

Виды киберпреступлений по российскому уголовному законодательству

Иванова Лилия Викторовна

кандидат юридических наук

доцент, доцент кафедры уголовного права и процесса, Тюменский государственный университет

625000, Россия, Тюменская область, г. Тюмень, ул. Ленина, 38

✉ ivanova_liliya@mail.ru



[Статья из рубрики "Уголовный закон и правопорядок "](#)

Аннотация.

Предмет исследования составили положения науки уголовного права о киберпреступности, нормы уголовного законодательства о преступлениях в сфере компьютерной информации и преступлениях, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также положения нормативных правовых актов в области информационной безопасности и информационных технологий. Целью исследования является установление круга деяний, составляющих киберпреступления с точки зрения российского уголовного права, а также предложение совершенствования уголовно-правовых норм в части дифференциации уголовной ответственности за совершение преступления с использованием информационных технологий. Рассматриваются различные точки зрения ученых на понимание киберпреступлений, выделяются признаки таких деяний. В основу исследования положен системный подход, использованы такие методы, как логический, нормативно-догматический и сравнительно-правовой методы познания. Анализ различных точек зрения ученых, системное толкование норм законодательства позволило прийти к выводу об универсальности термина «киберпреступления» для характеристики преступлений, совершаемых при помощи информационных технологий, несмотря на отсутствие его определения в нормативных правовых актах. Новизна исследования заключается в изложении современного понимания киберпреступлений, к которым необходимо относить все преступления, совершаемые посредством ИТ-технологий. Обращается внимание на непоследовательность законодателя в закреплении в составе преступлений признака совершения деяния с использованием электронных или информационно-телекоммуникационных сетей и в не установлении такого признака в преступлениях, часто совершаемых посредством Интернета. В целях дифференциации уголовной ответственности обосновывается необходимость дополнения всех составов преступлений Уголовного кодекса РФ, которые могут быть совершены с использованием информационных технологий, соответствующим квалифицирующим признаком.

Ключевые слова: киберпреступность, высокие технологии, информационные преступления, компьютерные преступления, интернет, телекоммуникационные сети, электронные сети, информационные технологии, кибербезопасность, цифровое пространство

DOI:

10.25136/2409-7136.2019.1.28600

Дата направления в редакцию:

31-01-2019

Дата рецензирования:

11-01-2019

Развитие общества в настоящий период связано с цифровизацией практически всех сфер жизнедеятельности. В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [\[1\]](#), отмечается, что информационные системы, социальные сети стали частью повседневной жизни россиян. Пользователями сети «Интернет» в России в 2016 году стали более 80 млн. человек.

Информационные и телекоммуникационные сети стали незаменимыми помощниками в решении не только рабочих вопросов (посредством системы электронного документооборота, деловой переписки через Интернет и т. д.), но и бытовых (оплата товаров онлайн, получение госуслуг через специальный сайт и т. д.). Информационное пространство с каждым днем наполняется новыми данными. В то же время повсеместное распространение новейших технологий таит в себе угрозы посягательства на личную безопасность и собственность, на безопасность общества в целом и государства, то есть несет угрозу причинения вреда наиболее важным общественным отношениям, охраняемым Уголовным кодексом Российской Федерации.

В последнее время наблюдается неуклонный рост преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий. Так, если с января по ноябрь 2017 года было зарегистрировано 82440 таких преступлений, то за аналогичный период 2018 года зарегистрировано уже 156307 таких преступлений, что на 89,6% больше показателей периода прошлого года [\[2\]](#). Ущерб от киберпреступлений оценивается в 2018 году свыше 400 млрд. рублей, а ущерб мировой экономике от подобных деяний по прогнозам в 2019 году может возрасти до 2 трлн. долларов США, а в 2020 году – до 3 трлн. долларов США [\[3\]](#). При этом нельзя забывать о высокой латентности такого рода преступлений [\[4, с. 8-9\]](#).

Киберпреступность возникла несколько десятилетий назад с активным развитием информационных систем. На международном уровне впервые данный термин был использован в 1986 году [\[5, с. 29\]](#).

Не углубляясь в содержание понятия «киберпреступление» на международном уровне, что заслуживает самостоятельного исследования, отметим отсутствие единого подхода к пониманию киберпреступлений на уровне отдельных стран и международного сообщества в целом [\[6, 7, 8\]](#).

В Российской Федерации правовая основа борьбы с киберпреступлениями впервые появилась с принятием Уголовного кодекса Российской Федерации (далее – УК РФ), вступившего в силу с 01 января 1997 года, в котором появилась глава 28 «Преступления в сфере компьютерной информации», хотя отдельные законопроекты появлялись и

ранее, однако не были приняты [\[9, с. 56, 10, с. 27\]](#). Например, проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией» 1991 года, законопроект о внесении изменений в УК РСФСР 1994 г. и 1995 г.

Появление новых составов преступлений в УК РФ обусловило проведение ряда исследований компьютерных преступлений [\[11, 12, 13, 14, 15, 16\]](#). Вместе с тем преступления, связанные с информационными технологиями не ограничиваются только преступлениями в сфере компьютерной информации. В ряде составов УК РФ закреплены соответствующие конструктивные или квалифицирующие признаки совершения общественно опасного деяния с использованием электронных, информационно-телекоммуникационных сетей.

В настоящей работе на основе системного подхода, а также логического, нормативно-догматического и сравнительно-правового методов познания представлен анализ норм УК РФ, в которых отражаются отдельные признаки совершения преступлений с использованием высоких технологий с целью установления круга деяний, составляющих киберпреступления с точки зрения российского уголовного права, а также в целях предложения совершенствования уголовно-правовых норм в части дифференциации уголовной ответственности за совершение преступления с использованием информационных технологий.

Объектом исследования являются общественные отношения, обеспечивающие уголовно-правовое противодействие киберпреступлениям. Предметом исследования выступили положения науки отечественного уголовного права о киберпреступлениях, нормы российского уголовного закона о преступлениях в сфере компьютерной информации и преступлениях, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также положения российского законодательства в области информационной безопасности и информационных технологий.

Следует отметить, что такой широко распространенный в научной литературе и средствах массовой информации термин как «киберпреступление» не встречается и тем более не раскрывается в современном российском законодательстве. Между тем, в Концепции внешней политики Российской Федерации [\[17\]](#) в числе вызовов и угроз современного мира, имеющих трансграничную природу, называется киберпреступность. Внедрение современных механизмов и технологий противодействия киберпреступности является одним из приоритетных направлений цифровой трансформации органов прокуратуры Российской Федерации [\[18\]](#). Но содержание категории «киберпреступность» также не раскрывается на законодательном уровне.

Для эффективного противодействия любому негативному явлению необходимо определиться с его содержанием.

«Киберпреступление» – термин иностранного происхождения, образованный из двух составляющих «кибер» и «преступление». Как отмечается, в Оксфордском словаре кибер (cyber) определяется как: «относящийся к компьютерам, информационным технологиям, виртуальной реальности» [\[19, с. 35\]](#). Следует отметить, что в российском законодательстве при характеристике виртуального пространства и высоких технологий используются такие прилагательные как «цифровое», «информационное».

Стратегия национальной безопасности Российской Федерации [\[20\]](#) говорит о новых

формах противоправной деятельности с использованием информационных, коммуникационных и высоких технологий – преступности в информационной сфере.

Согласно Доктрине информационной безопасности Российской Федерации [\[21\]](#), под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. По сути, информационная безопасность и кибербезопасность – это синонимы, но если первый раскрывается в нормативном правовом акте, то второй – нет.

Наряду с термином «киберпреступления», ученые используют такие категории как: «преступления в сфере информационных технологий» [\[8, 22\]](#), «информационные преступления» [\[23, 24\]](#), сетевые компьютерные преступления [\[25\]](#), интернет-преступления [\[26, 27\]](#). Мы согласны с суждением А. И. Халиуллина о том, что наиболее верным и нейтральным термином по-прежнему остается «киберпреступления» в силу быстро изменяющихся процессов в области информационных технологий и появления новых способов обмена информацией [\[28, с. 35\]](#).

Рассматривая признаки киберпреступлений исследователями называется несколько характерных черт.

Во-первых, киберпреступления совершаются с использованием средств компьютерной техники и в отношении информации, находящейся (используемой и обрабатываемой) в сети «Интернет» [\[29, с. 45\]](#). Использование компьютерных устройств и информационно-телекоммуникационных сетей выступает в качестве средства совершения преступления, а использование вредоносных программ - в качестве орудия совершения преступления [\[30, с. 15\]](#).

Во-вторых, в таких преступлениях присутствуют два объекта посягательства (общественные отношения в сфере безопасности обращения компьютерной информации и общественные отношения, связанные с ней, и имеющие взаимосвязь с реальным миром, например, отношения собственности) [\[28, с. 36\]](#).

В-третьих, для киберпреступлений характерно использование специальных познаний в компьютерной сфере или специальных программных комплексов для совершения преступных деяний [\[31, с. 21\]](#).

Представляется необходимым дополнить данный перечень указанием на умышленный характер действий, так как при совершении киберпреступления лицо осознает общественную опасность деяния, предвидит наступления вредных для общества или отдельного лица последствий и желает наступления этих последствий, либо относится к ним безразлично. Киберпреступления исключают совершение их по небрежности или легкомыслию.

Основная особенность, отличающая киберпреступления от иных противоправных деяний заключается в использовании компьютерных технологий и сети Интернет при совершении преступления. Компьютер или компьютерная сеть играют в данном случае ведущую роль

[\[32, с. 20\]](#).

Содержательное наполнение категории киберпреступлений должно соответствовать действующему уголовному законодательству.

Как отмечалось, Уголовный кодекс Российской Федерации содержит главу 28 «Преступления в сфере компьютерной информации», включающей в себя всего четыре статьи с 272 по 274.1 УК РФ: 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, неправомерное воздействие на критическую информационную инфраструктуру РФ.

Зачастую киберпреступления рассматриваются как синонимы компьютерным преступлениям, под которыми понимают только вышеназванные специальные составы УК РФ. Так, А. Н. Сухаренко, анализируя статистические данные по киберпреступлениям, рассматривает только преступления в сфере компьютерной информации, по сути ставя знак равенства между данными категориями [\[33\]](#). Иногда к компьютерным преступлениям относят также мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) [\[31, с. 21\]](#). Представляется, что в данном случае нарушается системность норм, так как основным непосредственным объектом мошенничества являются отношения собственности: именно поэтому ст. 159.6 УК РФ расположена в главе 21 УК РФ. Отношения по сбору, хранению и передачи компьютерной информации выступают дополнительным объектом. В то время как в ст. 272 – 274.1 УК РФ эти отношения выступают основным непосредственным объектом. Следует отметить, что отдельными исследователями разграничиваются категории «компьютерные преступления» и «преступления в сфере компьютерной информации», причем первые включают в себя последние [\[34, с. 23; 35, с. 55\]](#). На наш взгляд, при таком подходе под компьютерными преступлениями, по сути, рассматриваются киберпреступления, но учитывая, что помимо компьютера в настоящее время существует множество других устройств, позволяющих выйти в цифровую среду, категория компьютерных преступлений в понятийном аппарате представляется неполной, так как не охватывает, например, преступлений, совершаемых через мобильный телефон, не являющийся компьютером. Поэтому еще раз подчеркнем универсальность и жизнеспособность термина «киберпреступление».

Помимо преступлений в сфере компьютерной информации в ряде статей УК РФ содержится конструктивный либо квалифицирующий признак совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»».

Конструктивный признак использования высоких технологий при совершении преступления содержится только в ст. 137 УК РФ, уже отмеченной ст. 159.6 УК РФ, а также в ст.ст. 171.2, 185.3, 258.1, 282 УК РФ. При этом не всегда понятна логика законодателя по установлению, а вернее, неустановлению такого признака. В частности, в ч. 3 ст. 137 УК РФ предусмотрена ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или

психическое расстройство несовершеннолетнего, или иные тяжкие последствия. При этом аналогичный признак отсутствует в общем составе по ч. 1 ст. 137 УК РФ. Причем законодатель предусмотрел наказание за распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Но упустил из виду распространение в виртуальном мире. Очевидно, что распространение сведений посредством сети «Интернет», например, в социальных сетях, несет в себе не меньшую общественную опасность.

В качестве признака, повышающего общественную опасность содеянного и влекущего более строгое наказание, совершение деяния с использованием электронных или информационно-телекоммуникационных сетей содержится всего в тринадцати составах уголовного закона: три состава в главе «Преступления против жизни и здоровья» (ст.ст. 110, 110.1, 110.2 УК РФ), один состав в главе «Преступления против семьи и несовершеннолетних» (ст. 151.2 УК РФ), один состав в главе «Преступления против общественной безопасности» (ст. 205.2 УК РФ), пять составов в главе «Преступления против здоровья населения и общественной нравственности» (ст.ст. 228.1, 242, 242.1, 242.2, 245 УК РФ), один состав в главе «Экологические преступления» (ст. 258.1 УК РФ), два состава в главе «Преступления против основ конституционного строя и безопасности государства» (ст.ст. 280, 280.1 УК РФ).

В связи с этим представляется неполным определение, данное Э. Л. Кочкиной, определяющей киберпреступление как «совокупность преступлений, запрещенных Уголовным кодексом РФ, совершаемых в киберпространстве, где основными непосредственными объектами преступного посягательства выступают: конституционные права и свободы человека и гражданина; общественные отношения в сфере компьютерной информации и информационных технологий; общественные отношения в сфере экономики и экономической деятельности; общественные отношения в сфере государственной власти; общественные отношения в сфере здоровья населения и общественной нравственности» [\[36, с. 167\]](#). Как видно, в числе непосредственных объектов киберпреступлений не названы жизнь и здоровье, общественные отношения, обеспечивающие общественную безопасность, общественные отношения по охране окружающей среды, общественные отношения, обеспечивающие основы конституционного строя РФ.

Необходимо отметить, что в УК РФ содержится еще несколько составов, которые, на наш взгляд, можно отнести к киберпреступлениям. Так, п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав – кража с банковского счета, а равно в отношении электронных денежных средств, ст. 159.3 УК РФ устанавливает ответственность за мошенничество с использованием электронных средств платежа, ст. 187 УК РФ в части неправомерного оборота электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Отнесение данных составов к киберпреступлениям возможно благодаря предмету преступления, которым выступают либо безналичные денежные средства, либо электронные средства, либо электронные носители информации, то есть всё то, что появилось как результат развития информационных технологий и внедрения их в банковский сектор.

При этом не только вышерассмотренные преступления могут быть совершены посредством высоких технологий. Так, например, незаконное приобретение или сбыт оружия может осуществляться, в том числе, через Интернет, однако в ст. 222 УК РФ,

данный квалифицирующий признак не нашел отражения, как в ст. 228.1 УК РФ применительно к наркотическим средствам, психотропным веществам или их аналогам. Или, например, незаконная розничная продажа алкогольной и спиртосодержащей пищевой продукции, несмотря на законодательный запрет, осуществляется через Интернет. Специалисты Brand Protection Group-IB посчитали экономику теневого алкорынка: средняя посещаемость сайта, реализующего алкоголь с доставкой, составляет 190 пользователей в сутки или 5 700 человек в месяц. При конверсии 0,7% и средней стоимости одной покупки в 1 100 рублей, 4 000 онлайн-магазинов зарабатывают от 174,5 млн рублей в месяц. Таким образом, оборот нелегальной интернет-продажи алкоголя по итогам 2018 года составил порядка 2,1 млрд. рублей, что на 23% выше, чем годом ранее [37]. Но в соответствующем составе преступления не предусмотрено усиление ответственности в случае незаконной продажи алкоголя посредством Интернет.

Учитывая, что совершение преступления посредством цифрового пространства становится всё более распространенным, облегчает виновному достижение преступной цели, а следовательно, повышает общественную опасность содеянного, представляется необходимым включение в качестве квалифицирующего признака совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»» во все статьи УК РФ, за исключением тех преступлений, которые даже теоретически не могут быть совершены посредством IT-технологий. Например, убийство матерью новорожденного ребенка, заражение ВИЧ-инфекцией никак не может быть совершено с использованием информационно-телекоммуникационных сетей. Включение же такого признака в большинство статей УК РФ позволит дифференцировать уголовную ответственность.

Таким образом, на современном этапе развития информационного общества киберпреступления необходимо рассматривать как умышленные деяния, совершаемые с использованием IT-технологий. К киберпреступлениям относятся специальные киберпреступления и общеуголовные киберпреступления. Специальные киберпреступления – это преступления в сфере компьютерной информации. Общеуголовные киберпреступления – это иные преступления, совершаемые с использованием высоких технологий. К ним относятся преступления, в составе которых присутствует в качестве конструктивного или квалифицирующего признак совершения деяния с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также преступления, составы которых в качестве предмета преступления называют электронные средства, электронные носители информации. В целях дифференциации уголовной ответственности необходимо включить во все составы общеуголовных преступлений, которые могут быть совершены посредством высоких технологий квалифицирующий признак совершения деяния с использованием электронных или информационно-телекоммуникационных сетей.

Библиография

1. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 10.05.2017.
2. Статистика преступности (январь – ноябрь 2018 года); Статистика преступности (январь – ноябрь 2017 года). – URL: <https://мвд.рф/folder/101762/item/15304733/>
3. МИД РФ: ущерб мировой экономике от киберпреступности в 2019 году может достичь \$2 трлн. – URL: <https://tass.ru/politika/5551244> вместо 2
4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры

- борьбы. Автореф. дис. ... канд. юрид. наук. – Владивосток, 2005. – 26 с.
5. Бутусова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3. С. 28 – 31.
 6. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М.: Норма, 2017. – 528 с.
 7. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. N 3. С. 10 – 13.
 8. Хисамова З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий // Юридический мир. 2016. N 2. С. 58 – 62.
 9. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. – 496 с.
 10. Шайхаттарова С.В. Россия и международные стандарты по борьбе с киберпреступностью // Международное уголовное право и международная юстиция. 2016. N 4. С. 26 – 29.
 11. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук. М., 1998. – 161 с.
 12. Воробьев В.В. Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация: дис. ... канд. юрид. наук. Нижний Новгород, 2000. – 201 с.
 13. Ушаков С.И. Преступления в сфере обращения компьютерной информации: теория, законодательство, практика: дис. ... канд. юрид. наук. Ростов-на-Дону, 2000 – 176 с.
 14. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): дис. ... канд. юрид. наук. Волгоград, 2001. – 193 с.
 15. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. ... канд. юрид. наук. Красноярск, 2002. – 202 с.
 16. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук. Ижевск, 2002. – 189 с.
 17. Указ Президента РФ от 30.11.2016 N 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 01.12.2016.
 18. Приказ Генпрокуратуры России от 14 сентября 2017 г. N 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Законность. 2017. № 12.
 19. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Право и кибербезопасность. 2014. N 2. С. 33 – 38.
 20. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 31.12.2015.
 21. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 06.12.2016.
 22. Абрамян Т.А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий // Юрист. 2018. N 5. С. 68 – 72.
 23. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. N 18. С. 53 – 56.

24. Особенности противодействия киберпреступности подразделениями уголовного розыска / под ред. Б.П. Михайлова, Е.Н. Хазова. М.: ЮНИТИ-ДАНА: Закон и право, 2016. – 151 с.
25. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009. – 480 с.
26. Дремлюга Р.И. Интернет-преступность: монография. Владивосток: Изд-во Дальневосточного ун-та, 2008. – 240 с.
27. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола. Ижевск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2015. – С. 120 – 125.
28. Халиуллин А.И. Подходы к определению киберпреступления // Российский следователь. 2015. N 1. С. 34 – 39.
29. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 44 – 46.
30. Зиборов О.В., Иванов М.А., Чекунов И.Г. Состояние кибербезопасности современного информационного общества // Вопросы кибербезопасности. 2017. № 2. С. 15 – 18.
31. Турышев А.А. Уголовно-правовые инструменты защиты информационного общества // Законы России: опыт, анализ, практика. 2017. N 10. С. 19 – 23.
32. Трунцевский Ю.В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. N 21. С. 19 – 22.
33. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. N 2. С. 2 – 5.
34. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996. – 182 с.
35. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук. Казань, 2017 – 243 с.
36. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 162 – 169.
37. Group-IB: оборот нелегальной онлайн-продажи алкоголя в 2018 году превысил 2,1 млрд рублей. URL: <https://www.group-ib.ru/media/alco-2018/>