Северо-Западный институт (филиал) федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский государственный юридический Университет
имени О.Е. Кутафина (МГЮА)»

Сборник материалов Дискуссионной молодежной сессии «Проблемы законотворчества и правоприменения в условиях цифровизации» (5 декабря 2019 года)



Вологда
2020

Северо-Западный институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный юридический Университет имени О.Е. Кутафина (МГЮА)»

Сборник материалов Дискуссионной молодежной сессии «Проблемы законотворчества и правоприменения в условиях цифровизации» (5 декабря 2019 года)

Вологда
2020

УДК 340.116
ББК 67.022.14
П78

Ответственный редактор:
Пеганова Ю.А.,
начальник отдела организации научной работы
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)

Подготовка и обработка научных материалов для научного издания,
научно-техническое редактирование научных материалов:
Пеганова Ю.А., Кругликова Е.В.

Проблемы законотворчества и правоприменения в условиях цифровизации : сборник материалов Дискуссионной молодежной сессии (г. Вологда, 5 декабря 2019 года) / Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА); ответственный редактор Пеганова Ю. А.- Вологда: Фонд развития филиала МГЮА имени О. Е. Кутафина в г. Вологде, 2020.- 107 с.- Текст: электронный.

ISBN 978-5-6044393-0-2

В настоящем издании представлены материалы Дискуссионной молодежной сессии «Проблемы законотворчества и правоприменения в условиях цифровизации», организованной в рамках II Регионального юридического форума «Правовые основы деятельности органов исполнительной государственной власти области и органов местного самоуправления», 5-6 декабря 2019 года.

В сборнике нашли отражение результаты современных исследований, проведенных молодыми учеными в различных отраслях юридической науки.

Статьи публикуются в авторской редакции. Авторы несут ответственность за содержание статей, за достоверность приведенных в статье фактов, цитат, статистических и иных данных, имен, названий, ссылок и прочих сведений.

Сборник предназначен для студентов, аспирантов, преподавателей, практикующих юристов и специалистов других отраслей с целью использования в учебной и научной деятельности.

УДК 340.116
ББК 67.022.14

ISBN 978-5-6044393-0-2

© Северо-Западный институт (филиал)
Университета имени О.Е. Кутафина (МГЮА), 2019
© Фонд развития филиала МГЮА
имени О.Е. Кутафина в г. Вологде, 2020

Оглавление

Очное участие:

Подобрей К.А. ЭЛЕКТРОННОЕ ПРАВОСУДИЕ: СОДЕРЖАНИЕ, МИРОВАЯ ПРАКТИКА, РОССИЙСКИЙ ОПЫТ 5
Лукина П.О., Едемская М.В. ПРОБЛЕМЫ «ВЕЕРНЫХ» ИСКОВ В РАЗРЕЗЕ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ ДЕЛ... 7
Гладилова С.И. СУДЕБНОЕ РАЗБИРАТЕЛЬСТВО ПОСРЕДСТВОМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ 9
Селякова М.В., Соловьева А.А. ПРЕДСТАВИТЕЛЬСТВО ПО ВИДЕОКОНФЕРЕНЦ-СВЯЗИ В АРБИТРАЖНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ РЕАЛИЗАЦИИ 11
Быкова С.Н. ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ ЭЛЕКТРОННОЙ ПОДПИСИ 13
Желтова Е.Д., Лобанова М.С. ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В АРБИТРАЖНОМ ПРОЦЕССЕ 16
Королева И.А., Степанов М.А. ЭЛЕКТРОННЫЕ СООБЩЕНИЯ КАК ДОКАЗАТЕЛЬСТВА В АРБИТРАЖНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ ИХ ИСПОЛЬЗОВАНИЯ, ПРАКТИКА ПРИМЕНЕНИЯ 18
Тимофеева Д.В., Рудкова Р.И. ИНФОРМАЦИЯ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ КАК ДОКАЗАТЕЛЬСТВО В АРБИТРАЖНОМ ПРОЦЕССЕ 20
Ильина З.А. ПРОБЛЕМА КУПИРОВАНИЯ СУДЕБНЫХ РЕШЕНИЙ ПО ГРАЖДАНСКИМ ДЕЛАМ В РОССИЙСКОЙ ФЕДЕРАЦИИ 23
Ворошилова Е.А. ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В БАНКОВСКОЙ СФЕРЕ 25
Логинов Н.Е. ПЕРЕХОД НА ПОЛНОСТЬЮ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ: ЗА И ПРОТИВ 28
Суровцева Е.С. СМАРТ-КОНТРАКТ КАК ПЕРСПЕКТИВА ОФОРМЛЕНИЯ ГРАЖДАНСКИХ ОТНОШЕНИЙ 30
Зыков А.И. СУДЕБНАЯ ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 33
Селякова М.В. КИБЕРПРЕСТУПНОСТЬ КАК НОВАЯ КРИМИНАЛЬНАЯ УГРОЗА 36
Ямпольская Т.В. НЕОБХОДИМОСТЬ ОТВЕТСТВЕННОСТИ МЕДИЙНЫХ ЛИЦ ЗА СОДЕЙСТВИЕ ПРЕСТУПНИКАМ ПУТЕМ ОКАЗАНИЯ ИМ РЕКЛАМНЫХ УСЛУГ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 39
Цветов П.С. СТАТЬЯ 159^6 УК РФ, КАК ПРЕСТУПЛЕНИЕ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 41
Соловьева А.А. ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ ПРОТИВ ДЕТЕЙ ПОСРЕДСТВОМ СЕТИ «ИНТЕРНЕТ»: МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ 43
Иванова Д.В. СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ 45
Лисенков Д.М. ФИНАНСОВО-ПРАВОВОЙ РЕЖИМ В ЭПОХУ ПЕТРА I 47
Заочное участие 49
Потапов А.В. ЭЛЕКТРОННЫЙ ТРУДОВОЙ ДОГОВОР: ПРОБЛЕМЫ ТЕОРИИ И ПРАВОПРИМЕНЕНИЯ 49
Юлдашев Д.М. МОДЕРНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА ОБ ИЗЪЯТИИ ЗЕМЕЛЬНЫХ УЧАСТКОВ ДЛЯ НЕДРОПОЛЬЗОВАНИЯ В УСЛОВИЯХ ИННОВАЦИОННОЙ ЭКОНОМИКИ 51
Астахова А.А. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ РАЦИОНАЛЬНОГО ИСПОЛЬЗОВАНИЯ ЗЕМЕЛЬ СЕЛЬСКОХОЗЯЙСТВЕННОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА 53

Максимова А.С., Стебнева И.С. СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНСТИТУЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ И ФРАНЦИИ 56
Китов А.В. ОТВЕТСТВЕННОСТЬ ЗА ИЗЪЯТИЕ АККАУНТОВ У «ЗАКОННЫХ» ПОЛЬЗОВАТЕЛЕЙ В ИНТЕРНЕТЕ 59
Алексеева А.А., Устинова А.В. ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ №152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ» И РЕГЛАМЕНТ ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕВРОПЕЙСКОГО СОЮЗА «О ЗАЩИТЕ ФИЗИЧЕСКИХ ЛИЦ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И О СВОБОДНОМ ОБРАЩЕНИИ ТАКИХ ДАННЫХ, А ТАКЖЕ ОБ ОТМЕНЕ ДИРЕКТИВЫ 95/46/ЕС»: СРАВНИТЕЛЬНО-ПРАВОВОЙ АСПЕКТ 61
Вихарева М.Р. ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ 64
Зажигин В.В. РИСКИ ОТ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 66
Гагарин А.Н. КРИМИНАЛИЗАЦИЯ ГЛАВЫ 28 УК РФ «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» 68
Косова М.В. ГОСУДАРСТВО И ПРАВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 69
Суровцева Е.С. ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: ПЕРСПЕКТИВЫ БОРЬБЫ С НИМИ 72
Урюпина М.М. К ВОПРОСУ О РОЛИ СОЦИАЛЬНЫХ СЕТЕЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ 74
Никитенко А.А. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 76
Косолысова П.И. ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 78
Шабашова Н.А. РЕАЛИЗАЦИЯ СТ. 171.2 УК РФ НА ПРИМЕРЕ ИНТЕРНЕТ-КАЗИНО 82
Дубинин М.Е. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕХАНИЗМ ЕЕ ОБЕСПЕЧЕНИЯ 85
Гусева Е.С. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ ПРЕСТУПЛЕНИЙ 89
Маркова Е.А. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ КОНСТИТУЦИОННОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ 91
Багров А.Ю. МЕХАНИЗМ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙВ ИНТЕРНЕТЕ 95
Тихонов И.С. ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 97
Усынин С.А. МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА 100
Силова Д.Л. КРИПТОВАЛЮТА КАК ПРЕДМЕТ ХИЩЕНИЯ 102
Лисенков Д.М., Быкова С.Н. КАК НЕОЖИДАННО СТАТЬ УЧРЕДИТЕЛЕМ ИЛИ УЧАСТНИКОМ ЮРИДИЧЕСКОГО ЛИЦА? 105

Очное участие

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ: СОДЕРЖАНИЕ, МИРОВАЯ ПРАКТИКА, РОССИЙСКИЙ ОПЫТ

Подобрей Кирилл Александрович,
курсант 2 курса юридического факультета ВИПЭ ФСИН России.
*Научный руководитель**:***
Кузнецова Елена Владимировна,
доцент кафедры государственно-правовых дисциплин ВИПЭ ВСИН России, к.ю.н., доцент

Понятие и содержание электронного правосудия неоднократно становилось предметом исследования в современной правовой науке, однако единой позиции относительно понимания данного явления не сложилось. Некоторые авторы под электронным правосудием понимают целую систему разрешения споров, включающую в себя руководство процессом и судебным разбирательством, оборот судебных документов, доступ к судебной информации, судебные извещения, правовой поиск, внутренние судебные процедуры и т.п.[1]. Другие предлагают рассматривать данное явление в широком и узком смыслах. В широком смысле электронное правосудие - это совокупность различных автоматизированных информационных систем-сервисов, предоставляющих средства для публикации судебных актов, ведения «электронного дела» и доступа сторон к материалам «электронного дела». В узком же смысле «электронное правосудие» - это «возможность суда и иных участников судебного процесса осуществлять процессуальные действия в электронной форме (например, такие действия, как подача в суд документов или участие в судебном заседании посредством системы видеоконференцсвязи)» [2].

Легального определения электронного правосудия в нашем государстве нет. Однако можно привести официальную позицию Комитета министров Совета Европы, в соответствии с которой под электронным правосудием понимается использование информационных компьютерных средств в реализации правосудия всеми заинтересованными сторонами с целью повышения его эффективности и качества работы. В электронное правосудие включаются электронное общение, обмен данными, доступ к информации судебного характера[3].

Анализ понятия и содержания электронного правосудия логично дополнить характеристикой его реализации в зарубежных государствах. Так, в США, Великобритании, Сингапуре, Южной Корее и некоторых других странах многие сервисы, развиваемые в России в последние годы, были запущены еще в начале и середине 2000-х гг.

Процессуальное законодательство США дает судам возможность определять правила подачи исковых заявлений и иных документов с помощью электронных средств. В середине 2000-х в США была внедрена глобальная система Case Management/Electronic Case Files

[1] См.: Жданова, Ю. А. Правовая природа электронного правосудия и его место в системе институтов информационного общества // Административное право и процесс. 2015. № 4. С. 81.
[2] См.: Романенкова С.В. Понятие электронного правосудия, его генезис и внедрение в правоприменительную практику зарубежных стран // Арбитражный и гражданский процесс. 2013. № 4. С. 29.
[3]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-м собрании заместителей министров). URL: http://idemocracy.ru/projects/articles/42-ec2009edem.html (дата обращения – 28.11.2019).

(CM/ECF). Данная система позволяет интегрировать системы внутреннего документооборота судов с возможностью взаимодействия с участниками процесса через Интернет[1].

В Южной Корее, где уровень распространения мобильной связи еще в 2005 году составлял примерно 75%, с помощью SMS-сообщений осуществлялась рассылка судебных повесток и извещений о наложении штрафов и взысканий. В настоящее время электронное правосудие в Корее реализовано на очень высоком уровне: через интернет можно отслеживать ход дела, подавать иски, ходатайства и т.д.[2] Система адаптирована для работы с ней на любых типах устройств.

В Финляндии действует законодательство об электронных коммуникациях в суде и в государственном секторе. К настоящему времени разработаны и действуют две системы: TUOMAS и SANTRA, причем первая используется для многочисленных гражданских дел, наиболее актуальных для граждан. В отношении уголовных дел действует система SAKARI, охватывающая работу прокуроров и судов со ссылкой на систему, которую использует полиция[3].

Во Франции действует электронный кабинет, позволяющий адвокату и судебному представителю дистанционно подавать документы в суд и получать извещения о ходе дела. Схожий, но более обширный по функционалу проект реализуется в настоящее время в Казахстане. Здесь действуют сервис «Судебный кабинет», форум «Талдау» и новая автоматизированная информационно-аналитическая система «Төрелік», которые позволяют ознакомиться с правоприменительной практикой судов, статистикой, подать документы в суд в электронном виде и т.п.[4]

Список примеров реализации электронного правосудия за рубежом можно продолжать. Однако и из приведенных выше следует, что, электронное правосудие понимается как информатизация самого судебного процесса, процессуальных действий и в целом сферы, связанной с ним: доступность информации о правосудии, обратная связь с судебной системой и т.д. Как правило, элементами механизма электронного правосудия считаются открытость и доступность информации о деятельности судов, включая архив судебных дел, электронный документооборот, электронное консультирование, дистанционная связь и мобильное правосудие.

В Российской Федерации элементы системы электронного правосудия начинали вводиться еще в середине 2000-х. С 2006 г. создается государственная автоматизированная система «Правосудие» (ГАС «Правосудие»). Предполагалось, что она станет общим информационным полем для всех судов общей юрисдикции, арбитражных судов и Верховного Суда РФ. При этом система должна была, с одной стороны, обеспечить информационную доступность судебной системы, а с другой – сохранить конфиденциальность определенных данных.

Однако нормативная регламентация возможности обращения в суд в электронном виде появилась значительно позднее, только с 1 января 2017 года стало возможным обращение в суды общей юрисдикции в электронной форме.

В настоящее время лучше всего элементы электронного правосудия в России развиты в арбитражных судах. Это обусловлено высокой нагрузкой, требующей максимально возможной оптимизации. В системе арбитражных судов функционирует картотека арбитражных дел, календарь судебных заседаний, банк решений арбитражных судов,

---

[1] FAQs: Case Management/Electronic Case Files (CM/ECF)/ URL.: https://www.uscourts.gov /courtrecords/electronic-filing-cmecf/faqs-case-management-electronic-case-files-cmecf (датаобращения: 4.12.2019).

[2] Глава КС Кореи: "Мы научим любой суд электронному документообороту". URL: http://rapsinews.ru/international_publication/20111101/256952969.html (дата обращения 13.11.2019 г.)

[3] Electronic tools for criminal justice in Finland – best practice case // E-tools for criminal case management within selected EU Member States. URL.: https://www.dadinternational.org /images/PDF/4_Finland.pdf (датаобращения – 18.11.2019)

[4] См.: Электронное правосудие в Казахстане. URL.: https://www.zakon.kz/4920071-elektronnoe- pravosudie-v-respubliki.html (дата обращения – 11.12.2019); Судебный кабинет: единое окно доступа к электронным сервисам судебных органов Республики Казахстан. URL.: http://office.sud.kz/ (дата обращения – 11.12.2019).

система, позволяющая участникам процесса отслеживать движение дела и принятые по нему процессуальные решения («Электронный страж») и система передачи в суд документов в электронном виде («Мой арбитр»). Элементы электронного правосудия в арбитражных судах вполне соответствуют, а в некоторых случаях и превосходят стандарты электронного правосудия, сложившиеся в зарубежной практике.

Для создания наиболее эффективной системы электронного правосудия в России требуется использовать опыт как зарубежный, так и национальный. Распространение опыта арбитражных судов на суды общей юрисдикции (особенно мировые, районные) несомненно, положительно скажется на развитии доступности правосудия. Отметим, что, не смотря на многолетнюю работу ГАС «Правосудие», интернет-портал системы не имеет ни качественной мобильной версии, ни мобильного приложения, ни сервиса личного кабинета, то есть функций, позволяющих в современном динамичном мире получать оперативный доступ к информации о деятельности судов общей юрисдикции с любого устройства.

Для распространения качественной, оперативной и доступной информации о деятельности судов следовало бы, на наш взгляд, привести официальные сайты Конституционного суда, управлений Судебного Департамента при ВС РФ, районных судов, мировых судей в соответствие с современными стандартами информационного наполнения сайтов.

Весьма импонирует реализованная в системе арбитражной юстиции и в зарубежных странах идея личного кабинета (судебного офиса), ее реализация актуальна и для системы судов общей юрисдикции. Следует рассмотреть вопрос и возможности обращения в суд, в том числе в электронной форме через многофункциональные центры, что обеспечит доступность правосудия для граждан, не имеющих навыков работы с электронными сервисами. Требуют совершенствования и некоторые аспекты нормативной регламентации электронного правосудия в России, однако эти вопросы требуют самостоятельного исследования.

ПРОБЛЕМЫ «ВЕЕРНЫХ» ИСКОВ В РАЗРЕЗЕ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ ДЕЛ

Лукина Полина Олеговна, Едемская Марина Владимировна -
студентыСеверо-западного иниститута (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич -
старший преподаватель кафедры государственно-правовых дисциплин
Северо-западного иниститута (филиала)
Университета имени О.Е. Кутафина (МГЮА)

Внедрение автоматизированной системы распределения (АРД) дел было предназначено для обеспечения возможности избежать ангажированности в процессе формирования состава суда для рассмотрения конкретного дела. Тем не менее это привело к тому, что недобросовестные участники судебного процесса нашли новые способы обыгрывать эту ситуацию в свою пользу и «выбирать» нужного судью для рассмотрения своего спора. Эту проблему продолжают фиксировать в арбитражных судах, поэтому необходимо разобраться в этом вопросе и предложить варианты решения.

АРД основано на принципе случайного распределения дел, который призван обеспечить транспарентность, исключив фактор заинтересованности при формировании

состава суда, а также на принципе равномерности, который обеспечивает эффективность судебной организации посредством управления судебной нагрузкой.[1]

Такое распределение направлено в первую очередь в целях реализации положений части 1 ст. 18 Арбитражного процессуального кодекса Российской Федерации (далее - АПК РФ), согласно которому состав суда для рассмотрения конкретного дела, в том числе с участием арбитражных заседателей, формируется с учетом нагрузки и специализации судей в порядке, исключающем влияние на его формирование лиц, заинтересованных в исходе судебного разбирательства, в том числе с использованием автоматизированной информационной системы. При этом независимость и беспристрастность суда (п. 3 ст. 2 АПК РФ) обеспечиваются в значительной мере порядком формирования его состава.[2]

Правовое положение распределения дел в автоматизированном режиме (при наличии необходимого программного обеспечения) закреплено в п. 31 Регламента арбитражных судов Российской Федерации, утвержденного Постановлением Пленума Высшего Арбитражного Суда Российской Федерации от 5 июня 1996 г.[3] В Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций), утвержденной Постановлением Пленума Высшего Арбитражного Суда Российской Федерации от 25 декабря 2013 г., определен, в частности, порядок использования системы АРД.[4]

Таким образом, меры направлены на то, чтобы председатели судов не имели никакого влияния на распределение дел между судьями, исключалась коррупция и несправедливая нагрузка. Тем не менее появились другие способы работы с АРД, влекущие злоупотребление правом.

Актуальной проблемой современного общества в направлении деятельности судов в условиях АРД, является подача так называемых «веерных» исков. Смысл сводится к подаче искового заявления путем выбора «нужного» судьи в обход автоматизированной системы, которая предполагает невозможность вмешательства и какого – либо влияния посторонних лиц. Механизм такого злоупотребления состоит в одновременной подаче в суд нескольких исковых заявлений, в которых сознательно допущены недостатки. Возможна ситуация подачи в арбитражный суд нескольких идентичных исковых заявлений с приложением к каждому из них неполного комплекта документов, предусмотренных частью 1 ст. 126 АПК РФ. Например**,** могут быть опущены доказательства уплаты государственной пошлины, направления искового заявления другой стороне, отсутствовать выписки из ЕГРЮЛ и т.п.

При получении таких исковых заявлений, судьи действуют в порядке статьи 128 АПК РФ - выносят определения об оставлении без движения искового заявления, к которым не приложены все документы, предусмотренные частью 1 ст. 126 АПК РФ, именно этого последствия и добивается недобросовестный истец. Таким образом, возникает ситуация, при которой сторона может выбирать, определение какого конкретного судьи она будет выполнять. Исправив сознательно допущенное нарушение путем представления недостающих документов, недобросовестная сторона, фактически, определяет, какой конкретно судья примет дело к своему производству.

По другим оставленным без движения исковым заявлениям сторона сама ходатайствует об их возвращении или ожидает возвращения указанных исковых заявлений судом на основании части 4 ст. 128 АПК РФ.

---

[1] Капустин О.А. Организация автоматизированного распределения дел в федеральном суде общей юрисдикции, 2019.

[2]Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ (ред. от 12.11.2019).

[3] Постановление Пленума Высшего Арбитражного Суда РФ от 5 июня 1996 г. N 7"Об утверждении Регламента арбитражных судов".

[4]Постановление Пленума Высшего Арбитражного Суда РФ от 25 декабря 2013 г. Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций).

В ч. 1 ст. 125 АПК РФ установлена возможность подачи искового заявления посредством заполнения формы, размещенной на официальном сайте арбитражного суда в информационно-телекоммуникационной сети «Интернет». Она позволяет недобросовестному истцу ссылаться на технический сбой, незнание компьютерных программ и т.д., чтобы отклонить возможные сомнения в добросовестности пользования процессуальными правами.

Арбитражное процессуальное законодательство не содержит норм, позволяющих эффективно противодействовать подобному злоупотреблению процессуальными правами. Ответственность недобросовестной стороны за попытку «выбрать» судью также не предусмотрена законом.

Можно предложить следующие способы минимизации данной проблемы:

1) Внесение в автоматизированную систему распределения дел изменений, которые бы позволили уведомлять истца автоматически, без участия судьи, о тождественности поданных им исковых заявлений, чтобы исключить возможность истцу ссылаться на технические ошибки.
2) Выявление системой «веерных» исковых заявлений, посредством разработанных объективных критериев отбора, и передача всех их одному судье.
3) Внесение поправок в действующее Арбитражное процессуальное законодательство, дающих возможность суду налагать судебный штраф, в случае непринятия истцом мер к оперативному отзыву тождественных исковых заявлений, а также совершения повторяющихся злоупотреблений.

Следует отметить, что в настоящее время в системе арбитражных судов накоплен определенный опыт выявления «веерных» исковых заявлений и пресечения подобной практики.

Например, применительно к Арбитражному суду города Москвы в марте 2012 года была опубликована выписка из протокола заседания его Президиума. «…Признать принятие одного из предъявленных в суд тождественных исков обстоятельством, свидетельствующим о намерении стороны выбрать судью и могущим вызвать сомнение в беспристрастности судьи, - основанием для самоотвода или отвода судьи по заявлению процессуального противника лица, подавшего иск.»[1]. В таком случае судья должен заявить самоотвод, а иск заново попасть в систему автоматического распределения дел.

Несмотря на высокий уровень развития информационного общества, возможность подачи «веерных» исков является пробелом отечественного законодательства, от которого не защищены даже самые современные правовые системы. Исходя из анализа сложившегося положения, можно сделать вывод, что приоритетным направлением разрешения этого недостатка должно стать техническое обновление автоматизированной системы распределения дел, позволяющее контролировать подачу тождественных исков и пресекать это, проверять поданные иски в системе по реквизитам. Кроме того, представляется необходимым установить ответственность за злоупотребление правом.

СУДЕБНОЕ РАЗБИРАТЕЛЬСТВО ПОСРЕДСТВОМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

Гладилова София Игоревна,
студент Вологодского государственного университета (ВоГУ)
*Научный руководитель**:***
Вонтова Наталия Евгеньевна,
старший преподаватель Вологодского государственного университета (ВоГУ)

[1] Выписка из протокола N 3 заседания Президиума Арбитражного суда города Москвы 19 марта 2012 г. // http://www.msk.arbitr.ru/node/13746.

Современные технологии кардинально меняют процесс отправления правосудия. Причиной того является необходимость упрощения процедуры судопроизводства и, как следствие, повышение его оперативности.

В теории процессуального права определяется, что судебное разбирательство – основная и главенствующая стадия. В рамках ее осуществления суд совершает такие процессуальные действия, как: заслушивает объяснения лиц, участвующих в деле; исследует и оценивает доказательства, представленные сторонами; устанавливает фактические обстоятельства рассматриваемого дела; определяет действительные права и обязанности участников спорного правоотношения; выносит законное и обоснованное постановление по делу.

Развитие видеоконференцсвязи при отправлении гражданского судопроизводства призвано обеспечивать выполнение конституционных и законодательных требований, а также добровольно взятых на себя Российской Федерацией обязательств по международным договорам и соглашениям в части соблюдения принципа доступности правосудия; процессуальной экономии судопроизводства и др. Первичное внедрение информационных технологий прошло при реализации уголовного судопроизводства. Эффективность такого внедрения позволила распространить данный опыт на арбитражное и гражданское судопроизводство.

Видеоконференцсвязь (ВКС) – способ осуществления установленных законом процессуальных действий при использовании программно-технических средств передачи аудио- и видеоинформации по каналам связи с одним или несколькими абонентами.

Федеральный закон от 26.04.2013 № 66-ФЗ «О внесении изменений в Гражданский процессуальный кодекс РФ», закрепил порядок использования в гражданском судопроизводстве систем видеоконференцсвязи при рассмотрении дел в судах первой инстанции, в том числе при осуществлении предварительного судебного заседания, в инстанциях по пересмотру судебных постановлений, а также при рассмотрении заявлений о пересмотре судебных постановлений по вновь открывшимся или новым обстоятельствам[1].

Согласно отчету Судебного департамента при Верховном Суде РФ, на рассмотрение судов первой инстанции в 2018 году поступило 17 270 149 гражданских дел. Из них с использованием ВКС были рассмотрены 12 089 дел, что 2 раза превышает показатели 2017 года (6772). Хотя, стоит отметить, что процент использования ВКС на практике все равно минимален[2].

Главными проблемами повсеместного внедрения ВКС в судебное производство России, помимо финансирования, является низкий уровень правового регулирования, защита информации, передаваемой с помощью связи. Для повышения уровня безопасности выделяются огромное количество бюджетных средств и трудовых ресурсов, так как нарушение хотя бы одного из аспектов безопасности данных (целостности, конфиденциальности, доступности) может принести огромный ущерб, как судам, так и участникам процесса, но, несмотря на это указанная проблема остается не решенной. Кроме того, в Гражданском процессуальном кодексе РФ не перечислены основания отказа в удовлетворении ходатайства. Отметим, что в арбитражном законодательстве данный вопрос решен.

В связи с тем, что специальную аппаратуру для реализации программы закупили только для малой части судов, суд имеет право отказать в ходатайстве об использовании видеоконференцсвязи. Важной проблемой является также то, что отсутствует возможность обжаловать определение суда об отказе в удовлетворении ходатайства.

---

[1] Ишонина А.С., Лапаев И.С. Проблемы законодательного регулирования порядка применения систем видеоконференц-связи в гражданском судопроизводстве // Вопросы современной юриспруденции: сб. ст. по матер. LX междунар. науч.-практ. конф. № 4(55). – Новосибирск: СибАК, 2016. – С. 14-18.

[2] Сводные статистические сведения о деятельности федеральных судов общей юрисдикции и мировых судей за 2018 год [Электронный ресурс]: Режим доступа://cdep.ru/index.php?id=79&item=4891.

Хочется отметить, что низкий уровень информирования населения, о возможности применения ВКС при отправлении правосудия также замедляет процесс его широкомасштабного внедрения на территории Российской Федерации.

Таким образом, положение о применении ВКС в гражданском судопроизводстве имеет ряд недостатков: в ГПК не раскрывается определение «технической возможности проведения ВКС»; не обозначены основания, по которым суд может отказать в удовлетворении ходатайства о назначении ВКС; отсутствует возможность обжаловать определение суда об отказе в удовлетворении ходатайства. Для реализации права граждан на судопроизводство посредством использования систем ВКС представляется целесообразным, предусмотреть в Гражданском процессуальном кодексе решение обозначенных проблем.

В завершении хочется отметить, что независимо от некоторых спорных моментов, видеоконференцсвязь при проведении судебного разбирательства действительно необходима. Именно она позволяет решать ряд проблем (невозможность личной явки на процесс, нахождение участников процесса на территориях, отдаленных от судов и др.) и является гарантом реализации важнейшего принципа судопроизводства – доступности правосудия.

ПРЕДСТАВИТЕЛЬСТВО ПО ВИДЕОКОНФЕРЕНЦ-СВЯЗИ В АРБИТРАЖНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ РЕАЛИЗАЦИИ

Селякова Мария Вячеславовна, Соловьева Анастасия Анатольевна,
студенты 4 курса Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич,
старший преподаватель кафедры государственно правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА)

1 октября 2019 г. вступил в силу Федеральный Закон от 28.11.2018 г. N 451-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации", согласно которому представителями в арбитражном суде могут быть только лица с высшим юридическим образованием или ученой степенью по юридической специальности[1].

В связи с данными изменениями можно выделить ряд проблем, которые коснутся участников арбитражного процесса.

Во-первых, поскольку арбитражные суды в основном рассматривают споры, возникающие из предпринимательской или иной экономической деятельности, а участниками таких споров, как правило, являются лица, непосредственно осуществляющие предпринимательскую деятельность, и соответственно обладающие специальными знаниями в данной области, то арбитражный процесс в целом не всегда нуждается в профессиональном представительстве со стороны лиц, имеющих высшее образование в области юриспруденции.

Во-вторых, лица, осуществляющие предпринимательскую деятельность, отличаются практической вовлеченностью в экономическую деятельность, основанную на предпринимательском риске, и при необходимости привлечения представителя для защиты своих интересов в арбитражном суде, большее значение будут иметь теоретические и практические знания представителя в области бизнеса, а не формальное наличие высшего юридического образования.

1http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=335745&fld=134&dst=1000000001,0&rnd=0.960909273168074 8#05450778294679879 (дата обращения: 24.11.2019).

В-третьих, возникает необходимость в проверке профессионального статуса представителя. Фактически диплом о высшем юридическом образовании будет одним из обязательных документов, подтверждающих статус представителя наряду с ходатайством доверителя или доверенностью. В настоящее время порядок проверки достоверности диплома о высшем образовании отсутствует, а на суд, рассматривающий дело, не возложена обязанность проверки действительности соответствующего документа, в том числе и при помощи открытых ресурсов Рособрнадзора[1].

В-четвертых, с внедрением в судебный процесс современных информационных технологий с 2010 года предусмотрена возможность участия представителей в судебном заседании с помощью систем видеоконференц-связи (далее – ВКС). Это нововведение обеспечило реализацию права на судебную защиту лиц, которые находятся в удаленной местности от суда и не имеют возможности присутствовать лично в судебном заседании.

Кроме того, ВКС способствует реализации принципа процессуальной экономии, который выражается, как в экономии судебных издержек на обеспечение участия представителей (расходы на проезд к месту судебного заседания, на наем жилого помещения и другие), так и в экономии времени судебного разбирательства (отпадает необходимость откладывать судебное заседание и ждать пока представитель доедет из Калининграда во Владивосток).

К сожалению, во многих малонаселенных районах и городах сложно найти профессионального представителя с высшим юридическим образованием, который при этом обладал бы знаниями и навыками в сфере экономической деятельности и смог бы оказать действительно квалифицированную помощь в спорах по арбитражным делам.

Также, для проведения судебного заседания с помощью ВКС необходимо установить техническую возможность проведения ВКС суда, рассматривающего дело и суда, организующим ВКС. Под технической возможностью осуществления ВКС понимается наличие в арбитражных судах, участвующих в ВКС, исправной системы ВКС и объективной возможности проведения судебного заседания данным способом в пределах установленного законом срока рассмотрения дела. При назначении судебного заседания, проводимого с использованием систем ВКС с арбитражными судами других регионов, лицо, ответственное за организацию проведения ВКС суда, рассматривающего дело, должно учитывать следующие обстоятельства:

- часовой пояс, действующий на территории региона;
- график дежурств судей по организации судебных заседаний с использованием систем ВКС в арбитражном суде Российской Федерации, которому планируется направить поручение;
- «План видеоконференций»[2].

По данным моментам на практике возникает множество проблем. Большинство из них связаны с отказом суда в ходатайстве о проведении судебного заседания с помощью ВКС. Напомним, что существует только два основания для отказа в удовлетворении ходатайства об участии в судебном заседании путем использования систем ВКС: отсутствие технической возможности или проведение закрытого судебного разбирательства.

Так, Арбитражный суд Воронежской области отказал в удовлетворении указанного ходатайства, поскольку отсутствует техническая возможность для проведения судебного разбирательства, так как разница во времени с Арбитражным судом Республики Хакасия

1 Дружинина Ю. Ф., Трезубов Е. С. Профессиональное представительство в цивилистическом процессе в свете судебной реформы // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2019. Т. 3. № 2. С. 165-172. DOI: https://doi.org/10.21603/2542-1840-2019-3-2-165-172 (дата обращения: 24.11.2019).

[2]Постановление Пленума ВАС РФ от 25.12.2013 N 100 (ред. от 11.07.2014) Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций) - https://sudact.ru/law/postanovlenie-plenuma-vas-rf-ot-25122013-n/ (дата обращения: 23.11.2019);

составляет +4 часа[1]. В другом деле Арбитражный суд Кабардино-Балкарской Республики отказал в удовлетворении ходатайства также из-за отсутствия технической возможности, но в этом случае она была связана с графиком сеансов ВКС в указанную дату в данном суде[2]. Как мы видим, большинство отказов суды основывают на отсутствии технической возможности, поскольку это понятие подлежит расширительному толкованию и под его содержание могут попадать любые обстоятельства. Следует отметить, что отказ в удовлетворении указанного ходатайства не может быть признан обстоятельством, которое могло бы свидетельствовать о лишении участника процесса возможности реализовать свои процессуальные права.

Таким образом, даже если в конкретной местности имеется возможность для участия представителя в судебном заседании с помощью ВКС, но он не имеет высшего юридического образования, то данная процедура становится невозможной. Данное обстоятельство затрудняет реализацию принципа процессуальной экономии.

По данным статистики Судебного департамента при Верховном Суде РФ[3] в 2017 и 2018 годах с помощью ВКС было рассмотрено 0,3% от общего числа рассмотренных арбитражными судами дел. Довольно небольшой процент, который, как мы считаем, связан с низкой технической оснащенностью судов оборудованием для ВКС, а также иными техническими неполадками, которые могут возникнуть во время судебного процесса (низкое качество связи, перебои в работе, пропало изображение/звук и т.п.), что приведет к сомнению в справедливости вынесенного судебного решения (что-то не услышали, не поняли; объяснили, но вас не услышали и т.д.).

Федеральной целевой программой «Развитие судебной системы России на 2013-2020 годы» предполагалось оборудовать 2500 залов судебных заседаний и кабинетов судей арбитражных судов системами ВКС к 2018 году[4]. Если верить данным Министерства экономического развития РФ[5], в 2018 году было оборудовано 2259 залов и кабинетов, что свидетельствует об эффективном внедрении систем ВКС в Арбитражные суды РФ.

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Быкова Светлана Николаевна,
студент 3 курса Северо- Западного института (филиала)
Университета им. О.Е. Кутафина (МГЮА)
Научный руководитель:
Шелепина Елена Александровна,
заведующий кафедрой гражданского права и гражданского процесса
Северо- Западного института (филиала)
Университета им. О.Е. Кутафина (МГЮА), к.ю.н., доцент

Ни для кого не секрет, что все вокруг подвергается цифровизации. Перо и бумагу заменила электронная почта, телефонная связь давно уже стала мобильной, предметы

[1]Решение Арбитражного суда Воронежской области от 26.03.2019 по делу № А14-11134/2018 - https://sudact.ru/arbitral (дата обращения: 23.11.2019)
[2]Решение Арбитражного суда Кабардино-Балкарской Республики от 23.04.2019 по делу № А20- 6099/2018 - https://sudact.ru/arbitral (дата обращения: 23.11.2019);
[3]http://www.cdep.ru/userimages/sudebnaya_statistika/2019/Obzor_sudebnoy_statistiki_arbitragnih_sudov_v_2018.pdf (дата обращения: 23.11.2019);
[4]Постановление Правительства РФ от 27.12.2012 N 1406 «О федеральной целевой программе "Развитие судебной системы России на 2013 - 2020 годы» " http://www.consultant.ru/document/cons_doc_LAW_140638/b133a7b61b64e004cdc913e66130aa61d9f266d0/ (дата обращения: 23.11.2019);
[5]https://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2019/410 (дата обращения: 23.11.2019).

бытовой техники наделяются свойствами электронного ума, а многие документы стало возможным подписывать без использования пишущих принадлежностей. Именно об электронной подписи – цифровом способе удостоверения прав – пойдет речь в данной работе.

Электронная подпись – реквизит электронного документа, полученный в результате преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искомой информации (принцип целостности), ее принадлежность (принцип авторства) и факт подписи (принцип неотказуемости).

Сфера применения такого способа удостоверения весьма обширна: на электронных торговых площадках, при подаче документов в контрольные (например, в Федеральную налоговую службу) и регистрирующие (например, в Федеральную службу государственной регистрации, кадастра и картографии) органы. Ей же подписываются электронные листы нетрудоспособности, она же позволяет организовать электронный документооборот как внутри компании, так и с внешними контрагентами.

Правовое регулирование осуществляется федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» и рядом государственных стандартов. Важно отметить, что указанным законом установлен принцип соотносимости (равенства по юридической значимости в гражданском обороте) собственноручной и электронной подписи. Таким образом, предоставление документа с электронной подписью без личного присутствия фактически приравнивается к традиционной форме удостоверения.

Электронная подпись в применении имеет ряд преимуществ. Во-первых, она соответствует тенденции цифровизации. В эпоху интернета и электронной связи возможность организовать электронный документооборот весьма актуальна. Кроме того, электронная подпись документа, для примера, абстрактным директором компании – это быстро. Рядовой сотрудник все той же абстрактной компании может либо отправить и получить документ непосредственно в электронном виде по внутренним каналам связи, избегая тем самым личных встреч и бумажной волокиты. В таких случаях, когда директор нашей абстрактной компании работает в другом городе или находится в командировке, электронная подпись существенно сокращает сроки удостоверения.

Существует еще один случай, когда электронная подпись единоличного исполнительного органа, обладающего правом представлять компанию, и, соответственно, подписывать документы от имени компании, находится у рядовых сотрудников или начальников структурных подразделений. В данной ситуации заметно проще и быстрее удостоверить необходимую документацию надлежащим образом, так как ее не нужно перенаправлять или эти действия просто производятся быстрее, так как адресат находится структурно в иерархии компании ближе к отправителю. Однако данная ситуация влечет за собой в некоторых случаях негативные последствия, о чем будет сказано ниже.

Во-вторых, при подаче в контрольные органы несущественно, но увеличиваются сроки. Мы знаем, что последний день срока, в том числе и для подачи, например, налоговой отчетности, заканчивается в 23:59:59. Однако на практике зачастую это время меняется в зависимости от графика работы контрольного органа. Представим, что упомянутый налоговый орган работает в день, который для отчитывающегося лица является последним днем срока, до 17:00. Тогда де-юре срок для подачи отчетности длится до 23:59:59, а де-факто он заканчивается в 17:00. Такую несправедливость не допускает электронная подпись, и документы, надлежаще оформленные и удостоверенные соответствующим образом, будут приняты контрольным органом даже в том случае, когда они поступили после окончания рабочего дня.

И последний, но не по значимости, положительный момент заключается в сущности удостоверения при помощи электронной подписи: ей удостоверяется не документ, а содержание. Редкий бумажный документ содержит требование о подписи на каждом из его листов, в законе такая обязанность не закреплена. Судебной практике известны случаи, когда условия договора недобросовестной стороной менялись заменой части (листа) бумажного

экземпляра. Изменение содержания после удостоверения электронной подписью, несомненно, возможно, что соответствует принципам гражданского оборота. Но данный факт обязательно будет отображаться в документе, что не позволит злоупотреблять односторонней заменой содержания. В том случае, когда часть содержания документа изымается из общей массы (например, дополнительное соглашение, текст которого находится только у одной стороны впоследствии этой стороной скрывается), факт данного изъятия так же будет зафиксирован.

В то же время, не стоит о свойственных электронной подписи недостатках. Мы разделим их на две группы: технические и правовые. К техническим относится:

1) Стоимость (подразумевается стоимость самой цифровой подписи на носителе, так и установочных программ шифрования)

2) Скептицизм участников как гражданских, так и административных правоотношений

3) Отсутствие универсальности: во-первых, для участия в различных правоотношениях требуется свой вид подписи (в том числе для подписи документов в разные органы государственной власти), во-вторых, в гражданских отношениях отсутствие электронной подписи у контрагента означает невозможность ее применения

Рассмотрим более детально правовые проблемы, среди которых стоит вначале отметить возможность пользования электронной подписью другого человека. Данная конструкция отношений сходна с представительством из обстановки (п.1 ст.182 ГК РФ) и удобна для применения в корпоративных целях, о чем уже говорилось выше. Однако ответственность из договоров и по иным основаниям, созданным с использованием данного способа удостоверения, несет ее собственник. Подлинность электронной подписи невозможно оспорить, так как это уникальные коды, закрепленные за ее владельцем. А доказать факт подписания другим лицом практически невозможно.

Рассмотрим еще один отрицательный момент, который касается выдачи сертификата и носителя ключа электронной подписи. Во-первых, выдача осуществляется на основании ряда, порой, общедоступных документов. Для физического лица это паспорт, номера страхового свидетельства государственного пенсионного страхования заявителя и идентификационного номера налогоплательщика заявителя. Что важно, предоставлять можно заверенные копии. Такой набор документов заявителя, например, имеется во многих государственных органах, у работодателя и т.д. Во-вторых, получение может осуществляться доверителем, при этом в законодательстве не содержится положение о нотариальной форме доверенности. Некоторые исследователи считают такую возможность основным слабым местом системы электронных подписей[1].

Совокупность вышеуказанных факторов привело к многочисленным лжеоформлениям электронной подписи на имя третьих лиц. Для чего это нужно? Например, для создания юридического лица под фиктивным учредительством третьих лиц – для избежания налогообложения и материальной и иных видов ответственности. В 2019 году мошеннические действия распространились и на сферу недвижимого имущества: было обнаружено несколько заключённых при помощи электронной подписи договоров безвозмездной передачи в собственность объектов недвижимости физических лиц (договор дарения).

В одном из таких случаев, по делу о подаренной квартире суд признал сделку недействительной в соответствии со статьей 168 ГК РФ как сделку, совершенную с нарушений требований закона и при этом посягающую на публичные интересы либо права и охраняемые законом интересы третьих лиц. Большую роль в разрешении данного дела сыграло признание ответчиком исковых требований. Однако не известно, как бы поступил суд в случае, если бы новый собственник квартиры оказался добросовестным приобретателем по возмездной сделке. Не ясно также, каким образом доказывать

[1] https://cyberleninka.ru/article/n/osnovy-grazhdanskopravovogo-regulirovaniya-elektronnoy-podpisi.

первоначальному собственнику факт мошенничества и не подписания им договора передачи имущества.

В связи с этим, предлагается, во-первых, усложнить процедуру получения сертификата и носителя ключа электронной подписи. Полагается, что осуществлять выдачу должны государственные органы или бюджетные учреждения, кроме того, необходимы изменения в части представления пакета документов, например, наличие оригинала документа, удостоверяющего личность. Во- вторых, нормативно закрепить возможность или невозможность отказа от электронной подписи. Например, при обращении в Росреестр для совершения сделок с недвижимостью с применением электронной подписи, об этом будет уведомляться собственник данных объектов. Однако остается вопрос о применении последствий недействительности такой сделки в отношении добросовестного приобретателя.

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В АРБИТРАЖНОМ ПРОЦЕССЕ

Желтова Екатерина Дмитриевна, Лобанова Мария Сергеевна,
студенты Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич,
старший преподаватель кафедры государственно-правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)

С развитием Интернета юридическим лицам и гражданам стала доступна подача исковых заявлений, не выходя из дома. Безусловно, данный прорыв является очень важным для арбитражного процесса и законодательства в целом. Вместе с этой возможностью появились новые термины и понятия в нормативно-правовых актах. Одним из таких является «электронная подпись».

Юридическое значение электронной подписи определяется п. 2 статьи 160 Гражданского кодекса Российской Федерации[1], в котором говорится о том, что электронная подпись является аналогом собственноручной. И здесь можно выделить первую и очень важную проблему. Как и собственноручную, электронную подпись можно подделать.

В соответствии с Федеральным Законом «Об электронной подписи»[2] выделяются её следующие виды:

1.Простая электронная подпись;

2. Усиленная электронная подпись:

а) усиленная неквалифицированная электронная подпись;

б) усиленная квалифицированная электронная подпись.

Конечно, если мы будем пользоваться усиленной квалифицированной электронной подписью, то упомянутой нами выше проблемы не возникнет. Она обладает дополнительными признаками защищенности, что практически полностью гарантирует, что её подделать нельзя.

Касательно двух других видов, то как раз они наиболее подвержены риску. Проблема заключается в том, что возможность идентификации лица, которое поставило подпись, очень низкая.

Многие юристы предлагают обезопасить себя следующими способами:

[1]"Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 18.07.2019) (с изм. и доп., вступ. в силу с 01.10.2019).
[2]Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" (с изм. и доп., вступ. в силу с 31.12.2017).

а) прописать в учредительных документах лицо, имеющее полномочия по пользованию электронной подписью;

б) в Положениях об электронном документообороте предусмотреть запрет на передачу электронной подписи другим лицам. [1]

Сделав это, мы значительно уменьшим риск передачи электронной подписи иному лицу. Дополнительно у нас будет субъект, который в случае “утечки” данной информации будет нести ответственность.

Но на наш взгляд этого недостаточно. Нужно отметить, что особую роль играют и лица, которые как раз имеют дело с электронной подписью и вообще электронным делопроизводством. Мы считаем, что как раз-таки они должны обладать специальными знаниями, а также с некоторой периодичностью проходить переподготовку в этой области.

Поскольку в нашей стране данная тема недостаточно развита, то для нас особую роль будет играть опыт зарубежных стран. Например, в Германии Закон об электронной подписи был принят еще в 2001 году. Это на 10 лет раньше, чем у нас. Следовательно, немецкие специалисты имеют больше знаний, а также опыта работы в данной сфере.

Вторая проблема заключается в том, что некоторые судьи не принимают доказательства, подписанные электронной подписью. Это создает ряд проблем.

Например, такая ситуация произошла в деле № 2-2395/2017 Железнодорожного районного суда г. Улан-Удэ[2]. Суд посчитал, что истцом не представлено доказательств совершения ответчиком действий по заключению договора займа, а именно того, что он вошел на сайт истца с целью получения пароля (доступа в личный кабинет), направления ответчику sms-сообщения с кодом подтверждения (простой ЭП), введение указанного кода ответчиком в специальное окно (личный кабинет). Следовательно, истцом не представлено доказательств заключения договора займа с ответчиком.

Участникам процесса после такого решения не только придется потратить дополнительное время, чтобы получить какие-либо доказательства совершенных действий, но и возможно, деньги.

Не единичны случаи, когда приходилось проводить экспертизу.

Но и в проведении экспертизы есть некоторые проблемы. Они заключаются в том, что ее необходимо заказывать в аккредитованном центре, в котором создан сертификат ключа проверки электронной подписи. Удостоверяющий центр подтверждает действительность сертификата ключа электронной подписи. Однако в случаях, когда электронная подпись выдана одним удостоверяющим центром, другим центром она не может быть проверена. Поэтому, если документ удостоверен разными электронными подписями, выданными разными центрами, экспертизу необходимо будет заказать в каждом из таких центров. И если просто оплатить экспертизу для некоторых юридических лиц непосильная задача, то оплата двух экспертиз явно склоняют к мысли не предоставлять документ, подписанный электронной подписью, в качестве доказательства.

Еще сложность вызывает и тот момент, что удостоверяющий центр может подтвердить подлинность ЭЦП только в том случае, если сертификат ключа подписи ещё действует. Если он уже не действует, лицу необходимо будет найти доказательства того, что она была подлинной в тот момент, когда сертификат действовал. А это зачастую сделать просто невозможно.

Думаем, тут будет логично сказать и о том, что в Российской Федерации практически нет организаций, которые могут оказать данную услугу.

Поскольку арбитражным судом рассматриваются споры с участием и иностранных лиц, неизбежно возникает вопрос о статусе на территории Российской Федерации электронных подписей, созданных по законодательству иностранных государств.

---

[1] Цигал М. «Электронная подпись: проблемы правового обеспечения. Способы защиты в суде» - https://zakon.ru (дата обращения 28.11.2019 года).

[2] Решение № 2-2395/2017 от 5 июня 2017 г. по делу № 2-2395/2017 Железнодорожный районный суд г. Улан-Удэ (Республика Бурятия).

В Российской Федерации и в зарубежных странах разные подходы к обеспечению конфиденциальности и целостности информации. В связи с этим непросто получить признание иностранных сертификатов. Так же, из-за строгих правил, достаточно сложно получить сертификат подлинности электронной подписи.

Нерешенность этого вопроса создает проблемы при подаче документов и доказательств в электронном виде иностранным лицом.

Если подвести итог всему вышесказанному, то нужно отметить, что тема об электронных подписях недостаточно раскрыта: информации очень мало как в литературе, так и в сети «Интернет». Простому обывателю в данном вопросе разобраться будет сложно, а значит, и пользоваться электронной подписью он не будет. Однако, судя по практике, не избежать проблем и тем, кто обладает специальными знаниями.

Мы выделили, на наш взгляд, три основных проблемы, связанные с применением электронной подписи в арбитражном процессе:

1. Возможность подделки электронной подписи;
2. Отказ судом в принятии документов, подписанных электронной подписью;
3. Признание иностранных электронных подписей арбитражными судами РФ.

Решение этих проблем облегчит "жизнь" для многих юридических лиц. Сойдет на нет вопрос о проблеме реализации права как на саму подачу искового заявления через Интернет, так и предоставлении доказательств; судебный процесс перестанет быть долгим и затратным. Надеемся, что в ближайшее время данные вопросы будут законодательно решены.

ЭЛЕКТРОННЫЕ СООБЩЕНИЯ КАК ДОКАЗАТЕЛЬСТВА В АРБИТРАЖНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ ИХ ИСПОЛЬЗОВАНИЯ, ПРАКТИКА ПРИМЕНЕНИЯ

Королева Ирина Алексеевна, Степанов Матвей Андреевич,
студенты 4 курса Северо-Западного института (филиала)
Университета им. О.Е. Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич,
старший преподаватель кафедры государственно-правовых дисциплин
Северо-Западного института (филиала)
Университета им. О.Е. Кутафина (МГЮА).

Социальные сети, электронная почта и другие мессенджеры стали неотъемлемой частью нашей современной жизни. На сегодняшний день практически каждая организация пользуется электронной перепиской для общения с контрагентами, обмена информацией и др. Преимущества получения информации по электронной почте очевидны, прежде всего - это существенная экономия времени, а также удобство взаимодействия сторон.

В 2016 году Федеральным Законом № 220-ФЗ были внесены изменения в п. 3, ст. 75 АПК РФ, которыми было законодательно закреплена возможность использования документов, полученных с помощью информационно – телекоммуникационной сети «Интернет» в качестве письменного доказательства.[1] Казалось бы, что проблем с применением электронных сообщений в судебной практике не должно быть, однако же это не совсем так.

К примеру, одной из проблем является возможность модификации электронного сообщения (исправления, удаления). В настоящий момент, такие мессенджеры как WhatsApp, Telegram, ВКонтакте позволяют в течение 24 часов изменять содержание уже

[1]Федеральный закон от 23.06.2016 N 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» // опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru - 23.06.2016.

отправленных сообщений, а также удалять его. Поэтому на практике может возникнуть проблема с доказыванием того факта, что сообщение содержало иной смысл или вовсе было отправлено контрагентом.

Поэтому, во избежание удаления или изменения переписки в будущем, необходимо зафиксировать её у нотариуса. Он в свою очередь составит протокол, который в дальнейшем может использоваться в суде в качестве доказательства. Анализируя судебную практику, можно сделать вывод о том, что электронная переписка принимается судами в качестве доказательства в большинстве случаев лишь при нотариальном ее подтверждении.

Например, в деле № А40-123065/18ответчик ООО «ЧТО ДЕЛАТЬ СОФТ» предоставило в качестве доказательства исполнения договора оказания услуг в отношении ООО «Керамходинг» электронную переписку. Суд оставляя апелляционную жалобу без удовлетворения, обосновывает свою позицию тем, что электронная переписка не предусмотрена договором, в котором также не определены сторонами электронные адреса сторон. Кроме того, переписка не была нотариально подтверждена, в связи с чем, данные представленные письма не являются надлежащим доказательством в силу норм ст. 68 АПК РФ исходя из относимости и допустимости доказательств.[1]

Обеспечить в качестве доказательства переписку можно также с помощью включения соответствующего пункта в текст договора. Так, стороны могут прописать в договоре, что документы, переданные посредством электронной и факсимильной связи, обладают силой оригинала.

В деле № А23-9647/2017 истец ООО «Гранитстройресурс» просил суд взыскать с ответчика ООО «Белстройпроект» денежные средства по договору поставки в размере 519 000 рублей. В целях соблюдения досудебного порядка урегулирования спора истец отправил по электронной почте ответчика претензию с требованием о погашении задолженности. Договором стороны предусмотрели возможность использования электронной переписки. В договоре указан конкретный адрес электронной почты ответчика. Претензия была проигнорирована им, поэтому истец обратился в суд. Переписка была воспринята судом в качестве надлежащего доказательства по делу, в связи с чем исковые требования были удовлетворены.[2]

Еще одной проблемой использования в качестве доказательств электронных сообщений является проблема идентификации отправителя электронных сообщений. Ответчик в суде часто обосновывает свою позицию тем что, во время переписки с истцом невозможно точно установить отправителя сообщений и поэтому просит признать электронную переписку недопустимым доказательством по делу. Технически можно установить, с какого компьютера была произведена отправка, но персонифицировать лицо, отправившее сообщения на практике сложно. Использование свидетельских показаний в данной ситуации возможно, но суд может не принять их во внимание, так как свидетели не обладают специальными познаниями, достаточными для подтверждения факта отправки или прочтения электронного сообщения.[3]

Проблема заключается в том, что при регистрации в социальных сетях, создании электронных почтовых ящиков не запрашивается информация, которая удостоверяет личность пользователя, его учредительные документы, а указание ФИО, семейного положения не позволяет однозначно его идентифицировать.

Нередко для идентификации отправителя электронного сообщения суды учитывают тот факт, что отрицание одной из сторон принадлежности почтового ящика противоречит

---

[1] Постановления Девятого Арбитражного Апелляционного суда 28.05.2019 в деле № А40-123065/18 // URL: https://sudact.ru

[2] Решение Арбитражного суда Калужской области от 19.03.2018 по делу № А23-9647/2017 // URL: https://sudact.ru

[3] Шароватова С. С., Чуракова Е. Н. Электронные сообщения как доказательства в арбитражном процессе // Актуальные проблемы современной науки в 21 веке. – 2016. - №1. С. 117-119.

другим доказательствам. Например, были оплачены счета, отправленные на электронный адрес, и присутствует результат работ, за который производилась оплата.

Примером судебной практики может служить Постановление Девятого Арбитражного Апелляционного суда по делу № А40-134500/12 о взыскании неосновательного обогащения и процентов. Между ООО «Торговый Дом «Тагильский» (истец) и ООО «Веб автоматика» (ответчик) была достигнута предварительная договоренность заключить договор на разработку веб приложения (сайта в сети «Интеренет»). Далее ответчиком по электронной почте был направлен проект договора со всеми существенными условиями истцу для согласования (оферта), а также счета на оплату в размере 50% от общей суммы договора. Истец перечислил указанные денежные средства. В обоснование исковых требований истец указывает, что договор между сторонами не был заключен, поскольку существенные условия между сторонами не были согласованы, и считает, что перечисленные в качестве предоплаты денежные средства подлежат возврату, как неосновательное обогащение. Отказывая в удовлетворении исковых требований суд первой инстанции обосновывает свою позицию тем, что из электронной переписки сторон следует, что услуги ответчиком фактически оказывались, и более полугода истец фактически пользовался результатами оказанных услуг, а также, что существенные условия договора были согласованы сторонами. В апелляционной жалобе истец обосновывает свою позицию тем, что не установлен факт принадлежности ему электронного адреса, с которого осуществлялась переписка. Суд, отказывая в удовлетворении апелляционной жалобы ссылается на то, что именно на указанный электронный адрес были получены счета для оплаты, которые впоследствии были оплачены истцом.[1]

Таким образом, проанализировав судебную практику можно сделать вывод о том, что электронные сообщения в качестве допустимых доказательств в арбитражном процессе принимаются судом при соблюдении нескольких условий. Во - первых, возможность идентификации отправителя и получателя электронного сообщения. Это будет возможно, если включить в текст договора пункт об осуществлении электронной переписки с перечислением всех электронных адресов и номеров телефонов, с которых будет осуществляться взаимодействие сторон. Во - вторых, установление подлинности электронной переписки. Подлинность может быть подтверждена нотариальным осмотром, технической экспертизой, электронной подписью. В - третьих, установление полномочий отправителя и получателя на принятие решений относительно предмета переписки. Для того, чтобы не возникало сомнений, относительно того, кем ведется переписка необходимо указывать или запрашивать конкретные ФИО, должности, управомочивающие документы.

ИНФОРМАЦИЯ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ КАК ДОКАЗАТЕЛЬСТВО В АРБИТРАЖНОМ ПРОЦЕССЕ

Тимофеева Дарья Вадимовна, Рудкова Регина Игоревна,
студенты 4 курса Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич,
старший преподаватель кафедры государственно-правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА)

Перечень доказательств, которые можно использовать в споре, открытый. Арбитражно – процессуальный кодекс допускает письменные и вещественные

[1] Постановление Девятого Арбитражного Апелляционного суда от 9.04.2013 по делу № А40-134500/12 // URL: https://sudact.ru

доказательства, объяснения лиц, участвующих в деле, заключения экспертов, консультации специалистов, показания свидетелей, аудио- и видеозаписи, иные документы и материалы. (ч. 2 ст. 64 АПК). Это значит, что можно прибегать к любым видам и формам доказательств, но они должны отвечать критериям относимости и допустимости.

В законах нет ограничений в способах доказывания факта распространения сведений через сеть Интернет. Однако нужно заранее выбрать способ обеспечения доказательства[1].

На практике часто возникают сложности именно с допустимостью доказательств, а точнее, с ее практической стороной: фиксацией, оформлением, заверением. Допустимыми доказательствами являются, в том числе сделанные и заверенные лицами, участвующими в деле, распечатки материалов,размещенных в информационно-телекоммуникационной сети (скриншот)[2], с указанием адреса интернет-страницы, с которой сделана распечатка, а также точного времени ее получения. Такие распечатки подлежат оценке судом при рассмотрении дела наравне с прочими доказательствами (статья 67 ГПК РФ, статья 71 АПК РФ). Особенно остро этот вопрос стоит из-за информатизации всех сфер общественной жизни. С появлением и развитием технологий появляются новые формы и виды доказательств, что требует выработки алгоритмов их надлежащего представления в суд, но анализ судебной практики показывает, что и "традиционные" доказательства могут вызвать определенные затруднения.

С развитием Интернета, а именно социальных сетей, возросла ценность данных, которые содержатся в социальных сетях, в особенности в личных страницах пользователей. Еще недавно сложно было себе представить, чтобы в судебном споре адвокат представлял в качестве доказательства скриншот[3] аккаунта оппонента из социальных сетей. Тем не менее, сейчас количество дел, в которых используются такие доказательства, позволяющие установить связи между сторонами сделок или участниками процесса, растет на глазах, а еще два-три года назад таких дел не было вообще.

Одно из самых распространенных обстоятельств, которое сегодня доказывается сведениями из социальных сетей, – это родственная связь. Она устанавливается через «дружбу» в Facebook. Помимо родства так доказывается и факт знакомства участников процесса или их дружба «в жизни». Это часто используют управляющие в делах о банкротстве, истцы, оспаривающие сделки с заинтересованностью, а также стороны процесса, пытающиеся доказать заинтересованность эксперта, арбитражного управляющего и других значимых процессуальных фигур.

Так, в Арбитражном суде Москвы, истцы при помощи фотографий из социальной сети «Инстаграмм» доказали, что двое ответчиков состояли в гражданском браке и часто выезжали за границу. Последний факт имел ключевое значение в деле о банкротстве, что позволило истцам одержать победу, использовав в качестве доказательственного материала фотографии из социальной сети. Истцы доказали: мужчина и женщина, руководители двух фирм, прекрасно знали друг друга и вместе отдыхали на Майорке. С помощью сделки, видимо, пытались спрятать денежные средства от кредиторов. В данном случае ответчиками были руководители двух компаний, заключившие крупную сделку. Одна из компаний проходила процедуру банкротства, но нашла миллиард рублей, чтобы заплатить по контракту другой. Истцы заподозрили, что сделка состоялась только для того, чтобы увести деньги со счетов банкрота. Вопрос был в том, знало ли руководство второй фирмы, что сотрудничает с банкротом, или это добросовестные люди, надеявшиеся, что свой миллиард получили честно? Адвокаты истцов-кредиторов принесли в суд заверенные нотариусом распечатки из социальных сетей: по фотографиям стало ясно, что оба руководителя не просто знакомы, у них не только финансовые, но, похоже, и очень личные отношения. В

[1] п. 7 постановления Пленума ВС от 15.06.2010 № 16 "О практике применения судами Закона Российской Федерации "О средствах массовой информации").

[2] П. 55 Постановление Пленума Верховного Суда РФ от 23.04.2019 N 10 «О применении части четвертой Гражданского кодекса Российской Федерации».

[3] Постановление АС Московского округа от 31.10.2016 по делу № А40-226103/2015.

итоге сделка была признана недействительной. По словам адвоката Натальи Колеровой, представлявшей интересы кредитора, использование данных из социальных сетей в качестве доказательств, становится в некоторых делах необходимостью. «Социальные сети сегодня являются важным источником получения доказательств наряду с другими источниками» - говорит Наталья Колерова.

Юридическое закрепление найденных в сети материалов, которые в суде могут быть использованы, как доказательства по делу, возможно только при помощи нотариуса. По данным Федеральной нотариальной палаты ежегодно к нотариусам обращаются более 20 тысяч граждан, чтобы зафиксировать какие-то материалы из сети Интернет. Могут также попросить наложить печать на электронную переписку или размещенные в сети объявления, и, даже если данные исчезнут из Всемирной паутины, доказательства будут у людей на руках. Пользуясь фильтрами, в социальных сетях сегодня можно найти почти кого угодно.

По словам президента Федеральной нотариальной палаты Константина Корсика, поскольку информационные технологии сегодня приобретают все большее значение, именно нотариусы становятся ключевым звеном обеспечения стабильности гражданского оборота, так как помогают юридически закреплять факты и в целом защищать права граждан.

Стоит отметить, что Суды не во всех случаях принимают заверенную представителем простую распечатку страницы сайта в сети Интернет либо так называемые "скриншоты". Современные технологии позволяют практически без ограничений внести любые изменения в такие документы. Поэтому суды относятся к ним критически[1]. Практика исходит из того, что, например, скриншот должен содержать дату и время[2] получения информации с сайта в сети Интернет[3].

Таким образом, для того, чтобы использовать информацию из социальных сетей в качестве доказательства по делу в арбитражном процессе необходимо совершить следующие действия:

Во – первых, сделать скриншот. Понятие скриншота раскрывается в постановлении Федерального арбитражного суда Волго-Вятского округа от 27 апреля 2011 г. по делу № А82-12456/2010. Данным судом рассматривалась кассационная жалоба истца на определение Арбитражного суда Ярославской области от 14.01.2011 и постановление Второго арбитражного апелляционного суда от 03.03.2011. Этими судебными актами заявление истца было возвращено на основании пункта 4 части 1 статьи 129 АПК РФ. Суд пришел к выводу о том, что представленные в отношении ответчика распечатка с сайта Федеральной налоговой службы, а в отношении самого истца копия выписки из Единого государственного реестра юридических лиц не могут быть признаны достоверными документами, содержащими сведения о месте нахождения ответчика. Кассационная жалоба была удовлетворена и дело направлено на новое рассмотрение по следующим основаниям. Скриншот - это страницы в сети Интернет (снимок экрана, показывающий то, что видит пользователь на экране монитора), подтверждающие размещение информации, подлежащей раскрытию[4]. Предоставляя суду скриншот, заверенный надлежащим образом, истец исполнил требование пункта 9 части 1 статьи 126 АПК РФ.

Также, как уже указывалось выше, на скриншоте должны быть проставлены дата и время получения информации с сайта в сети Интернет.

Во – вторых, заверить распечатку с сайта в сети Интернет надлежащим образом, обратившись к нотариусу[5].

---

[1] Постановление 17ААС от 31.08.2012 по делу № А60-20330/2012.

[2] Письмо ФНС России от 31.03.2016 № СА-4-7/5589 "Об использовании "скриншотов" в качестве доказательств в арбитражном суде".

[3] Постановление ФАС Уральского округа от 15.10.2013 по делу № А07-513/2013.

[4]Постановление Федерального арбитражного суда Волго-Вятского округа от 27 апреля 2011 г. по делу № А82-12456/2010.

[5] Письмо Федеральной налоговой службы от 31 марта 2016 г. № СА-4-7/5589 О понятии «скриншот» («снимок экрана») и порядке его использования.

В последнее время прослеживается важная тенденция - суды начали принимать данные из социальных сетей (переписки, фото и видео материалы) в качестве доказательства в судебных спорах. Использование информации из социальных сетей может служить доказательством, например, в делах о банкротстве; спорах, связанных с долговыми обязательствами и некоторых других делах, рассматриваемых в суде.

Поскольку заверенные нотариусом страницы интернет-сайтов уже давно принимаются судами, вряд ли можно говорить о социальных сетях как о новом виде доказательств, а значит, и какого-то особого нормативного регулирования или разъяснений высших судебных инстанций не потребуется. Скорее можно говорить о некоторой специфике социальных сетей по сравнению с другими интернет-ресурсами и обстоятельств, которые можно установить с их помощью.

ПРОБЛЕМА КУПИРОВАНИЯ СУДЕБНЫХ РЕШЕНИЙ ПО ГРАЖДАНСКИМ ДЕЛАМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ильина Злата Андреевна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Афанасьева Наталья Андреевна,
старший преподаватель кафедры гражданского права и гражданского процесса
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)

В гражданском процессе активно развивается концепция электронного правосудия, суть которой заключается в информационном обмене сведений о судопроизводстве между гражданами, организациями и государственными учреждениями. Важное направление концепции - публикация судебных актов на официальных сайтах судов в сети «Интернет» в режиме открытого доступа. Подготовка судебного акта к публикации - это необходимость, обусловленная требованиями статьи 15 Закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" [1]. Подготовка в основном сводится к изъятию из судебного акта той или иной информации. Согласно федеральному закону от 27.06.2006 N 152-ФЗ "О персональных данных" под "обезличиванием персональных данных" понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [2]. Деперсонификацию судебного акта можно определить как замену в тексте судебного акта персональных данных инициалами, псевдонимами или другими обозначениями, не позволяющими идентифицировать участников судебного процесса или иные сведения, относящиеся к информации ограниченного доступа. Перечень данных, относящихся к категории персональных, а значит, подлежащих исключению из текстов судебных актов, размещаемых на сайте суда, закреплен в статье 15 Закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации". К ним, в частности, отнесены:фамилии, имена и отчества участников судебного процесса, дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность, идентификационный номер налогоплательщика - физического лица, основной государственный регистрационный номер индивидуального предпринимателя, страховой номер индивидуального лицевого счета;сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса, если эти сведения относятся к существу дела.**Не подлежат исключению**: ИНН ИП, ИГРН ИП, ФИО истца, ответчика, третьего лица, гражданского истца, гражданского ответчика, административного истца, административного

ответчика, заинтересованного лица, лица, в отношении которого ведется производство по делу об административном правонарушении, ФИО секретаря судебного заседания, судьи, рассматривавшего дело, а также прокурора, адвоката и представителя.[1], [3].

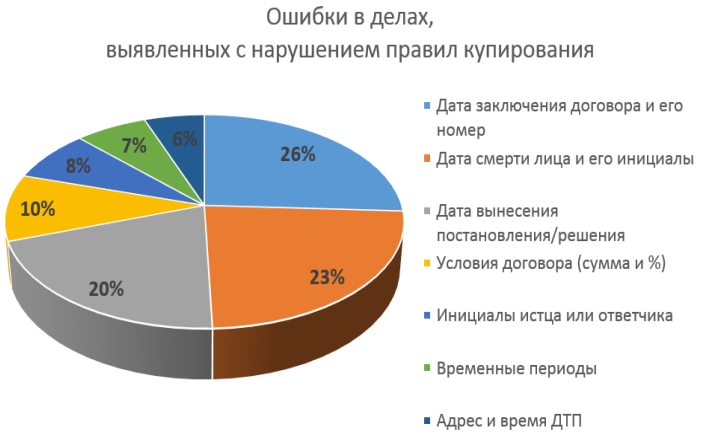
Нами было проведено исследование соблюдения правил купирования судебных актов вологодскими судами. Выборке подверглись все категории дел. Исследование проходило на уровне судов первой инстанции - районных и приравненных судов (Вологодский и Череповецкий городские суды; Бабаевский, Кичменгско-городецкий, Кирилловский, Вытегорский, Устюженский, Шекснинский, Белозерский, Грязовецкий, Верховажский, Тарногский, Кадуйский, Тотемский, Вашкинский, Никольский, Нюксенский и Сокольский районные суды Вологодской области).Методом сплошной выборки нами было выбрано по 15 судебных актов с официально сайта каждого суда, которые были проверены на предмет нарушения правил купирования. На основании полученных данных можно сделать следующие выводы: лидирующие позиции по количеству дел с нарушением правил купирования занимают Вологодский городской суд (14 дел из 15) и Бабаевский районный суд (13 дел из 15). Меньше всего дел с нарушениями было выявлено в Никольском и Нюксенском районных судах (4 дела из 15), а также в Сокольском районном суде (3 дела 15) (см. диаграмму 1)

Диаграмма 1



Анализ ошибок купирования судебных актах показал, что в ошибочно наиболее часто следующие купируются обычно не данные, купированию: подлежащие заключения дата номер (26%), договора и его дата смерти лица и его инициалы (23%), дата вынесения постановления/решения (20 %), условия договора (10%), инициалы истца или ответчика (8%), временные периоды (7%), адрес и время ДТП (6%) и другие (см. диаграмму 2).

Диаграмма 2



Анализируя полученные данные, мы задались вопросом, почему существует такая большая разница в количестве судебных актов, где нарушены правила купирования. На наш взгляд, такие результаты могут быть следствием большой загруженности суда. Согласно статистическим данным Управления Судебного департамента в Вологодской области, средняя нагрузка судей за 12 месяцев 2018 года в Вологодском городском суде по гражданским и административным делам составила 38 дел на 1 одного судью, в Бабаевском районном суде- 20, в Череповецком городском суде – 23, Никольском

районном суде – 63, Нюксенском районном суде – 12, Сокольском районном суде – 17 [4]. Таким образом, прослеживается закономерность: чем больше загруженность судей, тем больше ошибок при купировании судебных актов. Кроме того, анализ судебных актов показал, что нарушения правил купирования у одного судьи носят однородный характер, ошибки являются типовыми. На наш взгляд, указанное свидетельствует о том, что в данном суде не осуществляется единых контроль за деятельностью по купированию судебных актов. Например, такая ситуация сложилась в Вологодском городском суде Вологодской области. Подытоживая изложенное, отметим, что для судов Вологодской области в большей степени характерна проблема излишнего купирования данных, нежели недостаточного купирования, что само по себе положительно. Показательно, что изначально существовала тенденция максимального купирования индивидуализирующих данных в судебном решении, затем фактов излишнего купирования стало меньше, но данная проблема продолжает существовать. Как представляется, осложняет ситуацию неопределенность законодательного и подзаконного регулирования процедуры изъятия данных и перечня данных, подлежащих изъятию (не определен исчерпывающий перечень данных, подлежащих исключению). Ещё одной причиной является недостаточная правовая грамотность специалистов, осуществляющих купирование судебных решений. Мы предлагаем следующие пути решения проблем излишнего купирования судебных актов:

1. Написание методических разработок по унификации приемов деперсонификации текстов судебных актов. Унифицированный свод правил позволит выполнять грамотное изъятие данных.
2. Законодательное закрепление всех данных, подлежащих исключению. Список данных указанных в статье 15 Закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" следует дополнить указанием на охраняемые законом тайны- врачебную, тайну личной жизни, тайну переписки
3. Регулярный мониторинг деятельности специалистов, занимающихся деперсонификацией, с целью контроля правильности и законности осуществления действий в этой сфере.

1. Федеральный закон от 22.12.2008 N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" // [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_82839/ (дата обращения: 20.10.2019).

2. Федеральный закон от 27.06.2006 N 152-ФЗ "О персональных данных" // [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 17.10.2019).

3. Постановление Президиума Верховного Суда РФ от 27 сентября 2017 г. “Об утверждении Положения о порядке размещения текстов судебных актов на официальных сайтах Верховного Суда Российской Федерации, судов общей юрисдикции и арбитражных судов в информационно-телекоммуникационной сети «Интернет» // [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71684972/ (дата обращения: 31.10.2019).

4. Нагрузка судей районных (городских) судов за 12 месяцев 2018 года// [Электронный ресурс]. URL: http://usd.vld.sudrf.ru/modules.php?name=stat&id=121(дата обращения: 31.10.2019)

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В БАНКОВСКОЙ СФЕРЕ

Ворошилова Екатерина Алексеевна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ядрихинский Сергей Александрович,

доцент кафедры административного и финансового права
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

«Человек свободен,
если он должен подчиняться
не другому человеку, а закону».
Иммануил Кант
«Код - это закон».
Лоуренс Лессиг

В настоящее время технологии развиваются очень активно и применяются во всех сферах общественной жизни – начиная с бытового уровня (смартфоны, «умная бытовая техника») и заканчивая уровнем глобальным (военная техника, космическое оборудование и др.). С каждым годом инновации развиваются и то, что представлялось нам необычным и уникальным некоторое время назад, сейчас является неотъемлемой частью нашей повседневной жизни.

В.В. Путин в ежегодном Послании Федеральному Собранию Российской Федерации отметил: "...в мире сегодня накапливается громадный технологический потенциал, который позволяет совершить настоящий рывок в повышении качества жизни людей, в модернизации экономики, инфраструктуры и государственного управления. Насколько эффективно мы сможем использовать колоссальные возможности технологической революции, как ответим на ее вызов, зависит только от нас. И в этом смысле ближайшие годы станут решающими для будущего страны".[1]

В научном сообществе уже давно активно идут дискуссии на тему проблем правового регулирования и возможностях использования технологии блокчейн в различных сферах общественной жизни. В данной статье будут рассмотрены возможности применения данной технологии в банковской сфере.

Для начала хотелось бы обратиться к теоретическому аспекту такого сложного понятия как блокчейн. Стоит заметить, что оно не относится к числу устоявшихся даже среди специалистов в области IT-индустрии. Возьмем за основу определение, данное А.И. Савельевым: "Блокчейн представляет собой децентрализованную распределенную базу данных ("учетную книгу") обо всех подтвержденных транзакциях, совершенных в отношении определенного актива, в основе функционирования которой лежат криптографические алгоритмы".[2]

Из предлагаемого определения можно выделить следующие признаки, которые характерны для блокчейна: децентрализованный характер хранения информации, безопасность, которая определяется использованием криптографии, автоматизированность и прозрачность.

В соответствии с перечнем поручений главы Российской Федерации от 21 октября 2017 г. N Пр-2132 по итогам совещания по вопросу использования цифровых технологий в финансовой сфере[3] Правительству Российской Федерации совместно с Банком России в рамках реализации программы"Цифровая экономика Российской Федерации", поручено обеспечить внесение в законодательство Российской Федерации изменений, предусматривающих определение статуса цифровых технологий, применяемых в финансовой сфере, и их понятий.

---

[1]Послание Президента Российской Федерации Федеральному Собранию от 1 марта 2018 г. // Парламентская газета. 02.03.2018. N 8.

[2] Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. N 5. С. 96.

[3] Перечень поручений по итогам совещания по вопросу использования цифровых технологий в финансовой сфере // Президент России. URL: http://kremlin.ru/acts/assignments/orders/55899.

Во исполнение указанных поручений разработаны следующие проекты федеральных законов: "О цифровых финансовых активах", "Об альтернативных способах привлечения инвестиций (краудфандинге)", "О системе распределенного национального майнинга". При этом указанные законопроекты прямо не определяют термин "блокчейн".

Наиболее заметной эта технология стала в связи с ажиотажем, возникшим по поводу другого явления, привнесенного эпохой цифровизации, - криптовалют, так как их технологической основой стал именно блокчейн. Уже сегодня его используют для организации документооборота, проведения расчетов, заключения смарт-контрактов, ведения различных реестров и иных целей. Так, например, в своем докладе за 2016 г. главный научный советник Правительства Великобритании предложил создать общеевропейскую систему учета НДС на базе технологии блокчейн. Другой пример - эстонская виртуальная программа электронной регистрации резидентов. Первым актом, официально оформленным с помощью такой системы, стала регистрация брака двух резидентов Лондона родом из Испании.[1]

Как мы видим, в современном обществе огромное количество возможностей применения и использования технологии блокчейн, но самой популярной все же остается финансовый сектор, поэтому остановимся на применении блокчейна в банковской сфере. Банки в силу специфики своей деятельности постоянно должны сверять и согласовывать данные, актуальность которых каждая компания поддерживает в своей базе самостоятельно. При необходимости двустороннего обмена эти процессы слишком медленны и неэффективны. На наш взгляд, блокчейн сможет значительно упростить процесс согласования данных. Хотелось бы отметить основные преимущества возможностей блокчейна в банковской сфере:

1. **Быстрые и дешевые переводы**. Это особенно актуально для трансграничных переводов и микроплатежей, где банковская комиссия может быть сопоставима с суммой перевода. Пока в банках такие транзакции проходят долго (до 3-5 рабочих дней) и стоят дорого (от 1% от суммы). В мировом масштабе это огромные расходы. В криптовалютных сетях переводы занимают несколько минут и стоят существенно дешевле. Так, транзакция на 45,5 тысяч биткоинов (около 280 млн.долл.) летом 2018 года в блокчейне стоила всего $0,04 и прошла за несколько минут. В такую же сумму обошлась транзакция в сети Лайткоин на сумму 100 млн. долл. весной 2018 года.
2. **Возможность автоматизировать процессы и быстро обрабатывать операции.** Это позволяет снизить издержки и сократить штат сотрудников. Блокчейн дает возможность избавиться от сложного документооборота, ведь любую операцию можно проследить. Гарантом неизменности данных служит сама технология, человеческий фактор исключается. Уже есть проекты на блокчейне в сфере выдачи кредитов, идентификации клиентов, корпоративного финансирования.
3. **Обеспечение иммутабельности сделок.** То есть невозможности внести изменения задним числом и подделать отчетность. Банковская система не прозрачна. Блокчейн позволит сделать все операции прозрачными и повысить уровень доверия между всеми участниками.

Обратимся к использованию технологии блокчейн банками РФ. Так, Сбербанк и ФАС России запустили пилотный проект Digital Ecosystem по обмену документами на основе технологии блокчейн, в октябре 2017 г. Сбербанк провел первую в России платежную транзакцию по технологии блокчейн; Альфа-Банк совместно с ООО "Сбербанк Факторинг" и крупнейшим в России ретейлером ПАО "М. Видео" участвовали в разработке открытой

[1]Блокчейн: цепная реакция // EY. URL: http://www.ey.com/Rublication/vwLUAssets/EY-blockchain-tom-rus/SFile/EY-blockchain-tom-rus.pdf.

платформы для применения блокчейн-технологий в области финансирования поставщиков на условиях отсрочки платежа (факторинга); Райффайзенбанк принял участие в проекте Национального расчетного депозитария по выпуску облигаций ПАО "МегаФон" с использованием технологии блокчейн; Альфа-Банк в сделке с S7 Airlines использовал сразу два взаимодействующих смарт-контракта Ethereum: один - только для открытия аккредитива, второй - для его закрытия.[1]

Стоит заметить, что внедрение блокчейна в банковскую сферу представляет собой парадокс, так как суть блокчейна состоит в децентрализации, а банковской системы — в полной централизации и тотальном контроле. Биткоин (как главный пример применения блокчейн-технологий) был создан как альтернатива традиционной платежной системе, то есть в противовес банкам. Другими словами, сейчас в банковскую систему пытаются интегрировать то, что было задумано для ее разрушения.

Инвестиции в блокчейн могут разрушить существующую бизнес-модель банков. Если блокчейн оправдает ожидания, банки смогут предоставлять услуги быстрее, дешевле и проще, что приведет к падению их доходов. Кроме того, под угрозой могут оказаться миллионы рабочих мест. Несмотря на серьезные недостатки существующей банковской системы, у нее есть свои плюсы: есть разработанная регуляторная база, страхование вкладов, возможность отменить ошибочную транзакцию и получить возмещение в случае хакерской атаки. У блокчейн-сетей всего этого пока нет, зато есть много проблем, которые нужно решить: это проблемы с масштабируемостью, пропускной способностью и безопасностью.

Таким образом, можно сделать вывод о том, что на сегодняшний день является очевидным то, что банки, которые уже сегодня используют технологии блокчейн в своей деятельности, в будущем получат огромные преимущества и расширят сферу своего влияния на финансовых рынках.

«ПЕРЕХОД НА ПОЛНОСТЬЮ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ: ЗА И ПРОТИВ»

Логинов Никита Евгеньевич,
студент 2 курса Вологодского Государственного Университета (ВоГУ)
Научный руководитель:
Углицких Дмитрий Васильевич,
и.о. заведующего кафедрой юриспруденции
Вологодского Государственного Университета (ВоГУ), к.ю.н., доцент

В условиях повсеместного развития цифровых технологий всё чаще можно увидеть то, как разные элементы правовой системы переходят в иной, цифровой, формат. Данная тема не является однозначной, учитывая уровень настоящего научно-технического развития. Как и во многих других вопросах мнения делятся на положительные и негативные. Рассматриваемым в данной работе предметом станут электронные документы, а именно проблемы и плюсы от полного перехода всех носителей информации на цифровой формат.

В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»[2] электронные документы, подписанные квалифицированной электронной подписью, приравниваются к документам на бумажном носителе, подписанным личной подписью. По факту электронные документы содержат тот же перечень информации, что и документы на бумажном носителе, однако для полноценного их использования необходимо использовать электронную подпись. Подпись же позволяет определить лицо, подписавшее данный документ, также позволяет определить обнаружить факт внесения изменений в

[1]Нурмухаметов Р.К., Степанов П.Д., Новикова Т.Р. Технология блокчейн: сущность, виды, использование в российской практике // Деньги и кредит. 2017. N 12.
[2] Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ // СПС КонсультантПлюс.

документ после момента его подписания. При том без наличия цифровой подписи документы на данном этапе не будут иметь юридическую силу. Всё это необходимо для обеспечения безопасности документооборота в гражданских и государственных процедурах.

Но отходя от технических деталей, обеспечивающих безопасные способы обмена документами и их заключения, хотелось бы отметить общие плюсы и минусы.

Сначала обратимся к минусам, которые ярко выделяются и не имеют никаких спорных факторов в оценке:

1. При полном переходе на электронные документы гражданским организациям и государственным учреждениям придётся усиленно поддерживать работоспособность архивов и баз, в которых будут храниться все экземпляры электронных документов со всеми необходимыми для их юридического функционирования. Повышение приоритета для подобной деятельности вызовет повышение расходов на содержание технического оборудования. Как бы то ни было, на данный момент и так принимаются меры для поддержания работы этих баз, однако этот пункт на данный момент не имеет завышенного приоритета, так как документы и записи могут храниться на бумажных носителях, и они не зависят от технических сбоев любого вида.

2. Как бы то ни было, но даже в условиях защиты электронного документооборота при помощи института электронных подписей, все цифровые материалы имеют структуру нулей и единиц. Ни одна защита, кроме полной изоляции системы от любой сети, не может гарантировать безопасность баз документов. Кроме вторжения в базы, также можно подделать данные электронной подписи любого уровня. Возможно, специалистов, способных на подобного уровня взломы, мало, однако их существование всё ещё ставит под угрозу весь документооборот вне зависимости от субъектов юридических отношений.

3. Для подобного перехода необходимо снабдить каждый субъект права всеми необходимы техническими средствами. Договоры представляют собой волевое решение субъекта вступить в определённые правоотношения. Если у этого субъекта права не будет возможности изъявлять свою волю или же своими действиями реализовать свои законные права и приобретать обязанности, то он будет фактически лишён дееспособности. Данные последствия недопустимы и будут нарушать принципы конституционного и гражданского права.

4. Для оперирования электронными системами необходимо будет нанимать специального квалифицированного администратора, либо же необходимо повысить навыки работы с электронными ресурсами у населения. При смене поколений такое, разумеется, будет менее востребовано, однако на данном этапе социального развития сохраняется большое число граждан, которые имеют низкие навыки обращения с компьютерами и телефонами современных образцов.

5. При осуществлении полного перехода на электронные документы необходимо будет переносить все бумажные документы в новые электронные базы данных, что несомненно будет являться тяжёлой работой для всего штата любой организации, которая занимается документооборотом. Необходимо будет не только перенести документы, но и проверить правильность внесения их в базы данных.

Учитывая перечисленные выше минусы, может сложиться довольно негативное мнение о полностью электронном документообороте из-за довольно длительного и болезненного переходного периода от смешанной системы документооборота к электронной. Однако подобная система не лишена своих плюсов, от которых едва ли откажется субъект, если минимизировать минусы, которые имеют по большей части временный характер.

Далее будут разбираться плюсы, которые принесёт переход на полностью электронный документооборот. Данные плюсы также не имеют заранее определённой ценности, так как у каждого субъекта есть свои личные приоритеты относительно всех выделенных последствий.

1. При условии полной обеспеченности всех субъектов необходимым оборудованием значительно вырастет обмен информацией между субъектами правоотношений. Как пример

подобного явления можно выделить набирающую популярность портала государственных услуг Российской Федерации. Граждане получили возможность дистанционно подавать все необходимые заявления, оплачивать счета и записываться в очереди к определённому сроку. Пусть некоторые критикуют неудобства доставляемые пользовательским интерфейсом портала, однако он значительно повысил порядок работы органов государства с гражданами.

2. Все электронные базы крайне легко можно структурировать по избранному критерию, что позволит упорядочить любую документацию, которая доступна организации. Например, подобные функции могут не позволить аппарату организации ошибиться при разработке документа, создав документы с одинаковыми номерами.

3. Перевод документооборота в электронную форму характеризуется изменением информационного формата. Нынешние пользовательские интерфейсы обеспечивают наглядность информации, которой оперирует пользователь. При разработке документа есть мгновенный доступ к любому предыдущему документу, разработанному организацией. Это облегчит разработку отсылочных и бланкетных документов, так как любой документ можно будет открыть любой необходимый документ без лишних трат времени. Также в электронном документообороте будет полноценная возможность добавить системы гиперссылок внутри базы данных. Подобные функции реализованы в системе КонсультантПлюс, которые значительно облегчают деятельность юристов любого уровня.

4. Помимо наглядного доступа к документам при их разработке, возможно отслеживать каждый документ в реальном времени и отслеживать его путь от отправителя к получателю, а также наглядно обозначать действительность документа. Подобное также реализовано в правовой системе КонсультантПлюс.

5. При использовании полностью электронного документооборота любой субъект в любом месте, где есть сеть, сможет открыть и изучить необходимый документ. Также любой субъект сможет изменить этот документ без необходимости создавать новый отдельный вариант в случае ошибки. При том, используя институт цифровой подписи, можно будет увидеть, когда были внесены последние изменения в документ.

Как можно заметить, большая часть минусов касается только периода времени, но в перспективе исправятся и исчезнут. Общество в данный момент не готово для резкого перехода на иной формат документооборота, потому необходимо повышать сферу влияния электронного документооборота над бумажным, чтобы минимизировать убытки субъектов правоотношений и проблемы с культурной неподготовленностью. На данный момент можно лишь совершенствовать способы борьбы с вторжением в цифровую сферу недобросовестных лиц. Электронный документооборот будет итогом естественного развития общественных отношений в условиях повышения технических достижений. Сейчас растёт авторитет безналичных способов оплаты, разрабатываются и вводятся электронные личные документы, которые уже являются основой для подобного пути развития. Смена поколений минимизирует слои населения, которые не умеют обращаться с техникой. Развитие пользовательских интерфейсов облегчит взаимодействие субъектов с правовыми сферами, что является хорошим показателем при прогнозировании перспектив перехода на электронный документооборот.

СМАРТ-КОНТРАКТ КАК ПЕРСПЕКТИВА ОФОРМЛЕНИЯ ГРАЖДАНСКИХ ОТНОШЕНИЙ

Суровцева Екатерина Сергеевна –
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Карпикова Людмила Валерьевна,
преподаватель кафедры гражданского права и гражданского процесса
Северо-Западного института (филиала)

Университета имени О.Е. Кутафина (МГЮА)

В последнее время чрезвычайную актуальность приобрели вопросы правового регулирования гражданско-правовых отношений, опосредованных информационными технологиями. Одна из причин актуальности этих вопросов: массовое внедрение со стороны государства указанных технологий. Так, распоряжением Правительства Российской Федерации была утверждена программа до 2024 года «Цифровая экономика Российской Федерации». Главной целью этой программы является то, что она направлена на подготовку концепции по совершенствованию правового регулирования с целью развития цифровой экономики.

Сегодня мы являемся свидетелями разработки и распространения в обществе совершенно новых технологий, например, Blockchain, главная цель которых: улучшение жизни граждан.

Сразу разберемся с понятием. Блокчейн – (от англ. blockchain – цепочка блоков) распространенная база данных, устройства хранения которой не подключены к общему серверу[1].

Если говорить простыми словами, то смарт-контракт – самоисполняемый компьютерный код, который записывается в блокчейн и хранится на множестве компьютеров. Смарт-контракт или «умный» контракт позволяет обмениваться активами – акциями, деньгами, другими видами собственности без участия посредников.

Представим такую ситуацию: у вас есть загородный дом, который вы намерены продать, и есть покупатель, который намерен купить. На сегодняшний момент для того, чтобы совершить эту сделку, необходимо обратиться в различные финансовые, нотариальные и иные организации, а также уплатить госпошлины и иные взносы. А с помощью смарт-контракта это можно сделать напрямую.

То есть, продавец – компьютерный код – покупатель. У нас все тот же загородный дом, продавец и покупатель договорились о том, что при достижении определенного условия – поступление оплаты посредством Bitcoin, другая сторона осуществляет передачу загородного дома. Эти отношения были оформлены в виде «умного» контракта на основании Blockchain. Система получает данные о том, что оплата произведена, а значит, дом переходит в собственность нового владельца. Никакой дополнительной авторизации или подтверждения со стороны получателя товара не требуется - все условия были заданы изначально сторонами, и сам компьютер контролирует их выполнение.

«Умные» контракты демонстрируют новый этап в развитии автоматизации договорных отношений: они могут не только заключаться без участия человека, но и исполняться без участия человека. При этом исполнение договора в данном случае предполагает автоматизированную передачу определенного актива[2].

На основании изложенного можно сделать вывод о том, что «умный» контракт - это договор, существующий в форме программного кода, действующего на платформе Blockchain, который обеспечивает автономность и самоисполнимость условий такого договора по наступлению заранее определенных в нем обстоятельств.

Разрешение правовых споров, возникающих при использовании «умных» договоров - задача суда. Как и любое судебное доказательство смарт-договор должен представлять собой совокупность фактов, способных подтвердить имеющие значения для правильного разрешения судебного дела.

С 1 октября 2019 года вступили в силу изменения в базовые положения Гражданского Кодекса РФ, касающиеся цифровых прав, а также ряд связанных с ними изменений. В

[1] https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD

[2] Савельев А.И. Статья: Договорное право 2.0: "умные" контракты как начало конца классического договорного права "Вестник гражданского права", 2016, N 3.

обновленной редакции Гражданского Кодекса РФ делается попытка для дальнейшей легализации смарт-контрактов как способа исполнения обязательств по договору.

В статье 309 Гражданского Кодекса РФ добавлен абзац, который разрешает исполнение обязательств без совершения какого-либо волевого акта, но с применением информационных технологий.

Эксперты утверждают: смарт-контракты можно разумно использовать для типовых, повторяющихся сделок (поставка, аренда, аккредетивы, обеспечение тендеров, лицензионные платежи), исполнение которых легко отследить.

Разберем на примере выборов в государстве. Если перевести все базы данных в электронный вид и подключить к ним смарт-контракт, можно добиться законных выборов. По всему миру известны приписки «мертвых душ» за того или иного кандидата. Если оракул (по запросу контракта предоставляет достоверные данные, необходимые для корректной работы контракта) обнаружит в системе свидетельство о смерти, он обнуляет голос.

Другим примером являются наследственные права. В скором времени деятельность нотариусов, которые бережно оформляют и хранят ваш договор, будет в меньшей степени. С помощью этой технологии можно добиться автоматической передачи всех средств и прав после вашей смерти определенному человеку.

Следует отметить, Государственная Дума Российской Федерации на пленарном заседании 16 октября 2019 года приняла в первом чтении поправки в Основы законодательства Российской Федерации о нотариате, касающиеся нового этапа развития электронного нотариата в рамках национальной программы «Цифровая экономика»[1]. Закон дает возможность участникам электронного делопроизводства сэкономить время на удостоверении документов и сделок. При оформлении сделок можно будет обмениваться электронными сообщениями, а не бумажными документами.

Рассмотрим пример смарт-контракта в недвижимости. Впервые в мире квартира подобным образом была продана в Украине на правом берегу Киева. Для проведения сделки использовался смарт-контракт Эфириума (виртуальная машина), а также децентрализованный американский маркетплейс Propy (международный рынок недвижимости). Покупателем стал советник этой площадки, а также основатель издания TechCrunch Майкл Аррингтон. Оплата происходила в криптовалюте Эфириум. На данном этапе развития смарт-контрактов процесс происходил так:

1. Покупатель и продавец заключили контракт, и покупатель внес депозит, необходимый для оплаты жилья.
2. Поскольку участники сделки находились в разных уголках мира, с помощью площадки локальному представителю покупателя была выдана доверенность от его имени, удостоверенная местным нотариусом.
3. Propy предпринимает необходимые действия по проведению сделки — оплата работы оценщика, всевозможных сборов.
4. Продавец встречается с представителем покупателя у нотариуса для подписания документов.
5. Происходит перерегистрация права собственности на покупателя — данные вносятся в реестр.
6. Как только смарт-контракт получает данные из реестра, он разблокирует деньги, и они переходят к продавцу.

Вот так выглядит часть контракта. Здесь описан процесс подписания договора участниками, а недвижимость замораживается в ожидании завершения процесса.

1 http://duma.gov.ru/news/46634/ Приняты в первом чтении поправки о «цифровом нотариате».

```
function sign(string _hash) returns(bool) {
  if (selledId == msg.sender)
    sellerSigned = true;
  if (buyerId == msg.sender)
    buyerSigned = true;
  if (brokerId == msg.sender)
    brokerSigned = true;

  if (sellerSigned && buyerSigned && brokerSigned) {
    metaPA = _hash;
    status = Status.payment;
    StatusUpdate(status);
    PropertyManager proeprtyManager =
        PropertyManager(propyContractAddress);
    assert(propertyManager.setPropertyToPendingState(propertyId));
  }
  updatedAt = now;
  return true;
}
```

Таким образом, перспективы у смарт-контракта поистине огромные. Эти перспективы способны кардинально изменить многие сферы жизни общества: от недвижимости до страхования, голосования на выборах и многое другое. Но стоит отметить, что технология Blockchain все еще находится на стадии тестирования, и после того, когда работа устройства будет многократно протестирована и не останется изъянов, данная технология получит свое признание в обществе, в том числе как система оформления гражданских отношений без посредников и лишних затрат.

СУДЕБНАЯ ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Зыков Александр Иванович,
студент 4 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Страхов Сергей Евгеньевич,
старший преподаватель кафедры государственно-правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)

На современном этапе перехода Российской Федерации к «цифровому» обществу защита интеллектуальных прав должна являться одним из наиболее приоритетных направлений правового регулирования. Применение в различных областях человеческой деятельности таких цифровых технологий, как Интернет, блокчейн, виртуальная реальность, социальные сети, цифровые технологические платформы, использование искусственного интеллекта и робототехники, повлекло за собой предпосылки для формирования нового гражданско-правового регулирования вновь образуемых отношений.

В правовой среде возникало достаточно много дискуссий о соотношении информации и интеллектуальной собственности, выдвигались предложения об абсолютизации права на информацию. Как представляется, отождествление информации и охраняемых объектов интеллектуальной деятельности является неверным[1]. Для решения проблемы абсолютного права на информацию в Гражданский кодекс Российской Федерации (далее – ГК РФ) были внесены изменения – ст. 783.1 ГК РФ, предусматривающая новую правовую конструкцию – договор об оказании услуг по предоставлению информации.

Отечественное гражданское законодательство в ст. 1248 ГК РФ предусматривает юрисдикционную форму защиты, включающий общий (судебный) и специальный (административный) порядки. Административный порядок применяется только в исключительных случаях, перечень которых определен в указанной выше статье: подача и рассмотрения заявок на выдачу патентов на изобретения, полезные модели, промышленные образцы, товарные знаки и прочие[2].

В нашем научном исследовании рассмотрим судебный порядок защиты интеллектуальных прав и их основные проблемы. Для начала проанализируем, какие именно объекты подлежат защите. Так, в ст. 1225 ГК РФ указан исчерпывающий перечень объектов, на которые распространяет действие право интеллектуальной собственности, например, произведения науки, литературы, искусства, полезные модели, промышленные образцы и прочие. В соответствии со ст. 1226 ГК РФ интеллектуальные права включают в свой состав исключительное, личное неимущественное и иные права (право следования, право доступа).

В соответствии с ч.1 ст. 44 Конституции Российской Федерации предусматривается и гарантируется защита интеллектуальной собственности. Конституционный Суд РФ в своих постановлениях указывал, что на суды возложена обязанность применять положения законодательства об интеллектуальной собственности исходя из системной взаимосвязи с основами гражданского законодательства, а также в контексте общеправовых принципов равенства, справедливости, учитывая требование соразмерности, и, соблюдая баланс частных и публичных интересов[3].

Рассмотрение дел, связанных с разрешением споров о защите интеллектуальных прав, относится к компетенции арбитражных судов, специализированного арбитражного суда – Суда по интеллектуальным правам и судам общей юрисдикции (Московский городской суд). Вопросы о разграничении компетенции между судами определяются на основании ст.ст. 22, 24, 26, 27 Гражданского процессуального кодекса (далее – ГПК), ст.ст. 27, 28, 33, 34 Арбитражного процессуального кодекса (далее – АПК РФ), гл. IV.1 ФКЗ «Об арбитражных судах в Российской Федерации»[4].

Актуальными вопросами при осуществлении судебной защиты интеллектуальных прав в условиях цифровизации можно назвать следующее.

Во-первых, возникают проблемы при определении роли администратора домена как информационного посредника. Любой вид ответственности предполагает доказательно объективных и субъективных признаков состава того или иного правонарушения. При подаче иска в суд необходимо выяснить надлежащего ответчика, что в свою очередь не означает снятие бремени доказывания отсутствия вины с такого лица. Для решения

---

[1] С.В. Усольцева. Правовое регулирование интеллектуальной собственности в условиях цифровой экономики. (Обзор законопроектной работы) // Право будущего: Интеллектуальная собственность. Инновации. Интернет: Ежегодник. Вып. 1 / РАН. ИНИОН. Центр. социал. науч.-информ. исслед. Отд. правоведения;. Каф. предпринимательского права МГУ им. М.В. Ломоносова. Отв. ред. Афанасьева Е.Г. – М. 2018. – С. 21.

[2] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ // Российская газета. № 289. 22.12.2006.

[3] Постановление Конституционного Суда РФ от 13.02.2018 № 8-П. По делу о проверке конституционности положений пункта 4 статьи 1252, статьи 1487 и пунктов 1, 2 и 4 статьи 1515 Гражданского кодекса Российской Федерации в связи с жалобой общества с ограниченной ответственностью ПАГ // Официальный интернет-портал правовой информации http://www.pravo.gov.ru.15.02.2018.

[4] Федеральный конституционный закон от 28.04.1995 № 1-ФКЗ. Об арбитражных судах в Российской Федерации. // Собрание законодательства РФ. 01.05.1995. № 18. ст. 1589.

обозначенной проблемы Судом по интеллектуальным правам (далее – СИП) был выработан подход для квалификации действий лиц, которые выполняют функции информационного посредника. СИП в Постановлении № А56-81870/2018 от 26.02.2019 г. оценил доводы, согласно которым следовало осуществить рассмотрение дело в отсутствии администратора домена, на котором размещен сайт, содержаний сведения, которые нарушают исключительные права заявителя. Судом было указано, что для доведения информации до всех пользователей в сети Интернет должны принимать участие следующие субъекты:

- администратор домена;
- владелец сайта;
- регистратор доменов;
- провайдер хостинга;
- лица, которые размещают ссылки поисковой системы.

Решение вопросов об отнесении выше указанных лиц к информационным посредникам и о привлечении их к ответственности или предъявлении к ним требований о пресечении нарушения, зависит от характера деятельности, которую они осуществляют[1]. Судом было принято решение, что в случае отсутствия доказательства совершения лицом действий, которые на направлены на нарушение исключительных прав, то привлекать его в качестве третьего лица не требуется.

В соответствии с абз. 3 п.78 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» презюмируется, что владельцем сайта является администратор доменного имени, адресующего на соответствующий сайт[2].

В Постановлении Президиума СИП от 28.03.2014 г. № СП-21/4 закреплено, что у администратора доменного имени отсутствует возможность снять с себя или переложить ответственность за нарушение исключительного права на другое лица даже путем заключения договора, например, договора об аренде доменного имени[3].

Заслуживает внимания дело из судебной практики Великобритании. Судом рассматривается первый в судебной практике иск к биржевому искусственному интеллекту. Саматур Ли Кин-Кан подал в суд на компанию Tyndaris Investments, в связи с неудовлетворительными результатами работы ее искусственного интеллекта. Генеральный директор компании рассказал истцу о возможностях нового искусственного интеллекта, который использовался для извлечения максимальной прибыли при работе с автоматизированными интерфейсами хедж-фондов. Истец предоставил возможность искусственному интеллекту управлять своим капиталом, но понес одни убытки.Данный случай — первый прецедент судебного разбирательства, связанного с потерей финансов из-за действий искусственного интеллекта[4].

Во-вторых, вопрос о программе, как совокупности дистрибутива и базы данных. В Постановлении Пятнадцатого арбитражного апелляционного суда от 08.06.2009 г. по делу № А53-15817/2008-С2-32 указано, что под дистрибутивом (программой для ЭВМ для первоначальной установки программного обеспечения) понимается форма распространения

[1] Постановление Суда по интеллектуальным правам от 26.02.2019 N С01-1271/2018 по делу N А56-81870/2018 // URL: http://ras.arbitr.ru/.

[2] Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10. О применении части четвертой Гражданского кодекса Российской Федерации. // Российская газета. № 96. 06.05.2019.

[3] Постановление Президиума Суда по интеллектуальным правам от 28.03.2014 № СП-21/4. Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров. // URL: http://ipcmagazine.ru/official-cronicle/the-questions-that-arise-when-considering-domain-disputes.

[4]Суд рассматривает первый в истории иск к биржевому искусственному интеллекту // URL: https://www.techcult.ru/robots/6761-sud-rassmatrivaet-pervyj-isk-k-birzhevomu-iskusstvennomu-intellektu

программного обеспечения, которая содержит программы для инициализации системы, программу-установщик, набор специальных файлов, которые образуют ядро программы[1].

Так, СИП в Постановлении от 16.10.2018 г. по делу № А53-27792/2017, воспроизведя приведенную формулировку, отметил: "Вместе с тем в случае если на жестком диске содержится и работоспособная запись программы для ЭВМ, и дистрибутив программы с названием этой же программы, для установления факта нарушения исключительного права, обусловленного наличием такого дистрибутива, подлежит установлению факт различия между исходными кодами установленной программы и дистрибутива, поскольку, как правило, установленная программа и ее дистрибутив являются одной и той же компьютерной программой, так как в их основе лежит одинаковый исходный код[2].

Таким образом, СИП разъяснил, что использование программы для ЭВМ, содержащей базу данных, образует, во-первых, нарушение исключительного права на дистрибутив, благодаря которому устанавливается оболочка программы, а во-вторых, право на саму базу данных. При этом для установления факта использования самой программы необходимо соотнести исходный код дистрибутива и базы данных[3].

Подводя итоги работы, необходимо отметить, что отечественное законодательство требует дальнейшей модернизации для того, чтобы обеспечить соответствие правовой охраны обладателей интеллектуальных прав запросам общества и новым возможным моделям бизнеса. Суды должны принимать решения, которые будут обеспечивать надлежащую охрану результатов интеллектуальной деятельности, поощрения инноваций, появлений новых товаров, работ и услуг.

КИБЕРПРЕСТУПНОСТЬ КАК НОВАЯ КРИМИНАЛЬНАЯ УГРОЗА

Селякова Мария Вячеславовна,
студент 4 курса Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА)
Научный руководитель:
Попаденко Елена Викторовна,
доцент кафедры государственно правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е.Кутафина (МГЮА), к.ю.н., доцент

XXI век – эпоха информационного общества. Компьютеры и коммуникационные системы охватили все сферы жизнедеятельности общества и государства, а глобальная сеть Интернет предоставляет неограниченные возможности для развития информационных технологий. В условиях цифровизации возникла новая форма преступности – киберпреступность. Особенностью совершения таких преступлений являются их дистанционный и даже трансграничный характер преступных действий когда в условиях отсутствия физического контакта преступник, объект преступного посягательства и потерпевший могут находиться на территориях разных государств; возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно;

[1] Постановление Пятнадцатого арбитражного апелляционного суда от 08.06.2009 № А53-15817/2008-С2-32 // URL: http://kad.arbitr.ru/Card/4798aa2f-4d38-469a-ad2b-640158a38a83.
[2] Постановление Суда по интеллектуальным правам от 16.10.2018 N С01-658/2018 по делу № А53-27792/2017 // URL: http://ras.arbitr.ru/.
[3] Постановление Суда по интеллектуальным правам от 27.07.2015 № С01-553/2015 по делу N А53-17988/2014 // URL: http://ras.arbitr.ru/

многоэпизодный характер деяния при множественности потерпевших, которые могут и не подозревать, что они подверглись преступному воздействию[1].

Следует отметить, что если в конце XX века доля таких преступлений была невелика, то по данным Генеральной Прокуратуры РФ только за период январь-август 2019 года правоохранительные органы России выявили 180 тыс. преступлений, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[2]. Приведенные данные позволяют говорить о том, что преступления с использованием компьютерных сетей стали обычными формами преступности.

В виду этого у мирового сообщества возникла обеспокоенность по поводу того, что компьютерные сети и электронная информация могут использоваться для совершения деяний, представляющих угрозу как для частных лиц, так и для государств. В силу сказанного существует необходимость в разработке и осуществлении общей политики в противодействии киберпреступности как на национальном уровне, так и на международной арене. И здесь мы сталкиваемся с рядом проблем.

1.Определение термина «киберпреступности». Простой анализ термина «киберпреступность» подсказывает, что это преступность в киберпространстве, под которым понимается «физическое и нефизическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи»[3]. Таким образом, кибирпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных[4]. С этой позиции, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. В этой связи возникает вторая проблема.

2.Определение круга деяний, относимых к киберпреступлениям. Так, в России традиционно к киберпреступлениям относят неправомерный доступ к компьютерной информации (ст. 272 УК РФ), распространение вредоносных компьютерных программ (ст. 273 УК РФ), а также мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Ограничиваются ли киберпреступность только указанным перечнем составов преступлений? Очевидно, что нет.

На международной арене закреплены закреплены иные составы киберпреступлений. Так, Конвенция "О преступности в сфере компьютерной информации" 2001 года делит преступления на четыре группы и в каждой предусматривает несколько составов преступлений:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ; противозаконный перехват; воздействие на данные; воздействие на функционирование системы; противозаконное использование устройств);
- правонарушения, связанные с использованием компьютерных средств (подлог с использованием компьютерных технологий; мошенничество с использованием компьютерных технологий);
- правонарушения, связанные с содержанием данных (преступления, связанные с детской порнографией);

[1] Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. - №1. –С.104-106. – URLhttps://moluch.ru/th/9/archive/66/2365/ (дата обращения: 24.11.2019).

[2] https://genproc.gov.ru/smi/news/genproc/news-1703326/ (дата обращения: 24.11.2019).

[3]https://docplayer.net/17880697-Itu-toolkit-for-cybercrime-legislation.html (дата обращения: 25.11.2019).

[4] Кашлев Ю.Б. Становление глобального информационного общества и место России // Информация. Дипломатия. Психология. — М., 2002. — С. 18—20.

- правонарушения, связанные с нарушением авторского права и смежных прав[1].

Вместе с тем сегодня такие информационно-коммуникационные технологии как Интернет могут быть использованы не только как средство и способ совершения преступлений, но и как политический инструмент. Примером могут послужить события вокруг Украины, когда информационные технологии активно используются сторонами конфликта для формирования и продвижения выгодной для себя версии на международной арене. В этой связи «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества» 2009 года упоминает о следующих деяниях, которые также следует относить к проявлениям киберпреступности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) угроза безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер[2].

Помимо уже упомянутых международных договоров сегодня международным сообществом разработано еще несколько соглашений в области борьбы с киберпреступлениями: Конвенция Совета Европы о киберпреступности и Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества, а также Конвенция о кибербезопасности и защите личных данных Африканского союза, Соглашение о сотрудничестве государств – членов Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, Директива 2013/40/EU Европейского парламента и Совета Европейского союза об атаках на информационные системы, Конвенция о борьбе с преступлениями в области информационных технологий арабских государств. Однако, все перечисленные соглашения имеют рекомендательный характер. Вместе с тем для противостояния киберпреступности необходимо создание единых унифицированных правил борьбы с таким преступлениями. Главной целью создания универсального акта в данной сфере является модернизация правовых норм, регулирующих отношения по борьбе с киберпреступностью и обеспечение единства норм международного и национального права с целью наиболее быстрого расследования преступлений и розыска преступников, а также осуществление сотрудничества между государствами. Предпосылками для принятия единого международного акта по предотвращению киберпреступлений являются:

- отсутствие единого для всех государств перечня составов преступлений, которые попадают под понятие «киберпреступления» (например, виновный может скрываться на территории иностранного государства, где отсутствует состав преступлений, предусматривающий наказание за совершенные им действия и, следовательно, остается безнаказанным);
- существование пробелов и противоречий в национальных законодательствах различных стран, что не позволяет выработать единый ход расследования киберпреступлений и задержания киберпреступников в наиболее короткие сроки.

---

[1] «Конвенция о преступности в сфере компьютерной информации» ETS № 185 от 23.11.2001 года https://base.garant.ru (дата обращения: 25.11.2019).

[2]«Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» от 16.06.2009 года http://docs.cntd.ru (дата обращения: 25.11.2019).

Таким образом, международное сотрудничество по борьбе с киберпреступностью активно развивается: принятые международно-правовые акты создают основу для дальнейшего формирования единой международно-правовой политики противодействия киберпреступности.

НЕОБХОДИМОСТЬ ОТВЕТСТВЕННОСТИ МЕДИЙНЫХ ЛИЦ ЗА СОДЕЙСТВИЕ ПРЕСТУПНИКАМ ПУТЕМ ОКАЗАНИЯ ИМ РЕКЛАМНЫХ УСЛУГ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Ямпольская Татьяна Вадимовна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Ни для кого не секрет, что преступность развивается вместе с человечеством. Стоит освоить новые каналы связи, так сразу к ним подсоединяются и различного рода преступники. А порой преступные схемы развиваются столь стремительно, что за ними не успевает законодатель. Сейчас с точностью можно сказать, что многие способы хищений претерпели значительные изменения под действием новых информационных технологий и давно вышли на новый уровень. Например, самые активные финансовые пирамиды и мошеннические схемы активны только в интернете. Однако, чем более совершенными становятся схемы, тем менее доверчивыми становятся обыватели.

Как же злоумышленник может добиться совершения определенного действия от будущего потерпевшего? Разумеется, он может втереться в доверие и долго пытаться выманить имущество. Однако никто не гарантирует, что данное лицо будет расположено к такому виду обмана. Именно в этом случае и подключают информационные технологии и медийных лиц.

Уже почти никто не верит всплывающей рекламе в интернете, а у многих и вовсе подключен AdBlock, прошли те времена, когда улыбчивое лицо на яркой рекламной вывеске могло гарантировать приток клиентов. Граждане не доверяют малоизвестным лицам. А создание личного бренда требует больших затрат, да и успех при данном подходе не гарантирован. Именно тут в схеме и появляются медийные лица.

Они и являются тем самым фильтром, который переводят обывателей на ресурсы злоумышленников. В данном случае, для участников преступной схемы решается несколько важных задач:

1- Они получают информационную поддержку.

2- Медийное лицо повышает доверие к данному ресурсу.

3- Медийное лицо фильтрует обывателе и на ресурс переходят уже заинтересованные лица.

В свою очередь медийное лицо чаще всего осведомлено о том, что оказывает рекламные услуги лицам, чьи деяния имеют признаки состава преступления, но получая значительно больший гонорар нежели при предоставлении обычных рекламных услуг соглашается.

Почему же такую важную роль в совершении данных деяний теперь играет реклама? Обратимся к примерам.

Первым примером могут послужить случаи со «StartCom[1]»и «Cashbery»[2]. В отношении данных проектов на сегодняшний день нет каких-либо судебных решений или уголовного преследования, однако существую реальные признаки преступления, предусмотренного статьёй 172.2 УК РФ[3]. Обе организации на данный момент прекратили выплаты вкладчикам. А отсутствие реальных активов и активная рефренная программа даёт основания полагать, что имела место организация деятельности по привлечению денежных средств физических лиц в крупном размере, при которой выплата дохода лицам, чьи денежные средства привлечены ранее, осуществляются за счет привлеченных денежных средств иных лиц при отсутствии инвестиционной и иной законной предпринимательской или иной деятельности, связанной с использованием привлеченных денежных средств и иного имущества, в объеме, сопоставимом с объемом привлеченных денежных средств и иного имущества. Ситуация осложняется тем, что обе возможные пирамиды инвестировали «в будущее», а именно Bitcoin и прочие криптовалюты, виртуальную реальность, 3D-концепты, искусственный интеллект и робототехнику. Проще говоря, вопрос о финансовых вложениях сложно проверяем. Однако Центробанк уже объявил компанию «Cashbery» финансовой «пирамидой»[4].

Вопрос о деятельности данных организаций возник почти сразу после их появления на рынке. Большие гонорары блогерам, калькулятор доходности (точной прибыли) на сайте, нежелание разрешать в суде споры с теми, кто говорил об обмане в медиа пространстве, отзывы пользователей. Всё это свидетельствует о спорном характере деятельности данных организаций. Однако блогеры считают возможным рекламировать подобные проекты и привлекать людей по своим реферальным ссылкам (с каждого привлеченного они получают свой процент или фиксированную сумму). Но почему мы можем утверждать, что именно медийное лицо занимает важнейшую роль в привлечении вкладчиков? На это указывают сами потерпевшие в частности в своей петиции на сайте www.change.org под названием: «Привлечь к уголовной ответственности организаторов пирамиды Startcom». В данной петиции они также приводят список известных блогеров и каналов на YouTube, поверив которым они вложили свои денежные средства в данный проект. Фактически, не увидев рекламу от лица, к которому у них сформировалась определенная симпатия, потерпевшие не вложили бы деньги.

Вторым примером может послужить реклама, связанная со ставками на спорт, а именно с букмекерскими конторами и каперами. В первом случае показательным был случай с 1xBet[5], где менялись коэффициенты по ходу матчей, блокировались и взламывались аккаунты. Однако даже при наличии огромного количества негативных отзывов, официального запрета деятельности на территории РФ, многие медийные лица продолжают рекламировать данную контору, как «честного букмекера», не забывая прикреплять свою реферальную ссылку. Во втором случае рекламируют 100% точные прогнозы на спорт и лиц их предоставляющих. Чаще всего процент верных прогнозов совпадает с числом случайного угадывания и никак не соответствует заявленным 100%[6].

Третьим примером могут послужить экстрасенсорные и другие оккультные услуги. Здесь можно сослаться на нашумевшее журналисткое расследование Бориса Соболева «Идущие к черту». В чем же здесь заключается роль медийных лиц? По телевиденью

---

[1] https://loxotrona.net статья «Развод Стартком (startcom.pro)! Как раскрутить ХАЙП и создать фейковые отзывы».

[2] Официальный сайт газеты «Известия» https://iz.ru Окончательно вывели: «Кэшбери» обещает выплаты со 2 ноября. Клиенты финансовой пирамиды и эксперты не верят в это. Автор: Анастасия Алексеевских, Татьяна Гладышева.

[3] https://modusvivend.ru Статья: «Кэшбери рухнул как по маслу».

[4] Официальный сайт газеты Комерсантъ статья: Деньги инвесторов «Кэшбери» ушли «на каникулы» https://www.kommersant.ru/daily?from=header_gazeta.

[5] YouTube канал «ДВИЖНОВ» https://www.youtube.com/channel/UCwmiOABPxkm40Cins7luBZA.

[6] https://loxotrona.net Статья: «Как обманывают капперы в ставках на спорт: отзывы, схемы развода, мошенники».

транслируется передача, где заслуженные скептики: Марат Башаров, братья Сафроновы доказывают, что экстрасенсорные способности – это не миф, и у лиц, участвующих в этом шоу, они есть. Хоть ведущие призывают не ходить на приемы к экстрасенсам, однако на фоне подтверждаемых чудес, это выглядит весьма несостоятельно. Как показало то же расследование, а также участие некоторых экстрасенсов на премии имени Гари Гудини, сверх способностями участники передачи не обладают. Однако, благодаря подобным передачам и участию в них медийных лиц, граждане нашей страны охотно идут на приемы, оставляя там крупные суммы денег.

Есть установленные случаи мошенничества в данной сфере, подтвержденные приговором суда. Например, дело центра парапсихологии и коррекции судьбы «Мерлион»[1]. Здесь рекламным лицом предстал ведущий «Необъяснимо-но факт» Сергей Дружко. По данным из СМИ мы можем утверждать, что примерная сумма ущерба для граждан от деятельности данного центра составляло около 150 млн в месяц[2].

Что же объединяет все эти случаи? Лицо, которое фактически помогало мошенникам привлечь аудиторию не в одном из случаев не понесло и скорее всего не понесет никакой ответственности, хотя его участие является одним из основных условий успеха схемы. Без известных лиц рекламная компания мошенников не имела бы успеха или не смогла бы причинить настолько значимый ущерб гражданам. Однако на данный момент не один вид юридической ответственности по отношению к данным лицам не применим.

СТАТЬЯ 159[6] УК РФ, КАК ПРЕСТУПЛЕНИЕ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Цветов Павел Сергеевич,
студент 4 курса Вологодского государственного университета (ВоГУ)
Научный руководитель:
Углицких Дмитрий Васильевич,
и.о. заведующего кафедрой юриспруденции
Вологодского государственного университета (ВоГУ), к.ю.н.

В настоящее время действие уголовного закона во времени и в пространстве охватывает достаточно большое количество групп общественных отношений. Законы являются живыми – они появляются и изменяются при необходимости, если меняется сами устои жизни общества. К негативным же последствиям этого является то, что злоумышленники никуда не пропадают, а наоборот начинают адаптироваться, чтобы научится обходить те или иные нормы в будущем. В современном мире идет очень быстрыми темпами развитие информационной составляющей в обществе. Телевиденье, интернет все это внедряется в нашу жизнь все плотнее и глубже. В тоже время и злоумышленники, зная это начинают придумывать различные способы совершения преступления, но уже с использованием информационных технологий. Именно поэтому законодатель вносит изменения в действующий закон, чтобы в случае совершения таких действий, была возможность привлечь лиц к уголовной ответственности. Однако из этого вытекает немаловажная проблема, которая, к сожалению, мешает вменению данной статьи лицам, за преступные деяния. Суть проблемы заключается в сложности поиска и обнаружения лиц, в сети интернет. Вся эта система настолько глобальна, что существуют различные способы, которыми пользуются злоумышленники, вследствие чего их потом невозможно отследить или установить исходные данные, для установления личности виновного.

Именно поэтому необходимо говорить об этих проблемах, ведь научные исследования продолжаются в различных сферах, в том числе и в информационном пространстве, и

[1] Приговор № 1-16/2015 1-385/2014 от 24 апреля 2014 г. по делу № 1-16/2015.
[2] https://www.vesti.ru Статья: «Империя обмана: в Москве судят псевдоцелителей из "Мерлиона"».

возможно появится какой-нибудь механизм, для более упрощенного и точного поиска преступников, совершающим преступление в этой сфере[1].

Итак, для того чтобы определиться с тем, какие действия будут являться преступными, предусмотренными статьей 159^6 УК РФ, нужно сначала определить, что в общем считают за преступления в сфере высоких технологий. Своего рода киберпреступность это совершение преступления лицами, с использованием информационных сетей, как способы совершения преступления. Достаточно большой перечень преступлений, которые могут быть совершены в сети интернет, к ним, например можно отнести – распространение вредоносных программ, злом учетных записей различных пользователей, распространение противоправной информации (клевета, ложная доносы или ложное сообщение о преступлении) и другие. В этих случаях такие преступления в какой-то степени будут нести большую общественную опасность, чем преступления совершенные при обычных условиях и обстоятельствах. Дело в том, что информационные сети они достаточно обширны и распространяют свое действие на неопределенный круг лиц, тем самым может возникнуть ситуация, что ложное сообщение о террористическом акте увидят несколько миллионов человек, и резонанс будет в несколько сотен раз больше, чем объявлять об этом на улице. Конечно все, о чем мы говорим, это довольно субъективное мнение, но необходимо понимать, что интернет своего рода является одной большой площадкой, на которой огромное количество людей, общается обменивается различной информацией и т. д. В тоже время злоумышленники, тоже являясь частью этой сети могут с помощью специальных средств завладеть той или иной информацией, что в свою очередь уже является явным видом хищения[2].

Теперь нам необходимо обратиться к самой статье уголовного кодекса, с целью изучения. Сама по себе статья 159^6 включает в себя преступление против собственности, а именно мошенничество в сфере компьютерной информации. Законодатель перечисляет нам, какие именно действия будут считаться незаконными и попадать под эту статью. К таким действиям относят – ввод; удаление; блокирование; модификация компьютерной информации, или любого иного вмешательства в функционирование средств хранения информации, обработки или передачи компьютерных сетей с целью хищения имущества или приобретении права на чужое имуществ[3]. Из фабулы статьи нам становится понятно, что довольно больше количество действий, а учитывая фразу «либо иного вмешательства» можно говорить о неограниченности действий, за которые предусмотрена ответственность вместе с этим привносит определенную сложность для определения виновности лиц, а также вопросы привлечения к ответственности. Довольно сложно в настоящий момент обнаружить, а что самое главное доказать вину тех или иных лиц, совершивших преступление. Конечно, разумеется, проводятся экспертизы и устанавливается от куда именно и с какого устройства были совершены действия, явившиеся причиной похищения какой-либо информации. Но в свою очередь преступники, также разрабатывают специальные программы для сложности отслеживания сигнала или смены электронного адреса, благодаря которому невозможно будет установить местоположение злоумышленников. Таким образом проблема и будет заключаться в сложности применения данной статьи, как и в принципе большинства статей, связанных с преступлениями в сфере высоких технологий. На сегодняшний день, следственным органам для раскрытия таких дел, все чаще приходится обращаться к специалистам в этой области, ведь без специальных знаний найти преступника будет достаточно сложно. И с каждым годом число дел, возбуждающихся по данным основаниям, только растет, поскольку как уже было сказано раннее, наш законодатель развивается вместе с обществом, но в тоже время и преступники также развиваются, ищут новые способы для

[1] Воронин М. Ю, Смольянинов Е. С. Уголовная политика в сфере высоких технологий // Закон и право. 2018. № 1.

[2] Доровских Л. А. Преступления в сфере высоких технологий. Киберпреступность // 2016. № 4 (28).

[3]"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 04.11.2019)УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации.

совершения преступления. Поэтому разработка и исследование таких статей, как 159[6] необходимо, ведь для того, что бы соблюдать принцип неотвратимости уголовного права необходимо понимать, что нет ни одного поля, хоть правового, или общественного, где были бы бессильны органы следствия, что говорит о полной свободе действий со стороны злоумышленников, такого нельзя допускать и в случае исследования и изучения таких информационных технологий в дальнейшем станет намного проще при расследовании других, похожих дел.

И в заключение необходимо сказать о том, что на данном этапе весь мир развивается быстрыми темпами. Уже давно отходят на второй план вооружение страны или ее промышленный потенциал, сейчас идет борьба за технологии в том числе и информационные. На современном этапе все важные события в геополитике не обходятся без использования информационных технологий, но в тоже время все страны негласно пытаются заполучить информацию другой страны, либо как-то на нее повлиять. И поскольку даже на таком высоком уровне идет борьба за информацию, то на законодательном уровне внутри страны обязательно необходимо наличие правового акта, регулирующего такие отношения, но главное – они должны быть живыми, должны применяться для нормальной работы государства и общества в целом.

Список использованных источников:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 04.11.2019)УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации
2. Воронин М. Ю, Смольянинов Е. С. Уголовная политика в сфере высоких технологий // Закон и право. 2018. № 1.
3. Доровских Л.А. Преступления с сфере высоких технологий. Киберпреступность// 2016 №4 (28)

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ ПРОТИВ ДЕТЕЙ ПОСРЕДСТВОМ СЕТИ «ИНТЕРНЕТ»: МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ

Соловьева Анастасия Анатольевна,
студент 4 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Попаденко Елена Викторовна,
доцент кафедры государственно правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА, к.ю.н., доцент

Проникновение информатизации во все сферы жизни общества изменило характер преступности и способы совершения преступлений. Сегодня все больше и больше преступлений совершается с использованием информационно-коммуникационной сети «Интернет». Так, по данным Генеральной Прокуратуры России, каждое седьмое преступлений в России совершается с применением IT-технологий[1]. Вследствие отсутствия у подобных преступлений территориальных границ, преступления, совершенные с использованием сети «Интернет» стали транснациональной проблемой.

Самой уязвимой категорией населения, в отношении которой совершаются преступления в сети «Интернет», считаются дети и подростки, не достигшие 18 лет. Они активно пользуются современными источниками информации и проводят в сети несколько часов ежедневно. Новые технологии открывают для детей широкий спектр возможностей, но

[1] Новости в России и в мире – ТАСС [Электронный ресурс] / URL: https://tass.ru/obschestvo/7056912.

при этом могут способствовать и нанесению им вреда, включая ведение такой преступной деятельности, как их сексуальная эксплуатация в виде создания и распространения детской порнографии. При этом применение информационно-коммуникационных технологий значительно упрощает совершение преступных деяний и одновременно привлекает внимание большего числа «пользователей» порнографических материалов.

Так, с 2014 года по 2015 год гражданин США Стивен Чейз вел веб-сайт под названием «Playpen», который позволял пользователям общаться в чате, обмениваться изображениями порнографического содержания и приобретать анонимно изображения материалов о сексуальном насилии над детьми. Данный сайт имел более 150 000 пользователей со всего мира и был признан Федеральным бюро расследований США крупнейшим в мире веб-сайтом детской порнографии. В сентябре 2016 года С. Чейз был признан виновным по нескольким обвинениям, связанным с детской порнографией и эксплуатацией детей и приговорен к 30 годам лишения свободы за эти преступления.

Проведенное ФБР расследование дела Чейза было беспрецедентными по своему масштабу и охвату и впоследствии привело к уголовному преследованию 25 производителей детской порнографии, 51 человека за сексуальное насилие над детьми, а также выявлению потерпевших от сексуального насилия детей не только в США, но и в Европе[1].

Сегодня набирает популярность такое явление как гибергруминг или онлайн груминг – новый вид сексуального насилия против детей в интернете. Суть его заключается в том, что злоумышленники регистрируются в социальных сетях под видом ровесников, общаются с детьми, устанавливают доверительные отношения с целью получения интимных фото и видео, в некоторых случаях, с последующим шантажом и угрозами, чтобы получить еще более откровенные материалы. Существуют даже чаты и сообщества преступников, в которых они публикуют полученные от несовершеннолетних материалы сексуального характера.

Например, Интерполом была проведена операция «Strikeback», в результате которой было арестовано 58 человек, обвинявшихся такой форме сексуальной эксплуатации, при которой авторы угрожают обнародованием сексуальной информации или фотографий жертв. Одной из жертв данной преступной организации стал Дэниел Перри, который покончил с собой из-за шантажа, организованного преступной группой. Группа заманила Перри в сексуальный контакт по скайпу, а затем угрожала ему обнародовать изображения[2].

Во многих зарубежных странах кибергруминг уже криминализован. Например, были внесены изменения в Уголовный кодекс Германии, согласно которым любой, кто обращается к ребенку в интернете, для провоцирования на сексуальную откровенность подлежит суровому наказанию. За такие действия § 176 Abs. 4 Nr. 3 «Сексуальное насилие над детьми» Уголовного кодекса Германии (StGB) предусматривает тюремное заключение в тюрьме на срок от трех месяцев до пяти лет.[3] В российском уголовном праве такой состав преступления отсутствует, а подобные действия могут быть квалифицированы только как приготовление к совершению преступлений, предусмотренных ст. 131 и 135 УК РФ. Хотя данное явление имеет место быть и в России.

Так, согласно материалам дела, следователи Главного следственного управления СК РФ по городу Москве обнаружили фото несовершеннолетних девочек со всей страны в компьютере московского фельдшера Центра экстренной медицинской помощи, которых он искал в социальной сети «ВКонтакте». Познакомившись с ними под видом владелицы рекламного агентства, он просил их обнажиться или прислать свои интимные фото под предлогом фотосессии для модного журнала. Затем, угрожая опубликовать весь компромат в Интернете, требовал раздеться полностью и совершать различные непристойные действия.

---

[1] Соединенные Штаты Америки против Стивена У. Чейза [Электронный ресурс] / URL: doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._steven_w_chase.html?lng=en&tmpl=sherloc.

[2] Операция Strikeback [Электронный ресурс] / URL: https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback.html?lng=en&tmpl=sherloc.

[3] Кибергруминг в Германии [Электронный ресурс] / URL: http://rechtsrat.top/cybergrooming/.

Следствие установило причастность лица к 27 преступным эпизодам. Всего потерпевшими признано 18 девочек в возрасте от 9 до 13 лет.[1]

Для эффективного противодействия описанных видов киберпреступлений необходимо объединение усилий всего мирового сообщества, а также создание единых унифицированных правил борьбы с таким преступлениями и установление мер ответственности. Однако на данном этапе универсальное соглашение о борьбе с преступностью с использованием информационных технологий отсутствует.

Сегодня международным сообществом разработано несколько международных договоров в этой области. Самый известный акт в сфере противодействия киберпреступности – разработанная Советом Европы Конвенция «О преступности в сфере компьютерной информации», подписанная в Будапеште 23.11.2001 г. В этом документе правонарушения, связанные с детской порнографией отнесены к группе преступлений, связанных с содержанием данных.

В рамках других региональных организаций также действуют различные соглашения в сфере борьбы с киберперступлениями и, в частности, с детской порнографией, осуществляемой посредством сети «Интернет». Например, Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества от 16 июня 2009 г., Конвенция о борьбе с преступлениями в области информационных технологий Лиги арабских государств от 21 декабря 2010 г., Конвенция о кибербезопасности и защите персональных данных Африканского союза от 27 июня 2014 г., Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. Вместе с тем все перечисленные акты носят рекомендательный характер, поэтому единого подхода в международно-правовом сотрудничестве государств по борьбе с киберпреступлениями против детей еще так и не сложилось. Сегодня уже назрела острая необходимость, в разработке универсального соглашения с подробным перечнем уголовно наказуемых деяний и установлением минимального размера ответственности за их совершение.

Кроме того, для решения данной проблемы необходимо в рамках всего мирового сообщества создать единую базу данных о лицах, которые были замечены в производстве, передаче, публикации, продаже, экспорте и импорте детской порнографии в сети «Интернет», ее просмотре, а также в запросах в «Интернете», скачивании на компьютер, распространении адресов ресурсов.

СОЦИАЛЬНЫЕ СЕТИ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

Иванова Дарья Владимировна,
студент 4 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафна (МГЮА)
Научный руководитель:
Костикова Наталия Александровна,
доцент кафедры уголовного процесса и криминалистики
Северо-Западного института (филиала)
Университета имени О.Е. Кутафна (МГЮА, к.ю.н.

В век информационных технологий большую часть времени люди проводят в виртуальном пространстве, в том числе в социальных сетях. Человек общается с другими

[1] Кузнецова М. Мосгорсуд вынес приговор фельдшеру, развращавшему детей по интернету / М. Кузнецова // Московский комсомолец. — 2014. — 26 апр.

людьми, находит необходимую информацию, узнает что-то новое, но самое главное, совершает преступления, используя интернет-пространство.

Социальные сети, являясь информационным ресурсом, успешно используются и правоохранительными органами в целях предотвращения и раскрытия преступлений, а также идентификации и последующего задержания подозреваемых. Примеров этому немало. В Иркутске возбудили уголовное дело по факту жестокого обращения медсестры с ребенком-инвалидом, поводом стало видео, размещенное в социальных сетях (ноябрь 2019). В Хабаровске вынесен приговор 25 августа 2017 г. в отношении двух девушек, которые жестоко обращались с животными, после чего выложили фото и видео в социальную сеть**.**

Однако для получения значимой информации из социальной сети необходимо совершить ряд действий, которые значительно затягивают процесс расследования преступления. Разберемся в системе получения и приобщения подобных доказательств к материалам уголовного дела.

Если страница в социальной сети находится в открытом доступе, то получение информации осуществляется посредством осмотра переписки с участием специалиста в информационной сфере. Специалист привлекается в силу того, что информация в социальных сетях, как и во всей информационно-телекоммуникационной сети «Интернет», подвержена наибольшему изменению. По результатам следственного действия составляется протокол по правилам, установленным в УПК РФ.

Для поиска человека по социальным сетям (открытым страницам) и установления его личности, как правило, требуются небольшие временные затраты и достаточно познаний следователя. Если же речь идет об изъятии переписки с личной страницы необходимо осуществить комплекс действий, достаточно затратных по времени. Во-первых, необходимо направить в суд ходатайство о проведение такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами (п. 12 ст. 29 УПК РФ). Во-вторых, полученное решение суда необходимо направить в организацию, создавшую социальную сеть. В-третьих, получить информацию от данной организации, которая предварительно проверяет информацию и решение суда. Более сложная ситуация складывается в том случае, если это касается иностранной организации, получение информации затягивается, что негативно влияет на процесс расследования преступления. Данный способ получения информации используется для предотвращения нарушения ст. 23 Конституции РФ

Если следователь располагает носителем соответствующей информации (мобильный телефон, планшет, компьютер, через которые осуществлялся доступ в социальные сети), и владелец отказывается добровольно предоставить интересующие сведения, то может быть назначена компьютерно-техническая экспертиза.

Информация, извлеченная из социальных сетей, может носить ориентирующий характер и способствовать проведению следственных действий.

На примере одной из страниц из социальной сети «ВКонтакте» (https://vk.com/denis_pichugov) мы постараемся найти необходимую ориентирующую информацию.

На странице в разделе информации мы видим: дату рождения, город, а также несколько ссылок на другие социальные сети: youtube, skype, Instagram. Кроме того, в новостной ленте размещены различные видео и репосты с групп, тематикой которых является паркур.

В разделе видео находим большое количество клипов, снятых как самостоятельно, так и с помощью других лиц (различные связки из уличной акробатики).

Переходя по ссылкам, указанным в разделе информации, можно увидеть, что там дублируются видео, находящиеся на странице во «ВКонтакте». Изучая данную информацию из различных источников, можно установить противоречия: если человек ведет разные страницы в разных стилях, использует разные речевые обороты и другие способы, можно предположить наличие фальсификации в одной из социальных сетей.

Вернемся к анализу ранее указанной страницы. Из вышесказанного следует несколько выводов. Во-первых, молодой человек занимается паркуром, а также участвует в различных мероприятиях в этой сфере. Во-вторых, страницы, расположенные в других социальных сетях, ведутся этим же человеком. В-третьих, молодой человек владеет навыками работы в программах, позволяющих монтировать видео и обрабатывать фотографии. В-четвертых, молодой человек владеет навыками видеосъемки.

Данная информация, полученная со страницы во «ВКонтакте», поможет установить круг общения, возможность нахождения в каких-либо местах, а также уровень владения программами для обработки изображений.

С каждым годом развивается тенденция распространение фотографий с геолокацией, что значительно облегчает деятельность следователя в случае подтверждения алиби. Однако стоит заметить, что для проверки данной информации необходимо привлечение специалиста, который достоверно сможет указать о том, является ли данная метка подлинной или нет, что в свою очередь сможет доказать и отсутствие алиби.

Социальные сети используются и для поисков лиц. Несмотря на то, что обычно поиск ведут обычные граждане, полученная информация используется для оперативных целей.

Рассмотрим на примере одной из групп во «ВКонтакте», которая как раз и помогает в поиски людей (https://vk.com/pso_tyneodin). Обратим внимание на ориентировку, которая оформляется практически в соответствии установленными требованиями: дата исчезновения, место исчезновения, приметы, в чем был одет, фотография, номера телефонов для связи.

Если просмотреть группу, то можно увидеть, что в случаях, не требующих отлагательств (обычно исчезновение детей), организуется сбор волонтеров с дальнейшим проведением инструктажа. Проанализировав информацию за период 6 сентября 2019 года – 28 ноября 2019 года, получаем следующие результаты. Было найдено 20 человек (живых), погибших – 10 человек, пропавших без вести – 8 человек. Обращая внимание на данную статистику, можно сделать вывод, что социальные сети помогают в поисках людей, а также позволяют уменьшить нагрузку на оперативных служащих. Однако стоит заметить, что поиск людей через такие группы часто проходит с участием оперативных работников, координирующих деятельность волонтеров, что также уменьшает время поиска людей, а это, в свою очередь, приводит к вероятности нахождения человека живым.

Из всего вышесказанного следует, что социальные сети как источник ориентирующей информации имеют практическое значение, полученные сведения являются вспомогательными и используются для дальнейшего получения доказательств и проведения следственных действий. В конечном итоге можно говорить о сокращении срока расследования преступлений.

Однако если речь идет о получении доказательственной информации в рамках следственных действий (следственный осмотр, получение информации о соединениях абонентов и/или абонентских устройств, компьютерно-техническая экспертиза), то возникают определенные сложности процессуального и иного характера, которые приводят к значительному затягиванию расследования.

ФИНАНСОВО-ПРАВОВОЙ РЕЖИМ В ЭПОХУ ПЕТРА I

Лисенков Дмитрий Михайлович,
студент 3 курса Северо-Западного института (филиала)
Университета им. О.Е.Кутафина (МГЮА)
Научный руководитель:
Ядрихинский Сергей Александрович,
доцент кафедры административного и финансового права
Северо-Западного института (филиала) Университета
им. О.Е. Кутафина (МГЮА), к.ю.н., доцент

В любом государстве, на любом этапе его существования особую важность представляет его материально-хозяйственная составляющая, а именно финансово-экономическая основа. Конечно, в разные временные промежутки она выражалась по-разному, начиная от «полюдья», которое датируется периодом правления первых князей древнерусского государства, заканчивая системой налоговых и неналоговых сборов в наше время.

В данной статье будет рассмотрен финансовый режим Российской империи Петровской эпохи, и проведен сравнительный анализ с нашим временем. Данный период времени выбран, потому что именно в начале 18 века в России происходил процесс активной индустриализации, которая во-первых, положила начало развития промышленности, и, соответственно, массовому созданию рабочих мест, продукта с целью сбыта, что стало предпосылкой получения прибыли; во-вторых, только с этого времени в нашем государстве начинает зарождаться процесс переработки и добычи собственных ресурсов (добыча железа, камня, соли), что раскрыло сырьевой потенциал государства, тем самым придав ему значение для мировой торговли; и, наконец, в-третьих, именно с этого периода Российская Империя начинает вести реальные дипломатические отношения с другими государствами, тем самым снимая с себя изоляцию от внешнего мира и вливаясь в международную экономику (в широком понимании этого слова).

Именно деятельность Петра и его реформы смогли вывести экономическую ситуацию в Империи из состояния «моральной экономики» на этап становления рыночной экономики в стране. Попробуем разобрать правовой аспект данных реформ. После создания высшего органа в империи (после Императора, конечно) в 1711 – Сената – Петр I четко осознавал необходимость создания системы отраслевого управления, в связи с чем на смену приказному управлению были созданы Коллеги. В 1718 году их реестр был утвержден, хотя и активно подвергался изменениям. Необходимо отметить, что временные интервалы создания Коллегий разные, но нас будут интересовать только: Камер-коллегия - орган который занимался казенными сборами, установлением и изменением податей, Штатс-контора – орган наиболее важный для нас, который занимался распределением финансов в империи в широком смысле слова, а так же Ревизион-коллегия – выполняющая контрольно-счетную функцию.

В каждой новосозданной коллегии имел место быть свой генеральный регламент, который устанавливал сферы работы ведомства, его основные функции и задачи. Анализируя данные документы можно определить, что система финансов в империи работала следующим образом: Камер-коллегия руководила сбором всех государственных доходов, включая доходы от государственных казенных заводов и монополий, с 1719 года по разрешению Сената вводила новые налоги и сборы, Штатс-контора осуществляла составление расходных статей бюджета (штатов) и руководство производством расходов по различным отраслям управления. Контроль и проверку с данной цепочке замыкала Ревизион-коллегия.

Необходимо отметить, что данная система была не полностью русской идеей, дело в том, что Петр 1 позаимствовал финансовое управление у Швеции, и оно достаточно хорошо прижилось в России. Справедливости ради необходимо так же отметить, что Швеция как государство на тот момент была полностью суверенной и самодостаточной страной, государственная машина в которой работала на пике возможностей того времени.

Как мы можем увидеть, только с 18 века в России начинает формироваться тот образ финансовой системы, которая существует и по сей день, ведь многие органы несмотря на разницу в названиях достаточно имеют схожие функции с современными. Конечно, максимально приближенная к современной финансовая система в Империи была в 1916-1917 году, но деятельность Петра 1 во многом соответствовала передовым идеям того времени.

Заочное участие

ЭЛЕКТРОННЫЙ ТРУДОВОЙ ДОГОВОР: ПРОБЛЕМЫ ТЕОРИИ И ПРАВОПРИМЕНЕНИЯ

Потапов Андрей Владимирович,
аспирант Юридического факультета МГУ им. М.В. Ломоносова
Научный руководитель:
Костян Ирина Александровна,
профессор кафедры Трудового права Юридического факультета МГУ им. М.В. Ломоносова, доктор юридических наук

Электронные технологии прочно вошли в нашу повседневную жизнь. На протяжении последних 7 лет на различнызх научных форумах, в СМИ активно обсуждается проблема внедрения электронного кадрового документооборота. Несколько лет назад Правительством РФ был подготовлен проект ФЗ "О внесении изменений в Трудовой кодекс Российской Федерации" (в части использования документов в электронной форме) (далее проект), который направлен на реализацию возможностей использования в трудовых отношения документов в электронной форме[1]. Предполагается, что введение электронного документооборота в сферу труда значительно сократит текущие расходы.

Сегодня большинство граждан страны получают разнообразные госуслуги в электронной форме, в том числе и с целью участия в трудовых отношениях. Для обеспечения гибкости рынка труда в нашей стране создан и успешно функционирует портал, который позволяет осуществлять поиск работы в России и за рубежом, проверить содержание своего трудового договора, пожаловаться на нарушение прав работодателем – это сервис Онлайнинспекция РФ[2].

Для работодателя также много возможностей, в частности, он может пройти онлайн - самопроверку по проверочным листам на этом же сайте, что позволит еще до прихода инспектора устранить все нарушения трудового законодательства. Сводный план проверок работодателей разрабатывается Генеральной прокуратурой РФ и публикуется в специальном разделе на официальном портале ведомства. Такие самопроверки очень эффективны и оправдывают риск-ориентированный подход государства к решению многих проблем в сфере труда.

Риск-ориентированный подход представляет собой такой метод организации государственного контроля, при котором интенсивность проведения проверок зависит от того, к какой категории риска относится работодатель в соответствии с показателями, утвержденными профильными министерствами и ведомствами[3]. Классификация по группам риска происходит по результатам ответов уполномоченных представителей работодателя на вопросы, содержащиеся в проверочном листе. Группа риска зависит от численности работников, количества несчастных случаев, задолженности по заработной плате, административных правонарушений в сфере труда и т.п.

Заметим, что уже с 1 июля 2018 г. используются проверочные листы при проведении плановых проверок всех категорий работодателей, что удобно именно для самих работодателей, так как инспектор обязан ориентироваться именно на те положения, которые закреплены в проверочном листе. Сами проверочные листы размещены на сайте Онлайнинспекии РФ, их огромное количество, по многим вопросам и направлениям, что особенно важно для работодателя, т.к. любой работодатель может практически по всем

[1] «Известия» [Сайт] URL: http://izvestia.ru/news.
[2] https://онлайнинспекция.рф
[3] Потапова Н.Д., Потапов А.В. Новеллы государственного контроля в сфере труда. Закон и право. № 9. 2018. С. 82.

вопросам найти ответы и оценить насколько он точно соблюдает трудовое законодательство. При этом ожидается, что основная масса проверок будет проводиться в форме самопроверок в автоматическом режиме на сайте Онлайнинспекция РФ.

Помимо онлайн-самопроверок работодателем планируется создание возможности заключать трудовой договор в электронной форме через ГИС «Электронный трудовой договор», доступ к которой будет свободный. Через систему «Электронный трудовой договор» стороны будут иметь возможность составить текст трудового договора и подписать его с помощью электронной подписи, а документы в бумажной форме работник сможет получить в МФЦ. Такой документ смогут заверить работники центра, имеющие доступ ко всем документам ГИС[1], т.е. будет полная база данных о работодателях и работниках, имеющих электронную подпись.

Рассмотрим некоторые проблемы правоприменения при заключении трудового договора в электронной форме. Законодатель предлагает новое понятие письменной формы документов – это документы, оформленные на бумажном носителе и подписанные соответствующим лицом или его представителем собственноручно и (или) документы в электронной форме, подписанные соответствующим лицом или его представителем с использованием электронной подписи. Электронный документооборот предполагает наличие электронной подписи у обеих сторон трудовых отношений, т.е. одна из проблем – это наличие электронной подписи, а для некоторых работников – еще и умение ею пользоваться.

Сейчас ТК РФ допускает электронный документооборот для дистанционных работников, однако в проекте такого ограничения нет, и это значит, что электронный документооборот будет доступен для всех работников. Ограничение сферы применения электронной формы было бы не обоснованным, т.к. это удобно, значительно ускоряет документооборот, снижает затраты работодателя и укрепляет доверие к новым технологиям.

Проект предусматривает, что использование электронной подписи в трудовых отношениях допускается при соблюдении трех условий: работодатель принял соответствующий локальный нормативный акт; работник ознакомлен с ним под роспись; работодатель принял организационно-технические меры для использования электронной подписи. Использование электронной подписи предполагается в добровольном порядке, а при несогласии работника собственноручной подписи.

Нет сомнений в том, что правоприменение выявит все «за» и «против», но в любом случае трудовой договор должен быть в письменной форме – электронной или нет – решать самостоятельно работнику.

Мы разделяем опасения главы ФНПР М. Шмакова о том, что даже небольшой сбой на сервере может привести к потере данных о трудовых отношениях[2]. Риск утраты персональных данных работника может вызвать проблему подтверждения стажа, что лишит работника права на достойное социальное обеспечение.Полагаем, что для минимизации риска разглашения персональных данных и их утраты можно производить резервное копирование информации работодателем самостоятельно, а также через индивидуальный персонифицированный учет ПФР, через применение технологии блокчейн для сохранения информации и реестра трудовых договоров[3]. Добавим, что за необеспечение сохранности персональных данных на работодателе лежит риск привлечения к административной ответственности.

Еще одним нововведением будет электронная трудовая книжка, представляющая собой базу данных о трудовой деятельности, формируемая путем передачи работодателем сведений в электронном виде в ПФР[4] начиная с 2020 года. Бумажная и электронная книжка

---

[1] Петербургский правовой портал. [Сайт]URL: http://ppt.ru/news/137532.

[2] «Известия» [Сайт] URL: http://izvestia.ru/news.

[3] Потапова Н.Д., Потапов А.В.Электронный трудовой договор. Закон и право. № 8. 2017. С. 67.

[4] Проект Федерального закона N 748684-7 "О внесении изменений в Трудовой кодекс Российской Федерации (в части формирования сведений о трудовой деятельности в электронном виде)"(ред., внесенная в ГД ФС РФ,

будут иметь равную юридическую силу. Полный отказ от бумажных трудовых книжек запланирован на 2021 год, для тех работников, кто впервые будет устраиваться на работу. По прогнозам Минтруда России уже в 2020 году выгода работодателей от того, что не нужно приобретать трудовые книжки составит 0,7 млрд. рублей.[1] При этом возможна проблема получения работником сведений о работе. Если раньше, до введения электронных трудовых книжек работник мог получить информацию о стаже как через личный кабинет в ПФР, так и непосредственно у работодателя, но основным документом, подтверждающим стаж работника, была все-таки бумажная трудовая книжка, то с введением электронных трудовых книжек у работника появляется больше возможностей. Так, он вправе получить сведения о трудовой деятельности несколькими удобными способами: у работодателя по последнему месту работы - на бумажном носителе или в «цифре» с усиленной квалифицированной электронной подписью (при ее наличии у работодателя); в МФЦ- на бумажном носителе; в ПФР - на бумажном носителе или в «цифре» с усиленной квалифицированной электронной подписью; портала Госуслуг (функций) - в «цифре» с усиленной квалифицированной электронной подписью. Однако при всем удобстве и простоте цифровых технологий может возникнуть проблема достоверности внесенных данных в электронные трудовые книжки. Так, если при внесении записи в бумажной трудовой книжке работник, так сказать «на месте»,- непосредственно у работодателя знакомиться с вновь вносимыми записями, то при электронных трудовых книжках вся информация будет передаваться в ПФР, работник сможет ознакомиться с ней через «Личный кабинет» в ПФР. Тут же возникают вопрос - что делать, если записи не соответствуют действительности? Законодатель предусмотрел более сложный путь - в таком случае работник должен письменно сообщить о проблеме работодателю, а тот внести соответствующие изменения, соответственно, работник сможет проконтролировать исправления через «Личный кабинет» ПФР. Скорее всего для «возрастного» работника такая система может показаться более сложной и непонятной, но для молодого поколения – вполне обычной. Считаем, что указанные способы действительно удобны и выгодны с точки зрения сокращения времени на передачу информации, снижения трудозатрат, однако для достаточно большого процента работающего населения, по-прежнему, использование цифровых технологий является определенным психологическим барьером и «недоступной формой общения с работодателем».

МОДЕРНИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА ОБ ИЗЪЯТИИ ЗЕМЕЛЬНЫХ УЧАСТКОВ ДЛЯ НЕДРОПОЛЬЗОВАНИЯ В УСЛОВИЯХ ИННОВАЦИОННОЙ ЭКОНОМИКИ

Юлдашев Джохонгир Мухиддинович,
студент Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Воронина Наталья Павловна,
доцент кафедры экологического и природоресурсного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), к.ю.н., доцент

В соответствии со стратегическими целями и задачами государственной энергетической политики в области недропользования, определенными Энергетической стратегией России на период до 2030 г., утвержденной распоряжением Правительства Российской Федерации от 13 ноября 2009 г. 1715-р, изъятие земельного участка в целях проведения работ, связанных с недропользованием, направлено не только на получении

текст по состоянию на 08.07.2019) [Сайт] URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=185272#001731427339836955.

[1]Сайт Минтруда России. [Сайт] URL:https://rosmintrud.ru/labour/relationship/327.

прибыли хозяйствующим субъектом, но и на достижение интересов общества (Российской Федерации), в том числе по обеспечению стабильного, бесперебойного и экономически эффективного удовлетворения внутреннего спроса на нефть и нефтепродукты для обеспечения стабильных поступлений в доходную часть консолидированного бюджета страны[1].

Учитывая, что доходы получаемые за счет добычи минерального сырья и экспорта товарных руд и продуктов их переработки, составляют более половины поступлений в доходную часть бюджета Российской Федерации, особо необходимо отметить, что основная их часть – это доходы, получаемые от нефте- и газодобычи.

При этом, на практике зачастую наблюдается ситуация, при которой недропользователь не может получить права на земельные участки, находящиеся в частной собственности или государственной собственности, но предоставленные иным лицам на определенных нормативными правовыми актами вещных правах, по причине отказов собственников данных земельных участков на предоставление земельных участков для проведения работ, связанных с недропользованием.

Данная ситуация усугубляется еще и тем, что появляются судебные решения, согласно которым изъятие земельного участка для работ, связанных с недропользованием, не является основанием для изъятия земельного участка для государственных и муниципальных нужд.

Так, в рамках дела № 2а-143/2018 Беловским судом Кемеровской области проверялась законность приказов Департамента по недропользованию по Сибирскому федеральному округу (Сибнедра) об изъятии земельных участков у правообладателей для государственных нужд.

В результате, судом было установлено, что наличие лицензии на пользование недрами не является достаточным основанием для изъятия земельного участка для целей недропользования ввиду того, что осуществление данного вида деятельности не свидетельствует об удовлетворении потребностей публично-правового образования, направленных на достижение общественных интересов. Таким образом. судом было установлено, изъятие земельного участка для целей недропользования не соответствует основаниям изъятия земельного участка для государственных нужд по причине отсутствия цели достижения публичного интереса и удовлетворения общественных потребностей.

Существование данной ситуации требует обращения к нормам действующего законодательства РФ и их тщательного анализа.

Так, согласно подпункту 3 пункта 1 статьи 49 Земельного кодекса РФ[2] (далее – ЗК РФ) изъятие земельных участков для государственных или муниципальных нужд осуществляется в исключительных случаях по основаниям, предусмотренным федеральными законами.

Данная норма взаимосвязана с ч. 2 ст. 25.2 Закона РФ от 21.02.1992 № 2395-1 «О недрах»[3] (далее – Закон о недрах), согласно которой допускается осуществлять изъятие для государственных или муниципальных нужд земельных участков, если такие земельные участки необходимы для ведения работ, связанных с пользованием недрами.

В силу п. 2 ст. 56.3 ЗК РФ принятие решения об изъятии земельных участков для государственных или муниципальных нужд в целях, не предусмотренных пунктом 1 ст. 56.3, должно быть обосновано лицензией на пользование недрами (в случае изъятия земельных участков для проведения работ, связанных с пользованием недрами, в том числе осуществляемых за счет средств недропользователя).

[1]Распоряжение Правительства РФ от 13.11.2009 № 1715-р «Об Энергетической стратегии России на период до 2030 года» // Собрание законодательства РФ. 2009. № 48. Ст. 5836.

[2] Российская газета. 2001. 30 ноября.

[3]Закон РФ от 21.02.1992 № 2395-1 (ред. от 02.08.2019) «О недрах» // Российская газета. 1995. 15 марта.

Так, законодателем было установлено, что наличие лицензии на пользование недрами является основанием для изъятия земельного участка для государственных и муниципальных нужд.

Другим вопросом, требующим раскрытия, является вопрос наличия государственных нужд, в случае изъятия земельного участка для целей недропользования.

Для этого, в первую очередь, необходимо обратиться к ст. 9 Конституции РФ, согласно которой земля и другие природные ресурсы используются и охраняются в Российской Федерации как основа жизни и деятельности народов, проживающих на соответствующей территории[1].

В соответствии с ч. 2 ст. 2 Закона о недрах владение, пользование и распоряжение государственным фондом недр в пределах территории Российской Федерации в интересах народов, проживающих на соответствующих территориях, и всех народов Российской Федерации осуществляются совместно Российской Федерацией и субъектами Российской Федерации.

Часть 1 ст. 35 Закона о недрах устанавливает, что основной задачей государственного регулирования отношений недропользования является обеспечение воспроизводства минерально-сырьевой базы, ее рационального использования и охраны недр в интересах нынешнего и будущих поколений народов Российской Федерации.

Важное имеет значение содержание ч. 3 ст. 36 Закона о недрах, согласно которой федеральный орган управления государственным фондом недр и его территориальные органы не могут выполнять функции управления хозяйственной деятельностью предприятий, осуществляющих разведку и разработку месторождений полезных ископаемых либо строительство и эксплуатацию подземных сооружений, не связанных с добычей полезных ископаемых, и заниматься коммерческой деятельностью.

Из вышеуказанного, можно сделать вывод о том, что государство реализует свои права в отношении государственного фонда недр путем предоставления участков недр, целью осуществления данной деятельности является удовлетворения публичных интересов.

Обобщив все вышеизложенное, можно отметить, что недропользование направлено на удовлетворение публичных нужд, а лицензия на право пользования недрами – это документ, который обосновывает наличие этих нужд, поэтому на недропользователя не накладывается обязанность дополнительно подтверждения наличия государственных нужд.

Таким образом, для модернизации законодательства об изъятии земельных участков для работ связанных с недропользованием, с учетом имеющейся негативной судебной практики, значения данной отрасли для доходной части бюджета Российской Федерации, необходимости достижения стратегических целей и выполнения задач государственной энергетической политики в области недропользования, определенных Энергетической стратегией России на период до 2030 г., утвержденной распоряжением Правительства Российской Федерации от 13 ноября 2009 г. № 1715-р, считаем необходимым внесение изменений в ст. 49 ЗК РФ, в виде установления самостоятельного основания изъятия земельного участка – проведение работ, связанных с недропользованием.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ РАЦИОНАЛЬНОГО ИСПОЛЬЗОВАНИЯ ЗЕМЕЛЬ СЕЛЬСКОХОЗЯЙСТВЕННОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА

Астахова Александра Александровна,
студент магистратуры Московского государственного

[1]Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

юридического университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Воронина Наталья Павловна,
доцент кафедры экологического и природоресурсного права
Московского государственного юридического университета
имени О.Е. Кутафина (МГЮА), к.ю.н., доцент

Правовое регулирование оборота земель сельскохозяйственного назначения имеет большую значимость в связи с особыми плодородными свойствами такой земли. Развитие этой отрасли как приоритетная цель современного экономического развития позволяет решать не только проблемы увеличения объема производства продовольственной продукции, но и решения проблемы занятости населения.[1]

Целью и направлением развития земельного законодательства Российской Федерации должно стать определение современного состояния правового регулирования отношений, связанных с выработкой комплекса мер правового характера по созданию условий, сводящих к минимуму легальную возможность ненадлежащего использования земель сельскохозяйственного назначения, по выявлению фактов ненадлежащего использования этих земель, а также по правовому воздействию на лиц, допускающих такое использование.[2]

Безусловно, отдельной задачей для государства в лице его уполномоченных органов является создание и наличие такого правового и информационного механизма, который позволяет иметь возможность оперативного, своевременного и быстрого выявления земельных участков, используемых нерациональным и ненадлежащим образом либо неиспользуемых вообще; их изъятия и предоставления другим лицам.

В исторической перспективе, в отсутствие каких-либо электронных ресурсов выявление таких земельных участков было достаточно трудоёмким процессом. Приходилось прилагать немало физических усилий: вести многочисленные книги учета, где было достаточно сложно систематизировать и структурировать всю информацию; составлять и издавать топографические бумажные карты. Однако государственная защита прав собственности была бы затруднительна без полной и достоверной информационной базы, отражающей состояние объектов недвижимости.

Сегодня, выявление неиспользуемых земельных участков происходит путем осуществления государственного земельного надзора и муниципального земельного контроля, проводимых в соответствии с Земельным Кодексом Российской Федерации. Для осуществления данных функций органам государственной власти и органам местного самоуправления необходим пакет данных, например:

- о правообладателе земельного участка;
- об основных и дополнительных сведениях о земельном участке;
- сведения о том, были ли ранее в отношении собственника неиспользуемого земельного участка вынесены какие-либо административные предписания и др.

Также стоит отметить, что на момент 2019 года человечество имеет большое количество цифровых технологий абсолютно в различных сферах жизни, что облегчает работу людей по многим направлениям их деятельности. Процесс цифровизации не прошел стороной и правовое регулирование рационального использования земель сельскохозяйственного назначения. Неизбежно встает вопрос – а как это работает? Ответ достаточно прост. На базе цифровых технологий создано большое количество электронных ресурсов, которые помогают в жизни и в работе не только государственным органам, но и физическим и юридическим лицам. То есть это все те электронные ресурсы, которые

[1]"Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года" (разработан Минэкономразвития России). – 25 марта 2013.
[2]Елисеева И.А.Правовой режим земель сельскохозяйственного назначения: проблемы законодательства и практики // Законы России: опыт, анализ, практика. - 2018. - N 10.

помогают узнать, какие земельные участки не используются и предоставить данные участки в пользование. Ознакомимся с некоторыми из таких ресурсов.

ЕГРН (Единый государственный реестр недвижимости) – это достоверный источник информации об объектах недвижимости на территории Российской Федерации. Выпиской из ЕГРН подтверждаются кадастровый учет, возникновение и переход права на объекты недвижимости. ЕГРН ведет Федеральная служба государственной регистрации кадастра и картографии (Росреестр), подотчетная Министерству экономического развития РФ. Минэкономразвития с Росреестром при участии Кадастровой палаты планирует разработать единые форматы электронных документов для перехода к совершению сделок по регистрации недвижимости преимущественно в электронном виде. «Цифровой блок Белого дома хочет видеть формализованную стратегию цифровизации Росреестра, который является ключевым поставщиком государственных данных» - отметили в газете «Комерсантъ». Вице-премьер Максим Акимов назвал это ведомство одним из лидеров по оказанию госуслуг в цифровой форме (их доля составляет 65%), поскольку десять лет назад оно создавалось на изначальной «цифровой подложке». Следующее десятилетие, по его словам, должно быть пройдено «под флагом тотальной цифровизации». Ключевой задачей ведомства в 2019 году названо завершение ввода в промышленную эксплуатацию Федеральной государственной информационной системы ведения Единого государственного реестра недвижимости (ФГИС ЕГРН) и обеспечение требуемой инфраструктуры для миграции данных.

Публичная кадастровая карта - онлайн-сервис, в котором в графической и текстовой форме воспроизводятся сведения, содержащиеся в Едином государственном реестре недвижимости, а также вспомогательные инструменты. Карта предназначена для использования неограниченным кругом лиц, сведения карты являются общедоступными. Она регулярно обновляется и актуализируется, период обновления данных карты зависит от региона. Сайт позволяет физическим и юридическим лицам искать на карте границы земельных участков и объектов, узнавать кадастровую стоимость, находить свободные участки, собирать информацию для решения юридических земельных вопросов. Данный сайт носит информационно-ознакомительный характер. Для кадастровых инженеров и компаний, оказывающих кадастровые услуги, сайт позволяет находить клиентов.

Гектар 35. Губернатор Вологодской области О.А. Кувшинников поручил Правительству области разработать концепцию проекта «Вологодский гектар» на примере федерального проекта «Дальневосточный гектар», который бы позволял максимально эффективно задействовать неиспользованные сельскохозяйственные земли. С этой целью был издан региональный Закон «Об особенностях предоставления в собственность гражданам земельных участков из фонда перераспределения земель сельскохозяйственного назначения на территории Вологодской области» от 28 декабря 2018г. Новацией «Вологодского гектара» является создание государственной информационной системы «Вологодский гектар», с помощью которой граждане и юридические лица Российской Федерации, находясь в любом уголке нашей страны, могут подать заявку на получение «Вологодского гектара».

Государственный (национальный) доклад о состоянии и использовании земель в Российской Федерации в 2017 году.

Доклад о состоянии и использовании земель является официальным изданием Федеральной службы государственной регистрации, кадастра и картографии. В докладе приводится информация о состоянии и использовании земель сельскохозяйственного назначения; данные государственного мониторинга земель и государственного земельного надзора; данные распределения земель по формам собственности; сведения о наличии земельных участков, находящихся у граждан для различных целей использования и т.д.

Доклад Министерства сельского хозяйства РФ о состоянии и использовании земель сельскохозяйственного назначения Российской Федерации в 2016 году.

Доклад о состоянии и использовании земель сельскохозяйственного назначения является официальным изданием Министерства сельского хозяйства Российской Федерации.

В докладе приводится информация о состоянии и использовании земель сельскохозяйственного назначения на территории Российской Федерации в динамике за последние годы в целом и по видам угодий, а также о плодородии почв таких земель. Оценки, приведенные в Докладе, получены на основе данных обследований и наблюдений, проводимых федеральными государственными учреждениями и центрами; проверок, осуществляемых территориальными управлениями Россельхознадзора, а также сведений, представленных в Государственных (национальных) докладах о состоянии и использовании земель в Российской Федерации.

Актуальность рассматриваемой темы подчеркивается и проведением с 9 октября по 12 октября 2019 года крупнейшего отечественного аграрного форума «Золотая осень» на территории знаменитой московской Выставки достижений народного хозяйства (ВДНХ) во время Недели агропромышленного комплекса, которая была приурочена ко Дню работника сельского хозяйства и перерабатывающей промышленности. На данном форуме было указано, что Правительство РФ выстраивает свою работу в этой сфере по нескольким направлениям, одним и самым важным из которых является цифровизация сельского хозяйства. К этому блоку относится создание полной базы данных о состоянии агропромышленного комплекса и возможность аграриев проще взаимодействовать с государственными органами.

Только имея актуальную информационную базу об использовании земель сельскохозяйственного назначения можно оперативно выявлять неиспользуемые земельные участки или земельные участки, использование которых идет нерациональным и ненадлежащим образом, с последующей целью их предоставления другим более эффективным собственникам.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНСТИТУЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ И ФРАНЦИИ

Максимова Анастасия Сергеевна, Стебнева Ирина Сергеевна,
студенты Российской академии народногохозяйства и
Государственной службы при Президенте РФ
Челябинскийфилиал (РАНХиГСЧФ)
Научный руководитель:
Запрутин Денис Григорьевич,-
доцент Российской академии народного хозяйства и
Государственной службы при Президенте РФ
Челябинский филиал (РАНХиГСЧФ)

На сегодняшний день предоставляется возможным наблюдать разнообразие мировой конституционно-правовой практики, и важно уметь правильно сопоставлять и анализировать опыт других стран, чтобы найти новые решения, для усовершенствования собственной нормативно-правовой базы. Рост актуальности анализа конституционной практики, не только в России но и в других странах предопределен процессами глобализации и модернизации, влекущими трансформацию конституционно-правовых баз и модификацию научных исследований. Уникальный опыт конституционного строительства имеет место в истории Франции. В истории принятия и реформирования конституций этой и нашей страны можно обнаружить не мало схожих черт. Известным фактом является и то, что французский опыт использовался при создании действующей российской Конституции.

Конституционное развитие Франции, имеет богатую историю. В 1791 году Франция становится третьей страной в мире, закрепившей политический строй и многие другие аспекты жизнедеятельности страны в основном законе. Ныне действующая конституция страны является 17-ой по счёту, она оформила 22-ой политический режим. У нынешней

Российской Конституции предшественников на порядок меньше. Так в 1918 году была принята конституция РСФСР, а 1924, 1936 и 1977 года стали годами принятия Конституций СССР. Действующая Конституция РФ была принята 12 декабря 1993 года по результатам всенародного голосования. Уделим внимание структуре обеих конституций. В сравнении с Конституцией Франции,

Преамбула Конституции РФ представляет собой вводную часть, которая предшествует основному тексту конституции. Задачей преамбулы является передача основного смысла Конституции. В ней представлены основополагающие цели, реализация которых - главная задача государства. Прежде всего, это утверждение прав и свобод человека, а также гражданского мира и согласия в РФ. Первый раздел включает в себя 9 глав. Второй раздел представляет собой заключительные и переходные положения. Конституцией Франции официально считается основной закон 1958 г. Это консолидация нескольких основополагающих документов: Декларация прав человека и гражданина 1789г.; Преамбула конституции.; Конституция 1958 года. Иногда так же отдельным документом, входящим, в консолидацию, считают Хартию окружающей среды 2004 года.[1] Наряду с короткой преамбулой содержится 93 статьи, которые объединяются в 15 разделов. Несмотря на то, что по количеству статей основной закон Франции значительно меньше, количество разделов в нем куда больше. Это может быть связанно с прохождением большего исторического пути. Вместе с тем, Конституции можно признать достаточно похожими. Нельзя забывать и о их принципиальных различиях, отраженных на практике. Конституция Франции вступила в свои права раньше Российской. Их общей чертой является то, что они провозглашают разделение властей и закрепляют основные права и свободы граждан. Разделение властей, это сходство, но то, каким образом оно оформлено, является отличием. В каждой стране складывается своя система ценностей и авторитета власти. Нерушимым условием остается лишь то, чтобы ни одна власть не должна подавлять другие.

Сравним основные статьи, отражающие суть модели управления страны.

Статус Президента по Конституции. В Конституции РФ статусу Президента РФ посвящена отдельная глава 4. В статье 80 пункте 2 указано, что Президент РФ является гарантом Конституции РФ, прав и свобод человека и гражданина. В свою очередь в Конституции Франции статусу Президента республики представлен Раздел II. В статье 5 указано, что Президент следит за соблюдением Конституции. Он является основным гарантом национальной независимости, целостности территории, соблюдения международных договоров. Возьмем во внимание и другие выдержки статей. Срок полномочий во Франции представлен в статье 6. Президент избирается на 5 лет всеобщими прямыми выборами. До 2000года этот срок был равен 7 годам. Касаемо РФ, срок полномочий указан в статье 81, составляет он 6 лет. Если говорить о более раннем варианте, то до внесения поправок в 2008 году этот срок составлял 4 года. Сроки примерно одинаковые - 5 и 6 лет. Но сам факт увеличения срока Президента в России на два года, и уменьшения во Франции на тот же период, говорит, о возможно противоположных тенденциях восприятия статуса Президента и его роли в государстве. Отлично и то, что в Конституции РФ представлены дополнительные требования: «Может быть избран гражданин РФ не моложе 35 лет, постоянно проживающий в РФ не менее 10 лет».

Перейдем к полномочиям. В основном законе Франции в статье 8 закреплено, что Президент Республики назначает Премьер-министра. В Конституции РФ в статье 83 указано, что Президент назначает с согласия Государственной Думы Председателя Правительства РФ. В данной ситуации, в отличие от Франции это не единоличное решение. Статья 11 Конституции Франции закрепляет возможность проведения референдума и по предложению Президента и по Предложению Правительства. Касаемо этого момента в Конституции РФ в статье 84 пункте в) указано, что Президент назначает референдум в порядке, установленном федеральным конституционным законом. Статья 16 французской Конституции определяет

[1] Чиркин. В Е. Вызовы современности и развитие Французской конституции// В.Е Чиркин -2018

действия в экстремальных обстоятельствах. Президент Республики принимает все меры, которые диктуются этими обстоятельствами, после официальной консультации с Премьер-министром, с председателями палат, а также с Конституционным советом. В Конституции РФ относительно этого вопроса есть статья 88. Президент Российской Федерации вводит на территории РФ или в отдельных ее местностях чрезвычайное положение с незамедлительным сообщением об этом Федеральному Собранию. В случае с РФ, Президент обязан уведомить, но он не обязан консультироваться с кем-либо, как это происходит во Франции. Представлена некоторая самостоятельность в этом вопросе.[1]

Полномочия и статус Президента можно признать схожими в некоторых положениях. Не смотря на то что фигура Президента Франции представлена достаточно сильно, во многих моментах он скован необходимостью советоваться и консультироваться с другими ветвями власти. Деятельность Президента отслеживается Советами того или иного рода. (Данным Советам так же посвящены отдельные Разделы 7 и 11.) Во Франции есть некая децентрализация, делегирование части управления на другие гос. органы, хотя есть и включенность Президента во все ветви власти.

Еще наиболее интересными главами будут разделы III, IV, V Конституции Франции. В них представлены: Правительство, Парламент и отношения между ними. Разделы III и IV в сравнении аналогичных глав 6 и 5 Конституции РФ, не так объемы по своему содержанию, но это компенсируется наличием дополнительного раздела V, который урегулирует взаимоотношения между этими гос. органами. В французской Конституции, разделе, посвященном правительству, закреплены основные задачи и цели Правительства, полномочия премьер министра и функции члена Правительства. Полномочия Премьер-министра представлены в статье 21: он руководит деятельностью Правительства. Несет ответственность за национальную оборону. Обеспечивает исполнение законов.

Глава 6 Конституции РФ включает структуру Правительства РФ, статус Председателя Правительства, функции и полномочия Правительства, а также взаимодействие с другими органами, в частности с Президентом и Гос. Думой. Полномочия Председателя Правительства РФ в статье 113 представлены более скромно: основные направления деятельности регламентируются другими законодательными документами. Здесь, как и во многих других моментах Конституция РФ переносит конкретизацию и закрепление функций, полномочий и статуса в целом на другие нормативно-правовые акты

Раздел 4 Конституции Франции посвящен Парламенту, и, как и раздел 3, имеет небольшой объем. Включает в себя статьи конкретизирующие цели Парламента, количественный состав, форму и организацию работы. Глава 5 Конституции РФ представляет структуру Федерального собрания, сроки избрания палат, вопросы, находящиеся в ведение, функции, форму и организацию работы, кто может быть членом Государственной Думы и Совета Федерации и др. Как и в предыдущем сравнении, глава Конституции РФ более подробна.

Раздел 6 Конституции Франции, как уже упоминалось выше, определяет взаимоотношения между Правительством и Парламентом. Определяется список полномочий, задач и функций, форма и организация работы.[2]

Не маловажным фактором, является и возможность внесения поправок в действующие конституции. Оба основных закона являются по своему типу жесткими, внесение в них поправок требует исполнения определенных регламентов и правил. Конституция Франции по способу изменения является "особо жестокой", для её пересмотра требуется проведение двух этапов - принятие поправок и их ратификация. Проект пересмотра согласно ст. 89 должен быть одобрен палатами парламента в идентичной

[1] Конституция Российской Федерации: офиц. Текст.- М: ЭКСМО, 2018- 36с

[2]Конституция Франции (на русском языке) [https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/constitution/constitution_russe_version_aout2009.pdf]

редакции. После принятия поправок требуется их обязательная ратификация, которая может быть осуществлена двумя способами: либо на, либо в Конгрессе.

Говоря о Конституции России, предложение вносится в Государственную Думу и рассматривается в трех чтениях. После закон обязательно должен быть опубликован и направлен в законодательные органы субъектов РФ. Они обязаны рассмотреть закон о поправке в течение одного года со дня его принятия. После того как не менее чем две трети субъектов РФ одобрят данный закон, он направляется Президенту РФ для подписания и официального опубликования.

Проведя сравнительный анализ, можно сделать определенные выводы. Во-первых, Конституция Франции имеет более усложненную структуру и историю своего принятия. Во-вторых, различным является и восприятие статуса президента. Также во Франции есть необходимость президенту консультироваться при принятии важных решений. Конституция Франции детализирована и даже раздроблена по отношению к основному закону РФ в своем содержании. Разделы включают в себя многие другие вопросы, никак не упомянутые в Конституции РФ. В случае нашей страны, они представлены скорее другими нормативно-правовыми актами. К тому же чуть ранее уже отмечалась тенденция Конституции РФ оставлять возможность закреплять некоторые положения путем ФКЗ, ФЗ и т.д.[1] Если говорить о содержании Глав и Разделов, то оно тоже различно. В отношении РФ по большей части четко прописаны основные моменты и вопросы ведения той или иной ветви власти, что кажется нам более рациональным, возможно более близкого знакомства со своим основным законом. Но, даже в этом случае, иногда не хватает детализированности и большей ясности. Так же значение имеет и расположение разделов и статей в общей структуре. Относительно РФ оно достаточно логично обосновано. Все эти различия, на наш взгляд, могут быть вызваны более обширным историческим опытом французской Конституции, наличием большей практики в принятии различных «пробных ее версий», а также разностью менталитетов. Но не смотря на все это можно найти много полезного и необходимого для реализации и усовершенствования своей конституционно-правовой базы.

ОТВЕТСТВЕННОСТЬ ЗА ИЗЪЯТИЕ АККАУНТОВ У «ЗАКОННЫХ» ПОЛЬЗОВАТЕЛЕЙ В ИНТЕРНЕТЕ

Китов Александр Владимирович,
студент 3 курса обучения Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Для начала надо поставить некоторые вопросы, чтобы наиболее полно раскрыть данную проблему. Один из ключевых вопросов: Можно ли считать кражу самого аккаунта преступление? Российское законодательство пока обходит эту тему стороной, но дискуссии, которые активно проходят на различных форумах говорят нам, что данная проблема есть.

Сложность признания кражи аккаунта заключается в некоторых правовых вопросах:

1) Являются ли аккаунты в социальных сетях или различных интернет платформах собственностью? Если не собственность то, что это?

2) Поддается ли контролю киберпространство? Можно ли его отрегулировать с помощью законодательства, которое мы применяем оффлайн («вне сети») и возможно ли это?

[1] Мишин А.А. Конституционное право зарубежных стран. Учебник. - М.: Белые альвы, 2017.

3) Хорошо ли, что государство пытается вмешиваться в киберпространство и нужно ли это?

Законодательство Российской Федерации говорит нам, что право собственности содержит в себе несколько прав, которыми обладает только собственник: владение, пользование и распоряжение.

Владение это фактическое господство лица над вещью. Пользование – основанная на законе возможность извлечения полезных свойств вещи. Да у лица создавшего аккаунт и являющегося пользователем данного аккаунта действительно есть право владения и пользования, а вот в праве распоряжения есть некоторые “подводные камни”. Распоряжение – основанная на законе возможность определения юридической судьбы вещи. Но аккаунт на данный момент является интеллектуальной собственностью компании. Между компанией и пользователем заключается лицензионный договор. Приведу пример одной не без известной игры «ArcheAge». Локализатором игры в России является компания «Mail.ru Group». К лицензионному соглашению заключаемому с пользователем, идет приложение «Правила Игры «ArcheAge», где нам нужен пункт 3, который гласит: ”Всем Лицензиатам в Игре запрещено осуществлять следующие действия со своими игровыми аккаунтами и игровыми персонажами: продажа; покупка; обмен; передача; дарение; распространение информации о намерении совершить указанные действия как самим Лицензиатом, так и любыми третьими лицами.”. Да, из этого следует, что все в рамках правового поля, но я хотел бы отметить то что это интеллектуальной собственностью является платформа которой мы пользуемся, а информация содержащаяся на наших пользовательских аккаунтах принадлежит нам. Наше право на тайну переписки и информацию охраняется законом. Из выше сказанного сложно назвать аккаунт вещью, а тем более его квалифицировать, как имущество на которое может распространяться право собственности.

Тогда отвечу на вопрос что такое аккаунт? Аккаунт – это учетная запись на сайте, портале или в мобильном приложении. В аккаунте содержится информация общего доступа, которую мы сами о себе выкладываем (дата рождения, возраст, увлечения, место учебы или работы, реальные ФИО, фотографии и т.п.) и информацию, которую видят отдельные пользователи являющимися твоими собеседниками в киберпространстве.

Кража по ч.1 статьи 158 УК РФ, является тайное хищение чужого имущества. Под хищением в статьях настоящего УК РФ понимаются совершенные с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества. Но как мы уже выяснили, собственником пользователь аккаунта не является, в виду отсутствия у него всех прав собственника. Встает вопрос: “А как же тогда защитить права пользователя, у которого изъяли аккаунт из пользования?”. Тут нам могут помочь “Поддержка пользователей” – это своего рода “правоохранительный орган” в различных социальных сетях и электронных платформах. “Поддержка” – занимается возвратом аккаунтов, “законным” пользователям с которыми было заключено лицензионное соглашение. Конечно, все понимают чем отличается “поддержка пользователей” и “правоохранительный орган”. Наличие властных функций отсутствующие у “поддержки пользователей”. В рамках своей социальной сети и электронной платформы “поддержка пользователей” действительно может наказывать, как недобросовестных (нарушающих лицензионное соглашение) пользователей так и лиц, которые изымают аккаунты у их “законных” пользователей.

У правоохранительных органов тоже есть рычаги влияния на граждан совершающих преступления в сети интернет. УК РФ предусматривает по меньшей мере два состава по которым можно привлекать к уголовной ответственности, но они связаны не с изъятием аккаунта у “законного” пользователя, а связаны с информацией хранящейся на данном аккаунте. Это статья 138 Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений УК РФ и статья 272 Неправомерный доступ к компьютерной информации УК РФ.

Поддается ли контролю киберпространство? Да, сейчас мы это можем наблюдать по тем ФЗ уже вступившим в силу: Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" получившим прозвище в народе Закон о «суверенном интернете». Также ещё только проходящим Федеральное собрание, но нет никаких оснований, что данный закон не будет принят “Закон об обязательной предустановке российского ПО на смартфоны”.

Можно ли киберпространство отрегулировать с помощью законодательства, которое мы применяем оффлайн («вне сети») и возможно ли это? Думаю, что любое законодательство это нормотворчество. Из чего я делаю вывод, что попытаться отрегулировать можно. Что из это получится? Вот вопрос, на который сложно дать однозначный ответ.

Хорошо ли, что государство пытается вмешиваться в киберпространство и нужно ли это? Я думаю, что это неизбежно в силу сущности государства. Государство хочет узаконить все отношения возникающие, чтобы защищать интересы своих граждан и себя в киберпространстве. Киберпространство же не очень радо видеть ещё одного “игрока” на своем поле, так как очень сложно выделить границу суверенитета государства в интернет пространстве, а ещё сложнее понять, что находится в его компетенции.

Список использованных источников

Нормативно-правовые акты:

1. «Конституция Российской Федерации»(принята всенародным голосованием 12.12.1993)(с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)// «Собрание законодательства РФ», 04.08.2014, N 31, ст. 4398.
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ // Собрание законодательства Российской Федерации от 15 декабря 2003 г. N 50. Ст. 4848.
3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 03.08.2018) / Собрание законодательства РФ, 05.12.1994, N 32, ст. 3301
4. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 01.09.2018) / Собрание законодательства РФ, 29.01.1996, N 5, ст. 410
5. Федеральный закон “О финансовой аренде (лизинге)” от 29.10.1998 года № 104-ФЗ с изменениями и дополнениями от 29.01.2002 года // Российская газета - 1998 - № 211 от 5.11. 1998 г. - С. 4, 6; 2002 - № 21 от 2.02.2002 г.

ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ №152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ» И РЕГЛАМЕНТ ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕВРОПЕЙСКОГО СОЮЗА «О ЗАЩИТЕ ФИЗИЧЕСКИХ ЛИЦ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И О СВОБОДНОМ ОБРАЩЕНИИ ТАКИХ ДАННЫХ, А ТАКЖЕ ОБ ОТМЕНЕ ДИРЕКТИВЫ 95/46/ЕС»: СРАВНИТЕЛЬНО-ПРАВОВОЙ АСПЕКТ

Алексеева Алена Алексеевна, Устинова Алина Витальевна,
студенты Российской академии народного хозяйства и
Государственной службы при Президенте РФ
Челябинской филиал (РАНХиГСЧФ)
Научный руководитель:
Запрутин Денис Григорьевич,
доцент Российской академии народного хозяйства и
Государственной службы при Президенте РФ
Челябинской филиал (РАНХиГСЧФ)

В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение.[1] Научный прогресс существенно облегчил доступ в получении любой информации, включая персональную, тем самым вторгаясь в сферу свободы человека.[2]Проблема обеспечения безопасности персональных данных стала одной из самых обсуждаемых на сегодняшний день. Об этом свидетельствует большое количество произведенных в последние годы атак на персональные данные человека. Появляется необходимость совершенствования правового механизма защиты персональных данных.

В данном контексте представилось необходимым произвести анализ и сравнение Федерального закона России №152-ФЗ «О персональных данных» и Регламента Европейского парламента и Совета ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС». В работе также использовались научные исследования Кафтанниковой В.М., Шумекеевой Г.Б.

Целью научной работы является сравнительный анализ нормативных правовых актов РФ и ЕС, регулирующих вопросы о персональных данных, и выявление сходств и различий отдельных положений данных актов. Для достижения поставленной цели необходимо решить ряд задач:

1) обозначить определение термина «персональные данные» и проанализировать принципы и условия обработки и хранения данных в РФ и ЕС;

2) изучить права и обязанности сторон, обрабатывающих данные;

3) обозначить органы, осуществляющие контроль и надзор за обработкой персональных данных и исследовать меры ответственности и санкции в случае нарушения требований обработки персональных данных;

4) выдвинуть предложения по совершенствованию законодательства, касающегося персональных данных.

Прикладная часть исследования выполнена на основе метода сравнительно-правового анализа, также были использованы общенаучные и специальные методы исследования: синтез, обобщение, дедукция, сравнительный анализ, логическое заключение.

Основная цель ФЗ «О персональных данных» и Регламента ЕС заключается в обеспечении защиты права человека на защиту персональных данных. Согласно ст.3 ФЗ «О персональных данных» и ст.4 Регламента ЕС, под персональными данными подразумевается любая информация, относящаяся к прямо или косвенно определенному физическому лицу (субъекту персональных данных). Основываясь на ст.1 ФЗ России субъектами правоотношений являются федеральные органы государственной власти, органы государственной власти субъектов РФ, иные государственные органы, органы местного самоуправления, иные муниципальные органы, юридические и физические лица. Обрабатываются данные от имени оператора. Объект - отношения, связанные с обработкой персональных данных граждан государства. В Регламенте ЕС субъекты правоотношений - физическое или юридическое лицо, органы государственной власти, агентства или иные органы, которые обрабатывают данные от имени контролера. Объектом являются персональные данные физических лиц.

В обоих актах используется понятие «трансграничная обработка», что означает передачу персональных данных субъекту, находящемуся на территории иностранного государства. Проанализировав территориальное действие, было выявлено, что Регламент ЕС действует на территории ЕС и за его пределами. А ФЗ России действует для граждан непосредственно на

---

[1] Парасеков А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. №110(06). URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-pravovogo-regulirovaniya-zaschity-personalnyh-dannyh-v-rossii-i-za-rubezhom (дата обращения: 20.11.2019).

[2] Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира // Право: современные тенденции: материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). — Краснодар: Новация, 2018. — С. 47-49.

территории государства. Однако ст. 12 предусматривает передачу данных за пределы государства в случае, если эта страна является стороной Конвенции Совета Европы[1].

Перейдем к принципам обработки и хранения персональных данных. Согласно ст.5 ФЗ «О персональных данных» и ст.5 Регламента ЕС, общими принципами являются: законность, ограниченность достижением конкретных целей, справедливость, а также принятие необходимых мер, гарантирующих своевременное удаление или исправление неточных данных. В Регламенте ЕС также отмечается, что обработка данных должна осуществляться беспристрастно и прозрачным образом в отношении субъекта данных.[2] В ФЗ «О персональных данных» отмечены обеспечение точности и достаточности данных, а также их уничтожение либо обезличивание по достижении целей обработки.

Обратимся к ст.6 ФЗ «О персональных данных» и ст.6 Регламента ЕС (общие условия): «Обработка данных считается законной при условиях, если субъект дал согласие на обработку; если обработка необходима для защиты жизненных интересов субъекта данных».[1] Стоит отметить, что ФЗ «О персональных данных» содержит больший перечень условий обработки данных.

Ст.10 ФЗ России и ст.9 Регламента ЕС на общих основаниях не допускает обработку данных, касающихся расовой / национальной принадлежности, политических взглядов, религиозных убеждений, интимной жизни.[3] Обработка допускается если: субъект дал прямое согласие; обработка выполняется в сфере трудового законодательства, социального обеспечения и в других случаях. Ст.8 Регламента ЕС затрагивает обработку персональных данных ребенка. Она является законной, если ребенку исполнилось 16 лет, или согласие было дано лицом, обладающим родительской ответственностью. В ст.9 ФЗ России упоминается лишь, что в случае недееспособности субъекта согласие на обработку дает законный представитель субъекта.

Правам субъекта посвящены гл.3 ФЗ России и Регламента ЕС. К ним относят: право на доступ к его персональным данным; право на получение уведомления относительно изменения или уничтожения данных; право на запрос и получение данных субъекта в прозрачной и легкодоступной форме. В ФЗ «О персональных данных» также отмечены: право использовать данные в целях продвижения товаров, работ, услуг на рынке, в целях политической агитации.[1]

Гл. 4 нормативных актов прописывает обязанности оператора (контролера), например: предоставление субъекту необходимой информации; обеспечение записи, систематизации, накопления, хранения, уточнения, извлечения данных и другие. Регламентом ЕС предусмотрена должность инспектора по защите данных, задачами которого являются консультирование и контролирование лиц, обрабатывающих данные. А ст.42 свидетельствует о необходимости внедрения сертификационных механизмов защиты данных на различных уровнях.[2]

Контроль и надзор за обработкой данных, согласно ст.23 ФЗ России и гл.6 Регламенту ЕС осуществляется уполномоченным органом по защите прав субъектов: в Регламенте - надзорным органом, в РФ - Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.[1] Согласно ст.24 ФЗ России за нарушение требований законодательства, лица несут дисциплинарную, уголовную, административную ответственность и т.д.[4] В Регламенте ЕС более подробно обозначены правовые средства

---

[1] Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 20.11.2019).

[2] Регламент Европейского Парламента и Совета ЕС 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных URL: https://ogdpr.eu/ru/gdpr-2016-679 (дата обращения: 21.11.2019).

[3] Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 21.11.2019).

[4] Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 22.11.2019).

защиты субъектов и применяемые санкции, в гл.4 прописаны размеры административных штрафов.

Подводя итоги, можно сказать, что ФЗ России и Регламент ЕС обладают одинаковым назначением и целью и имеют схожие субъекты, при этом имеют различное территориальное действие. Акты провозглашают схожие принципы обработки и хранения данных, но имеют различную степень проработки условий обработки данных, принадлежащих несовершеннолетним. Акты гарантируют ряд общих, но в некоторых случаях, различных прав субъектов, а также устанавливают разный объем обязанностей и требований к лицам, работающих с данными. ФЗ России и Регламент ЕСрегламентируют осуществление контроля и надзора схожими органами власти, при этом устанавливают различные меры ответственности и санкции в случае нарушения требований данных актов.

Считаем нужным выдвинуть ряд предложений по совершенствованию ФЗ «О персональных данных». Во-первых, разработка системы безвозмездного предоставления гражданам электронной подписи значительно повысит конфиденциальность ряда операций и документов, позволит упростить получение согласия на обработку данных, особенно в случаях с несовершеннолетними. Во-вторых, законодательное ограничение срока хранения и введение обязательной процедуры уничтожения данных после истечения этого срока обезопасит граждан от нецелевого использования данного рода информации в дальнейшем. В-третьих, ужесточение мер ответственности для операторов и увеличение размеров штрафов за нарушения действующего законодательства позволит минимизировать такое явление, как утечка персональных данных.

В современных условиях интерес к изучению, взаимному использованию и обмену опытом развития нормативной правовой базы в области персональных данных стремительно растет, поэтому считаем, что как российскому, так и европейскому законодательству есть, что изменить и перенять из ФЗ России и Регламента ЕС.

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Вихарева Мария Руслановна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

На современном этапе развития общества цифровые технологии прочно закрепились в жизни людей. Они используются не только в личных целях простыми обывателями, но и, благодаря росту технологического развития, давно стали применяться в работе различных государственных структур.

Главной целью внедрения цифровых ресурсов в государственные органы является повышение эффективности механизмов государственной деятельности.

Использование информационных систем закреплено на законодательном уровне. Например, в Федеральном законе от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности» в статье 6 говорится о том, что «в ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде». Кроме того, применение

перечисленных средств предусмотрено Федеральным законом РФ от 14.11.2002 №138-ФЗ «ГПК» в части 7 статьи 10 «гласность судебного разбирательства» о возможности фиксирования судебного процесса лицами участвующими в деле и присутствующими на заседании.

В настоящее время использование цифровых технологий применяется в том числе при раскрытии и расследовании преступлений и продолжает развиваться. По сравнению с 2008 годом сводится не только к использованию фотоаппаратов и киноаппаратуры. Рассмотрим данную тему на примере деятельности органов следствия.

Одной из главных задач использования фото-, киносъемки и иных электронных ресурсов, о которых речь пойдет ниже, в следственных органах является поиск информации, которая может стать источником для начала проведения различных мероприятий в предварительном расследовании.

Одним из направлений выступает сбор доказательственной информации.

Например, получение таких данных, как изображение открытых участков местности осуществляется путём зондирования поверхности земли. В связи с этим между Следственным Комитетом РФ и Научным центром оперативного мониторинга Земли РКС (НЦОМЗ) заключено соглашение, на основании которого Следственный Комитет, следователи имеют возможность получать актуальную информацию о конкретном месте в конкретное время: местоположение движимых/недвижимых объектов и людей, что значительно упрощает их поиск. Чтобы понять, насколько эффективно сотрудничество с Научным центром, то стоит сказать о статистике. С 2016 года НЦОЗМ было обработано в интересах следствия 175 заявок о получении материалов космической съемки для расследования наиболее значимых и резонансных преступлений.[1]

Кроме того, эффективным в расследовании преступлений является использование нововведённых различных компьютерных систем автотранспорта, которые помогают установить необходимые данные о преступлении вследствие аварий. Такое устройство, как регистратор данных о событии АВТО (EDR ACU) может фиксировать различные параметры, например: состояние защелки замка ремней безопасности водителя/пассажира, находившегося на переднем сиденье; положение рычага переключения передач; обороты двигателя; показания спидометра и иную информацию, которая помогает установить следователю такие фактические обстоятельства дела, которые не могли бы быть выяснены без использования данного устройства, и сконцентрироваться на объективных данных, имеющих значение для дела.[2]

Также стоит обратить внимание на получение информации об абонентах связи. Ещё в 2010 году в УПК была введена статья 186.1 «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», в связи с которой в настоящее время используется аппаратно-программный комплекс «Сегмент-С». При помощи него следователи проводят анализ сетей сотовой связи, выявляют вероятное периодическое пересечение абонентов, совместное нахождение, маршруты движения, точки последней регистрации и другие данные, на основании которых могут производиться следственные действия в отношении найденных лиц.

Доступ к цифровым ресурсам имеют не только государственные структуры, но и граждане, с которыми они работают ежедневно. Поскольку в нынешний день использование социальных сетей находится на высоком уровне, то соответственно преступления в этой сфере тоже набирают обороты. В 2018 году было совершено около 150 000 преступлений, связанных с информационными технологиями. В связи с этим следственные органы стали активно проводить поисково-аналитическую работу в социальных сетях и изучения интернет-активности пользователя. Есть несколько комплексов для осуществления этой деятельности. Такие, как «Лис-М», «Belkasoft», например, позволяют найти не только

[1] https://ru-bezh.ru/press-releases/29797-speczialistyi-rks-pomogayut-raskryivat-prestupleniya-i-dobivatsy
[2] http://sudexpertiza.by/assets/docs/8vist/pre.pdf

конкретного пользователя в сети «Интернет», но и связанных с подозреваемым других лиц, а также выяснить другую информацию(кластеры, метрики центра и иные технические данные), необходимую для расследования дела, что значительно ускоряет и упрощает поиск лиц и информации.[1]

Для нынешнего времени не является новым использование в качестве доказательственной информации данных с мобильных устройств. Органы предварительного расследования могут получить доступ не только к находящейся непосредственно на устройстве информации, но и к удаленной: SMS, журналу звонков, фото-, видеофайлам и использованию браузеров. Она помогает в проектировании версий преступлений, в доказывании виновности/невиновности определенных лиц, а также установить наличие/отсутствие приготовительных действий к преступлению или сокрытие следов преступления. Но здесь нужно обратить внимание на использование обновленных современных программных ресурсов. Если до 2016 года следственные органы применяли в своей работе UFED TK (аппаратно-программный комплекс для криминалистических исследований мобильных устройств), то в 2017 году органы оформили заказ на усовершенствованную версию данного комплекса. С 2018 года стал применяться UFED Touch с последующими обновлениями. Это было вызвано в том числе тем, что продукция Apple получила большое распространение среди населения. И поскольку система блокировки считается одной из наименее уязвимых, то у государственных органов возникла потребность в получении данных с Apple. Поэтому усовершенствованием стала возможность использования UFED Touch для взлома данных устройств до версии 11.2.6, установленной на моделях iPhone 8 и iPhone X (по состоянию на 2018 год). Следовательно, у органов предварительного расследования появилась возможность выявлять преступления не только пользователей Android и Windows, но и Apple, что увеличивает статистику раскрываемости преступлений.[2]

В заключение необходимо сказать, что использование информационных ресурсов в деятельности государственных органов по раскрытию и расследованию преступлений является одной из первоочередных задач в связи с тем, что технологии постоянно развиваются. И соответственно, с увеличением различных программ растёт количество не только их пользователей, но и возможностей для совершения преступлений. Следовательно, чтобы незамедлительно реагировать на совершение противоправных деяний, получать наиболее полную информацию об обстоятельствах, необходимых для дела, и повышать эффективность в расследовании преступлений, органы предварительного расследования должны использовать в своей деятельности современные информационные ресурсы, которые должны постоянно обновляться и подстраиваться под темп развития технологий, для своевременного выполнения своих целей и задач. И, как видно из прогресса, применение технологий не стоит на месте и все больше внедряется в работу государственных органов.

РИСКИ ОТ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Зажигин Вадим Владимирович,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)

[1]Ткачев А.В. Исследование компьютерной информации в криминалистике / А.В. Ткачев // Эксперт-криминалист. 2012. N 4. С. 5 – 7.
[2]https://www.cnews.ru/news/top/2018-03-14_rossijskie_pravoohraniteli_zakupayut_tehniku_dlya

Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Понятия «преступления в сфере высоких технологий» в российском законодательстве нет. Ученые также расходятся во мнениях. Например, А.А. Комаров полагает, что преступления в сфере высоких технологий и преступления, совершаемые посредством сети Интернет совпадают по своей сути.[1] Л.А. Доровских утверждает, что преступление в сфере высоких технологий – это преступление, которое направлено на причинение вреда человеку, обществу и государству с использованием любых технических средств, которые могут иметь выход в Интернет[2]. Но если обратиться к нормативным актам Министерства внутренних дел Российской Федерации, то можно заметить, что в них идет отождествление преступлений в сфере высоких технологий с преступлениями, совершенными с использованием информационно-телекоммуникационных сетей, включая сеть Интернет и компьютеров. Это указано «Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» (приказ МВД России № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 06.10.2006 г. (ред. от 22.09.2009 г.).[3]

Преступления в сфере высоких технологий можно разделить на 4 группы в зависимости от мотива киберпреступника:

1. Преступление связано с неправомерным завладением чужим имуществом (как правило, денежные средства);
2. Преступление связано с неправомерным доступом к информации (с целью перепродажи или «для себя»);
3. Преступление связано с вмешательством в работу системы для доступа к управлению ей (для собственной выгоды, либо для ущерба конкуренту);
4. Другие преступления.

Комитет экспертов Совета Европы по оценке мер борьбы с отмыванием денег (сокр. MONEYVAL) выделяют несколько видов риска от киберпреступлений:

1. Технические
2. Операционные
3. Юридические
4. Географические.

Однако мне кажется данная классификация слишком обобщенной. Я бы предложил рассматривать риски более детально с учетом самой сути угрозы и потенциального ущерба обществу и государству.

Первым риском является относительная открытость баз данных. Чтобы подключиться к системе международной торговли и организовать поставку товаром из зарубежья очень просто, это может сделать любой желающий с наличием доступа в Интернет. А из-за того, что это сделать просто, то просто и незаконно подключиться к этой сети.

Вторым риском является скорость совершения киберпреступления, а также его низкая стоимость. Подключение к сети происходит довольно быстро, а преступники, как правило, уже знают, что ищут. Это значит, что украсть информацию или удалить её – дело нескольких минут. Низкая стоимость обусловлена тем, что для взлома сети не требуется практически ничего, кроме компьютера и подключения к Интернету.

Третьим риском я бы назвал относительную медлительность законодателя в сфере высоких технологий. Технологии не стоят на месте, они постоянно развиваются.

---

[1] Комаров А. А. О критериях общественной опасности, преступлений в сфере высоких технологий // Актуальные вопросы права, экономики и управления: сб. статей IX Международной научно-практической конференции. Пенза, 201

[2] Доровских Л. А. Преступления в сфере высоких технологий. Киберпреступность // издание. 2016. № 4 (28).

[3] Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 06.10.2006 г. (ред. от 22.09.2009 г.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 47.

Законодатель же не всегда успевает за введением новых терминов в законы. Это означает, что законодательство практически всегда отстает от киберпреступности, не вводя меры предупреждения и меры по борьбе с ней.

Четверым риском можно назвать анонимность совершения преступления в сфере высоких технологий. Хакер очень редко находится в непосредственной близости от своего объекта. Он может находиться вообще в другой стране или даже на другом континенте. К тому же многие страны ещё не ввели достаточно суровые наказания за преступления в данной сфере. Добавим сюда сложность в обнаружении и раскрытии преступлений такого рода.

Пятым риском является организованность киберпреступников. Успешная кибератака не может быть совершена одним человеком. Для этого организуются целые группы, порой – транснациональные. К тому же, действия киберпреступников могут быть связаны с элементами традиционной преступности для легализации полученных денежных средств.

Бороться с киберпреступностью необходимо, так как она может причинить серьезный материальный ущерб. В этом направлении уже раньше было создано Управление «К» в МВД РФ, которое борется с преступлениями в сфере информационных технологий и незаконным оборотом радиоэлектронных средств и специальных технических средств. А 1 ноября 2019 года на заседании коллегии МВД РФ было принято решение о создании подразделения, которое будет бороться с преступлениями в сфере IT. Связано это с ростом преступлений в данной сфере. Генеральная прокуратура сообщает, что 1 преступление из 7 совершается в сфере IT.[1]

КРИМИНАЛИЗАЦИЯ ГЛАВЫ 28 УК РФ «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Гагарин Андрей Николаевич,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

В XXI веке большую роль в нашей жизни играют Интернет-технологии. Они развиваются с каждым днём. Создаются различными компаниями программное обеспечение для смартфонов, компьютеров и.т.д. И в связи с этим увеличивается число преступлений в данной сфере. Если мы посмотрим статистку преступления в сфере компьютерной технологии, то мы можем увидеть следующее[2]:

	Ст. 272 УК	**Ст. 273 УК**	**Ст. 274**	**Ст. 274.1**
2016 год	62	123	-	
2017 год	74	128	-	
2018 год	50	79	-	-

И на основании данной статистики мы можем сделать следующий вывод, что в РФ высокий уровень преступлений в сфере компьютерных технологий.

В действующей редакции УК РФ посвящена 28 глава и называется она «Преступления в сфере компьютерной информации». Глава предусматривает четыре

[1] В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий // https://xn--b1aew.xn--p1ai/news/item/18809813 (дата обращения: 29.11.2019).
[1] Количество осужденных по данным составам преступления. Информация предоставлена с сайта [2] http://stat.xn-----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 //Дата обращения 28.11.2019.

состава преступления. Глава претерпела значительные изменения в частности предмета совершения преступления. В первоначальной редакции предмет преступления – это ЭВМ[1].

Со временем не только ЭВМ стал обладать функциями получения, обработки и передачи информации. И в 2011 году в главу 28 УК РФ были внесены изменения, и термин «ЭВМ» и всё, что с ним было связано был изменен на новый термин «компьютерная информация». И тем самым законодатель расширил предмет посягательств, поскольку теперь носителем компьютерной информации могла быть не только ЭВМ, но и иной другой предмет-носитель.

Что касается в плане санкций, то можно сказать, что они относительно мягкие. Штраф по ч. 1 ст. 272 УК РФ составляет 200 000 рублей и это очень низкий размер штрафа, поскольку объем причиненного имущественного вреда может быть горазда больше штрафа. И сторона, которой причинен преступлением вред взыскивает с обвиняемого материальный вред в соответствии с нормами ГК и ГПК. И, если он загладил причиненный вред, то он подлежит освобождению от уголовной ответственности на основании ст. 76.1 УК РФ. А остальную часть денежной суммы, он может свободно реализовать и при этом он не был подвергнут уголовному наказанию.

И исходя из вышесказанного я полагаю, что необходимо увеличить санкции данной статьи, чтобы количество преступлений по данной статье снизилось.

За последние пять лет участились случаи DDoS-атак[2], спаминга[3], фишинга[4]. И на данный момент это подробно не урегулировано УК РФ. Данные формы деяния предусмотрены ст. ст. 159, 272, 273УК РФ, И на мой взгляд было бы уместным с целью объединить схожие формы деяния в одну статью ввести в УК РФ новую статью 273.1 УК РФ «Хакерская атака». В примечании к данной статье давалось понятие «Хакерская атака». Под хакерской атакой в данной статье понималось бы действие, лица, обладающим специальными знаниями в области взлома и обхода программ безопасности с целью захвата контроля над различными уровнями компьютерных сетей. Субъект по данной статье – специальный – хакер[5]. Субъективная сторона выражалась в форме умысла как прямого, так и косвенного.

ГОСУДАРСТВО И ПРАВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Косова Марина Васильевна,
студент Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:

[1]Электро́нно-вычисли́тельная маши́на (сокращённо ЭВМ) — комплекс технических, аппаратных и программных средств, предназначенных для автоматической обработки информации, вычислений, автоматического управления // *Першиков В. И., Савинков В. М.* Толковый словарь по информатике / Рецензенты: канд. физ.-мат. наук А. С. Марков и д-р физ.-мат. наук И. В. Поттосин. — М.: Финансы и статистика, 1991. — 543 с. — 50 000 экз. — ISBN 5-279-00367-0.

[2]DoS — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

[3]Спам — массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получать.

[4]Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

[5] Хакер - квалифицированный компьютерный взломщик, злоумышленник, специализирующийся на поиске и использовании несанкционированного доступа в вычислительные сети или другое компьютеризированное оборудование для незаконного получения информации, извлечения выгоды, нанесения ущерба.

Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Развитие современного государства характеризуется совершенствованием цифровой экономики, которая образует внутренний рынок производства, использования и потребления цифровых и информационно-коммуникационных технологий в обществе[1].

Цифровизация, как таковая, направлена на достижение основной цели, которая состоит в цифровой трансформации уже существующих и создании новых отраслей экономики, трансформации сложившихся сфер жизнедеятельности в новые, современные и более эффективные, что возможным станет только в результате интеграции идей, действий, инициатив и программ, касающихся цифровизации, в национальные, региональные, отраслевые стратегии и программы развития.

Положительное воздействия технологий на эффективность, качество, стоимость и результативность деятельности – экономической, общественной и личной, обеспечило признание цифровизации как весьма эффективного механизма экономического роста.

Цифровыми технологиями одновременно образуются огромный рынок и индустрия, и платформа для эффективности и конкурентоспособности всех других рынков и индустрий. Создание высокотехнологичного производства и модернизация промышленности с применением новых информационно-коммуникационных и цифровых технологий, масштабы и темпы цифровых трансформаций становятся приоритетом экономического развития[2].

Выражением основных характеристик государственного развития стают масштаб и темпы цифровых трансформаций. Цифровые технологии при системном государственном подходе к их повсеместному внедрению приведут к значительному ускорению развития открытого информационного общества как существенного фактора развития демократии в стране, роста производительности, экономического роста, а также повышения качества жизни граждан.

Цифровое развитие государства предполагает решение комплекса задач, которые призваны оказать положительное влияние на экономику, бизнес, общество и жизнедеятельность страны в целом.

Основные цели цифрового развития государства заключаются:

– в ускорении экономического роста и привлечении инвестиций;

– в трансформации существующих секторов экономики в эффективные и конкурентоспособные;

– в технологической и цифровой модернизации промышленности с созданием высокотехнологичных производств;

– в доступности преимуществ и возможностей цифрового мира для населения страны;

– в развитие цифровых индустрий и цифрового предпринимательства, реализации человеческого потенциала[3].

Быстрее, дешевле и качественнее растут сектора экономики, которые используют цифровые технологии. Благодаря цифровым технологиям стают намного эффективнее такие сферы жизнедеятельности, как образование, медицина, транспорт. Они подвергаются модернизации, создавая при этом новую ценность и качество, поэтому весьма важно, чтобы происходила цифровизция экономики как можно более быстро. Ускоренное цифровое развитие предполагает:

---

[1] Баранов Д.Н. Сущность и содержание категории "цифровая экономика" // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление. 2018. № 2 (25). С. 16-17.

[2] Тян Н.Г. Готовность России к цифровизации // Глобальный научный потенциал. 2018. № 4 (85). С. 83.

[3] Коваленко Е.И. Доступ к информации: правовые гарантии в условиях информационного общества // Информационное право. 2019. № 3. С. 5.

– устранение законодательных, институциональных, фискальных и иных помех, которые препятствуют развитию цифровой экономики;

– стимулирование и мотивацию бизнеса и отраслей экономики в целом для их поощрения к цифровизации;

– создание спроса и формирование потребностей к цифровизации у граждан через внедрение масштабных проектов цифровых трансформаций государством, в том числе, на основе современных моделей государственно-частного партнерства;

– создание и развитие цифровой инфраструктуры как основы для использования преимуществ цифровых технологий в повседневной жизни и платформы для повышения эффективности экономики вообще;

– развитие и углубление цифровых компетенций граждан, обеспечение готовности их к использованию цифровых возможностей, преодоления сопутствующих этому рисков;

– развитие использующего цифровые технологии предпринимательства и создание соответствующих инфраструктур для поддержки и развития инновационной деятельности (включая аналоговые), внедрение с этой целью механизмов фондирования, стимулирования и поддержки[1].

Одно из направлений процессов информатизации заключается в формировании системы электронных государственных услуг как способа взаимодействия государства, населения и организаций по предоставлению информации, включая частные запросы, организации государственных (муниципальных) закупок, оказанию государственных услуг, формированию системы обратной связи (институт жалоб) и т.п.

Грамотная информатизация публичной администрации способствует открытости и прозрачности государственного сектора, поэтому современное государство должно стремиться к обеспечению своих граждан и бизнес-организаций контакты с учреждениями и публичными администрациями на основе электронного доступа[2].

В условиях функционирования цифрового государства существенному видоизменению подвергаются старые объекты правового регулирования и в то же время возникают новые, вызывающие затруднение в определении их принадлежности к определенным отраслям права или законодательства. К потенциальным объектам цифровизации могут быть отнесены государство, суверенитет, гражданство, личность, источники права и многое другое даже в недалекой перспективе.

Возникают также новые вызовы, которые связаны с инновационным типом правового регулирования, суть которого заключается в регулировании общественных отношений на опережение, постоянной его модернизации, затрагивающей и систему источников права, которые предполагают:

– взаимосогласование созданных государством и санкционированных им источников;

– возрастание роли корпоративного права, общих принципов права, судебных прецедентов, диспозитивных норм;

– появление нетрадиционных, дополнительных, гибких источников;

– переход основной нагрузки в вопросах правового регулирования от государства к другим, негосударственным субъектам (надгосударственным и «подгосударственным») за счет изменений в соотношении управления и самоуправления, централизации и децентрализации.

Право должно еще осмыслить новые вызовы, возникающие перед ним и обществом в эпоху цифрового развития. К числу таких вызовов относятся:

– формирование новых объектов правового регулирования в виде цифровой личности, цифрового суверенитета, цифровой Конституции, цифровой демократии и др., традиционному праву еще не известных;

---

[1] Курицына З.В. Роль государства в цифровизации экономики России // Центральный научный вестник. 2018. Т. 3. № 9S (50S). С. 35.

[2] Тян Н.Г. Готовность России к цифровизации // Глобальный научный потенциал. 2018. № 4 (85). С. 85.

– обеспечение прав и свобод человека в цифровом государстве;

– утрата государством существующих общеизвестно присущих ему свойств и элементов и приобретение новых;

– унификация правового регулирования;

– модернизация системы источников права и других его элементов[1].

Осмысление возникающих вызовов развитию правовой науки неизбежно задаст вектор и определит выбор между инновационным и традиционным правовым регулированием.

Литература:

1. Баранов Д.Н. Сущность и содержание категории "цифровая экономика" // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление. 2018. № 2 (25). С. 15-23.

2. Коваленко Е.И. Доступ к информации: правовые гарантии в условиях информационного общества // Информационное право. 2019. № 3. С. 4-8.

3. Курицына З.В. Роль государства в цифровизации экономики России // Центральный научный вестник. 2018. Т. 3. № 9S (50S). С. 35-36.

4. Тян Н.Г. Готовность России к цифровизации // Глобальный научный потенциал. 2018. № 4 (85). С. 83-85.

5. Черевко В.В. Цифровизация и правовые интересы Российской Федерации // Вестник Московского гуманитарно-экономического института. 2019. № 2. С. 132-137.

ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: ПЕРСПЕКТИВЫ БОРЬБЫ С НИМИ

Суровцева Екатерина Сергеевна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Высокий уровень развития информационных технологий - вот главная и отличительная черта XXI века. Эффективность борьбы с преступностью напрямую зависит от информационно-технологического оснащения этой деятельности.

За последнее десятилетие сети Интернет стали масштабным пространством, в котором люди могут: дистанционно работать, заниматься общественной деятельностью, общаться, получать информацию и т.д. Цифровые технологии настолько крепко вошли в нашу жизнь, что в настоящее время мы просто уже не можем представить без них своей жизни. Ежедневно мы выполняем различные коммуникации: операции с денежными средствами, прокладываем маршруты, покупаем билеты для путешествия (авиа, ж/д и др.), выбираем кафе/ресторан, сеанс в кинотеатре.

Но с появлением процесса глобальной цифровизации возникли новые угрозы и риски в сфере общественных отношений. Это связано с распространением киберпреступлений. В главе 28 Уголовного Кодекса Российской Федерации предусмотрена ответственность за преступления в сфере компьютерной информации. Но нет иных правовых актов в российском законодательстве, которые бы предусматривали соответствующие понятия и ответственность за незаконные действия в сфере информационных технологий.

[1] Черевко В.В. Цифровизация и правовые интересы Российской Федерации // Вестник Московского гуманитарно-экономического института. 2019. № 2. С. 134.

И так, под киберпреступлениями понимаются преступления, совершаемые в сфере информационных технологий[1]. Эти преступления отличаются латентностью, т.е. сложно раскрываемые, могут иметь трансграничный характер, т.е. могут совершаться на территории нескольких государств, и традиционно считаются «беловоротничковыми».

Генеральная прокуратура России опубликовала данные о росте преступности в РФ. Количество зарегистрированных преступлений разных видов увеличилось за год на 67%. Активнее всего развиваются преступления в сфере информационных технологий – рост оказался двукратным. За январь-сентябрь 2019 года в РФ было зарегистрировано 205 116 киберпреступлений. В первую очередь эти преступления совершены с использованием ИКТ или в сфере компьютерной информации[2].

Самыми популярны способами мошенничества являются:

1. **Обман по телефону.** На телефонный номер звонят незнакомые люди и говорят, что ваш близкий человек в беде (ДТП, попал в аварию и тд). Мошенники требуют передать деньги, чтобы «выручить потерпевшего». Суммы бывают самые разные от несколько сотен рублей до миллионов.
2. **SMS-просьба о помощи.** Приходит сообщение: «Мне срочно нужна помощь. Отправь 1000 рублей на этот номер, мама».
3. **Выигрыш в лотерее.** Вам приходит сообщение: «Вы выиграли в лотерее! Ваш выигрыш составил 1 млн. рублей! Для получения денег будет необходимо оформить перевод на реквизиты «123456789».».
4. **Звонок с информацией о блокировке банковской карты.** Мошенник представляется сотрудником банка и указывает, что у банка идет процесс перевыпуска всех банковских карт, для сохранения всех денежных средств необходимо сообщить ПИН-код.
5. **Распространение противоправной информации** (клевета, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду).
6. **Через Интернет**. Вредоносное вмешательство через компьютерные сети в работу различных систем.
7. **Преступления в Интернете, направленные против несовершеннолетних.** Сообщества в социальной сети Вконтакте «Синий Кит», «Черный Дельфин» и др.

В настоящее время преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ. Сотрудники этого управления занимаются борьбой с незаконным оборотом радиоэлектронных средств и специальных технических средств. В состав Управления «К» входит также Бюро специальных технических мероприятий (БСТМ), штат которого в МВД планируют существенно увеличить в 2020 году.

Как уже было упомянуто ранее, преступления в информационной сфере могут совершаться, когда злоумышленник и жертва находятся в разных странах. Поэтому необходимо создание международной координации борьбы с преступлениями такого рода. Такая координация есть, но РФ пока не подписала Конвенцию Совета Европы ETS №185 из-за несогласия с трансграничным доступом к компьютерным системам.

Однако в Министерстве Внутренних Дел РФ 1 ноября 2019 года было принято решение о создании в структуре Министерства подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологий», – сообщила официальный представитель МВД России Ирина Волк.

Глава МВД России подчеркнул, что эти новые подразделения будут сформированы по отраслевому принципу в пределах имеющейся штатной численности, как в центральном аппарате Министерства, так и в территориальных органах внутренних дел[3].

---

[1]https://ru.wikipedia.org/wiki/Преступления_в _сфере_высоких_технологий.

[2] https://genproc.gov.ru/stat/data/1724584/ Статистический сборник "Состояние преступности в России за сентябрь 2019 г."

[3] https://xn--b1aew.xn--p1ai/news/item/18809813 В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий

Таким образом, подтверждается актуальность обозначенной темы и необходимость в развитии и разработке положений и предложений деятельности государственных органов и органов местного самоуправления. А деятельность государственных органов и органов местного самоуправления зависит, в свою очередь, от высокого уровня развития информационных технологий и от информационно-технологического оснащения этой деятельности.

К ВОПРОСУ О РОЛИ СОЦИАЛЬНЫХ СЕТЕЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Урюпина Мария Михайловна,
студент 2 курса Северного (Арктического) Федерального Университета имени М.В. Ломоносова

В современном обществе все большее значение приобретают процессы цифровизации и информатизации. Эти явления не могут и не затрагивать и публично-правовую сферу.

Одним из элементов цифровизации является увеличение роли социальных сетей, как средства коммуникации и источника информации. Безусловно, большое значение в правовом аспекте данного явления принадлежит вопросам защиты персональных данных, уголовно-правовой оценке публикуемых при помощи сети «Интернет» сведений, а также технологическим способам обеспечения государственной и общественной безопасности. «Интернет», как воспринимаемая в общественном сознании область «вседозволенности» и «безграничной свободы», перестает быть таковой. Технические возможности контроля цифрового пространства возлагают на пользователей сети обязанность осуществления самоконтроля за действиями в социальных сетях в том числе. Вместе с тем, проводится повсеместная борьба с анонимными пользователями, исключается возможность создания анонимных аккаунтов в социальных сетях, от законодателей звучат предложения ужесточения порядка регистрации в социальных сетях – введение возрастного ограничения и верификации по паспорту.

В указанных примерах наблюдается стремление на законодательном уровне урегулировать интернет-пространство. В то же время, наблюдается тенденция увеличения роли и качественного изменения значения социальных сетей в процессе государственного управления. Однако, данная сфера при всей ее важности не является предметом должного законодательного регулирования.

Анализ практики использования государственными органами и должностными лицами различных социальных сетей показывает, что в основном они применяются в следующих целях:

- информирование населения о направлениях деятельности органа государственной власти;
- выявление общественного мнения;
- выражение субъективной позиции представителей органов государственной власти по значимым вопросам государственной политики;
- прием обращений граждан.

Так, например, Государственная Дума использует свои официальные аккаунты в социальных сетях для публикации новостей о внесенных предложениях, рассматриваемых и принятых законопроектах. Кроме того, активно проводятся при помощи специальных инструментов опросы общественного мнения по наиболее важным и острым вопросам.

Однако, подобная деятельность пресс-служб органов власти не регламентируется специальными положениями об организации информационной деятельности, отсутствуют и регламенты корпоративной этики сотрудников органов власти, осуществляющих данную деятельность.

Уникальную практику использования социальных сетей органами публичной власти можно обнаружить на муниципальном уровне. Постановление Мэрии города Грозного от 24 сентября 2018 года № 89 предусматривает порядок рассмотрения обращений граждан, поступивших на официальные страницы Мэрии города в социальных сетях[1]. Тем самым обеспечиваются дополнительные гарантии на обращение граждан в органы местного самоуправления. Данные нормы безусловно носят позитивный характер, т.к. значительно облегчают возможность обращения в муниципальные органы власти. Порядок подачи такого обращения прост: гражданин при помощи аккаунта в социальной сети отправляет заявление через предусмотренные интернет-платформой способы, администратор (сотрудник департамента отдела информации и печати департамента делопроизводства и социальной защиты) обрабатывает данное обращение и перенаправляет в необходимый отдел Мэрии города.

Принципиальную важность имеет в таком случае наличие специального нормативного правового акта, гарантирующего гражданам рассмотрение их заявление при таком способе его подачи. Официальные аккаунты в социальных сетях имеют большинство муниципальных образований, но преимущественно они выполняют исключительно информационное предназначение[2].

Особое место в вопросе роли социальных сетей в деятельности органов государственной власти занимают личные аккаунты представителей органов государственной власти, где они нередко высказывают в менее официальной форме свою позицию по каким-либо вопросам. Например, Председатель Правительства в своем аккаунте в социальной сети Twitter высказывает личное мнение о возможности перехода к четырёхдневной рабочей неделе, о некоторых событиях межгосударственного масштаба, о бюджетной политике, а также позицию относительно действий иностранных государств и др. С одной стороны, данные заявления носят неофициальный характер, поскольку не имеют никакой юридической силы, однако, воспринимаются в международной практике как официальная позиция государства и активно транслируются в средствах массовой информации.

Проблема использования социальных сетей в качестве подобного инструмента органов государственной власти заключается в технологической уязвимости аккаунтов в социальных сетях и отсутствия особого способа их защиты от внешнего «взлома».

Случаи, когда неизвестным удается получить доступ даже к уже упомянутому аккаунту Председателя Правительства – не редкость. Пока в подобных примерах от лица Председателя Правительства неизвестным удавалось публиковать только тексты бессмысленного содержания. Однако подобные ситуации могут иметь крайне неблагоприятные последствия, и, как заверяют эксперты, полностью обезопасить аккаунты представителей власти и гарантировать недопущение подобных казусов не представляется технической возможности[3].

Таким образом, роль социальных сетей в правовой сфере и деятельности органов государственной власти постепенно возрастает. В связи с этим, следует уделять большее внимание законодательному регулированию использования социальных сетей при осуществлении государственного управления и целесообразности такого использования, учитывая все технологические аспекты данного вопроса и уровень возможных негативных результатов, вследствие действий хакеров.

---

[1] Постановление от 24 сентября 2018 года N 89 Об утверждении Порядка рассмотрения обращений граждан, поступивших на официальные страницы (аккаунты) в социальных сетях Мэрии города Грозного [Электронный ресурс] Режим доступа: http://docs.cntd.ru/document/430360601.

[2] Рысай Б.Г. Обращения с жалобами граждан посредством социальных сетей // В поисках научных инноваций, Ростов-на-Дону, 2015. С. 75-83.

[3] Хакеры вдохнули «новую жизнь» в Twitter Дмитрия Медведева, Коммерсант [Электронный ресурс] Режим доступа: https://www.kommersant.ru/doc/3999428.

Список источников:

1. Постановление от 24 сентября 2018 года N 89 Об утверждении Порядка рассмотрения обращений граждан, поступивших на официальные страницы (аккаунты) в социальных сетях Мэрии города Грозного [Электронный ресурс] Режим доступа: http://docs.cntd.ru/document/430360601.
2. Рысай Б.Г. Обращения с жалобами граждан посредством социальных сетей // В поисках научных инноваций, Ростов-на-Дону, 2015. С. 75-83.
3. Хакеры вдохнули «новую жизнь» в Twitter Дмитрия Медведева, Коммерсант [Электронный ресурс] Режим доступа: https://www.kommersant.ru/doc/3999428.

ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Никитенко Анастасия Александровна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Негативной чертой такого позитивного явления как глобальная цифровизация стал рост преступности в сфере информационных технологий и совершенствование таких преступлений. Одной из основных причин возникновения преступлений в этой сфере стало информационно-технологическое переоборудование учреждений, предприятий и организаций, наделение их компьютерной техникой, базами данных, программным обеспечением. Повсеместная цифровизация стала глобальной угрозой и переманила на свою сторону не только добросовестных пользователей, но и преступников, для которых это также достаточно удобно.

Понятие преступление в сфере высоких технологий для уголовного права и криминалистики относительно новое. В современной криминологии понятие «высокие технологии» относится к информационно - телекоммуникационной среде, где преступления совершаются с использованием компьютеров или разнообразных средств связи.

Впервые данный термин стал использоваться в США, позднее и в других странах с высоко развитыми компьютерными технологиями в 60-х гг. XX в. Термин возник для удобства обозначения преступлений, орудием или предметом которых стали компьютерные средства или компьютерная информация.[1]

Некоторые ученые утверждают, что в юридическом смысле термин «компьютерное преступление» довольно слаб и предлагают заменить его более подходящим — «информационное преступление» по причине того, что объектом «является не техника, а информация, хранящаяся, обрабатываемая, передаваемая, той техникой».[2]

Ряд авторов уравнивают преступления, совершаемые в сфере высоких технологий с преступлениями, совершенными при помощи телекоммуникационных сетей, в том числе, сети Интернет. Так, Д. К. Чирков и А. Д. Саркисян относят преступления в сфере высоких

[1] См.: Кушниренко, С. П. Методика расследования преступлений в сфере высоких технологий: конспект лекций / С. П. Кушниренко. — СПб.: Санкт-Петербургский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2007. — с. 4 — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/65487.html (дата обращения: 30.11.2019).

[2] См.: Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1995. С. 81.

технологий к новым способам и видам совершения преступлений, возникшим в результате распространения информационно-телекоммуникационных сетей, сети Интернет.[1]

Интернет является одним из самых популярных средств обмена информацией для совершения противоправный действий со стороны недобросовестных лиц. Ежедневно с его помощью люди осуществляют поиск необходимой информации, совершают покупки, общаются, обмениваются данными, размещают информацию о себе, что делает каждого из нас максимально уязвимым и незащищенным перед угрозами современности, которые развиваются так же быстро и стремительно, как все то, что делает нашу жизнь в разы удобнее. Количество информации, передаваемой посредством глобальной сети Интернет имеет тенденцию к постоянному росту, что говорит о реальной зависимости государств и каждого отдельно взятого лица от информационной инфраструктуры.

Для более четкого понимания необходимо разграничить преступления в данной сфере и обратиться к классификации «цифровых преступлений», предложенной Осипенко А.Л., которая делит их на три группы:

- компьютерные преступления (хищение данных, нарушение авторских прав на программное обеспечение, хищение компьютерного времени, нарушение работы вычислительных систем и т. д.);
- преступления, «связанные с компьютерами» (в основном финансовое мошенничество);
- сетевая преступность (использование сетей Интернет для совершения незаконных сделок — распространение порнографии, торговля наркотиками, отмывание денег, уклонение от таможенных пошлин и т. д.).[2]

Термин «высокие технологии» научным сообществом трактуется широко и вызывает большое количество споров. В целом высокие технологии можно определить, как наиболее прогрессивные и новые технологии, которые включают множество отраслей: робототехнику, электронику, генную инженерию, нано технологии, информационные технологии и многое другое.

Получается, что «высокие технологии» - широкое и собирательное понятие, которое не следует ограничивать конкретным способом, средством, или орудием совершения преступления или сферой преступного посягательства. Такой подход к определению является наиболее разумным потому, как высокие технологии беспрерывно развиваются и совершенствуются, а вместе с ними развивается и преступность в данной сфере, которую можно представить в виде статистических данных для наглядности.

Согласно статистике, в 2017 году количество преступлений в сфере информационно-телекоммуникационных технологий возросло с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% - это почти каждое 20 преступление. Наиболее часто встречающимися киберпреступлениями являются создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ), неправомерный доступ к компьютерной информации (статья 272 УК РФ),.[3]

Если в 2017 году зарегистрировано 1 883 таких преступления (+7,7%), то за первое полугодие 2018 г. – 1 233 (+3,4%). При этом на 19,6% уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), увеличилось на 30,5% (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3%. Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Их количество в первом полугодии 2018 г. возросло в 7 раз.[4]

---

[1] См.: Чирков Д.К., Саркисян А.Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. – 2013. – № 1 (24). – С. 25–32.

[2] См.: Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт. М., 2004. С. 64

[3] https://genproc.gov.ru/smi/news/genproc/news-1431104/

[4] Там же.

Такая статистика говорит о том, что правоохранительные органы не могут противостоять росту преступности в данной сфере, что, возможно, связано с довольно-таки размытой правовой базой. Глава 28 Уголовного Кодекса РФ содержит в себе нормы, регулирующие преступления в сфере компьютерной информации. Этим законодатель ограничивает сферу высоких технологий в Уголовном законе. Нормы, не включенные в главу 28, но относящиеся к сфере высоких технологий содержатся в иных главах, которые регулируют совершенно иной объект. Такой разброс создает трудности для правоприменителя и вызывает сложности в борьбе с преступностью. Необходимо указать на то, что и сами преступники без особых усилий адаптируют свою деятельность под активно развивающиеся технологии, совершенствуют свои знания, тем самым влияя на раскрываемость преступлений.

Список использованных источников

1. Кушниренко, С. П. Методика расследования преступлений в сфере высоких технологий: конспект лекций / С. П. Кушниренко. — СПб. : Санкт-Петербургский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2007. — 67 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/65487.html (дата обращения: 30.11.2019).
2. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт. М., 2004. – 432 с.
3. Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1995. – 88 с.
4. Чирков Д.К., Саркисян А.Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. – 2013. – № 1 (24). – 184 с.
5. https://genproc.gov.ru/smi/news/genproc/news-1431104/

ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Косолысова Полина Игоревна,
студент Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Становление и развитие информационного общества в России потребовало переосмысления иерархии охраняемых уголовным законом общественных отношений. Действующим уголовным законом установлена ответственность за общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. Данная группа посягательств является преступлениями в сфере компьютерной информации. Они объединены законодателем в главу 28 Уголовного кодекса Российской Федерации (далее – УК РФ[1]). К указанным посягательствам относятся: неправомерный доступ к компьютерной информации; создание, использование и

[1] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 04.11.2019) // Собрание законодательства РФ.1996. № 25. Ст. 2954.

распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 272-274 УК РФ).

Интенсивность развития информационных технологий обуславливает необходимость и в изменении законодательства, которое должно отвечать их уровню развития. Уголовное законодательство должно отражать изменения видов преступлений, посягающих на информационную безопасность. Поэтому важно постоянное переосмысление информационной безопасности как социальной ценности и принятие адекватных мер уголовно-правового реагирования за посягательства на нее. Все это в совокупности определяет высокую значимость совершенствования теоретических и практических основ уголовно-правового механизма противодействия преступлениям против компьютерной безопасности, и анализ законодательной конструкции ст. 272-274.1 УК РФ – обладает прикладным значением, является актуальным направлением и предметом научного исследования в данной работе.

Отметим, что с 01 января 2018 года глава 28 УК РФ дополнена еще одним самостоятельным составом преступления - “Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации” (ст. 274.1 УК РФ)[1]. Данная норма введена законодателем в связи с принятием закона "О безопасности критической информационной инфраструктуры Российской Федерации". Данный закон также вступил в действие с 01 января 2018 года[2].

Преступления рассматриваемой категории посягают на общественные отношения, складывающиеся по поводу обеспечения конфиденциальности, целостности и доступности компьютерной информации, сохранности средств, используемых для ее обработки. Законодатель занимает активную позицию по их совершенствованию. Так, в 2011 году в рассматриваемую главу 28 были внесены кардинальные изменения - все три ее статьи предстали в новой редакции[3]. Однако заложенный в уголовном законе механизм привлечения к ответственности за вандализм - эффективен далеко не всегда.

Так, по официальным данным уголовной статистики, за 2018 год судами Российской Федерации за преступление, предусмотренное: ст. 272 УК РФ, было привлечено к ответственности 62 чел. (по основной квалификации) и 85 чел. (по дополнительной квалификации); ст. 273 УК РФ - 123 чел. (по основной квалификации) и 59 чел. (по дополнительной квалификации); ст. 274 УК РФ - 2 чел. (по дополнительной квалификации)[4]. Как видим, рассматриваемые преступления – получают достаточно широкое распространение в правоприменительной деятельности. При этом, следует учитывать высокую степень общественной значимости их объекта.

Основной объект преступлений, предусмотренных ст. 274 и 274.1 УК РФ – совпадает с объектом деяний ст. 272 и 273 – это общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Обратимся к анализу правоприменительной практики квалификации преступлений в сфере компьютерной информации и определим некоторые вопросы ее совершенствования. Научно-технический прогресс, совершенствование производства и, как следствие, удешевление компьютерной техники, программного обеспечения и услуг связи обусловили процесс непрерывного роста использования информационно-коммуникационных технологий. Можно с

---

[1] Федеральный закон от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ. 2017. N 31 (Часть I). Ст. 4743.

[2] Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ. 2017. N 31 (Часть I). Ст. 4736.

[3] Федеральный закон от 07.12.2011 N 420-ФЗ (ред. от 03.07.2016) "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" // Собрание законодательства РФ. 2011. N 50. Ст. 7362.

[4] Официальный сайт Судебного Департамента при Верховном Суде РФ. URL:http://www.cdep.ru/index.php?id=79 (дата обращения 28.11.2019).

уверенностью утверждать, что продолжается он и до настоящего времени. При этом, увеличение числа пользователей открыло новые возможности и для преступной деятельности.

Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасного поведения личности - компьютерной преступности (computer crime)[1]. Следует отметить, что в отечественной теории уголовного права нет общепринятой дефиниции подобного рода гибридных преступлений. Используются различные категории: информационные преступления, киберпреступления, преступления в сфере высоких технологий, интернет-преступления[2].

Информатизация преступности рождает ряд непростых вопросов для совершенствования уголовного закона по противодействию компьютерным преступлениям, например: каким должно быть оптимальное количество составов преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры; есть ли необходимость в изменении диспозиции традиционных составов преступлений; и др.

Так, ряд исследователей скептически отнеслась к криминализации мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ)[3]. Появление специальной нормы о мошенничестве в сфере компьютерной информации имело, по сути, обратный эффект, отмечают исследователи, поскольку вызвало еще больше проблемных вопросов[4].

Пленум высшей судебной инстанции отметил, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ[5].

Не вызывает сомнений, что самостоятельным видом преступлений, совершаемых с использованием ИКТ, являются компьютерные преступления, т.е. деяния, посягающие на охраняемую законом информацию и безопасность информационно-коммуникационной инфраструктуры. Природа данных преступлений специфична в том смысле, что само их происхождение, существование и, следовательно, совершение немыслимы без информационной среды. В этом аспекте отечественное уголовное законодательство, а именно главы 28 УК РФ, требует серьезной доработки. Научному сообществу и законодателю еще потребуется оценить необходимость криминализации DDoS-атаки, спаминга, фишинга и др.

В настоящее время все больше внимания уделяется цифровой безопасности и сам факт соблюдения тем или иным обладателем информации, предоставляющим информационные сервисы, принципов безопасности является составляющей деловой репутации. При этом все чаще объектом современных кибератак являются персональные данные пользователей атакуемых сервисов, а целью атаки является получение доступа к этим данным. В случаях возникновения таких инцидентов возникает проблема в доказывании ущерба, причиненного субъекту персональных данных, поскольку эти данные не оцениваются в каком-либо количественно-качественном выражении, могут дублироваться другими сервисами, и в случае утечки источник этой утечки почти не подлежит идентификации. В целях доказывания ущерба, причиненного кибератакой с неправомерным доступом к данным, целесообразным было бы

[1] Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. N 8. С. 73 - 80.
[2] Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: Монография. М., 2015. 136 с.
[3] Винокуров В.Н. Причинение вреда двум и более потерпевшим как основание ужесточения наказания и формы его закрепления в Уголовном кодексе РФ // Современное право. 2017. N 4. С. 98-103.
[4]Шевелева С.В. Свобода воли и субъективные признаки состава преступления // Актуальные проблемы российского права. 2014. N 3. С. 423 - 433.
[5] Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" // Бюллетень Верховного Суда РФ. 2018. N 2.

использование цифровых отпечатков (digital fingerprints), позволяющих отслеживать те или иные экземпляры файлов и источники их получения[1].

Большинство организаций не имеют возможности самостоятельно провести оперативное расследование обстоятельств осуществления злоумышленниками кибератаки в отношении их, поэтому рекомендуется незамедлительно обратиться в правоохранительные органы после выявления возникшей угрозы информационной безопасности. Также надлежит незамедлительно уведомить об инциденте безопасности провайдера, организующего доступ к сети, посредством которой осуществляется атака на сервер (провайдер сети Интернет, через который подключен атакуемый сервер или хостинг-провайдер, обслуживающий сервер, на котором размещен атакуемый информационный ресурс).

При появлении подозрений о совершении атаки надлежит осуществить блокирование счетов, доступ к которым возможен посредством сети Интернет, поскольку злоумышленник, имеющий целью хищение денежных средств с помощью полученной информации, постарается совершить его незамедлительно (определение суда от 24.04.2013 по делу N 22-2480 по ст. 273 УК РФ.

В целом, отметим, что построение информационно-коммуникационной инфраструктуры закономерно обуславливает формирование новой формы общественно опасного поведения личности - компьютерной преступности.

Следствием глобальной информатизации является изменение облика преступности в целом, которая в связи с использованием информационно-коммуникационных технологий приобретает все новые признаки. Процесс их использования в механизме преступления (информатизация преступности) актуализирует необходимость научного осмысления состояния и перспектив развития отечественного уголовного права.

Реформирование отечественного уголовного законодательства, регламентирующего преступные посягательства в сфере компьютерных технологий, должно осуществляться по трем основным направлениям:

- расширение перечня преступлений, посягающих на информационную безопасность (так, с 01 января 2018 года в УК РФ введена новая норма – ст. 274.1 УК РФ);
- криминализация новых высокотехнологичных форм посягательств на традиционно охраняемые уголовным законом общественные отношения;
- модернизация действующих составов преступлений путем детализации их совершения специфическим способом - с использованием информационно-коммуникационных технологий.

Список использованных источников:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 04.11.2019) // Собрание законодательства РФ.1996. № 25. Ст. 2954
2. Федеральный закон от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ. 2017. N 31 (Часть I). Ст. 4743.
3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ. 2017. N 31 (Часть I). Ст. 4736.
4. Федеральный закон от 07.12.2011 N 420-ФЗ (ред. от 03.07.2016) "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" // Собрание законодательства РФ. 2011. N 50. Ст. 7362.

[1] Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. 2017. N 1. С. 17 - 21.

5. Официальный сайт Судебного Департамента при Верховном Суде РФ. URL: http://www.cdep.ru/index.php?id=79 (дата обращения 28.11.2019)
6. Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. N 8. С. 73 - 80.
7. Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: Монография. М., 2015. 136 с.
8. Винокуров В.Н. Причинение вреда двум и более потерпевшим как основание ужесточения наказания и формы его закрепления в Уголовном кодексе РФ // Современное право. 2017. N 4. С. 98-103.
9. Шевелева С.В. Свобода воли и субъективные признаки состава преступления // Актуальные проблемы российского права. 2014. N 3. С. 423 - 433.
10. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" // Бюллетень Верховного Суда РФ. 2018. N 2.
11. Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. 2017. N 1. С. 17 - 21.

РЕАЛИЗАЦИЯ СТ. 171.2 УК РФ НА ПРИМЕРЕ ИНТЕРНЕТ-КАЗИНО

Шабашова Наталья Александровна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Понятие игорной деятельности содержится в ст.171.2 УК РФ, к такойдеятельности относится организация или проведение азартных игр (где игрок рискует, чтобы получить выигрыш): с применением специального оборудования для игр за пределами установленных игорных зон, в том числе в интернете; без наличия соответствующей лицензии на данные действия.

В соответствии с УК РФ за организацию азартных игр грозят наказания от штрафа до лишения свободы на длительный срок в зависимости от обстоятельств нарушения. Так, за совершение незаконной игорной деятельности без квалифицирующих признаков нарушителю в соответствии с ч.1 ст. 171.2 грозят следующие виды наказания: штраф в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до четырех лет, либо лишением свободы на срок до двух лет.

Если действия, описанные в первой части были проведены группой лиц по предварительному сговору или сопряженные с извлечением дохода в крупном размере, то наказания будут серьёзнее: штраф в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от трех до пяти лет либо лишением свободы на срок до четырех лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет или без такового.

Третья часть статьи 171.2 УК РФ за азартные игры предусматривает следующие наказания за деяния, совершенные организованной группой или лицом с использованием своего служебного положения или сопряженные с извлечением дохода в особо крупном размере: штраф в размере от одного миллиона до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от четырех до пяти лет либо лишением свободы на срок до шести лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Примечания. 1. Под систематическим предоставлением помещений в настоящей статье понимается предоставление помещений более двух раз.

2. Доходом в крупном размере в настоящей статье признается доход, сумма которого превышает один миллион пятьсот тысяч рублей, а в особо крупном размере - шесть миллионов рублей.

В ходе проведения проверки по данной категории дел следователю необходимо найти доказательства следующих главных моментов:

-виновным действительно организованы или проводились азартные игры;

-в деятельности использовалось специальное оборудование, непосредственно предназначенное для проведения таких игр;

-нарушителем организовано онлайн-казино;

-у организатора игорной деятельности нет лицензии, которая является обязательной для проведения игр.

Основные этапы расследования выглядят следующим образом. Оперативники устанавливают факт совершения преступной деятельности, личность нарушителей, полученный доход и способы сокрытия незаконных азартных игр. Сотрудники устанавливают наблюдение за незаконным казино и собирают необходимые сведения. Осуществляется установление местонахождения организаторов игорной деятельности. Оперативники совершают мнимую сделку, чтобы установить порядок работы преступной организации. Уполномоченные должностные лица проверяют документацию организации и оборудование, на котором проводятся игры. Проводится опрос возможных свидетелей, официальные осмотры места проведения игр, очные ставки, экспертизы и другие необходимые следственные действия.

Хотяпроведениеазартныхигрв интернетебылозапрещенофедеральнымзакономещев 2006 году, а с 2014 годаРоскомнадзорзаноситонлайн-казинов реестрзапрещенныхсайтов, пользователейза игрунаказатьнельзя, а закрытьмногиетакиеплощадкиневозможно — ихоператорызарегистрированыв офшорныхзонах. Теневойоборотрынкаинтернет-казинов Россииможноценитькак минимумв $3 млрд, говоритРБК.

Сервердля онлайн-казиноможнопоставитьгде угоднои оказатьсявне досягаемостивластей — в итогетакихсайтовпоявилосьмножество. ВРоссииинтернет-казинов основномнаходятсяв теснойсвязкес букмекерскимиконторами, покер-румами, игорнымисайтами, ломбардамии онлайн-ресурсамипо ставкамна спорт, где можетпредлагатьсяв завуалированнойформепопробоватьпоигратьв азартныеигры. Такиесайтыактивнорекламируются, например, с помощью файлообменныхресурсов, а такжечерез сайтыдля онлайн-просмотрафильмов. Запретрекламыонлайн-казинопрямопредусмотренв

- Федеральномзаконеот 13.03.2006 N 38-ФЗ (ред. от 08.03.2015, сизм. от 03.07.2016) «Орекламе»:

Статья 7. Недопускаетсяреклама: 1) товаров, производствои (или) реализациякоторыхзапрещенызаконодательствомРоссийскойФедерации;

- Кодексе Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 12.11.2019)

Статья 14.3 КоАП РФ. Нарушение законодательства о рекламе

1.Нарушение рекламодателем, рекламопроизводителем или рекламораспространителем законодательства о рекламе, за исключением случаев, предусмотренных частями 2 — 6 настоящей статьи, частью 4 статьи 14.3.1, статьями 14.37, 14.38, 19.31 настоящего Кодекса, — влечет наложение административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей; на должностных лиц — от четырех тысяч до двадцати тысяч рублей; на юридических лиц — от ста тысяч до пятисот тысяч рублей.

Также широко известен способ владения интернет-казино через офшорную лицензию таких государств и территорий, как Кюрасао, Мальта, Гибралтар.Например, для получения лицензии на работу в Евросоюзе онлайн-казино должно уплатить сбор в размере от нескольких десятков тысяч евро и получить разрешение комиссии, которая учитывает источники финансирования, наличие криминального прошлого у владельца, программное обеспечение, которое намерена использовать площадка, и т.д. Эта же комиссия следит за тем, выплачивает ли онлайн-казино выигрыши и не отмывает ли оно деньги.

Хитрая схема: принцип работы онлайн-казино

Начну с того, что интернет-казино категорически не подходят для инвестиций. Тем более для получения стабильного дохода. Большинство людей играют, чтобы утолить жажду азарта. И правильно делают, потому что тех, кто рассчитывают обеспечить себе безбедное существование за счет гемблинга, ждет громадное разочарование. Они обязательно потеряют свои деньги.

Есть ли реальное интернет-казино, которое работает честно?

Да, и не одно. Все они функционируют по лицензии, а также покупают или арендуют специальный игровой софт. В его основе генератор случайных чисел (настолько, насколько это технически возможно). Его данные интерпретируются в результаты спина, броска или карточной раздачи. Легальные онлайн-казино — дорогие проекты. В них нужно вложить очень много денег. Но затраты обязательно окупятся, потому что они приносят своим владельцам постоянную и очень высокую прибыль. Честные интернет-казино работают по лицензии Коста-Рики, Антигуа и Барбуды, Панамы, Мальты, Гибралтара, а также других государств, где сетевой игорный бизнес разрешен на законодательном уровне. Открывать онлайн-казино в России незаконно с 2007 года. Поэтому легальные русскоязычные площадки регистрируются за рубежом.

Мошенники в мире онлайн-казино

Обычно они мимикрируют под известные площадки и практикуют фишинг. Это когда электронный адрес отличается на несколько букв или очень похож на копируемый. Выиграть у мошенника нереально. Все автоматы взломаны и находятся на сервере, который принадлежит ему, а не производителю игры. Поэтому он полностью их контролирует. Даже если игроку чудом удастся одержать победу, ему ни за что не дадут вывести деньги. Онлайн-казино, которые обманывают, появляются регулярно. Единственный способ там заработать — стать владельцем, что не является законным в Российской Федерации.

Вывод

Судебная статистика за 2018 год показывает следующие результаты:

- 1306 правонарушителей осуждено;
- 0 оправдано;
- приговорены к лишению свободы 76;
- лишены свободы условно 567;
- приговорены к ограничению свободы 23;
- штраф получили 512;
- исправительные работы 1;
- обязательные работы 83;
- принудительные меры к невменяемым 1;

В 2016 году было осуждено 1277 преступников, а в 2017 1378.

Сравнивая результаты, можно отметить, что статистика нестабильна, число раскрытых преступлений то увеличивается, то уменьшается, однако преступления в сфере организации и проведения азартных игр в настоящее время имеют место быть, и в условиях развивающейся цифровизации становятся всё актуальнее.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕХАНИЗМ ЕЕ ОБЕСПЕЧЕНИЯ

Дубинин Максим Евгеньевич,
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич *-*
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

В настоящее время происходит активное развитие информационных технологий, следствием чего является выход проблем информационной безопасности государства на передний план в рамках системы обеспечения национальной безопасности страны. Растет роль таких составляющих национальной безопасности, как политическая, экономическая, военная, правоохранительная и т.д.

Современное информационное общество вводит новые геополитические ориентиры, которые определяют направления деятельности различных структур государства в информационном пространстве. В понятие «информационное общество» вкладывают множество смыслов, однако, суть в том, что распространение информации становится основной направляющей либо сдерживающей силой развития всех сфер жизни общества.

Развитие и внедрение информационных технологии помогают трансформации привычных критериев оценки военной мощи и политических возможностей государств. Видоизменяются и традиционные формы силового противоборства. На первый план выходят военные действия (различные по формам и способам применения войск и сил), основные цели которых достигаются за счет главным образом информационного превосходства, затем уже технологического.

В случае рассмотрения политической стабильности в контексте национальной безопасности, главной характеристикой стабильности государства становится способность эффективного реагирования на внешние угрозы. Учитывать необходимо и то, что политическая система способна адекватно реагировать на информационные агрессивные воздействия внешней среды, что позволяет говорить об обеспечении высокой степени политической стабильности в условиях глобализации.

Стабильное состояние политической системы, в свою очередь, должно способствовать повышению уровня управляемости социальными процессами, где обычные граждане могут реализовывать собственные права и политические интересы.

Вследствие этого, появляется всё большая необходимость в последовательной государственной политике в области обеспечения информационной безопасности, с обязательными определенными требованиями к субъектам информационных отношений, для дальнейшего стабильного развития общества.

В Российской Федерации динамично развиваются такие процессы информатизации как построение электронного государства и правительства, становление электронного правосудия и т.п. Это происходит в связи с возрастанием роли информационной сферы,

переосмыслением её сути в качестве важного фактора жизни, который непосредственно влияет на все виды национальной безопасности.

С каждым днем возникает потребность регламентации и правовой оценки информационных отношений. Уже успело сложиться понимание, что свобода информации будет являться главным атрибутом развивающегося гражданского общества. а защита информационного пространства в подобных условиях – это одна из основных задач государства и общества[1]. Соответственно, информационная безопасность становится всё более значимой в общей системе обеспечения национальной безопасности нашей страны.

Таким образом, информационная безопасность, являясь составляющей частью национальной безопасности, неоднозначно трактуется в современной научной литературе из-за чего требует особого исследования[2].

В настоящее время исследования проблем информационной безопасности продолжают пользоваться огромным вниманием у представителей различных наук[3]. Многими российскими авторами непосредственно были изучены теоретические основы категориального аппарата информационной безопасности.

Можно сказать, что информационная безопасность представляет собой сложное системное, многоуровневое явление, в котором внешние и внутренние факторы оказывают прямое воздействие на состояние и перспективы развития.

Термин «информационная безопасность» можно понимать в «узком» и «широком» смысле. В «узком» смысле информационная безопасность понимается как комплекс аппаратных и программных средств, которые обеспечивают сохранность, доступность и конфиденциальность данных в компьютерных сетях. Мотивация ученых, придерживающихся данного подхода достаточно проста: то, что в 1970-е г. называлось компьютерной безопасностью, а в 1980-е г. – безопасностью данных, сейчас именуется информационной безопасностью[4]. Исходя из подобной логики информационную безопасность можно определить как комплекс мер по защите информации от посягательств через неавторизованный доступ, разрушения, модификации, раскрытия и задержки в доступе. Здесь применялся термин «критические данные», т.е. данные, которые в случаях их случайного или умышленного раскрытия, изменения или разрушения, то есть возможности нанесения какого-либо ущерба, требуют защиты. Соответственно, цель информационной безопасности состояла в защите и гарантировании точности и целостности информации и минимизировании разрушения, которые могли иметь место. Информационная безопасность гарантирует достижение конфиденциальности критической информации; целостности информации и связанных с ней процессов создания, ввода, обработки и вывода; доступности информации, в случае необходимости; а также учета всех процессов, которые связаны с информацией.

Раскрывая понятие информационной безопасности в «широком» смысле, исследователи под информационной безопасностью России понимают состояние защищенности её национальных интересов в информационной сфере, которые определялись совокупностью комплексных интересов личности, общества и государства. Далее, на основе национальных интересов России в информационной сфере получает начало формирование стратегических и текущих задач внутренней и внешней политики государства по обеспечению информационной безопасности, то есть в данном контексте информационная безопасность подразумевает состояние защищенности информационной среды общества,

[1]Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. N 8. С. 73 - 80.с.

[2]Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. 190 с.

[3]Тарасенкова А.Н. Интернет: правовые аспекты безопасного использования. М.: Редакция "Российской газеты", 2017. Вып. 2. 160.

[4]Некрасов В.Н. Актуальные вопросы уголовно-правовой охраны инновационной деятельности в России // Актуальные проблемы российского права. 2017. N 7. С. 108 - 114.

которое в интересах граждан, организации и государства в целом обеспечивает её формирование, использование и развитие.

Интересен подход ученого А. К. Киселева, считавшего, что определение информационной безопасности через категорию «безопасность информации» является более логичной, нежели через категорию «национальные интересы», отмечая при этом, что в рамках обеспечения государственной безопасности не вся информационная сфера является объектом информационной безопасности. Однако, к сожалению, собственного определения термина «информационная безопасность» автор не предлагает, делая акцент на рассмотрение понятии «охрана» информации и ее «защита»[1].

В.И. Ярочкин рассматривает информационную безопасность «как единый целостный механизм, который объединяет средства, методы и мероприятия, направленные на использование в качестве защиты информации от разглашения, утечки и несанкционированного доступа к ней»[2].

Интересен подход В.А. Герасименко, который определяет информационную безопасность в качестве предотвращения и нейтрализации внешних негативных информационных воздействий на людей, общество в целом, а также на технические, технологические и организационные системы[3].

По мнению Л.И. Шершнев, при возникновении каких-либо новых направлении обеспечения информационной безопасности, что нельзя отрицать, в связи со столь быстрыми темпами развития современных информационных технологии и информационной техники, данное определение должно будет всякий раз вновь рассматриваться и дополняться.

Действующим уголовным законом установлена ответственность за общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. Данная группа посягательств является преступлениями в сфере компьютерной информации. Они объединены законодателем в главу 28 УК РФ. К указанным посягательствам относятся: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 272-274 УК РФ).

Преступления рассматриваемой категории посягают на общественные отношения, складывающиеся по поводу обеспечения конфиденциальности, целостности и доступности компьютерной информации, сохранности средств, используемых для ее обработки.

Доступность различных ресурсов, их целостность, конфиденциальность и поддерживающая инфраструктура и являются основными компонентами информационной безопасности.

Доступность информации – это широкая область деятельности, которой необходим комплексный систематический подход. Доступность представляет собой гарантию получения необходимой информации или информационной услуги пользователем за определенный период времени. Также, под доступностью информации понимается свойство системы, в которой вращается информация, характеризующаяся способностью обеспечения своевременного беспрепятственного доступа субъектов к интересующей их информации и готовности соответствующих автоматизированных служб к обслуживанию запросов, поступающих от субъектов.

При нарушении доступности, блокируется доступ к услуге или информации. Также следует отметить, что понятие «доступность» является субъективным в каждый момент

[1]Винокуров В.Н. Причинение вреда двум и более потерпевшим как основание ужесточения наказания и формы его закрепления в Уголовном кодексе РФ // Современное право. 2017. N 4. С. 98-103.

[2]Клебанов Л.Р. Уголовно-правовая охрана культурных ценностей / под науч. ред. А.В. Наумова. М.: Норма, Инфра-М, 2011. 352 с.

[3]Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. Г.А. Есакова. 7-е изд., перераб. и доп. М.: Проспект, 2017. 736 с.

времени для всех субъектов, которые потребляют услугу или информацию в данный период времени.

Целостность информации – это такое существование информации, при котором она остается в неискаженном виде (неизменном по отношению к определенному зафиксированному её состоянию). Следует добавить, что субъекты интересуются обеспечением более широкого свойства – достоверности информации. Оно состоит из целостности информации, то есть неискаженности и адекватности (точности и полноты) отображения состояния её предметной области.

Целостность информации условно можно разделить на статическую и динамическую. Статическая целостность информации представляет собой состояние неизменности информационных объектов от их исходного состояния, которое определяется автором или источниками информации.

Динамическая целостность информации состоит из вопросов корректного выполнения сложных действий с информационными потоками, например, анализа потока сообщений для выявления некорректных, контроля правильности передачи сообщений, подтверждения отдельных сообщений и др.

Целостность является необходимым аспектом информационной безопасности при использовании информации с целью управления различными процессами (техническими, социальными и т.д.). Так, ошибка в управляющей программе приводит к остановке управляемой системы, неверное трактование закона может привести к его нарушению, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью[1]. Данные примеры наглядно показывают нарушение целостности информации, которое может привести к плохим и непоправимым последствиям. Именно поэтому целостность информации следует выделять как одну из базовых составляющих информационной безопасности.

Конфиденциальность – это такая способность системы, которая позволяет ей обеспечивать целостность и сохранность информации ее пользователей. Если информация стала известной лицо, не располагающему полномочиями доступа к ней, то угроза это называется нарушением конфиденциальности. Оно возникает всякий раз, когда получен доступ к определенной секретной информации, которая хранится в вычислительной системе или передаваемой от одной системы к другой. Часто, когда происходит нарушение конфиденциальности, используется термин «утечка». Такие угрозы могут возникнуть в связи со сбоями работы программных и аппаратных средств, а также «человеческим фактором» (например, случайное делегировании какому-либо одному пользователю привилегий другого). Конфиденциальность в России является самым проработанным аспектом информационной безопасности.

Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасного поведения личности - компьютерной преступности (computer crime)[2]. Следует отметить, что в отечественной теории уголовного права нет общепринятой дефиниции подобного рода гибридных преступлений. Используются различные категории: информационные преступления[3], киберпреступления[4], преступления в сфере высоких технологий[5], интернет-преступления[6].

---

[1]Комментарий к Уголовному кодексу Российской Федерации / Под ред. С.В. Дьякова. М.: Юриспруденция, 2013. 912 с.

[2] Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. N 8. С. 73 - 80.

[3] См.: Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. М., 2007.

[4] См.: Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013.

[5] См.: Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015.

[6]См.: Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: Монография. М., 2015.

Информатизация преступности рождает ряд непростых вопросов для совершенствования уголовного закона по противодействию компьютерным преступлениям, например:

- каким должно быть оптимальное количество составов преступлений, посягающих на информацию и элементы информационно-коммуникационной инфраструктуры;
- есть ли необходимость в изменении диспозиции традиционных составов преступлений; и др.

Необходима серьезная системная работа.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ ПРЕСТУПЛЕНИЙ

Гусева Евгения Сергеевна,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

Современный мир – это век развития информационных технологий, где быстро продвигается создание специальных программ, информационных баз и средств опознания, с помощью которых сотрудники оперативных и следственных подразделений занимаются расследованием преступлений.

Современные информационные технологии, основанные на использовании различных методах получения, исследования и оценки исходных и дополнительных данных направлены на оптимизацию применения тактических приемов производства следственных действий в процессе расследования преступлений.

На практике используют как универсальные, так и специализированные программы обеспечения. Специальные программы обеспечения используют для автоматизации криминалистических учетов. Накопление и обработка информации для оперативно-справочных учетов осуществляется на центральном уровне. Для обработки информации разного вида применяются специальные автоматизированные системы. Для ведения дактилоскопической регистрации в России применяются системы «Узор», «Папилон». Учет похищенных ценностей осуществляется при помощи системы «Антиквариат». В Федеральном банке криминалистической информации используется универсальная система автоматизированных банков данных. Она функционирует на общероссийском и региональном уровне. В нее включаются сведения об особо опасных преступлениях, нераскрытых преступлениях, о лицах, скрывающихся от правоохранительных органов.

Особое значение для получения информации из смешанных источников имеет система «Образ++», которая является комплексной программой и позволяет работать в нескольких основных направлениях: работа с задержанными лицами с целью установления личности; работа с потерпевшими и свидетелями преступления и т.д. Преимущество автоматизированной системы заключается в том, что каждый человек, задержанный правоохранительными органами, проверяется по базе данных с целью установления личности. В качестве поисковых установок могут выступать реквизитные данные, субъективный портрет или изображение лица. Система автоматически формирует список изображений, ранжированный по степени схожести. Принятие решения об идентификации личности является прерогативой криминалиста. Если следствие не располагает

фотоматериалами, система также предложит список вероятных совпадений с отправленными на поиск данными. На основе полученного результата криминалист делает заключение об идентификации. На основании подробного словесного описания внешности и отдельных черт лица человека может быть составлен фоторобот. Информационно-поисковая система «Образ++» позволяет осуществлять поиск лиц по реквизитным данным, субъективному портрету и по фотороботу. В каждом из этих случаев система «Образ++» выводит список лиц с совпавшими данными, потерпевшими или свидетелями рассматривается ряд фотоизображений и осуществляется опознание.

Также для формирования образа подозреваемого (обвиняемого) с помощью компьютерных программ используется программа «Форвер», которая позволяет обеспечить высокую информативность сбора криминалистически значимых признаков при расследовании убийств. Данная программа позволяет определить круг лиц, подлежащих незамедлительной проверке на причастность к преступлению, с целью формулировки заданий оперативным работникам, а также формирует версии, образ подозреваемого (обвиняемого) путем анализа аналогичных преступлений в компьютерной базе данных. При использовании метода аналогии следователь может просмотреть всю базу уголовных дел и найти подобные преступления, а также, если возникнет необходимость, поднять их из архива. Поиск ведется с помощью простой сортировки всех занесенных в информационную базу уголовных дел по различным признакам, например, по полу, возрасту жертвы, способу убийства и сокрытия следов. Данный комплект признаков позволяет отсортировать группу дел, которые аналогичны между собой. В научной литературе встречается еще одно название данного метода - «поиска ближайшего соседа» - case based reasoning - CBR.

Еще одним видом компьютерных программ, используемых при расследовании преступлений являются биометрические системы ПАПИЛОН. Они обладают самыми высокими показателями надёжности и точности поисков. Программные и программно-технические решения ПАПИЛОН отвечают требованиям новейших информационных, коммуникационных и биометрических стандартов.

Есть множество видом систем ПАПИЛОН. Наиболее известными являются АДИС ПАПИЛОН и ПАПИЛОН «Живой сканер».

АДИС ПАПИЛОН обеспечивает создание, хранение и функционирование электронной базы данных дактилокарт и следов и автоматизацию процесса дактилоскопической идентификации для решения обширного круга задач:

•Установление личности по отпечаткам и следам пальцев рук и ладоней, в том числе путем проведения оперативных проверок по оттиску пальца в режиме реального времени

•Идентификация неопознанных трупов

•Установление причастности личности к ранее совершенным преступлениям

•Объединение преступлений, совершенных одним и тем же лицом.

Пользователями АДИС ПАПИЛОН в России являются подразделения Министерства внутренних дел, Федеральной службы безопасности, Федеральной службы по контролю за оборотом наркотиков, Федеральной службы исполнения наказаний, Федеральной миграционной службы и Министерства обороны.

Система электронного дактилоскопирования ПАПИЛОН «Живой сканер»

В состав системы ПАПИЛОН «Живой сканер» входит дактилоскопический ладонный сканер ПАПИЛОН ДС-45 (ПАПИЛОН ДС-45М) или дактилоскопический пальцевый сканер ПАПИЛОН ДС-30Н (ПАПИЛОН ДС-30НМ).

Система предназначена для создания электронных дактилокарт заданной формы, которые заносятся в собственную БД и могут быть переданы по каналам связи в АДИС ПАПИЛОН или в другую дактилоскопическую БД.

Используемый метод бескраскового дактилоскопирования защищен патентом России.

Система позволяет включить в состав дактилокарты качественные фотографические изображения дактилоскопируемого лица и его особых примет. Система поддерживает поиски по отпечатку пальца и текстовым данным в собственной БД дактилокарт.

Как правило, комплекс ПАПИЛОН «Живой сканер» связан с автоматизированной дактилоскопической информационно-поисковой системой (АДИС ПАПИЛОН). В этом случае его называют станцией дактилоскопирования или станцией регистрации. Если в состав установленного программного обеспечения, помимо ПО ПАПИЛОН «Живой сканер», входит ПО ПАПИЛОН «Фильтр», комплекс называют станцией регистрации и оперативных проверок.

Специализированные дактилоскопические сканеры ПАПИЛОН обеспечивают формирование качественных информативных изображений даже для «плохих» пальцев (излишне сухих, с низким рельефом папиллярного узора, со стертым папиллярных узором, т.н. «пальцев домохозяйки» и т.д.).

В целом, интеграция новых компьютерных технологий повысит эффективность работы правоохранительных органов при раскрытии и расследовании преступлений.

На данный момент компьютеры используют для обработки экспериментальных данных, полученных в ходе проведения физических, химических и других исследований. Универсальные программные системы позволяют выполнять вспомогательные расчеты по алгоритмам и формулам. Это значительно сокращает время работы экспертов, так как при проведении технологических, автотехнических экспертиз требуется выполнить большое количество дополнительных расчетов. Предусмотрено использование специализированных программ для выполнения расчетов при проведении бухгалтерских экспертиз.

Также создание программ, направленных на решение идентификационных и диагностических задач, предоставляет возможности для решения многих вопросов, например: провести сравнительное исследование следов рук со следами, зафиксированными на дактилоскопической карте, выполнить композиционные портреты.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ КОНСТИТУЦИОННОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ

Маркова Елизавета Александровна,
магистрант 2 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Анисимова Екатерина Александровна,
доцент кафедры государственно-правовых дисциплин
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

На сегодняшний день сложно представить наш мир без информационных технологий в каждой из сфер человеческой жизни, ведь информационные технологии- это процесс, включающий в себя совокупность средств и методов сбора, обработки, передачи и получения информации, которая, в свою очередь, является необходимым ресурсом общества. Органы государственной власти, в частности, судебная власть в лице Конституционного суда Российской Федерации, активно используют информационные технологии в своей деятельности.

Информационное обеспечение Конституционного суда Российской Федерации начинается с его официального сайта, который представляет собой информационный ресурс, дающий в сети Интернет достоверную информацию о деятельности суда и о конституционном судопроизводстве.

Информационные технологии так или иначе используются в каждой из стадий конституционного судопроизводства.

Деятельность Конституционного суда начинается с подачи обращения в форме запроса, ходатайства или жалобы. В соответствии с параграфом 22.1 главы 3 регламента Конституционного суда Российской Федерации, заявитель имеет право на обращение в

Конституционный суд Российской Федерации в электронном виде. Кроме того, для подачи обращения в электронном виде заявитель должен зарегистрироваться в размещенной на официальном сайте Конституционного Суда системе подачи документов «Обращение в КС РФ» посредством создания собственной учетной записи, образующей личный кабинет. Важно, что регистрация осуществляется путем заполнения регистрационной формы и присоединения к ней подтверждающих документов заявителя, переведенных в электронный вид изображений[1].

И уже только после прохождения процедур регистрации, активации учетной записи и выражения согласия с правилами функционирования системы подачи документов «Обращение в КС РФ» заявитель получает доступ к заполнению электронной формы, предназначенной для подачи обращения в Конституционный Суд.

Позиция Конституционного суда Российской Федерации на этот счет подтверждает, что вытекающее из Конституции Российской Федерации требование доступности правосудия не означает возможности для гражданина по собственному усмотрению выбирать способ и процедуру судебной защиты – они определяются на основе Конституции РФ федеральными законами[2].

Так, согласно Постановлению Конституционного Суда РФ от 22 апреля 2013 г. № 8-П судом установлено, что закрепленные в Конституции Российской Федерации и международных правовых актах общепризнанные стандарты правосудия, которые основаны на приоритете прав и свобод человека, верховенстве права, состязательности судопроизводства и юридическом равенстве участников судебного разбирательства, предполагают следование суда порядку судопроизводства, установленному законом, что должно исключать возможность неограниченного усмотрения в правоприменительной практике при определении содержания прав и обязанностей участников судопроизводства. Субъект, чье право на судебную защиту признается законом, не может быть поставлен в ситуацию недопустимой неопределенности относительно правил доступа к правосудию и своего участия в судебном разбирательстве[3].

Рассмотрение обращений, поступивших в Конституционный Суд после их регистрации в установленном Инструкцией по делопроизводству в Конституционном Суде порядке осуществляется сотрудниками соответствующих подразделений Секретариата Конституционного Суда.

Стадия предварительного рассмотрения обращения и его принятия (либо отказ в принятии обращения к рассмотрению) практически не связана с использованием информационных технологий. Обусловлено это задачей второй стадии судебного процесса, на которой жалоба передается одному или нескольким судьям Конституционного суда Российской Федерации на предварительное изучение для решения вопроса о возможности принятия жалобы к рассмотрению[4]. По итогам предварительного изучения обращения, Конституционный суд либо принимает его к рассмотрению либо отказывает в таком принятии.

В соответствии с установленной Конституционным Судом очередностью рассмотрения дел в заседаниях, а также с учетом загруженности судей делами, переданными им ранее, сложности и объема этих дел, Конституционный Суд при принятии дела к рассмотрению назначает по каждому делу судью-докладчика (судей-докладчиков). Соответственно, следуя регламенту Конституционного суда третья стадия

---

[1] Регламент Конституционного Суда РФ (ред. от 25.10.2018) // Текст редакции от 25.10.2018 опубликован в «Вестнике Конституционно- го Суда РФ», № 1, 2011.

[2] Определения Конституционного Суда РФ: от 17 ноября 2009 г. № 1427-О-О, от 23 марта 2010 г. № 388-О-О, от 22 марта 2012 г. № 555-О-О, от 26 мая 2016 г. № 1058-О-О, от 15 июля 2010 г. № 964-О-О, от 23 апреля 2013 г. № 593-О, от 29 сентября 2016 г. № 2105-О, от 26 января 2017 г. № 144-О.

[3] См.: Постановление Конституционного Суда РФ от 22 апреля 2013 г. № 8-П.

[4] ст. 41 Федерального конституционного закона от 21.07.1994 «1-ФКЗ (ред. от 30.10.2018) «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ, 25.07.1994, № 13, ст. 1447.

конституционного судопроизводства заключается в подготовке дела судьей-докладчиком (судьями-докладчиками) к судебному слушанию. До начала слушания дела, либо разрешения дела без проведения слушания, оригиналы обращения, всех приложенных к нему документов, отзывов на обращение, копии направленных требований и запросов Конституционного Суда, ответы на них, заключения экспертов, а также материалы, дополнительно полученные в процессе подготовки дела к рассмотрению, должны быть оформлены аппаратом судьи-докладчика в судебное дело. Судебное дело создается, пополняется и хранится в бумажной и электронной форме.

В целом, отмечая позитивную деятельность по внедрению информационных технологий в работу Конституционного суда, необходимо указать, что некоторые вопросы остаются актуальными до сих пор. Среди них именно дублирование на бумажный носитель обращений и судебных дел в целом, в том числе поступивших в суд в электронном виде. Каждое судебное дело на бумажном носителе нужно сформировать, описать, сшить процессуальные документы и представленные сторонами материалы в ходе судебного разбирательства. Кроме того, после рассмотрения судебное дело минимум в течение пяти лет должно храниться в архиве суда. Учитывая огромное количество судебных дел и сложность их оформления, можно сделать вывод о значительных расходах суда на материальное обеспечение и колоссальной нагрузке судебного аппарата.

Следующей стадией конституционного судопроизводства является рассмотрение и разрешение дела в пленарном заседании. Руководит заседанием председательствующий, при наличии кворума открывающий заседание. Председательствующий удостоверяется в явке участников процесса, проверяет полномочия представителей сторон. Сторонам и их представителям разъясняются их права и обязанности. После выступления сторон и признания судом исследования доказательств по делу завершенным, председательствующий в заседании объявляет об окончании слушания дела.

В соответствии с параграфом 50 главы 5 Регламента Конституционного суда в заседании Конституционного Суда сотрудниками секретариата Конституционного Суда осуществляется протоколирование[1]. Кроме того, для обеспечения полноты и точности протокола в каждом заседании ведется стенограмма, осуществляются аудио- и видеозапись, что опять же указывает на дублирование протоколов судебного заседания. Вопрос о необходимости ведения протокола в бумажном виде остается требующим корректировки, так как аудиозапись и видеозапись судебного заседания в полной мере отражают судебный процесс, фиксируя каждое процессуальное действие.

А вот использование информационных технологий при проведении судебного заседания посредством системы видеоконференцсвязи решает проблему доступности, позволяющую участникам судебного процесса из различных субъектов присутствовать в судебном заседании.

Заключительная стадия производства в Конституционном суде - принятие, оглашение, а также опубликование решения Суда. Итоговое решение по делу принимается Конституционным Судом РФ в закрытом совещании. Решение Конституционного Суда РФ принимается открытым голосованием посредством опроса судей. Председательствующий всегда голосует последним. Решение Конституционного Суда РФ, считается принятым при условии, что за него проголосовало большинство судей. Судья, не согласный с решением Конституционного Суда РФ, вправе письменно изложить свое особое мнение, которое приобщается к материалам дела. После подписания решения оно провозглашается в полном объеме в открытом заседании суда.

Согласно ст. 78 Федерального конституционного закона от 21.07.1994 N 1-ФКЗ (ред. от 29.07.2018) «О Конституционном Суде Российской Федерации» постановления и заключения Конституционного Суда Российской Федерации подлежат незамедлительному

[1] Регламент Конституционного Суда РФ (ред. от 25.10.2018) // Текст редакции от 25.10.2018 опубликован в «Вестнике Конституционно- го Суда РФ», № 1, 2011.

опубликованию в официальных изданиях органов государственной власти Российской Федерации, субъектов Российской Федерации, которых касается принятое решение. Решения Конституционного Суда Российской Федерации публикуются также в «Вестнике Конституционного Суда Российской Федерации», а при необходимости и в иных изданиях[1].

Рассматривая вопрос использования информационных технологий в производстве Конституционного суда Российской Федерации, нельзя не обратиться к опыту зарубежных стран.

В Германии наблюдается активное развитие электронного правосудия.

Необходимо отметить, что электронное правосудие в ФРГ представляет собой самостоятельное явление наряду с электронным правительством[2].Такой подход к определению подчеркивает самостоятельность судебной власти.

Электронное правосудие в Германии существенно продвинулось в своем развитии в связи с изданием двух законов, урегулировавших отдельные аспекты электронной коммуникации с судами. Первый Закон о реформе процесса в части вручения документов при осуществлении судопроизводства[3], ввел возможность вручения судами документов электронным способом. Второй Закон об адаптировании к современному правовому деловому обороту частноправовых требований о соблюдении формы и иных предписаний [4], закрепил в законодательстве понятие электронного документа с определением условий, при которых он может использоваться в качестве равнозначного в письменной форме документу.

Кроме того, в июле 2017 года в Германии был принят Закон о введении электронных дел в сфере юстиции и о дальнейшем содействии электронному правовому обороту[5], который обязывает суды к 1 января 2026 году вести судебные дела в электронном виде. До этого времени Федерация и земли могут предусмотреть ведение электронных дел в определенных судах либо в отношении определенных категорий дел посредством принятия своих нормативных правовых актов.

Соответственно, такие элементы электронного правосудия немецкой доктрины, как электронная коммуникация с судами и электронные судебные дела, вполне могли бы быть заимствованы Российской Федерацией, с учетом ежедневного прогрессирования информационных технологий в современном мире.

Список использованных источников:

1.Определения Конституционного Суда РФ: от 17 ноября 2009 г. № 1427-О-О, от 23 марта 2010 г. № 388-О-О, от 22 марта 2012 г. № 555-О-О, от 26 мая 2016 г. № 1058-О-О, от 15 июля 2010 г. № 964-О-О, от 23 апреля 2013 г. № 593-О, от 29 сентября 2016 г. № 2105-О, от 26 января 2017 г. № 144-О.

2. Постановление Конституционного Суда РФ от 22 апреля 2013 г. № 8-П;

3. Регламент Конституционного Суда РФ (ред. от 25.10.2018) // Текст редакции от 25.10.2018 опубликован в «Вестнике Конституционного Суда РФ», № 1, 2011.

4. Федерального конституционного закона от 21.07.1994 «1-ФКЗ (ред. от 30.10.2018) «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ, 25.07.1994, № 13, ст. 1447.

5.Petri, Dorfner 2011, 123.

[1] ст. 78 Федерального конституционного закона от 21.07.1994 «1-ФКЗ (ред. от 30.10.2018) «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ, 25.07.1994, № 13, ст. 1447.

[2] см.: Petri, Dorfner 2011, 123.

[3] Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren (Zustellungsreformgesetz — ZustRG) v. 25.06.2001 // Bundesgesetzblatt (далее — BGBl). 2001. I. Nr. 29. S. 1206.

[4] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr v. 13.07.2001 // BGBl. 2001. I. Nr. 35. S. 1542.

[5] Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs v. 5.07.2017 // BGBl. 2017. I. Nr. 45. S. 2208.

6.GesetzzurReformdesVerfahrensbeiZustellungenimgerichtlichenVerfahren (Zustellungsreformgesetz — ZustRG) v. 25.06.2001 // Bundesgesetzblatt (далее — BGBl). 2001. I. Nr. 29. S. 1206.

7.Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr v. 13.07.2001 // BGBl. 2001. I. Nr. 35. S. 1542.

8.Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs v. 5.07.2017 // BGBl. 2017. I. Nr. 45. S. 2208.

МЕХАНИЗМ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ В ИНТЕРНЕТЕ

Багров Алексей Юрьевич,
магистрант юридического факультета
Саратовского национального исследовательского
государственного университета имени Н.Г. Чернышевского
Научный руководитель:
Байниязова Зульфия Сулеймановна,
доцент Саратовского национального исследовательского
государственного университета имени Н.Г. Чернышевского, к.ю.н.,

Посредством электронной торговли потребители получают все больше возможностей для выбора и приобретения товаров, работ и услуг от большего числа поставщиков и по более низким ценам. Доля продаж посредством сети Интернет в общем объеме оборота розничной торговли ежегодно увеличивается. Онлайн-коммерция в сфере потребительских товаров во всем мире за 2018 г. возросла на 8%[1]. Так, ежедневно совершают покупки в сети Интернет порядка 2 млрд человек. Тем не менее, несмотря на явные преимущества, электронной торговле требуется надлежащее обеспечение правовыми средствами безопасности товаров, работ, услуг, раскрытие информации, защиту платежей и быстрое и справедливое разрешение споров.

В Законе РФ от 07.02.1992 № 2300-1 «О защите прав потребителей» (далее – Закон о защите прав потребителей) электронная торговля рассматривается как дистанционный способ продажи товара[2]. В дополнение к нему существуют Правила продажи товаров дистанционным способом[3], которые устанавливают общие правила при продаже товаров с использованием различных систем связи, исключающих возможность непосредственного ознакомления покупателя с товаром либо образцом товара при заключении такого договора.

Основными нарушениями прав потребителей при приобретении товаров (услуг) дистанционным способом в сети Интернет являются реализация опасных товаров, непоставка товара (неоказание услуги) либо нарушение сроков поставки товара (оказания услуги), реализация некачественного товара (услуги) или товара (услуги), не соответствующего описанию (ожиданию), целенаправленное введение в заблуждение потребителя относительно потребительских свойств товаров, сокрытие или неполное раскрытие информации о продавце (изготовителе, исполнителе), уклонение от рассмотрения требований потребителя, невозврат (уклонение от возврата) уплаченных потребителем

[1] См.: Дудченко А.В., Павловская В.Ю. Защита прав потребителей при реализации товара в сети Интернет // Закон и право. 2019. №11. С. 63-65.

[2] Закон РФ «О защите прав потребителей» от 07.02.1992 № 2300-1 (ред. от 18.07.2019) // Собрание законодательства РФ. 1996. № 3. Ст. 140; Собрание законодательства РФ. 2019. № 29 (часть I). Ст. 3858.

[3] Постановление Правительства РФ от 27.09.2007 №612 «Об утверждении Правил продажи товаров дистанционным способом» (ред. от 04.10.2012) // Собрание законодательства РФ. 2007. №41. Ст. 4894; Собрание законодательства РФ. 2012. № 41. Ст. 5629.

средств, отказ потребителю в возмещении убытков (неустоек). Отдельной проблемой является эффективное и оперативное пресечение распространения через сеть Интернет запрещенной и ограниченной к обороту продукции (применяемый судебный порядок пресечения деятельности сайтов продавцов, осуществляющих продажу такой продукции дистанционным способом, хотя и является действенным, однако сопряжен со значительными временными затратами, а регистрация и перенос на новый ресурс (доменное имя) запрещенной информации могут занимать несколько минут).[1]

Согласно законодательству, в обязанности продавца входит предоставление потребителю базовой информации для целостного восприятия приобретаемого товара, наиболее значимой стоит отметить наименование, серийный номер, данные о целях применения товара, оптимальный срок использования, правила эксплуатации и меры предосторожности. Вне зависимости от того, какой товар приобретается, к нему обязательно прикладывается руководство по эксплуатации, приклеиваются ярлыки как на сам товар, так и на тару, в которой он транспортируется.

Также продавцом должна быть обеспечена полная конфиденциальность персональных данных покупателя о совершаемой покупке.

Перед моментом заключения договора потребитель знакомится с возможными видами доставки, предоставленными ему со стороны продавца. Сделка считается заключенной в момент выдачи товарного чека, составления накладной, акта сдачи-приемки товара либо иного документа или сведений, подтверждающих оплату товара.

Когда договор уже заключен, товар оплачен и дожидается своей отгрузки, продавец не имеет права выполнять дополнительные платные работы без согласия покупателя. Продавец обязан приступить к оформлению и отправке заказа не позднее, чем через семь дней с момента заключения договора. В том случае, если сроки доставки не оговорены и не закреплены, она должна осуществляться в разумные сроки.

Из постановления Пленума Верховного Суда РФ от 28 июня 2012 г. № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» и п. 21 Правил продажи товаров дистанционным способом следует, что покупатель вправе отказаться от предоставляемого товара до момента его принятия, а в случае, если заказанный им товар принят, — то в течение семи дней со дня получения. Данную информацию покупателю должен предоставить продавец, однако в случае ее непредоставления покупатель вправе отказаться от товара в течение 90 дней со дня получения товара[2].

В том случае, если заказанный покупателем товар является индивидуальным, он не вправе от него отказаться, ведь данный товар может быть применен по назначению только им. Однако, если все же покупатель отказывается от товара по причине наличия недостатков, то в обязанности продавца входит возврат покупателю денежной суммы в полном объеме.

Качество приобретаемого товара должно соответствовать условиям заключаемого договора купли-продажи; если же такого пункта не предусмотрено, то приобретаемый товар должен полностью соответствовать целям его применения.

Если товар доставлен, но не в полном объеме, у покупателя есть возможность известить об этом продавца в течение 20 дней с момента получения товара. Устранение этого недостатка за отсутствием гарантийного срока составляет не более двух лет со дня передачи заявления об этом продавцу. В случае отказа продавца отправить недостающие элементы покупатель вправе требовать полную сумму, оплаченную за заказ, без возмещения части полученного товара.

Что касается возврата денежных средств, то он производится в соответствии с договором. Если в передаче денежных средств было задействовано третье лицо, то это не

[1] Распоряжение Правительства РФ от 28.08.2017 N 1837-р «Об утверждении Стратегии государственной политики РФ в области защиты прав потребителей на период до 2030 года» // Собрание законодательства РФ. 2017. №37. Ст. 5543.

[2]Постановление Пленума Верховного Суда РФ от 28.06.2012 г. № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» // Бюллетень Верховного Суда РФ. 2012. № 9.

освобождает продавца от обязанности полного возмещения денежной суммы, вне зависимости от причины возврата.

И здесь необходимо отметить, что одной из важных особенностей цифрового рынка международной торговли является возникновение посреднических технологических платформ (агрегаторов), таких как: Amazon, Uber, Alibabaили AirBnB. И поскольку они меняют экономические и конкурентные условия как на международном, так и национальном уровне, это, безусловно, влечет за собой регулирование их деятельности и учет в национальном законодательстве. В связи с этим в 2019 г. в России начали действовать поправки к Закону о защите прав потребителей, регулирующие приобретение товаров и услуг через Интернет, а именно через интернет-агрегаторы.

Обязанности, закрепленные за агрегаторами новой редакцией Закона о защите прав потребителей, являются в основном информационными. Так, владелец агрегатора обязан предоставить достоверную информацию о себе и продавце посредством ее размещения на своих сайте и (или) странице сайта в сети Интернет. Информацию о продавце (исполнителе) владелец агрегатора вправе довести до сведения потребителей посредством размещения на своих сайте и (или) странице сайта в сети Интернет ссылки на сайт продавца (исполнителя) в сети Интернет.

При этом установлены жесткие сроки для внесения изменений в такую информацию. Если продавец не довел до владельца агрегатора информацию об изменениях, владелец агрегатора не несёт за это ответственности. В этом плане потребитель, вступающий в отношения с владельцем агрегатора и добросовестно полагающийся на предоставленную информацию, оказывается незащищённым.

Владелец агрегатора отвечает, прежде всего, за информацию, представленную ненадлежащим образом. За неисполнение договора продавцом он не отвечает, если иное не предусмотрено договором между владельцем агрегатора и продавцом.

Владелец агрегатора обязан возвратить полученную сумму предоплаты при наличии следующих условий:

- товар (услуга), в отношении которого потребителем внесена предварительная оплата на банковский счет владельца агрегатора, не передан потребителю в срок (услуга не оказана в срок);
- потребитель направил продавцу (исполнителю) уведомление об отказе от исполнения договора купли-продажи (договора возмездного оказания услуг) в связи с нарушением продавцом (исполнителем) обязательства передать товар (оказать услугу) в установленный срок.

При этом владельцу агрегатора направляется подтверждение уведомления продавца об отказе от договора.

Таким образом, национальное законодательство делает определенные шаги по обеспечению защиты прав потребителей в сети Интернет, но пока они носят догоняющий и фрагментарный характер. И, несмотря на широкий спектр возможностей досудебного урегулирования споров, доминирующее положение среди способов защиты прав потребителей занимает судебный порядок.

ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Тихонов Илья Сергеевич,
студент Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:

Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

В связи с интенсивным развитием новых технологий, глобальной цифровизацией и изменением общественных отношений модифицируется и преступность, приобретая новые формы и проникая в различные сферы жизни. Качественные изменения, произошедшие в мире, оказали большое влияние на то, что информация в настоящее время приобретает все большую ценность. Однако вместе с пониманием значимости информации возникает и проблема ее защиты, что, безусловно, подразумевает воздействие не только с технической стороны, но и посредством законодательного регулирования.

Стоит отметить, что в науке складываются различные мнения по поводу понимания термина «высокие технологии». Данные дискуссии связаны с тем, что сфера, охватываемая этим понятием, довольно обширна и включает в себя информационные технологии, робототехнику, генную инженерию и многое другое. При этом в криминологии исследуемый термин ассоциируется, в первую очередь, с совершением преступлений в информационно-телекоммуникационной среде, а также с использованием средств связи и компьютеров[1].

В странах с высоким уровнем компьютеризации общественной жизни в настоящее время образовался самостоятельный вид преступлений – так называемые киберпреступления, преступления в сфере высоких технологий («high – techcrimes»). И поначалу, столкнувшись с данным явлением, правоохранительные органы начали применять традиционные нормы уголовного законодательства (о мошенничестве, краже и т.п.), однако данный метод оказался бездейственным, так как многие деяния не охватывались ранее существовавшими составами преступлений. Этот факт выявил проблему абсолютной неурегулированности новых общественных отношений.

Для изучения опыта зарубежной правовой регламентации обратимся к законодательству Японии, США и некоторых европейских стран и рассмотрим на их примере регулирование уголовной ответственности в области киберпреступности.

Первой страной, закрепившей нормы об уголовной ответственности за преступления в сфере высоких технологий, была Швеция. В апреле 1973 г. риксдаг принял закон «О данных», который определил следующие составы преступлений: незаконное проникновение в компьютерную систему и введение в компьютерную информацию ложных сведений, позволяющих совершить хищение денег, ценных бумаг, имущества, услуг либо ценной информации[2].

В 1986 году в Уголовный кодекс ФРГ были внесены изменения и также установлен ряд уголовно наказуемых деяний. Таким образом, была закреплена ответственность за умышленные деяния лиц с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных или данных, неправомочного использования; за действия, нарушающие обработку данных путем разрушения, повреждения, приведения в негодность установки для обработки данных или носителей информации; за нарушение тайны телекоммуникационной связи; за незаконное вмешательство в деятельность телекоммуникационных установок и др.

Законодательство Франции широко регламентирует ответственность за компьютерные преступления. Преступными деяниями здесь являются: перехват, хищение, использование или предание огласке сообщений, передаваемых средствами дальней связи; ввод или хранение в памяти ЭВМ запрещенных законом данных; изъятие или копирование

[1] Аносов А.В., Кашапова Е.С. Понятие преступлений в сфере высоких технологий // Академическая мысль. 2018. №4(5). С. 16.

[2] Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник удмуртского университета. 2011. №4. С. 115.

данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ, а также ознакомление с этими данными посторонних лиц; террористические акты, связанные с деяниями в области информатики и другие. Отличительной особенностью УК Франции в регулировании данной сферы является тот факт, что субъектами преступных деяний могут быть не только физические лица, но и юридические[1].

Особого внимания заслуживает опыт США в борьбе с киберпреступностью.

Первые попытки сформулировать и закрепить составы преступлений в сфере высоких технологий были предприняты на Конференции Американской ассоциации адвокатов в Далласе в 1979 году. В последующем положения, разработанные данной конференцией, были включены в Уголовный кодекс США. Вторым этапом стало принятие Конгрессом в 1986 г. закона «О мошенничестве и злоупотреблении с использованием компьютеров», который стал системообразующим и основным нормативным правовым актом в области защиты компьютерных сетей и электронных данных. Он предусматривает ответственность за компьютерное мошенничество, несанкционированный доступ к информации, шпионаж с использованием компьютерных технологий, повреждение данных (например, создание и распространение вирусов). Помимо этого данный закон разделил и защитил информацию, не относящуюся к военным тайнам, на три вида: информация, принадлежащая финансовым учреждениям (сведения о счетах в банках и т.п.); данные, принадлежащие правительственным учреждениям и сведения, принадлежащие международным организациям[2].

Количество компьютерных преступлений растет с увеличением темпов технического прогресса и количества пользователей сети «Интернет». В Японии тенденция возрастания количества киберпреступлений во многом была схожа с общемировой. Так, в 1993 году, на начальном этапе развития интернета, было зарегистрировано 32 преступления в сфере высоких технологий, в 1997 г. – 262, в 1998 г. – 415. В Уголовном кодексе Японии ответственность за компьютерные преступления при этом была введена уже 1987 г. Предметом закрепленных составов (внесение неверных записей в официальный документ, распространение сфальсифицированного официального документа, уничтожение частных и государственных документов, компьютерное мошенничество, вывод из строя ЭВМ, воспрепятствование бизнесу путем вывода из строя компьютеров и др.) стали записи на электромагнитном носителе и сами ЭВМ. Помимо этого одной из особенностей японского уголовного законодательства является то, что регулирование возможно не только нормами УК, но и нормами специально принятых законов. Так, 3 февраля 2000 года в Японии был принят закон «О несанкционированном проникновении в компьютерные сети», который дополнительно закрепил следующие составы: незаконное проникновение в компьютерные системы и информационные сети с целью кражи информации; причинение ущерба владельцам баз данных, сетей и систем; использование краденой информации с целью извлечения дохода.

Необходимо отметить также строгость наказания за перечисленные выше преступления, предусмотренные УК Японии: за фальсификацию электронных документов - каторжные работы сроком 5 – 10 лет или штраф в размере 500 тыс. – 1 млн. йен; за преступления против деловой репутации и бизнеса – лишение свободы с обязательным привлечением к труду на срок до 5 лет или штраф до 1 млн. йен; за компьютерное мошенничество – лишение свободы сроком до 10 лет. Введение таких санкций было обусловлено, в том числе и тем, что, начиная с 2001 года, Япония начала реализовывать комплексную программу внедрения и развития информационных технологий «Электронная Япония», которая предусматривала создание единой информационной среды и электронного документооборота для государственных органов; внедрение высоких технологий,

[1] Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. С. 235 - 236.

[2] Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник удмуртского университета. 2011. №4. С. 115.

обеспечивающих создание инфраструктуры сетей передачи данных; развитие электронной торговли[1].

В заключение можно сказать, что изучение зарубежного опыта регулирования борьбы с преступлениями в сфере высоких технологий, а также применение норм на практике представляет большой интерес и открывает множество проблем и вопросов для дискуссии. Но в первую очередь, проведение исследований необходимо для определения направлений реформирования современного российского уголовного законодательства в рассматриваемой области. Согласно статистике, приведенной на официальном сайте Генеральной прокуратуры РФ, количество преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с каждым годом растет: в 2016 г. - 65 949, а в 2017 г. – 90 587, при этом доля киберпреступлений от числа всех преступных деяний составляет 4,4% (в 2017 году)[2]. Исходя из всего вышесказанного, можно сделать вывод о возможности совершенствования отечественного уголовного права, в том числе путем заимствования зарубежного опыта, но с адаптацией для российских реалий.

Список использованных источников:

1. Аносов А.В., Кашапова Е.С. Понятие преступлений в сфере высоких технологий // Академическая мысль. 2018. №4(5). С. 15-19.
2. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. С. 231-237.
3. Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник удмуртского университета. 2011. №4. С. 114-118.
4. Морозов Н.А. Новые тенденции в преступности Японии и России // Проблемы экономики и юридической практики. 2013. №2. С. 112-116.
5. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс] // URL: https://genproc.gov.ru/smi/news/genproc/news-1431104.

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Усынин Сергей Александрович,
студент 3 курса Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

В настоящее время одним из самых распространённых преступлений в Российской Федерации является мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ). В первую очередь данный факт связан с ростом клиентов кредитных и банковских организаций, которые применяют платежные карты и системы мобильных платежей (ApplePay, AndroidPay и др.) в своих личных целях, не используя при этом

[1] Морозов Н.А. Новые тенденции в преступности Японии и России // Проблемы экономики и юридической практики. 2013. №2. С. 112-115.
[2] О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс] // URL: https://genproc.gov.ru/smi/news/genproc/news-1431104 (дата обращения: 04.12.2019).

должных мер безопасности. Чтобы защитить себя от преступных посягательств**,** граждане должны соблюдать простые правила безопасности при использовании электронных средств платежа: хранить банковскую карту так, чтобы преступники не смогли завладеть ею, не разглашать пароли, в случае утери незамедлительно обратиться в банк, выпустивший карту и др.

На официальном сайте МВД России ежемесячно публикуется информация (характеристика) о состоянии преступности в Российской Федерации. Главным информационно-аналитическим центром Министерства внутренних дел Российской Федерации по мошенничеству с использованием средств платежа предоставлена информация о количестве преступлений, совершенных за определенный отчетный период. По приведённым данным за январь-сентябрь 2019 года было зарегистрировано 10371 преступление, которые квалифицировали по статье 159.3 УК РФ. Стоит отметить, что прирост данных деяний составил 417,3%.[1] На основании приведенной статистики можно сделать вывод, что количество мошенничеств с использованием электронных средств платежа значительно растёт, что является отрицательным показателем. В целях защиты граждан от преступных посягательств и предупреждениях их совершения в средствах массовых информаций, а также на официальных сайтах правоохранительных органов активно публикуются материалы (памятки), в которых содержаться информация о действиях мошенников при получении незаконным путём денежных средств с карты потерпевшего и план действий, в случае если граждане подвергаются преступному посягательству.

Мошенничество с использованием электронных средств платежа является самостоятельным составом (по отношению к статье 159 УК РФ) и входит в главу преступлений против собственности УК РФ. В 2017 году Пленум Верховного Суда РФ принял постановление № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – Постановление). В нем судам разъясняется применение норм уголовного закона об ответственности за мошенничество и отдельные его виды. Пункт 17 данного Постановления закрепляет случаи, которые следует квалифицировать по статье 159.3 УК РФ, а именно, когда хищение имущества совершается с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или другой платежной карты путем сообщения уполномоченному сотруднику кредитной, торговой или другой организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. Не следует привлекать к уголовной ответственности за мошенничество с использованием кредитных средств платежа, а рассматривать деяния как кража (ст. 158 УК РФ) в следующих случаях:

Во-первых, когда путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного сотрудника кредитной организации;

Во-вторых, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты, переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием.[2]

Иногда преступники совершают хищение электронных платёжных средств и в последствии осуществляют мошеннические действия с их использованием. В этих случаях суды сначала в приговоре назначают отдельно наказания по статьям 158 и 159.3 УК РФ, а потом путём сложения наказаний выносят окончательное решение. Так, например, суд рассмотрел следующий случай:

«04 ноября 2018 года ФИО1, находясь в состоянии алкогольного опьянения, около здания «Столовая», тайно похитил из кармана трико, надетых на ФИО2 следующее

[1] См.: Состояние преступности в России за январь-сентябрь 2019 / [Электронный ресурс].- Режим доступа: https://media.mvd.ru/files/application/1669426.

[2] См.: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. N 2.

имущество: сотовый телефон, находящийся в чехле-книжке, с установленными в нем сим – картой оператора сотовой связи, картой памяти, а также банковскую карту с лицевым счетом №, на имя ФИО2, не представляющей материальной ценности, которая находилась внутри чехла-книжки вышеуказанного мобильного телефона. Своими преступными действиями ФИО1 причинил потерпевшему ФИО2 имущественный вред на общую сумму 5179 рублей. Кроме того, ФИО1, 04 ноября 2018 года, будучи в состоянии алкогольного опьянения, находясь около магазина, продолжая свои преступные намерения, направленные на тайное хищение денежных средств с банковской карты, принадлежащей ФИО2, передал ее своему знакомому Свидетелю. В свою очередь Свидетель, не осведомленный о преступных намерениях ФИО1 направленных на тайное хищение денежных средств с банковской карты с лицевым счетом №, будучи уверенным, что банковская карта принадлежит ФИО1 приобрел товары, путем прикладывания платежной карты к банковскому терминалу, установленному в магазине на общую сумму 4691 рубль. После этого Свидетель передал пакет с приобретенными товарами и банковской картой ФИО1.»[1]

В итоге суд признал виновным ФИО1 в совершении преступлений и назначил ему наказания:

- по пункту «г» ч. 2 ст. 158 УК РФ – исправительные работы с удержанием 10% заработной платы в доход Российской Федерации сроком на один год;

- по ч. 1 ст. 159.3 УК РФ – исправительные работы с удержанием 10% заработной платы в доход Российской Федерации сроком на шесть месяцев.

На основании ч. 2 ст. 69 УК РФ путем частичного сложения наказаний окончательное наказание по совокупности преступлений суд назначил в виде исправительных работ с удержанием 10% от заработной платы в доход Российской Федерации сроком на один год четыре месяца.

Таким образом, мошенничество с использованием электронных средств платежа является очень актуальным и рабочим составом по состоянию на 2019 год. Конечно же количество преступлений в этой сфере будет расти. Судам необходимо обращаться к разъяснениям Пленума Верховного Суда, для того чтобы правильно квалифицировать действия виновных при хищении чужого имущества с использованием электронных средств платежа, а правоохранительным органам находить новые способы выявления данных преступлений и эффективно использовать методы борьбы с ними.

Список использованных источников:

1) Судебная практика

1. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. N 2.

2. Приговор Альметьевского городского суда № 1-209/2019 от 30 мая 2019 г. по делу № 1-209/2019 // [Электронный ресурс]. - Режим доступа:https://sudact.ru/regular/doc/7gKKONVyqgg5/ (Дата обращения 30.11.2019)

2) Электронные ресурсы

3. Состояние преступности в России за январь-сентябрь 2019 // [Электронный ресурс]. - Режим доступа: https://media.mvd.ru/files/application/1669426 (Дата обращения 29.11.2019)

КРИПТОВАЛЮТА КАК ПРЕДМЕТ ХИЩЕНИЯ

Силова Дарья Леонидовна,
студент 3 курса Северо-Западного института (филиала)

[1] См.: Приговор Альметьевского городского суда № 1-209/2019 от 30 мая 2019 г. по делу № 1-209/2019

Университета имени О.Е. Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета имени О.Е. Кутафина (МГЮА), к.ю.н.

В настоящее время в научной литературе весьма актуальными и дискуссионными являются вопрос правового положения криптовалют и вопрос о наличии либо отсутствии возможности криминализации их хищения.

Главная проблема состоит в том, что в России за криптовалютами не закреплен никакой статус, и, следовательно, криптовалютные отношения ничем не урегулированы. (Для сравнения в Болгарии криптовалюта рассматриваются как финансовый инструмент).

Этот вопрос касается не только уголовного права в области преступлений против экономики, но и гражданского законодательства, так как криптовалюты в полной мере не подпадают ни под один объект гражданского права ввиду своих особенностей.

Вариантами разрешения данной проблемы можно назвать, например, признание за криптовалютами статуса:

- денежных средств, так как: с помощью криптовалют «покупаются» различные товары, однако денеги относятся к родовым вещам, а криптовалюты нельзя отнести к таковым ввиду того, они представляет собой особенный набор формул, что делает из них индивидуально-определенную вещь;
- товара, имущества либо информации;
- имущественных прав, однако проблема соответствия криптовалюты с имущественными правами в том, что не ясно, к кому может быть обращено требование.
- иного имущества.

Однако, признание того или иного объекта иным имуществом требует нормативного закрепления и наличия такого свойства, как оборотоспособность.

На наш взгляд, наиболее корректным будет придание им правового положения, схожего с бездокументарными ценными бумагами. Криптовалюты в таком случае станут предметом статей 159, 185, 185.4, 204, 290, 291, 291.1, 291.2, 304, 309 УК РФ. Однако опять же, по отношению у криптовалюты участие государственных структур исключается, что не позволяет полностью отождествлять криптовалюту и бездокументарные ценные бумаги.

Так как криптовалюта рассматривается в основном как предмет совершения преступления, то в таком случае нужно будет внести поправки в само понятие «предмет преступления» по причине того, что им признается элемент материального мира, в то время как криптовалюты не носят материального характера.

Сегодня судебная практика стоит на принципиальной позиции о том, что объектом хищения могут быть лишь предметы, указанные в ст. 128 ГК РФ. В связи с этим возникает обоснованный вопрос: как следует квалифицировать хищение криптовалюты? Можно выделить два основных подхода для наиболее оптимального варианта уголовно-правовой оценки хищений криптовалюты

Представляется, что выполняется посягательство на два объекта: отношения в сфере компьютерной информации и отношения в сфере собственности. Такое положение вещей полностью исключает квалификацию хищения криптовалюты лишь по ст. 272 УК («Неправомерный доступ к компьютерной информации»), поскольку в данном случае речь идет о способе создания условий для совершения последующего хищения.

Единовременное посягательство на указанные объекты при условии вмешательства в системы компьютерной информации или информационно-телекоммуникационные сети, вписывается в конструкцию состава, предусмотренного ст. 159.6 УК («Мошенничество в сфере компьютерной информации»). Особенностью данного состава преступления является то, что, по сути, с его введением была образована новая самостоятельная форма хищения,

которая предполагает, что завладение имуществом или приобретение права на него сопряжено с проникновением в информационную среду, в которой осуществляются различного рода информационные операции, юридические последствия которых состоят в приобретении участниками оборота имущества в виде денежных средств или имущественных прав[1].

На сегодняшний день можно выделить такую квалификацию преступного использования криптовалюты по законодательству РФ:

- хищение вверенной криптовалюты - данное деяние квалифицируется как растрата (ст. 160 УК РФ). Многие криптобиржи создают для своих клиентов специальные кошельки с целью хранения, учета криптовалюты, и существуют случаи хищения криптовалют сотрудниками криптобирж путем различных махинаций.

- незаконный обмен криптовалюты. На практике суды относят эти операции к незаконной банковской деятельности, поскольку они осуществляются вне банка или иной кредитной организации, но с использованием их возможностей, что составляет сферу применения ст. 172 УК РФ («Незаконная банковская деятельность»)

-фальшивые криптовалюты. Злоумышленники предлагают пользователям фальшивые криптовалюты, убеждая их в том, что они покупают новую, успешную и перспективную криптовалюту, которая достигнет не меньшей популярности, чем Биткоин.

- неуплата налога с криптоопераций. Квалифицируют данное деяние по ст. 198 УК РФ («Уклонение физического лица от уплаты налогов, сборов и (или) физического лица - плательщика страховых взносов от уплаты страховых взносов»).

- легализация преступно полученной криптовалюты. В практике судов встречаются примеры вменения легализации (ст. 174.1 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления») преступных биткоинов владельцам криптобирж, хакерам и всем, кто осуществляет теневые операции с криптовалютой. Б.

- хакерские атаки. Довольно часто биржи подвергаются атакам со стороны хакеров, что приводит к хищению средств клиентов. Привлекать хакеров к уголовной ответственности за это деяние следует по ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»). Намеренное затруднение доступа к информации о стоимости криптовалюты и ее последующее изменение квалифицируется по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»). Если хакеры также применили какую-либо вирусную программу, их действия будут дополнительно квалифицированы по ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ»).о

- фишинг. Популярным способом хищения криптовалюты является технология фишинга (phishing). Она заключается в получении чужих пользовательских данных с целью осуществления хищения в дальнейшем, например, через фейковый сайт, абсолютно похожий по интерфейсу на достоверный, но отличающийся от нее отсутствием всего лишь одной буквы в доменном имени. С одной стороны, фишинг можно расценивать как кражу (ст. 158 УК РФ), поскольку для нее неважно, каким образом добыты учетные данные потерпевшего, при том что виновный не воздействовал на цифровое пространство[2], так и мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ), так как получение пользовательских данных нарушает процесс обработки, хранения и передачи компьютерной информации, что позволяет хакеру незаконно завладеть чужим имуществом.[3].

Таким образом, постепенное вхождение в экономический оборот криптовалюты и её аналогов требует, прежде всего, отклик на уровне доктринальных разработок и впоследствии

[1]Яни П.С. Специальные виды мошенничества // Законность. 2015. N 8. С. 35 - 40.

[2] Абзац 1 п. 21 Постановления Пленума ВС РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

[3] Пункт 20 Постановления Пленума ВС РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

в законодательном регулировании защиты имущественных отношений. Они связаны с определением правового статуса криптовалюты и возможностью её отнесения к категории «имущество» для целей уголовно-правовой охраны отношений. Несмотря на некоторые допущения, хищение криптовалюты в рамках нынешнего правового регулирования представляет собой посягательство на два объекта, охватываемое составом мошенничества в сфере компьютерной информации и, и соответственно, не требующее от законодателя введения каких-либо новых специализированных составов или квалификации по их совокупности.

КАК НЕОЖИДАННО СТАТЬ УЧРЕДИТЕЛЕМ ИЛИ УЧАСТНИКОМ ЮРИДИЧЕСКОГО ЛИЦА?

Лисенков Дмитрий Михайлович, Быкова Светлана Николаевна,
студенты 3 курса Северо-Западного института (филиала)
Университета им. О.Е.Кутафина (МГЮА)
Научный руководитель:
Ширяев Владимир Феодосьевич,
доцент кафедры уголовного права и криминологии
Северо-Западного института (филиала)
Университета им. О.Е. Кутафина (МГЮА), к.ю.н.

Горькая правда нашей современности: мошенники всегда идут впереди закона. Не важно, в какой сфере, в каком масштабе и на какой территории. Не важно для мошенников, но важно для нас, так как в любом исследовании должен быть свой предмет. В данном исследовании мы рассмотрим развивающийся способ мошенничества: образование юридических лиц на подставное лицо с использованием электронной цифровой подписи (ст. 173.1 УК РФ).

Актуальность работы обусловлена частотой совершения данных преступлений. Новостные порталы периодически рассказывают о новых «генеральных директорах» и «учредителях», которые внезапно узнают об оформленных под их управлением юридических лицах[1].

Для всестороннего анализа данного преступления рассмотрим элементы и признаки его состава. Как мы знаем, последние делятся на объективные (объект и объективная сторона) и субъективные (субъект и субъективная сторона).

Субъект преступления общий, уголовная ответственность за совершение деяния, содержащего все признаки преступления, предусмотренного статьей 173.1 УК РФ наступает с 16 лет. Однако для выполнения объективной стороны, а именно для подделки или создания электронной подписи без ведома лица, на имя которого она создается, возможна лишь лицом, имеющим полную гражданскую дееспособность, то есть достигшим возраста 18 лет.

Ст. 173.1 УК РФ направлена на защиту и охрану установленного Федеральным законом от 08.08.2001 №129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» порядка образования юридического лица, что является непосредственным объектом преступления.

Субъективная сторона предполагает прямой умысел. Виновный осознает факт образования юридического лица через подставных лиц, и желает внести в государственный реестр юридических лиц запись о таком лице в качестве учредителя или участника образованного юридического лица.

Объективная сторона рассматриваемого преступления характеризуется деянием в форме действия, а именно образование юридического лица в любой предусмотренной

[1] https://habr.com/ru/post/453596/.

законом организационно-правовой форме через подставных лиц. При этом под подставным лицом понимается лицо, которое является учредителем (участником) юридического лица или органом (-ами) управления юридического лица и без ведома которых были внесены данные о них в единый государственный реестр юридических лиц, что соответствует примечанию в ст. 173.1 УК РФ. Подставное лицо имеет двойную природу: оно одновременно является потерпевшим (признак объекта) и средством совершения преступления (признак объективной стороны).

Специфическим в данном составе будет являться способ: использование электронной подписи подставного лица. Именно этот признак выделяет анализируемое нами преступление из общей массы деяний, подпадающих по признаки состава преступления, предусмотренного статьей 173.1 УК РФ. Предоставление в органы регистрации юридических лиц документов, подписанных электронной подписью, приравнивается к предоставлению документов с собственноручной подписью.

Итак, электронная подпись – реквизит электронного документа, полученный в результате преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искомой информации (принцип целостности), ее принадлежность (принцип авторства) и факт подписи (принцип неотказуемости).

Создатели и сторонники применения электронной подписи уверяют, что ее невозможно подделать. Однако злоумышленники пользуются не техническим способом ее подделки, а юридическим, то есть оформляют на то самое подставное лицо без его ведома, а фактическим созданием ключей и кодов занимаются уполномоченные на то коммерческие организации.

Законодательство об электронной подписи имеет как минимум одно слабое место: нормативное регулирование процесса оформления. Так, для удостоверения личности оформляющего лица потребуется всего лишь паспорт и свидетельство пенсионного страхования. Кажется, что тут не так, подделка паспорта – довольно сложный процесс. Дело в том, что в удостоверяющий центр, туда, где вам оформляют и выдают сертификат и носитель ключа электронной подписи можно приносить не оригиналы указанных документов, а заверенные надлежащим образом копии.

Мы провели устный опрос студентов СЗИ (ф) МГЮА в возрасте от 18 до 23 лет. Из них никто не интересовался в органах федеральной налоговой службы о регистрации его/ее в качестве учредителя или участника юридического лица. Ни один человек не смог с уверенностью перечислить все органы и организации, в которых имеются копии его/ее паспорта и свидетельства пенсионного страхования. Более того, 80% опрашиваемых не уверены в надлежащем хранении копий данных документов. Данная статистика говорит о том, что каждый из опрашиваемых находится в потенциальной «группе риска» стать подставным лицом.

Ситуация осложняется для подставного лица, но облегчается для субъекта преступления тем, что в удостоверяющий центр можно не приходить лично, а послать представителя с доверенностью. Ну а относительно преступного деяния, даже посылать не нужно, он сходит сам. К слову, доверенность может быть заверена обычным, а не нотариальным способом. Хотя что уж скрывать, преступников давно не смущает и нотариальное заверение. Например, опытным путем проверено, что в небольших муниципальных образования, где нет нотариусов, органы местного самоуправления заверяют доверенности без личного присутствия доверителя, веря представителям «на слово».

Следующая проблема выявляется на стадии возбуждения уголовного дела по факту совершения преступления, предусмотренного ч. 1 ст. 173.1 УК РФ. Органы предварительного расследования не справляются с задачей поиска преступников. Одним из признаков электронной подписи, как говорилось выше, является принадлежность ее определенному лицу (принцип авторства), и доказать факт неоформления электронной

подписи или ее неиспользования крайне сложно. А найти лиц, совершивших указанное деяние еще сложнее.

Так как преступление относится к категории преступлений небольшой тяжести, сроки давности привлечения к уголовной ответственности достаточно короткие – два года с момента совершения преступного деяния. Здесь возникает проблема обнаружения «подставным лицом» зарегистрированных не него юридических лиц. Например, уведомления из Федеральной налоговой службы приходят раз в год, а при указании ненадлежащего или неактуального адреса такие уведомления могут быть не получены вовсе. Как мы видим из опроса, самостоятельно люди также редко проверяют свой предпринимательский статус или его отсутствие.

При самостоятельном обнаружении лицом своего статуса учредителя или участника неизвестного ему юридического лица для возбуждения уголовного дела по другим, сопутствующим составам (например, по статьям 159, 174, 176 УК РФ) не достает наступления имущественного вреда определенного размера.

Мы видим, что оформить электронную подпись, а после с ее использованием – юридическое лицо, не так уж сложно для мошенников. В первую очередь это связано с некоторыми недоработками в законодательстве об электронной подписи, в частности, при определении порядка оформления и получения сертификата и носителя ключа электронной подписи.

Кроме того, так как подставное, а правильнее сказать подставленное, лицо зачастую узнает о существовании зарегистрированных на него организаций через какой-то промежуток времени, осложняется процесс возбуждения и расследования уголовного дела. Возможно, в статье 173.1 УК РФ следует выделить квалифицирующий признак «образование юридического лица на подставное лицо без его ведома», при этом увеличив максимальный срок лишения свободы, и, соответственно, срок давности привлечения к уголовной ответственности.