10 тысяч экстремистских электронных площадок, свыше 500 из которых – русскоязычные.

Таким образом, за последние десять лет террористические организации прочно обосновались во всех сегментах Интернета и социальных сетей и используют его в качестве основного инструмента по распространению своих идей.

Основной контингент интернет-пользователей – это представители молодежной среды. Молодые люди – активные пользователи глобальной сети, получающие львиную долю информации именно из интернет-пространства. Интернет окружает их повсюду: выйти в глобальную сеть можно при помощи различных гаджетов и устройств. Важным фактором в данном случае является тот факт, что мировоззрение молодых людей находится еще на стадии становления и развития. Поэтому Интернет, с его спектром мнений и взглядов, распространенностью идей разного смысла и содержания, может представлять реальную опасность. Данное суждение верно в отношении тех порталов и интернет-источников, которые созданы для распространения идей терроризма и религиозно – политического экстремизма.

С учетом этой роли сейчас можно выделить несколько основных направлений деятельности террористов в сети Интернет:

1) привлечение (вербовка, поиск) новых исполнителей терактов;
2) пропаганда террористической деятельности;
3) финансирование деятельности;
4) тренировка членов террористических группировок;
5) планирование террористических актов;
6) координация и исполнение террористических актов; 7) кибератаки.

Почему экстремизм все больше переходит к использованию информационно-телекоммуникационного прогресса? Факторов, обуславливающих данную тенденцию, несколько:

–глобальная информатизация всех сфер жизни общества понижаетстепень его безопасности;

–ускорение научно-технического прогресса увеличивает вероятностьприменения террористами в качестве средств поражения сугубо мирных технологий;

–терроризм все более становится информационной технологией особоготипа, т.к. террористы все шире используют возможности современных ИТсистем для связи и сбора информации; реалией наших дней становится так называемый «кибертерроризм»; большинство террористических актов сейчас рассчитаны не только на нанесение материального ущерба и угрозу жизни и здоровью людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей;

–«цифровое неравенство» и появление «проигравших» информационнуюгонку стран могут послужить причиной террористической активности против отдельных государств как средство асимметричного ответа.

Сейчас глобальная сеть Интернет все больше привлекает внимание террористов и не беспочвенно. Интернет обладает рядом особенностей, которые подталкивают к его многогранному использованию:

–легкость доступа;

–слабая цензура или полное отсутствие ее и какого-либоправительственного контроля;

–наличие огромной потенциальной аудитории пользователей,разбросанной по всему миру;

–анонимность связи;

–быстрое и относительно дешевое распространение информации.

Террористические организации безнаказанно используют Интернет, ведь сложно обнаружить и ликвидировать сетевые центры (серверы, домены, вебсайты). К тому же регистрировать доменные имена сайта можно в одной стране, а размещать информацию в другой. Различия в национальных законодательствах вызывают дополнительные сложности в борьбе с распространением материалов информационно-психологического воздействия через Интернет.

Экстремисты активно эксплуатируют возможности Интернета, как упоминалось выше, из-за легкого доступа, незначительных масштабов госрегулирования и цензуры или их полного отсутствия, потенциально огромных масштабов аудитории, анонимности, быстрой передачи информации, мультимедийности среды, позволяющей комбинировать различные типы информации - текстовую, графическую, аудиовизуальную. С помощью Интернета они могут «управлять восприятием» - то есть позиционировать себя точно такими, какими хотят казаться, без фильтров, налагаемых традиционными СМИ, а также создавать определенное волнение относительно нужных событий.

Методы информационного воздействия, которыми пользуются вербовщики и распространители противоправных идей, не новы. Это старые и хорошо известные средства подтасовки фактов, игры на необразованности или незнании определенных вещей, манипулирование тенденциозно подобранными новостями и яркая риторика. Эти методы идеально работают и в обычной жизни – вспомните, как легко «заводится» толпа на митингах, как просто вбрасывается любая, самая бредовая идея и, как в виде слухов, она начинает распространяться на любые расстояния, по пути обрастая фантастическими подробностями и домыслами.

Соцсети и блогосфера – это та же уличная толпа, только охват существенно больше и скорость распространения на порядки выше, а учитывая привычку большинства пользователей, увидев яркий, броский заголовок нажимать на кнопку «репост», «ретвит», или «поделиться» – можно сказать, что процесс распространения слухов превращается в неконтролируемое цунами.

Интернет может использоваться террористическими организациями и в качестве альтернативной площадки для подготовки своих членов. Сеть дает безграничные возможности для создания и распространения мультимедиа, содержащего информацию для обучения членов террористических группировок: детальные планы, инструкции, видеоролики и т.д. Наиболее ярким примером является онлайн-журнал Inspire, который, как сообщается, издается террористической организацией «Аль-Каида», в котором публиковались практические инструкции, как подготовить автомобиль для совершения террористического акта или как собрать бомбу в домашних условиях. Еще одним ярким примером может служить история теракта на Бостонском марафоне. Судя по опубликованным показаниям Царнаева, информацию по изготовлению СВУ он черпал из Интернета.

Удобство поиска и получения информации в Сети является важным фактором, определяющим следующее направление деятельности террористов в Интернете – планирование террористических актов. В Интернете возможно найти карты, фотоснимки местности со спутника (GoogleEarth) или фотоснимки (панорамы Google или Яндекс), записи или трансляции с камер видеонаблюдения, планы зданий и сооружений. В эпоху развития социальных сетей, блогосферы, сетевых информационных агентств у террористов также появляется возможность получать самые актуальные новостные сводки, фото и видеоматериалы. Социальные сети и сетевые программы, обеспечивающие функцию мгновенного обмена сообщениями или звонками, используются для координации действий бандгрупп, а надежная защита от дешифровки сообщений в подобных программах, отсутствие технических возможностей для полного анализа трафика усложняют обнаружение и идентификацию террористов или предотвращение террористических актов.

Отдельная история – кибератаки, служащие, в основном, для нарушения работы компьютерных сетей организаций. За последние годы появилось несколько достаточно известных экстремистских организаций, занятых именно кибертерроризмом, и имаратовская «Хакер Анонимус» тому яркий пример.

Таким образом, следует констатировать, что за последние десять лет экстремистские и террористические организации прочно обосновались во всех сегментах Интернета и используют его в качестве основного инструмента по распространению радикальной исламской идеологии. По прогнозам экспертов, исламисты будут и дальше развивать свое присутствие в сети Интернет.

Недооценивать данный ресурс нельзя. Нельзя и бороться с ним посредством простого запрета. Нужна детально проработанная государственная политика, которая могла бы адекватно реагировать на поведение граждан в сети, в том числе и социальных сетях. Мир, безусловно, изменился. Огромное число террористов и экстремистов ведут свою работу в социальных сетях. От того, насколько эффективно и успешно с ними будут бороться в том же Вконтакте, в котором иногда достаточно удачно подобранных несколько символов для вспыхивания общественных волнений и беспорядков, зависит в целом благополучие и спокойное гармоничное существование общества и государства. Как показывает нынешний опыт, путем простого запрета проблему не решишь, только усугубишь. Значит, нужны более действенные и изощренные методы борьбы.

В соответствии с Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», в ст. 5 Профилактика экстремистской деятельности говорится о том, что в целях противодействия экстремистской деятельности федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в пределах своей компетенции в приоритетном порядке осуществляют профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской деятельности[187]. Следовательно, в связи с обстановкой, на сегодняшний день особенно важна и необходима профилактическая работа, направленная на предупреждение экстремистской деятельности среди молодежи. Во

[187] Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности». Доступ из справ.-правовой системы «КонсультантПлюс».

Владимирской области уже седьмой год действует Правовая школа по профилактике экстремизма, целью которой является правовое просвещение и профилактика асоциальных явлений в молодежной среде. Я являюсь консультантом этого молодежного объединения. Сейчас, когда особенно остро стоит проблема вербовки молодых людей через сеть Интернет, в том числе через социальные сети, Правовая школа много работает в этом направлении: проводит родительские конференции, семинары, тренинги, круглые столы для молодежи. Мной разработана тема: «Основные пути и методы распространения идеологии терроризма через Интернет. Использование социальных сетей и блогосферы экстремистскими группировками».

Проблема на сегодняшний день актуальна среди молодежи. Как видно из всего вышеперечисленного, вариантов использования Интернета в противоправных целях – хватает, и недооценивать его возможности, по меньшей мере, недальновидно.

К.А. Чумак, М.М. Сергеев
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»
*Научный руководитель: **Е.О. Шамраева**, к.т.н., доцент информационных систем ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»*

МЕТОДЫ ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ ОТПЕЧАТКОВ ПАЛЬЦЕВ

Цифровая обработка изображений – область деятельности, в которой компьютеры используются в качестве инструмента создания и обработки изображений различного назначения: фотографий реальных объектов, изображений медицинского назначения, спутниковых снимков и т.д.

В современной жизни человек часто сталкивается с цифровыми методами обработки изображений. Например, для получения загранпаспорта необходимо пройти процедуры сканирования отпечатков пальцев, модификации фотографии путем нанесений цифрового трехтонового водяного знака. Органы местного самоуправления давно используют данную технологию, для выявления улик с места преступления путем сканирования отпечатков пальцев. Однако не всегда отпечаток получается четким и без изъянов. Дефекты снимков отпечатков пальцев можно устранить различными методами цифровой обработки изображений.

На изображении отпечатка пальца обычно выделяют признаки, такие как завитки, петли, дельты необходимые для идентификации. Однако на необработанном изображении из-за различных помех: грязь, складки, порезы, «смазанность» отпечатка папиллярные линии могут искажаться, что способствует ошибкам в распознавании признаков. Для устранения подобных ошибок изображение улучшают. При этом уменьшается зашумленность изображений, а модель, рассчитываемая по нему, становится более достоверной.

Интерес к методам цифровой обработки изображений исходит из двух основных областей ее применения, которыми являются повышение качества изображения для улучшения его визуального восприятия человеком и обработка

изображений для их хранения, передачи и представления в автономных системах машинного зрения.

Исходными данными для курсовой работы являются растровые изображения отпечатков пальцев. Растровое изображение представляет из себя мозаику из очень мелких элементов – пикселей. Растровый рисунок похож на лист клетчатой бумаги, на котором каждая клетка закрашена определенным цветом, и в результате такой раскраски формируется изображение. Растровая графика позволяет создать (воспроизвести) практически любое изображение, вне зависимости от сложности. Растровое представление изображения является лучшим для большинства устройств ввода-вывода графической информации, таких как мониторы, сканеры др.

Улучшение изображений входит в число наиболее распространенных методов обработки изображения. В основе реализации лежит идея выявления плохо различимых деталей или просто подчеркивание интересующих характеристик на исходном изображении. Восстановление изображения – область, также связанная с повышением визуального качества изображения. В отличие от улучшения, восстановление является объективным в том смысле, что методы восстановления опираются на математические или вероятностные.

При снятии отпечатков они не всегда получаются четким и без изъянов. Дефекты снимков отпечатков пальцев можно устранить различными методами цифровой обработки изображений. На изображении отпечатка пальца (рис.1) обычно выделяют признаки, такие как завитки, петли, дельты необходимые для идентификации. Однако распознавание признаков может быть затруднено из-за различных помех на изображении: зашумленный фон, разрывы папиллярных линий отпечатков, отдельные точки на изображении, которые являются лишними, «смазанность» отпечатка. Для устранения подобных дефектов изображение улучшают. При этом уменьшается зашумленность изображений, а модель, рассчитываемая по нему, становится более достоверной.

К изображению отпечатка пальца следует применить методы повышения качества изображений с целью четкого выделения папиллярных линий. Для

устранения проблемных участков исходных изображений были выбраны такие методы обработки изображений, как пороговое преобразование и морфологическая фильтрация.

а

б

Рисунок 1. Исходные изображения отпечатков пальцев

В общем случае пороговое преобразование рассматривается как операция, при которой производится сравнение с функцией ***T***, имеющей вид :

,

где *f* – некоторое изображение, содержащее светлые объекты на темное фоне или наоборот, *p(x,y)* – некоторая локальная характеристика точки *(x,y)* изображения.

Изображение *g(x,y),* получаемое в результате порогового преобразования, строится следующим образом:

В работе используется пороговая обработка с одним порогом (т.н. порог бинаризации), который определяется по гистограмме яркости изображения (рис.2, а,б). Результат применения порогового фильтра к изображениям отпечатков пальцев приведен на рис.3, а,б.

а б

Рисунок 2. Гистограмма яркости изображения: а) представленного на рис.1,а; б) представленного на рис.1,б

Изображения папиллярных линий стали более четкими, исчез серый фон, однако разрывы в папиллярных линиях и отдельные шумовые точки на изображении остались.

а

б

Рисунок 3 – Пороговая обработка: а) применение пороговой обработки к изображению на рис.1,а со значением порога бинаризации 84; б) применение пороговой обработки к изображению на рис.1,б со значением порога бинаризации 151

Они устраняются с помощью морфологических операций дилатации:

где A – исходное изображение; – центральное отражение, ; B – примитив; и эрозии:

.

Последовательное применение операций дилатации и эрозии к изображению отпечатков пальцев (рис.4) устраняет мелкие разрывы и удаляет отдельные точки.

Анализируя результаты обработки изображений отпечатков пальцев, можно сделать вывод, что данные методы хорошо подходят для обработки таких изображений, устраняют основные дефекты и недостатки.

а

б

Рисунок 4 – Применение морфологической фильтрации к изображениям отпечатков пальцев, представленных на: а) рис. 2,в; б) рис. 2,г

Список использованной литературы и источников

1. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений / пер. с англ. П.А. Чочиа П.А. М.: Техносфера, 2006.

2. *Грузман И.С., Киричук В.С. и др.* Цифровая обработка изображений в информационных системах / И.С. Грузман, В.С. Киричук, В.П. Косых, Г.И. Перетягин, А.А. Спектор. Новосибирск: Изд-во НГТУ, 2002.

Ю.С. Шайманова

ФГБОУ ВО «Саратовская государственная юридическая академия»

*Научный руководитель: **Е.В. Варламова**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА В ИЗБИРАТЕЛЬНЫХ КАМПАНИЯХ

Сегодня Интернет – это всемирная компьютерная сеть, подобная мировому океану информации, доступна каждому человеку на нашей планете. Благодаря мгновенному соединению и высокой скорости передачи данных, информацию в Интернете получить легко и просто.

В качестве примера использования сети Интернет в ходе выборов можно привести Соединенные Штаты Америки. Глобальная компьютерная сеть использовалась уже в ходе выборов 1996 года, когда кандидату, чтобы показать хороший результат, достаточно было просто разместить на веб-сайте электронную версию своей предвыборной программы.

В 2000 году команды обоих претендентов на пост американского президента стали использовать Интернет еще более продуктивно в целях сбора пожертвований на избирательную кампанию и привлечения в свои ряды новых сторонников. По словам «Нью-Йорк Тайм», электронные странички превратились в новое средство, с помощью которого кандидаты могли доносить свои идеи до широкой аудитории, которую им никогда не удавалось собирать в ходе традиционных предвыборных поездок по стране.

Первым опытом политического PRa в РУНЕТе в нашей стране, в России, можно считать трансляцию хода выборов 1996 г. на сайте «Национальной службы новостей», где впервые были опубликованы результаты президентских выборов во время подсчета голосов. С этого момента к возможностям Интернета активно обращаются политические партии, движения и их лидеры.

Проанализировав положительные стороны работы Интернета, можно выделить основные аспекты, делающие его одним из эффективных каналов распространения политической рекламы определенного кандидата.

Во-первых, он работает круглосуточно.

Во-вторых, Интернет обеспечивает возможность прямой и косвенной агитации за кандидата.

В-третьих, в сети содержание информации о кандидате может изменяться в зависимости от необходимости. Никакая иная реклама подобной гибкости в предоставлении информации не несет.

В-четвертых, в Интернете могут быть использованы цветные изображения, качественные видеофрагменты и звуковое оформление, что позволяет получить более информативное представление о кандидате.

Основная задача стратегического планирования в отношении использования Интернета в ходе избирательной кампании, состоит в повышении привлекательности электронных страничек и их непосредственной рекламы.

Влияние политических рекламных средств на массовое сознание и массовое поведение граждан является достаточно распространенным явлением.

Для любых партий, объединений, фондов, движений и даже отдельных политиков. Глобальная паутина оказалась великолепной находкой, которая помогает возвестить «городу и миру» о своих позициях, программах, доводить до сведения всех и вся об успехах своих организаций.

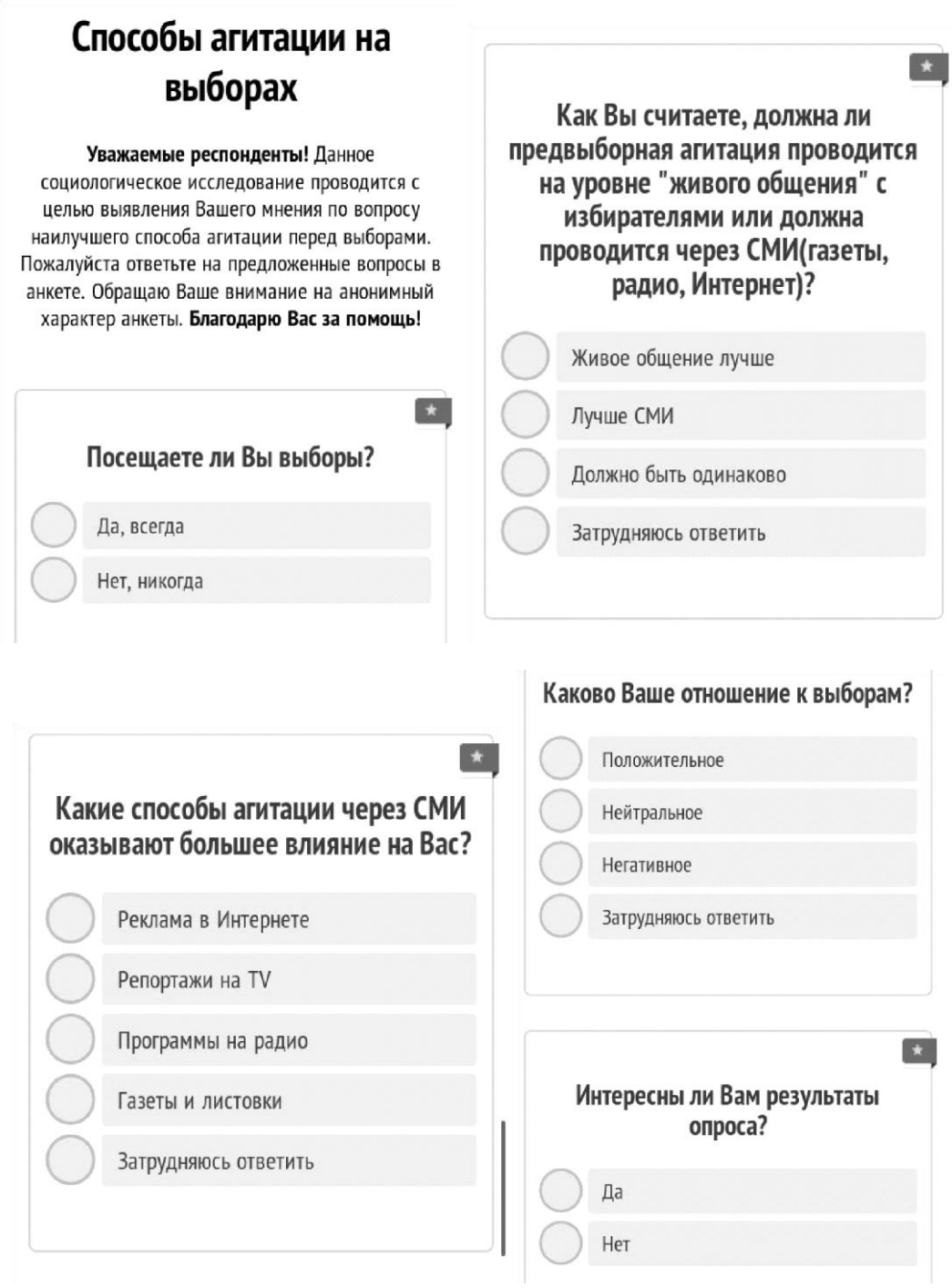
Действительно, СМИ являют действенной системой органов публичной передачи информации. Но что именно эффективно может повлиять на сознание граждан в ходе предвыборной агитации?

Чтобы ответить на этот вопрос, мной был проведен социологический опрос «Способы агитации на выборах».

Целью данного социологического опроса является выявление наиболее эффективной формы СМИ, влияющей на сознание граждан.

Количество респондентов составило 27 человек разного возраста и пола. Опрос был проведен через онлайн программу Survio.

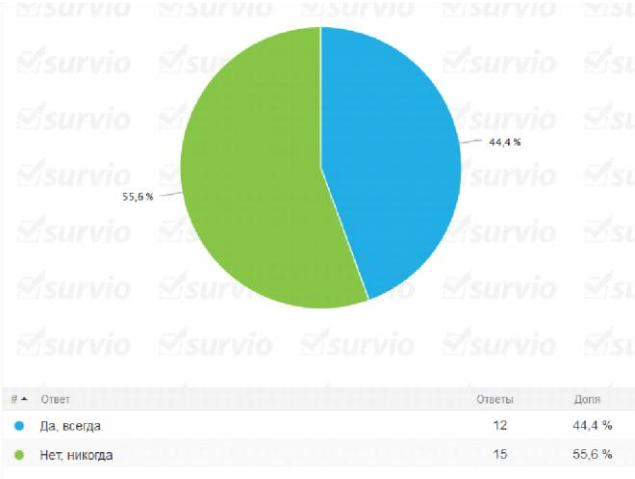
Анкета предоставлялась респондентам в следующем виде.



На первый вопрос - Посещаете ли Вы выборы?

«Положительно» ответило 12 человек, что составило 44%.

И «отрицательно» ответило 15 человек (56%).



#	Ответ	Ответы	Доля
1	Да, всегда	12	44,4 %
2	Нет, никогда	15	55,6 %

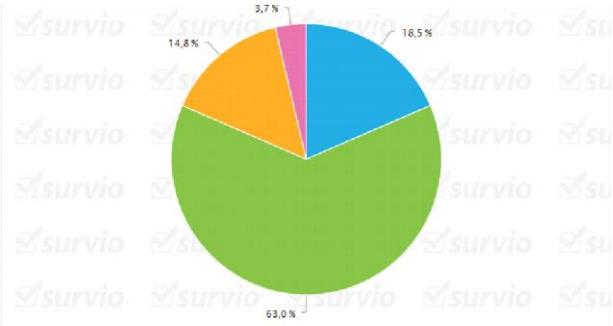
Во втором вопросе я узнала мнения о том, должна ли предвыборная агитация проводится на уровне "живого общения" с избирателями или должна проводится через СМИ (газеты, радио, Интернет).

Большинство опрошенных, а именно 17 человек (63%), ответило, что «лучше СМИ», чем живое общение.

«Живое общение лучше ответило» 18 человек (18,5%).

«Должно быть одинаково» - 4 (14,8%).

Вариант «Затрудняюсь ответить» выбрал 1 человек (3,7%).



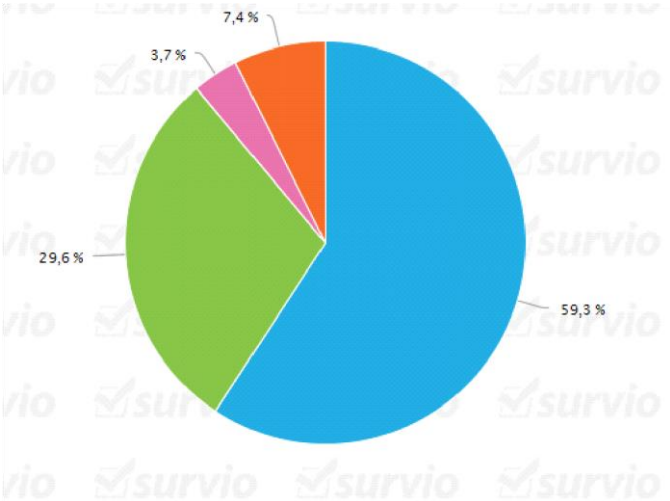
#	Ответ	Ответы	Доля
1	Живое общение лучше	5	18,5 %
2	Лучше СМИ	17	63,0 %
3	Должно быть одинаково	4	14,8 %
4	Затрудняюсь ответить	1	3,7 %

Третий вопрос звучал так - Какие способы агитации через СМИ оказывают большее влияние на Вас?

Самым популярным ответом стала «Реклама в Интернете» (16 человек).

Затем стали «Репортажи на TV» на этот вариант ответили 8 человек.

«Программы на радио» (0 человек), «Газеты и листовки» (1 человек) и затруднились ответить 2 человека.

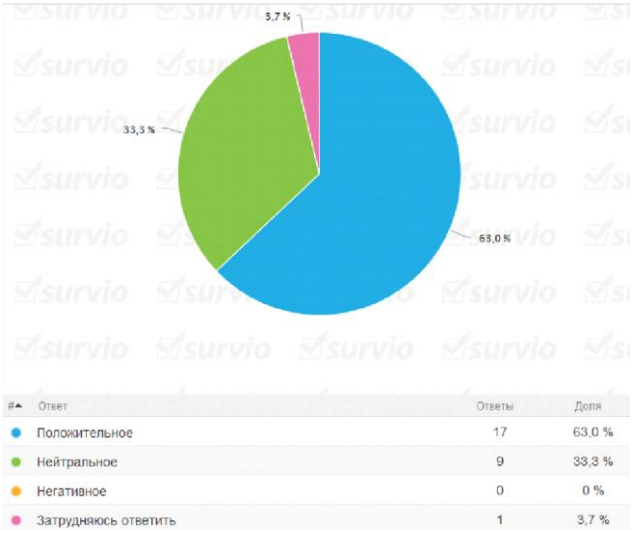


Далее вопрос был посвящен к определению отношения респондентов к выборам.

Вариант «положительно» выбрало 17 респондентов.

«Нейтрально» относится к выборам 9 опрошенных и негативно 0.

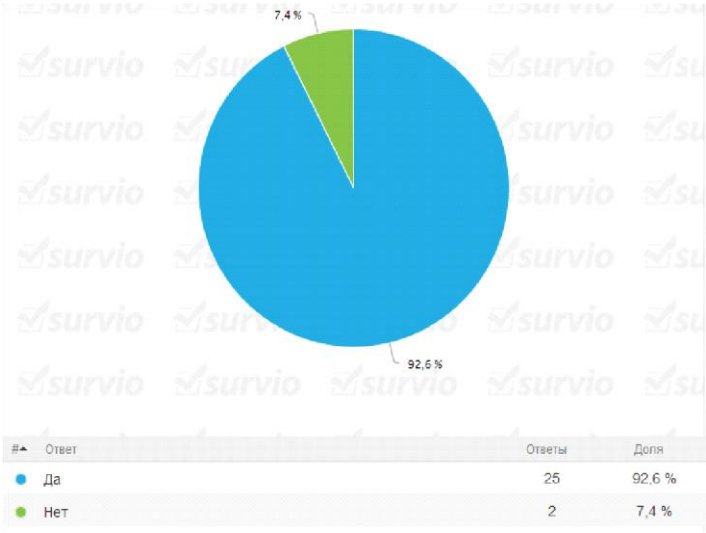
Затруднился при выборе ответа 1 человек.



Заключительный вопрос был нацелен на определение заинтересованности респондентов проблемой наилучшего способа агитации.

Заинтересованы результатом данного опроса 25 респондентов.

И 2 выбрали вариант Нет.



Таким образом, на основе проведенного социологического исследования можно сделать следующие выводы:

1. Респондентов, ответивших отрицательно на вопрос о посещаемостивыборов больше, чем тех, кто всегда посещает выборы. Разница составила 12%.

2. Большая часть опрошенных (63%) считает, что предвыборная агитациядолжна проводится через средства массовой информации.

3. Большинство респондентов (59,3%) считает, что реклама в Интернетеоказывает наибольшее влияние на избирателей, по сравнению с другими формами СМИ.

4. Положительное и нейтральное отношения к выборам у 63% и 33%опрошенных и ни одного негативного ответа.

5. Меньшая часть респондентов не заинтересована в результатахпроведенного опроса и 92% хотели бы узнать результаты социологического исследования.

Итак, политическая реклама в Интернете не только распространенное явление, но и достаточно популярное, которое эффективно воздействует на мнение граждан.

Далее мной был проведен анализ политической рекламы в рамках предвыборной кампании 2012 года по следующим критериям:

1. Текст на рекламе.

2. Визуальный образ кандидата.

3. Использование образов-символов (цвет фона, детали одежды).

Рассмотрим политическую рекламу кандидата на пост президента России Г.А. Зюганова.

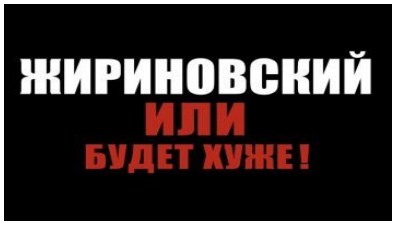
Зюганов сидит, слегка наклонив корпус вперед, такая поза говорит о прямом интересе и внимании. Данный жест можно расценить как внимание и интерес к проблемам и жизни в целом населения страны. На его лице заметна легкая улыбка, которая способствует тому, что люди подсознательно тянутся к тем, кто непринужденно убеждает в доброжелательном расположении. Его глаза смотрят вдаль, что означает ориентацию на перспективы и стремление изменить будущее. Вполне понятен выбор цветовой гаммы: красный фон рекламы, побуждающий потенциального избирателя к действию, дает надежду на возвращение прекрасного прошлого с цветущими садами и чистой рекой, которые изображены на заднем плане рекламной картинки.

Стратегия политической рекламного кампании основного кандидата в президенты В.В. Путина также строилась на использовании его изображения крупным планом.

Хотя поначалу избирательный штаб заявлял о том, что у премьера нет проблем с узнаваемостью. Однако В.В. Путин появился на рекламах, которые довольно удачно демонстрировали его открытое лицо, уверенный взгляд,

направленный вдаль, к счастливому будущему великой России. Это настроение поддерживают лозунги на всех предлагаемых вариантах рекламного продукта: «ВМЕСТЕ К ВЕЛИКОЙ РОССИИ, ВЕЛИКОЙ СТРАНЕ – СИЛЬНЫЙ ЛИДЕР», «ВЕЛИКОЙ СТРАНЕ – ДОСТОЙНОЕ БУДУЩЕЕ». В качестве фона выбран триколор, что, как известно, является национальным образомсимволом, который дает установку массовому сознанию на объединение для принятия важного политического решения.

Владимир Жириновский пошел по другому пути. Его рекламная кампания ориентирована на минимальное использование образов-символов и на максимально сильное эмоциональное воздействие на избирателя. На первый взгляд «картинка» кажется простой, но несет в себе большую смысловую нагрузку



Реклама кандидата в президенты В. Жириновского представляет собой только слоган, в котором четыре слова. Основной фон рекламы черный, который в России всегда символизирует сложные ситуации – это «жесткий» цвет. Слоган же выполнен в красном и белом тонах. Для написания фамилии Жириновского на плакатах использован белый, который в свою очередь символизируют мир, спокойствие. Красный, наоборот, возбуждает чувство тревоги за наше будущее. С помощью ключевых слов избирателя заставляют сделать выбор, так как осталось только два пути… «Жириновский или будет хуже!»

Политическая реклама Сергея Миронова в Президенты в Сети была практически незаметна и размещалась в основном на официальных сайтах партии «Справедливая Россия» и самого кандидата, в сервисе виртуальных дневников «Живом Журнале» и на YouTube.

Целевая группа данного кандидата – это так называемый «левый» электорат, в который входят пенсионеры и бюджетники, бывшие сторонники компартии,

отказавшиеся от дальнейшей поддержки коммунистов. Его избиратели недовольны политикой «Единой России» и считают, что обществу не хватает социальной справедливости, но при этом их пугает перспектива возврата в коммунистическое прошлое страны.

Пассивная предвыборная интернет-кампания лидера «Справедливой России» не внесла в имидж кандидата ничего нового. В президентской избирательной кампании основная ставка делалась на тот ресурс доверия, который партия получила на предыдущих думских выборах.

Итак, изучив несколько политических реклам в период предвыборной кампании 2012 г. на примере политической рекламы в Интернете, можно сделать следующий вывод. Прежде всего, хотелось бы отметить одну особенность изученного объекта – это то, что в данной избирательной кампании использовались особые PR-технологии, которые ввели тенденцию на полное слияние вербальных и невербальных характеристик рекламы, то есть лозунг как вербальная характеристика находился в прямой зависимости от образа-символа, который выступает невербальной характеристикой. Это и повысило заинтересованность населения в выборах. По насыщенности воздействия политической рекламы на электорат В.В. Путин существенно обошел всех своих конкурентов. Реклама остальных кандидатов в президенты РФ была менее выразительна. В процессе избирательной компании 2012 благодаря политической рекламе был усилен уже существующий имидж В. Путина.

Таким образом, Интернет становится всё более распространенной площадкой для размещения политической рекламы, которая ставит своей целью влияние на сознание электората и завоевание его политического выбора. Пока российская политическая реклама в Internet представляет собой если не экзотическое, то, по крайней мере, экспериментальное явление. Но уже многие российские политические партии и объединения имеют в Internet свои «страницы». Бесспорно, Интернет с его доступностью и огромной аудиторией, становится высокоэффективным средством политической борьбы, контролировать которое весьма трудно, если вообще можно.

Список использованной литературы и источников

1. *Лысенкова М.Ф.* Интернет-реклама в контексте политических технологий в современной России // NB: Вопросы права и политики. 2012. № 1. С. 1–20. URL: http://e-notabene.ru/lr/article_73.html.
2. *Романов А.А.* Учебное пособие «Реклама. Интернет-реклама». М., 2003. URL : http://www.twirpx.com/file/76924.
3. *Гуревич П.С.* Психология рекламы: Учебник для студентов вузов. М.: ЮНИТИ-ДАНА, 2012.
4. *Кузнецов П.А.* Политическая реклама. Теория и практика: учебное пособие для студентов вузов, обучающихся по специальностям «Реклама», «Связи с общественностью». М.: ЮНИТИ-ДАНА, 2012.
5. *Захаркин Р.А.* Технологии воздействия на массовое сознание в избирательной кампании // Труды Дальневосточного государственного технического университета. 2015. № 139. С. 78-87.

А.Р. Шайхутдинова

ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

*Научный руководитель: **Е.Г. Опыхтина**, к.ю.н, доцент кафедры гражданского и предпринимательского права ФГАОУ ВО «Казанский (Приволжский) федеральный университет»*

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОТРЕБИТЕЛЕЙ МЕДИЦИНСКИХТ УСЛУГ

На сегодняшний день проблемы защиты частной жизни граждан стоят на пике актуальности. Прежде всего, это связано с изобретением и развитием технических средств наблюдения, которые позволяют без труда анонимно вторгаться в частную жизнь, с применением электронно-компьютерных систем и информационных сетей, способных накапливать, хранить и использовать неограниченные объемы баз индивидуальных данных, не только не гарантирующих их сохранности, но их обработки без ведома субъекта персональных данных. Острота проблемы связана еще и с повышением коммерческой ценности любой информации, в том числе информации о персональных данных человека.

Особенно актуальна проблема охраны персональных данных в сфере оказания медицинских услуг, поскольку оказание медицинской помощи сопряжено с необходимостью тщательного анализа персональных данных пациента, относящихся к категории конфиденциальной информации.

В России, как и в других странах, главная особенность защиты личной информации в медицине – это необходимость обработки колоссального объема данных и исключительная важность персональных сведений. При этом в нашей стране есть ярко выраженная специфика.

С одной стороны, наша страна приступила к информатизации здравоохранения существенно позже по сравнению с Европой и США, которые также проходили подобную фазу «осознания проблемы» и необходимости ее решения, а для России она относительно нова и потому особенно болезненна.

С другой стороны, очевидно, что мероприятия по обеспечению информационной безопасности требуют существенного финансирования, а сейчас главные ассигнования идут на формирование ИТ-инфраструктуры (федеральных сервисов и региональных сегментов Единой государственной информационной системы в сфере здравоохранения), а не на ее защиту. Более того, в настоящее время штатным расписанием подавляющего большинства медицинских учреждений специалисты по информационной безопасности не предусмотрены. Техническое и программное обеспечение безопасности предполагает значительные финансовые затраты, как правило, не предусмотренные в бюджетах медицинских учреждений. Для сравнения: в финансово-кредитных организациях расходы на защиту информации составляют около 20% от совокупных расходов, предусмотренных для применения информационных технологий.

Основным же действующим законом, регламентирующим сферу обеспечения безопасности персональных данных является Федеральный закон от 27 июля 2006 г. № 152 «О персональных данных»[188]. Он предусматривает полный

[188] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. 2006. 29 июля.

комплекс мер по обеспечению сохранности персональных данных. В законе также несколько затрагивается вопрос обезличивания персональных данных, а именно В ст.5 п.7 говорится: "Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом." Данная оговорка некоторой степени снижает требования к конфиденциальности обезличенных персональных данных. Поэтому, как отмечают Секретов М.В., Ахметов Б.С., Сериков И.В., многие операторы персональных данных хранят информацию о пациенте в нескольких базах данных, так, чтобы при отдельном их использовании нельзя было точно идентифицировать личность пациента[189]. Цель такого подхода – снижение затрат на их обработку, однако такой подход нельзя считать наилучшим, ведь на самом деле такие базы данных будут потенциально опасны для субъектов персональных данных, и назвать их полностью обезличенными не считается возможным.

Эта же группа авторов предлагают два способа обезличивания персональных данных. Первый из них – применение токенов-носителей электронного ключа. Токен используется в системах персональных данных медицинских организаций в качестве идентификатора клиента. Здесь видится два недостатка. Первый – пациент может передать ключ другим лицам, таким образом, злоупотребив своим правом. Второй недостаток – немалые затраты на изготовление собственно ключа.

В качестве второго способа обезличивания данных предлагается механизм биометрического обезличивания. Суть данного механизма – использование отпечатка пальца пациента как биометрической информации, который бы позволил открыто хранить обезличенные истории болезней в медицинских организациях. То есть, человек сам будет выступать «ключом» к своим

[189] *Секретов М.В., Ахметов Б.С., Сериков И.В., Сауанова К.Т.* Защита персональных данных больных социально значимыми заболеваниями биометрическим обезличиванием электронных историй болезни // Труды международного симпозиума «Надежность и качество». 2012. Т. 2. URL: http://cyberleninka.ru/article/n/zaschitapersonalnyh-dannyh-bolnyh-sotsialno-znachimymi-zabolevaniyami-biometricheskim-obezlichivaniem-elektronnyhistoriy-bolezni (дата обращения: 28.03.2016).

персональным данным, гарантом свой безопасности. Данный способ представляется наиболее эффективным, но главный недостаток – отсутствие нормативный базы и материально-технических расходов на его осуществление. Однако разрешение этих проблем считаю возможным в ближайшей перспективе при разностороннем подходе со стороны разного рода специалистов. Безусловно, может потребоваться немалое количество времени для приведения данного механизма в действие, однако в итоге будет достигнута цель высокого уровня защиты персональных данных пациентов медицинских организаций, а в перспективе и отсутствие штрафов со стороны проверяющих органов, судебных споров.

И.И. Шалупня

ФГБОУ ВО «Саратовская государственная юридическая академия»
Межрегиональный юридический институт

*Научный руководитель: **П.В. Ересько**, к.п.н., доцент кафедры информатики ФГБОУ ВО «Саратовская государственная юридическая академия»*

КЛАССИФИКАЦИЯ И МЕРЫ ЗАЩИТЫ DOS И DDOS-АТАК

Под DoS-атаками подразумевают атаку хакеров на вычислительную систему с целью доведения ее до неисправности. DoS-атаки приводят к тому, что законные пользователи системы не могут получить доступ к предоставляемым серверам, или пользователям значительно затрудняется доступ к серверам. В настоящее время DoS и DDoS-атаки популярны, потому что приводят к неисправности практически любую систему, и при всем этом не оставляют каких-либо улик.

DoS-атака или атака как «отказ в обслуживании» подразумевает атаку на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен. Примеры: простои службы, приносящей доход, счета от провайдера и другие.

Если атака выполняется одновременно с нескольких компьютеров, то такую атаку называют DDoS-атака. Эта атака проводится с целью вызвать сбой в обслуживании хорошо защищенной крупной компании или организации

правительства. Размещение на популярном интернет-ресурсе ссылки на сайт, находящийся на непроизводительном сервере относят к непреднамеренным действиям, вызывающим DDoS-атаку. Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

Преступник сначала сканирует крупную сеть с помощью специально подготовленных схем. Схемы выявляют потенциально слабые узлы, на которые и производится впоследствии нападение. Затем преступник получает на них права администратора, и далее устанавливаются троянские программы, работающие в фоновом режиме. Компьютеры с троянами называются компьютерами-зомби. Пользователи компьютеров из данной крупной сети не подозревают, что являются потенциальными участниками DDoS-атаки. Далее преступник отправляет определенные команды компьютерам-зомби и те, в свою очередь осуществляют мощную DoS-атаку на тот компьютер, который является целью преступника[190].

Специалисты по защите информации выделили несколько причин использования DDoS-атак[191].

Личная неприязнь. Данная причина часто служит поводом для атак, как на крупные коммерческие компании, так и организации правительства. В 1999 году были атакованы веб-узлы Федерального бюро расследований (ФБР), которые впоследствии были недоступны в течение нескольких недель. Мотивом для данной атаки послужил недавний рейд Федерального бюро расследований (ФБР) против хакеров.

В качестве развлечения. В настоящее время большинство людей интересуются DoS-атаками, и многие хотят попробовать осуществить ее. Поэтому начинающие преступники часто осуществляют DoS-атаки ради развлечения.

---

[190] *Halpin H.* The Philosophy of Anonymous. Ontological Politics without Identity // Radical Philosophy. 2012.

[191] Хакеры атакуют эстонские правительственные сайты. URL: https://lenta.ru/news/2007/05/01/hackers (дата обращения: 01.03.2016).

Политический протест. Наиболее известными DDoS-атаками, где мотивом был политический протест, были акции в поддержку Памятника воину-освободителю в Эстонии - 2007 год, Южной Осетии - 2008 год, Wikileaks - 2011 год, Megaupload - 2012 год и EX.UA - 2012 год.

Недобросовестная конкуренция. DDoS-атаки также могут осуществляться по заказу недобросовестных конкурентов.

С целью вымогательства или шантажа. В случае проведения DDoS-атаки с целью вымогательства или шантажа преступник предварительно связывается с владельцем сайта.

Хакерам намного легче осуществлять DoS-атаки на систему, чем получать полный доступ к ней. Существуют большое количество причин, из-за которых может возникнуть DoS-условие, то есть такая ситуация, при которой пользователи не смогут получить полный доступ к ресурсам, предоставляемые сервером, либо доступ к ним затруднен: насыщение полосы пропускания, недостаток ресурсов[192].

Насыщение полосы пропускания за счет переполнения полосы пропускания, что служит осуществлению DoS-атаки, так как практически каждый компьютер подключен к сети Интернет. Обычно преступники пользуются флудом (англ. flood — «наводнение», «переполнение»). Под флудом понимают атаку, связанную с большим количеством бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию. Флуд имеет своей целью отказ в работе системы из-за исчерпания системных ресурсов, таких как процессора, памяти или каналов связи. Существует несколько разновидностей флуда.

– HTTP-флуд и ping-флуд.

– Smurf-атака (ICMP-флуд).

– Атака Fraggle (UDP-флуд).

– Атака с помощью переполнения пакетами SYN (SYN-флуд)[193].

---

[192] DoS-атака. URL: http://ru.rfwiki.org/wiki/DoS-атака (дата обращения 03.03.2016).

[193] *Ализар А.* Миллионы сайтов ушли в оффлайн из-за падения DNS-серверов GoDaddy // Хакер:

Преступники прибегают к такому виду DoS-атаки как недостаток ресурсов для захвата оперативной и физической памяти, процессорного времени. К видам DoS-атак относят: отправку «тяжелых» пакетов; переполнение сервера лог-файлами; плохую систему квотирования; недостаточную проверку данных пользователя; атаку второго рода; ошибки программирования.

Реализаторы, профессионально занимающиеся написанием программ эксплойтов, помогают атаковать сложные системы коммерческих предприятий или организаций.

1) Недостатки в программном коде.
2) Переполнение буфера.

Маршрутизация и атаки DNS.

1) DoS-атаки на уязвимости в программном обеспечении на DNScерверах.
2) DDoS атаки на DNS-серверы.

Все методы обнаружения можно разделить на несколько групп[194]:

1. сигнатурные – они основанные на качественном анализе трафика.
2. статистические – основанные на анализе трафика, в частностиколичественном.
3. гибридные (комбинированные) – сочетают в себе достоинствасигнатурного и статистического методов.

В 2012 году было проведено несколько DDoS-атак в крупном масштабе на DNS-серверы. Целью преступников из группы Anonymous было привести к неисправности всю глобальную сеть Интернет.

В ноябре 2002 года была проведена подобная атака. Данная атака считается самой глобальной DoS-атакой на DNS-серверы, потому что в результате ее проведения преступники смогли вывести из строя семь главных серверов.

Еще одна атака прошла 10 ноября 2012 года на компанию Go Daddy, являющуюся одной из самых крупных в мире хостинг-провайдеров. Последствия

материалы сайта. URL: https://xakep.ru/2012/09/11/59296 (дата обращения: 03.03.2016).

[194] DoS-атака. URL: http://ru.rfwiki.org/wiki/DoS-атака (дата обращения 03.03.2016).

атаки были разрушительными. Пострадал не только сам домен www.godaddy.com, но и более 33 миллионов доменов в сети Интернет, зарегистрированные данной компанией.

15 сентября 2012 года, крупная DDoS-атака на компанию CloudFlare, являющуюся сетью доставки контента, предназначенная для виртуального хостинга.

18 марта, по версии газеты Нью-Йорк Таймс, проводилась самая большая DDoS-атака в истории, жертвой которой стала компания Spamhaus, которая занимается занесением в черный список источников спама. Причиной атаки стало то, что Spamhaus занесла в черный список за рассылку спама голландского хост-провайдера Cyberbunker.

В основном защита от DoS-атак строится на правильной настройке компьютера. Последующие меры защиты способны защитить лишь от слабых DoS-атак, либо они будут использоваться для снижения ее эффективности.

Защита от HTTP-флуда. Для защиты от HTTP-флуда необходимо увеличить одновременное количество максимальных подключений к базе данных сервера, установить перед Web-серверомApache производительный Nginx для кэширования запросов.

Защита от ICMP-флуда. Для того чтобы защититься от ICMP-флуда, нужно отключить ответы на запросы ICMP ECHO.

Защита от UDP-флуда. Так как UDP-пакеты отсылаются на различные UDP-сервисы, для этого достаточно просто отключить их от внешнего мира и установить ограничение на количество соединений к DNS-серверу.

Защита от SYN-флуда. Данная защита строится на отключении очереди «полуоткрытых» TCP-соединений.

Имеется несколько универсальных советов, которые помогут подготовить компьютерную систему к DoS-атаке.

Все серверы, которые имеют доступ во внешнюю сеть, должны быть подготовлены к удаленной аварийной перезагрузке. Также желательно наличие

второго сетевого интерфейса, через который по ssh-соединению можно быстро получить доступ к серверу.

Программное обеспечение, которое установлено на сервере, должно быть в актуальном состоянии, то есть должно быть установлено последнее программное обеспечение, которое касается обеспечения безопасности системы.

Все сетевые сервисы должны быть защищены брандмауэром.

Полностью защититься от DDoS-атак, к сожалению, на сегодняшний день невозможно, так как надежных систем не существует.

Меры противодействия DDoS-атакам можно разделить на пассивные и активные[195].

1. Предотвращение. Профилактика причин, побуждающих тех или иных лиц организовывать и предпринять DDoS-атаки. Необходимо вовремя устранить причины DDoS-атак, после чего сделать выводы, во избежание таких атак в будущем.
2. Ответные меры. Применяя технические и правовые меры, нужно как можно активнее воздействовать на источник и организатора DDoS-атаки. В настоящее время существуют специальные фирмы, помогающие найти не только человека, проводящего атаку, но и самого организатора.
3. Программное обеспечение. На рынке современного программного и аппаратного обеспечения существует ПО, способное защитить малый и средний бизнес от слабых DDoS-атак. Данные средства обычно представляют собой небольшой сервер.
4. Фильтрация и блэкхолинг. Блокирование трафика, исходящего от атакующих машин.
5. Обратный DDOS – перенаправление трафика на атакующего. При достаточной мощности атакуемого сервера позволяет не только успешно отразить атаку, но и вывести из строя сервер атакующего.

[195] DoS-атака. URL: http://ru.rfwiki.org/wiki/DoS-атака (дата обращения 03.03.2016).

6. Устранение уязвимостей. Не работает против *флуд*-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов. Эта мера направлена на устранение ошибок в системах и службах.

7. Наращивание ресурсов. Абсолютной защиты не дает, но является хорошим фоном для применения других видов защиты от DDoS-атак.

8. Рассредоточение. Построение распределенных и дублирование систем, которые не прекратят обслуживать пользователей, даже если некоторые их элементы станут, недоступны из-за DoS-атаки.

9. Уклонение. Увод непосредственной цели атаки (доменного имени или IPадреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью атаки.

10. Активные ответные меры. Воздействие на источники, организатора или центр управления атакой, как техногенными, так и организационно-правовыми средствами.

11. Использование оборудования для отражения DDoS-атак.

12. Приобретение сервиса по защите от DDoS-атак. Актуально в случае превышения флудом пропускной способности сетевого канала.

13. Компания Гугл предоставляет свои ресурсы для отображения контента вашего сайта в том случае, если сайт находится под DDoS-атакой.

Заставляет задуматься фраза Б. Шнайера: «Только атаки дилетантов нацелены на машины. Атаки профессионалов нацелены на людей». В применении к нынешней ситуации хакеры-самоучки нацелены на искажение информации и уничтожении информации на компьютере, а профессионалы же целенаправленно собирают информацию с целью ее опубликования для причинения вреда крупным кампаниям.

Научное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных статей
по материалам Всероссийской научной Интернет-конференции студентов, магистрантов, аспирантов, молодых ученых, посвященной 85-летию ФГБОУ ВО «Саратовская государственная юридическая академия»

2-11 апреля 2016 года

Материалы публикуются в авторской редакции