WSCHODNI ROCZNIK HUMANISTYCZNY
TOM XVII (2020), № 1
s. 45-55
doi: 10.36121/njegorow.17.2020.1.045

Николай Егоров
(Адвокатская палата Московской области)

Использование электронных документов в целях совершения преступлений

Аннотация: Статья посвящена возникновению новых видов преступлений, получивших обобщенное название – киберпреступность, появившихся в результате широкого внедрения электронных цифровых технологий и электронного документооборота в начале 2000-х годов. Автор рассматривает различные формы и механизмы совершения киберпреступлений, которые не ограничиваются подбором паролей для осуществления несанкционированного входа в банковские системы с последующим хищением денежных средств. Большое количество преступлений совершается в результате подделки различных электронных документов путем внесения злоумышленниками изменений в электронные сообщения, которыми пользуются граждане в арбитражных спорах, коммерческих сделках, в том числе с недвижимостью. Автор утверждает, что с дальнейшим появлением новых видов электронных документов возникнут новые способы их подделки и использования с целью совершения преступлений. Подделка электронных документов будет очень развита в будущем во многих сферах общества.
Ключевые слова: преступление, подделка электронных документов, киберпреступность, банковские системы, недвижимость, электронное сообщение

Wykorzystywanie dokumentów elektronicznych w celach popełniania przestępstw
Streszczenie: Artykuł traktuje o pojawianiu się nowych rodzajów przestępstw, które otrzymały ogólną nazwę – cyberprzestępczości. Powstają one w wyniku powszechnego wprowadzenia elektronicznych technologii cyfrowych i elektronicznego zarządzania dokumentami na początku obecnego wieku. Autor rozważa różne formy i mechanizmy cyberprzestępczości, które nie ograniczają się jedynie do nieautoryzowanego wejścia do systemów bankowych, a następnie kradzieży środków. Wiele przestępstw popełnianych jest w wyniku fałszowania różnych dokumentów elektronicznych poprzez wprowadzenie przez cyberprzestępców zmian w wiadomościach elektronicznych wykorzystywanych przez obywateli w sporach arbitrażowych, transakcjach handlowych, w tym handlu nieruchomościami.

Autor twierdzi, że wraz z pojawieniem się nowych rodzajów dokumentów elektronicznych pojawią się nowe sposoby fałszowania i wykorzystywania ich do popełniania przestępstw. Fałszowanie dokumentów elektronicznych będzie bardzo rozwinięte w przyszłości w wielu obszarach społecznych
Słowa kluczowe: przestępczość, fałszowanie dokumentów elektronicznych, cyberprzestępczość, systemy bankowe, nieruchomości, komunikacja elektroniczna.

Use of electronic documents for the purpose of committing crimes
Annotation: The article is devoted to the emergence of new types of crimes that have received a generalized name-cybercrime, which arose as a result of the widespread introduction of electronic digital technologies and electronic document management in the early 2000s. the Author considers various forms and mechanisms of cybercrime, which are not limited to the selection of passwords for unauthorized access to banking systems with subsequent theft of funds. A large number of crimes are committed as a result of forgery of various electronic documents by making changes to the electronic messages used by citizens in arbitration disputes, commercial transactions, including real estate. The author claims that with *the* advent of new types of electronic documents, there will be new ways to forge and use them to commit crimes. Falsification of electronic documents will be very developed in many areas of society in the future.
Keywords: crime, forgery of electronic documents, cybercrime, banking systems, real estate, electronic communication.

Ежегодно цифровые технологии все больше вторгаются в жизнь человека. Дистанционное получение услуг, о которых еще пару десятилетий назад мы даже не помышляли, теперь стало для нас обычным делом. Приобретение различных товаров, заказ такси, торговля на биржах и даже получение образования сегодня возможны без выхода из своей квартиры. Необходим только компьютер, подключенный к глобальной сети Интернет.

Всеобщая цифровизация естественным образом затронула и различные документы, а также документооборот в целом. История возникновения электронного документооборота относится ко второй половине XX в., но более широкое применение цифровых документов началось лишь в начале 2000-х годов, что, несомненно, связано с развитием компьютерных технологий и их большей доступностью для населения. Электронный документооборот, несомненно, очень удобен. Скорость обработки документов повышается в разы, а количество ошибок при этом сокращается. Но широкое внедрение в общество цифровых технологий породило новый вид преступлений, которые получили обобщенное название - киберпреступность.

Понятие киберпреступности не ограничивается известным нам по кинофильмам подборам паролей для осуществления несанкционированного входа в банковские системы с последующим хищением денежных средств. Большое количество преступлений совершается путем подделки различных электронных документов.

Каждый документ является носителем определенной информации, в том числе содержащей юридически значимые сведения. С тех времен, как появились документы, возникли и преступления, связанные с их подделкой.

Случаи фальсификации документов известны еще с эпохи Древнего Рима. В России первые упоминания о подлоге документов датированы XIV-XV веками, в Псковской судной грамоте, а позднее и в Судебнике 1550 года, и в Соборном уложении 1649 года. Как следует из указанных памятников права, государство всегда было озабочено проблемой подделки документов и стремилось с этим бороться. Способы борьбы сводились к введению различных степеней защиты и созданию комплексных мероприятий для выявления документов, в которые внесены преступные изменения.

В 2011 году в России принят Федеральный закон «О цифровой подписи», в котором впервые сформулировано юридическое определение электронного документа, как информации в электронной форме, подписанной квалифицированной электронной подписью, равнозначной собственноручной подписи, кроме случаев, когда законодательством установлено требование о необходимости составления документов исключительно на бумажном носителе[1].

Законодательное определение, несомненно, не охватывает весь массив электронных документов, имеющих хождение, ограничиваясь лишь документами, созданными с использованием цифровой подписи. Но использование цифровой подписи еще не очень развито в России.

Назначением электронной подписи является идентификация личности подписанта документа, но есть и другие способы идентификации, например, адрес электронной почты, номер мобильного телефона. Поэтому правильнее было бы говорить, что электронный документ – это документ, содержащий достаточные сведения о лице, его издавшем или утвердившем, и, безусловно, удостоверяющий факты определенного значения.

Подделка документов во все времена имела корыстный мотив. Подделка электронных документов, как правило, направлена на хищение чужого имущества или получение необоснованной прибыли[2].

Одной из функций государства является защита граждан от преступных посягательств третьих лиц. Конституции многих стран мира, в том числе и России, содержат гарантии соблюдения прав граждан на частную собственность и государственную защиту потерпевших от преступлений[3]. Государство стремится идти в ногу со временем, создавая регуляторные механизмы во вновь появляющихся технологиях, в том числе в электронном документообороте. Стремление побыстрее накинуть «законодательную сеть» на новшества, зачастую превалируют перед здравым смыслом. Уже имеющиеся в данной области нормы не анализируются, взаимодействие действующих правовых положений с вновь вводимыми не

[1] См.: Федеральный закон Российской Федерации от 06.04.2011 N 63-ФЗ «Об электронной подписи». [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020)

[2] См.: Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2019). [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020)

[3] См.: Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020)

прогнозируются. Таким образом, создаются законодательные дыры, используемые криминалитетом для совершения преступлений. Создавая новый законодательный акт, необходимо моделировать его работу в правовой среде конкретного государства во всех отраслях, где этот акт может быть применен.

С 2017 года в России отменено обязательное требование к бумажному носителю свидетельства о регистрации права на недвижимое имущество. То есть при регистрации сделок с объектами недвижимости теперь необязательно иметь на руках бумажный документ. Информация обо всех объектах недвижимости содержится в едином электронном реестре. Предполагалось, что такое нововведение облегчит совершение сделок, не надо будет собирать и предоставлять большое количество документов, но на практике инновация обернулась потерей гражданами своего имущества. Сложно говорить о массовости недобросовестных сделок, их статистика пока еще не ведется, но уже в первый год отказа от привычных свидетельств, только по данным, полученным из открытых источников, количество подобных мошенничеств исчислялось десятками.

Каждая запись об объекте недвижимости, содержащаяся в реестре, несомненно, является электронным документом. Противоправное внесение изменений в реестр является способом подделки.

Механизм подделки является многоступенчатым, но достаточно простым. Он основан на несовершенстве законодательства и отсутствии какой-либо ответственности лица, уполномоченного государством регистрировать сделки с недвижимостью. Поскольку документы, удостоверяющие личность гражданина, пока еще существуют в обязательном бумажном виде, для подделки электронного реестра недвижимого имущества (а именно внесения недостоверных сведений о субъекте права) необходимо, чтобы в регистрирующий орган явился человек, имеющий паспорт с данными, совпадающими с данными владельца недвижимости, а именно: фамилия, имя, отчество, дата и место рождения. Сотрудник регистрирующего органа не обязан проверять действительность паспорта, отсутствие на нем следов подделки, он должен лишь проверить полноту объема подаваемых документов.

Для совершения подобного мошенничества необязательно похищать паспорт владельца недвижимости. Реестр не содержит сведений о номере паспорта, дате выдачи, месте регистрации. Теоретически достаточно найти человека, у которого совпадают фамилия, имя, отчество, дата и место рождения с настоящим владельцем. Но это маловероятно, поэтому в данной преступной схеме используются похищенные бланки паспортов, в которые вносятся необходимые сведения.

Приведу реальный пример из собственной адвокатской практики.

В 2017 году за оказанием юридической помощи обратилась женщина, которая, услышав в новостях о возможности любому гражданину узнать сведения из реестра недвижимости, в том числе о владельце имущества, решила на практике проверить как это работает. Она ввела данные принадлежащего ей дачного участка со строениями, расположенного в Новой Москве, и с удивлением узнала, что владельцем, согласно данным реестра, является совершенно посторонний человек.

Забегая вперед, сообщу, что подлинная запись в реестре недвижимости была восстановлена в судебном порядке, кроме того, правоохранительными органами было возбуждено уголовное дело, правда виновных так и не нашли, но схема преступления стала понятна.

В регистрирующий орган обратилась женщина, предъявившая паспорт с фамилией, именем, отчеством, датой и местом рождения, как и у настоящего владельца. Была совершена псевдосделка, в результате которой в реестр внесены сведения о новом владельце. То есть в электронный документ внесены юридически значимые недостоверные сведения. Несомненно, данное преступление совершено именно путем подделки электронного документа, то есть государственного реестра прав на недвижимое имущество.

Поскольку судебного решения о виновности конкретных лиц нет, то установленные факты буду представлять в виде случайностей.

Случайность первая. Наверное, она самая важная. Новым владельцем недвижимости случайно стал единственный участник и генеральный директор агентства недвижимости, осуществляющий деятельность в районе нахождения земельного участка и дома.

Случайность вторая. Офис этого агентства недвижимости случайно находился в том же здании, где находилось отделение регистрирующего органа, внесшего изменения в реестр.

Случайность третья. При внесении изменений в реестр был представлен паспорт гражданина Российской Федерации, выданный в Воронежской области. Мы все прекрасно знаем, что паспорт выдается гражданину по месту регистрации, но единственным местом регистрации в паспорте, согласно штампу, являлась Москва. Должностное лицо регистрирующего органа случайно не обратило на это внимание.

Случайность четвертая. Адресом регистрации в паспорте являлся несуществующий адрес. Регистратор также случайно не обратил на это внимание, хотя все возможности проверить у него были. Достаточно было просто посмотреть данные в том же реестре.

Да и проверить паспорт, который как позднее выяснилось значится среди похищенных, у регистратора не составляло труда. База недействительных и похищенных паспортов, в том числе бланков паспортов, находится в открытом доступе.

Выводы напрашиваются сами собой.

Как видно из представленного примера, для подделки электронного документа совсем не требуется специальных и глубоких познаний в области IT-технологий. Преступники, по сути, пользуются далеким от совершенства регламентом работы регистрирующего органа, действующего по принципу «одного окна», то есть граждане должны получать доступ к государственным услугам в заявительном порядке. Такой порядок удобен населению, но лишь при добросовестном отношении должностных лиц при подаче и проверке заявительных документов[4].

[4] Конькова А.Ю., Яганова А.А., *Современные тенденции подготовки кадров документоведов: комплексный подход при изучении административных регламентов предоставления услуг // Сборник материалов IV Международной научно-практической конференции «Управление документацией: прошлое, настоящее, будущее», посвященной памяти профессора Т.В. Кузнецовой*, отв.ред.и сост. Ю.М. Кукарина. Москва 2019, с. 377 - 399.

Использование при сделках с недвижимостью квалифицированной цифровой подписи не спасает от преступных посягательств.

Нет, случаи подбора цифрового кода, так называемого «токена», пока еще неизвестны. Преступления с использованием цифровой подписи совершаются путем неправомерного завладения кодом.

Это может быть подбор пароля к «токену», который на стадии получения является типовым, и если пользователь его не сменит, то подбор возможен с помощью специальных программ-генераторов; использования фишинговых программ, которые могут быть удаленно внедрены в компьютер пользователя, и с помощью которых злоумышленники получают доступ к паролю, и имеются другие способы.

Но самым распространенным, в этом я абсолютно уверен, является и будет являться в ближайшее время – недобросовестность сотрудников удостоверяющих центров.

За 2019 год в Москве выявлено несколько случаев сделок с недвижимостью с использованием цифровой подписи, выданной ненадлежащему владельцу. Уверен, что со временем число таких сделок будет только расти, тем более что выпуском электронных подписей занимаются коммерческие организации, а государство регулирует их деятельность только выдачей соответствующих лицензий. Личное присутствие гражданина требуется исключительно при первичном получении цифровой подписи, последующие получения (в случае утраты, истечения срока действия) возможны по доверенности. То есть мошенник обращается в сертификационный центр с заявлением об утрате токена и просит выдать новый, при этом предъявляет доверенность, подлинность которой сотрудник центра проверять не обязан. В результате стороннее лицо завладевает совершенно легитимной цифровой подписью, с помощью которой создает поддельные электронные документы от имени ничего не подозревающего лица.

Государство уже озаботилось проблематикой борьбы с подобными видами мошенничества. Но, как часто происходит в современных условиях России, законодатель, как способ решения проблемы, видит включение карательной функции государства, то есть введение законов, устанавливающих или ужесточающих ответственность за совершение преступлений. Корень проблемы остается и, вне всяких сомнений, будет давать новые ростки. Государство забывает о том, что предупреждать проблему, создавая защитные барьеры, гораздо проще, эффективнее и экономически выгоднее, чем бороться с последствиями.

В рассмотренном случае внесение изменений в регламент, в соответствии с которым работают регистрирующие органы[5], позволило бы если и не искоренить подобный вид преступления, то существенно усложнить их совершение. Серьезных изменений и финансирования это не требует. Например, введение в регламент обязанности должностного лица проверять предъявляемые документы

[5] См.: Приказ Росреестра от 27.09.2019 N П/0401 «Об утверждении Административного регламента Федеральной службы государственной регистрации, кадастра и картографии по предоставлению государственной услуги по предоставлению сведений, содержащихся в Едином государственном реестре недвижимости» (Зарегистрировано в Минюсте России 26.11.2019 N 56635). [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020).

по общедоступной базе утраченных и похищенных бланков паспортов, позволило бы выявлять и пресекать аналогичные преступления на начальной стадии, при этом участие граждан в выполнении функции государства по защите частной собственности и защите прав потерпевших от преступных посягательств, сводились бы к необходимому процессуальному минимуму. Установление понятия «выдачи электронной цифровой подписи», как государственной услуги, также существенно снизит количество преступлений, с использованием ЭЦП. Государству необходимо осознать, что электронная цифровая подпись – это важный электронный документ, находящийся на одном уровне с любым документом, удостоверяющим личность. Сложно себе представить, что выдачей, например, общегражданских паспортов будет заниматься коммерческая организация, пусть и имеющая соответствующую лицензию.

Всем известен такой способ передачи информации, как электронная почта (e-mail). Можно задаться вопросом: являются ли сообщения, отправленные посредством e-mail, электронными документами? Ответ очевиден: несомненно, являются. При этом мы не говорим о документах, изначально составленных в бумажном виде, а в последующем переведенных в электронный вид с использованием сканера.

В коммерческом праве есть такое понятие «традиции делового оборота». Так вот, обмен сообщениями посредством e-mail, как раз и является одной из традиций современного делового оборота.

В России электронные сообщения (документы) юридического статуса не имеют, хотя в большинстве стран эта коллизия разрешена путем принятия национальных законов на основе Типичного закона об электронной торговле, предложенной Комиссией ООН по международной торговле UNICTRAL. Основным положением данного закона является то, что любые сообщения, переданные путем электронного документооборота, являются носителями информации и имеют юридическую силу наравне с бумажными носителями[6]. Проект Федерального закона РФ «Об электронной коммерции», разработанный на основе закона UNICTRAL, до сих пор не принят, хотя его актуальность не вызывает сомнений.

В арбитражных спорах давно используется электронная переписка в качестве доказательств. Соответственно электронные письма – это полноценные документы, которые можно подделать.

Гражданское право России[7] не устанавливает обязательность бумажного носителя договора, устанавливая лишь обязательность письменной формы для отдельных его видов. Соответственно договоры правомерно заключать путем

[6] См.: Галяткина Н.А., *Электронная почта и мгновенные сообщения как часть документооборота компании (опыт, проблемы, решения)*, „Оформление документов" 2004, № 5.

[7] См. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (в ред. от 16.12.2010); Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ в ред. от 03.07.2019); Гражданский кодекс Российской Федерации (часть третья) от 26.11.2001 № 146-ФЗ (в ред.от 18.03.2019); Гражданский кодекс Российской Федерации (часть четвертая) от18.12.2006 № 230-ФЗ (в ред.от 18.07.2019); Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 N 10 «О применении части четвертой Гражданского кодекса Российской Федерации». [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020)

обмена сообщениями, в том числе посредством e-mail. Что и имеет широкое практическое распространение во всем мире. Реквизитами, позволяющими установить личность отправителя, в данном случае, является адрес e-mail. То есть уникальный набор букв, цифр и символов.

Кроме того, способствующим фактором для идентификации отправителя, могут являться налаженные деловые отношения и большой объем переписки в течение длительного периода времени, в течение которого у хозяйствующих субъектов складываются доверительные отношения, в том числе и к адресу электронной почты, который является идентификатором.

Внесение изменений в электронные сообщения при современной цифровизации не составляет труда для специалиста. Используются варианты атак на ЭВМ, основной из которых является так называемая «атака посредника» (man-in-the-middle). Если не вдаваться в технические подробности, суть данного способа сводится к тому, что в технический канал связи между двумя собеседниками вторгается злоумышленник, который контролирует переписку и имеет возможность вносить изменения в передаваемую информацию. То есть совершать подделку электронного документа[8].

Приведу пример из адвокатской практики.

Российская компания посредством электронной почты в течение нескольких месяцев вела переговоры с компанией из США о поставке оборудования. Между юридическими лицами уже имелись слаженные взаимоотношения, основанные на успешном опыте аналогичных поставок на протяжении четырех лет.

При обсуждении авансового платежа произошла «атака посредника». Между договаривающимися сторонами возникло иное лицо, которое перехватывало сообщения собеседников и получало возможность внесения в передаваемые сообщения существенных изменений.

В данном случае, в целях исключения возможности получения измененного сообщения надлежащим лицом, что привело бы к раскрытию плана хищения, преступниками использовалось внесение изменений в адрес электронной почты. При этом внесенные изменения имели визуальную схожесть с оригинальным адресом. В частности, имеющаяся в адресе электронной почты латинская буква «m» была заменена на сочетание букв «r» и «n». Таким образом, совершенно другой адрес электронной почты имел визуальную схожесть с оригинальным, собеседники попросту не заметили подмену. Интерфейс сообщений был полностью скопирован. Стороны продолжали обсуждать условия заключения контракта, не подозревая, что их сообщения модерируются мошенниками.

Злоумышленникам не нужно было понимать суть договора и технические особенности поставляемого оборудования, они просто копировали сообщения каждой стороны и пересылали их другой стороне.

Когда все условия сотрудничества были согласованы, наступил важный момент: обмен банковскими реквизитами для осуществления авансового платежа. В этот момент и произошла подделка электронного документа. Плательщику по договору в электронном письме в виде электронного документа, направляются

[8] См.: Рудниченко А. К., Колесникова Д. С., *Актуальность MiTM-атак в современных Wi-Fi-сетях*, „Молодой ученый" 2017, №3.

реквизиты банковского счета, который контролируется преступниками. После перечисления денежных средств переписка еще какое-то время продолжалась, чтобы не было возможности отозвать платеж, но как только деньги поступили на счет, то и переписка «атака посредника» сразу же прекратилась. Сумма похищенного составила 125 000 долларов США.

Анализируя причины, способствующие совершению этого преступления, сложно уличить государство в невыполнении своих функций. В данном случае к потере денежных средств привело отсутствие в конкретном хозяйствующем субъекте надлежащим образом созданных и функционирующих правил электронного документооборота. Введение уже распространённого правила двухфакторной аутентификации[9], то есть способа идентификации пользователя посредством получения информации двух разных типов и последующего сопоставления этой информации, позволило бы не допустить искажения финансовых документов для осуществления платежа в адрес мошенников.

Подобные способы совершения преступлений будут в ходу еще долгое время. Кибермошенники используют анонимайзеры и средства двойного VPN, то есть инструменты, позволяющие скрыть даже страну, из которой осуществляется атака.

Совершенно очевидно, что подделка электронных документов будет очень развита в будущем во многих сферах общества.

Несколько лет назад мы наблюдали за так называемым «дизельгейтом» - скандалом, который, по сути, произвел переворот в производстве двигателей внутреннего сгорания в Европе. Это было внесение недостоверных сведений в результаты испытаний новых двигателей, разрабатываемых компанией «Фольксваген». Изменения вносились именно в электронную часть документов. И в последующем эти данные передавались в правительственные органы и потребителю[10].

В настоящее время идет много обсуждений на правительственном уровне о введении в России электронных паспортов, электронных водительских удостоверений, документов на автомобили. Рано или поздно это произойдет. И совершенно очевидно, что с появлением новых видов электронных документов возникнут новые способы их подделки и новые способы использования поддельных документов с целью совершения преступлений.

REFERENCES – BIBLIOGRAFIA – БИБЛИОГРАФИЯ

Sources:

Federal'ny zakon Rossiyskoy Federatsii ot 06.04.2011 N 63-FZ «Ob èlektronnoy podpisi». [Èlektronny resurs] // Ofitsial'ny internet-portal pravovoy informatsii. URL: http://www.consultant.ru (data obrashcheniya: 12.08.2020).

Grazhdansky kodeks Rossiyskoy Federatsii (chast' chetvertaya) ot18.12.2006 № 230-FZ (v red.ot 18.07.2019);

[9] См.: Brian Donohue, *Двухфакторная аутентификация: что это и зачем оно нужно?*, „Kaspersky Daily" 09.07.2014. [Электронный ресурс] // URL: https://www.kaspersky.ru (12.08.2020).

[10] См.: Борис Захаров, *«Дизельгейт» обошелся концерну Volkswagen в 31,3 млрд евро*, „Российская газета" 18.03.2020 [Электронный ресурс] // URL: https://rg.ru (12.08.2020).

Grazhdansky kodeks Rossiyskoy Federatsii (chast' pervaya) ot 30.11.1994 № 51-FZ (v red. ot 16.12.2010);
Grazhdansky kodeks Rossiyskoy Federatsii (chast' tret'ya) ot 26.11.2001 № 146-FZ (v red.ot 18.03.2019);
Grazhdansky kodeks Rossiyskoy Federatsii (chast' vtoraya) ot 26.01.1996 № 14-FZ v red. ot 03.07.2019);
Konstitutsiya Rossiyskoy Federatsii (prinyata vsenarodnym golosovaniem 12.12.1993 s izmeneniyami, odobrennymi v khode obshcherossiyskogo golosovaniya 01.07.2020). [Èlektronny resurs] // Ofitsial'ny internet-portal pravovoy informatsii. URL: http://www.consultant.ru (data obrashcheniya: 12.08.2020).
Postanovlenie Plenuma Verkhovnogo Suda Rossiyskoy Federatsii ot 23.04.2019 N 10 «O primenenii chasti chetvertoy Grazhdanskogo kodeksa Rossiyskoy Federatsii». [Èlektronny resurs] // Ofitsial'ny internet-portal pravovoy informatsii. URL: http://www.consultant.ru (data obrashcheniya: 12.08.2020)
Prikaz Rosreestra ot 27.09.2019 N P/0401 \"Ob utverzhdenii Administrativnogo reglamenta Federal'noy sluzhby gosudarstvennoy registratsii, kadastra i kartografii po predostavleniyu gosudarstvennoy uslugi po predostavleniyu svedeny, soderzhashchikhsya v Edinom gosudarstvennom reestre nedvizhimosti\" (Zaregistrirovano v Minyuste Rossii 26.11.2019 N 56635). [Èlektronny resurs] // Ofitsial'ny internet-portal pravovoy informatsii. URL: http://www.consultant.ru (data obrashcheniya: 12.08.2020).
Ugolovny kodeks Rossiyskoy Federatsii ot 13.06.1996 № 63-FZ (red. ot 27.12.2019). [Èlektronny resurs] // Ofitsial'ny internet-portal pravovoy informatsii. URL: http://www.consultant.ru (data obrashcheniya: 12.08.2020).

Studies:

Donohue Brian, Dvukhfaktornaya autentifikatsiya: chto èto i zachem ono nuzhno?, „Kaspersky Daily" 09.07.2014. [Èlektronny resurs] // URL: https://www.kaspersky.ru (data obrashcheniya: 12.08.2020).
Galyatkina N.A., Èlektronnaya pochta i mgnovennye soobshcheniya kak chast' dokumentooborota kompanii (opyt, problemy, resheniya), „Oformlenie dokumentov" 2004, № 5.
Kon'kova A.Yu., Yaganova A.A., Sovremennye tendentsii podgotovki kadrov dokumentovedov: kompleksny podkhod pri izuchenii administrativnykh reglamentov predostavleniya uslug // Sbornik materialov IV Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Upravlenie dokumentatsiey: proshloe, nastoyashchee, budushchee», posvyashchennoy pamyati professora T.V. Kuznetsovoy, otv.red.i sost. Yu.M. Kukarina. Moskva 2019, s. 377 - 399.
Rudnichenko A. K., Kolesnikova D. S., Aktual'nost' MiTM-atak v sovremennykh Wi-Fi-setyakh, „Molodoy uchenyy" 2017, №3.
Zakharov Boris, \"Dizel'geyt\" oboshelsya kontsernu Volkswagen v 31,3 mlrd evro, „Rossiyskaya gazeta" 18.03.2020 [Èlektronny resurs] // URL: https://rg.ru (data obrashcheniya: 12.08.2020).

Источники:

Федеральный закон Российской Федерации от 06.04.2011 N 63-ФЗ «Об электронной подписи». [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020).
Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2019). [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020).
Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

[Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020).
Приказ Росреестра от 27.09.2019 N П/0401 «Об утверждении Административного регламента Федеральной службы государственной регистрации, кадастра и картографии по предоставлению государственной услуги по предоставлению сведений, содержащихся в Едином государственном реестре недвижимости» (Зарегистрировано в Минюсте России 26.11.2019 N 56635). [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020).
Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (в ред. от 16.12.2010); Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ в ред. от 03.07.2019); Гражданский кодекс Российской Федерации (часть третья) от 26.11.2001 № 146-ФЗ (в ред.от 18.03.2019); Гражданский кодекс Российской Федерации (часть четвертая) от18.12.2006 № 230-ФЗ (в ред.от 18.07.2019); Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 N 10 «О применении части четвертой Гражданского кодекса Российской Федерации». [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.consultant.ru (12.08.2020)

Литература:

Галяткина Н.А., *Электронная почта и мгновенные сообщения как часть документооборота компании (опыт, проблемы, решения)*, „Оформление документов" 2004, № 5.
Конькова А.Ю., Яганова А.А., *Современные тенденции подготовки кадров документоведов: комплексный подход при изучении административных регламентов предоставления услуг // Сборник материалов IV Международной научно-практической конференции «Управление документацией: прошлое, настоящее, будущее», посвященной памяти профессора Т.В. Кузнецовой*, отв.ред.и сост. Ю.М. Кукарина. Москва 2019, с. 377 - 399.
Рудниченко А. К., Колесникова Д. С., *Актуальность MiTM-атак в современных Wi-Fi-сетях*, „Молодой ученый" 2017, №3.
Brian Donohue, *Двухфакторная аутентификация: что это и зачем оно нужно?*, „Kaspersky Daily" 09.07.2014. [Электронный ресурс] // URL: https://www.kaspersky.ru (12.08.2020).
Борис Захаров, *«Дизельгейт» обошелся концерну Volkswagen в 31,3 млрд евро*, „Российская газета" 18.03.2020 [Электронный ресурс] // URL: https://rg.ru (12.08.2020).