DOI: 10.18287/2542-047X-2020-6-3-53-59
УДК 343
Научная статья / Scientific article

Дата: поступления статьи / Submitted: 27.01.2020
после рецензирования / Revised: 18.02.2020
принятия статьи / Accepted: 28.08.2020

О. А. Бойко
Омская академия МВД России, г. Омск-112, Российская Федерация
E-mail: mario011@mail.ru

А. С. Унукович
Омская академия МВД России, г. Омск-112, Российская Федерация
E-mail: unukovich94@mail.ru

ДЕТЕРМИНАНТЫ ЛАТЕНТНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: В 2019 году в Российской Федерации зарегистрировано 294 409 преступных посягательств, совершенных с использованием информационно-телекоммуникационных технологий, из которых раскрыто только 65 238 деяний. Определенная часть преступлений в информационно-телекоммуникационном пространстве остается вне поля зрения правоохранительных органов – латентной. Авторами статьи сформулированы понятия преступности в информационно-телекоммуникационном пространстве и латентных уголовно наказуемых деяний, совершаемых с использованием информационно-телекоммуникационных технологий. Анализируются детерминанты латентности преступлений, осуществляемых с использованием ИТТ. Формулируется вывод о необходимости целенаправленного воздействия на детерминанты латентной преступности, совершаемой с использованием ИТТ, позволяющего вывести из «тени» определенную часть противоправных посягательств.
Ключевые слова: информационно-телекоммуникационные технологии, преступность, понятие латентности и ее виды, детерминанты латентности преступлений в информационно-телекоммуникационной сфере.
Цитирование. Бойко О. А., Унукович А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. 2020. Т. 6, № 3. С. 53–59. DOI: http://doi.org/10.18287/2542-047X-2020-6-3-53-59.
Информация о конфликте интересов: авторы заявляют об отсутствии конфликта интересов.

O. A. Boyko
Omsk Academy of the Ministry of the Interior of Russia, Omsk, Russian Federation
E-mail: mario011@mail.ru

A. S. Unukovich
Omsk Academy of the Ministry of the Interior of Russia, Omsk, Russian Federation
E-mail: unukovich94@mail.ru

DETERMINANTS OF LATENT CRIMES COMMITTED USING INFORMATION AND COMMUNICATIONS TECHNOLOGIES

Abstract: In 2019, 294 409 criminal assaults were registered in the Russian Federation, committed using information and communications technologies, of which only 65 238 acts were disclosed. In addition, a certain part of crimes in the information and telecommunications space remains out of sight of law enforcement agencies-latent. The authors of the article have formulated the concepts of crime in the information and communications space and latent criminal acts committed using information and communications technologies. The article analyzes the determinants of latency of crimes carried out using it. The conclusion is formulated that it is necessary to purposefully influence the determinants of latent crime committed using ICT, which makes it possible to remove a certain part of illegal encroachments from the «shadow».
Key words: information and communication technologies, crime, concept of latency and its types, determinants of latency of pre-steps in the information and telecommunication sphere.
Citation. Boyko O. A., Unukovich A. S. *Determinanty latentnykh prestupleniy, sovershaemykh s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologiy* [Determinants of latent crimes committed using information and communication technologies]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samara University], 2020, Vol. 6, no. 3, pp. 53–59. DOI: http://doi.org/10.18287/2542-047X-2020-6-3-53-59 [in Russian].
Information about the conflict of interests: authors declare no conflict of interests.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

© **Ольга Альбертовна Бойко** – кандидат юридических наук, доцент кафедры криминологии, психологии и педагогики, Омская академия МВД России, 644112, Российская Федерация, г. Омск, пр-т Комарова, 7.

Тема кандидатской диссертации: «Криминологическая характеристика и предупреждение корыстно-насильственных преступлений, совершаемых в отношении женщин». Автор 38 научных публикаций, в том числе соавтор учеб-

© **Olga A. Boyko** – Candidate of Legal Sciences, assistant professor of the Department of Criminology, Psychology and Pedagogy, Omsk Academy of the Ministry of the Interior of Russia, 7, Komarova Avenue, Omsk, 644112, Russian Federation.

Subject of Candidate's thesis: «Criminological characteristics and prevention of mercenary-violent crimes committed against women». Author of 38 scientific works,

ного пособия «Актуальные проблемы виктимологии» (2017).

Область научных интересов: виктимология, виктимологическая безопасность.

© **Антон Станиславович Унукович** – адъюнкт кафедры криминологии, психологии и педагогики, Омская академия МВД России, 644112, Российская Федерация, г. Омск, пр-т Комарова, 7.

Автор 6 научных публикаций.

Область научных интересов: преступления, совершаемые с использованием информационно-телекоммуникационных технологий.

including textbook: «Actual problems of victimology» (2017)

Research interests: victimology, victimological safety

© **Anton S. Unukovich** – adjunct of the Department of Criminology, Psychology and Pedagogy, Omsk Academy of the Ministry of the Interior of Russia, 7, prospekt Komarova, Omsk, 644112, Russian Federation.

Author of 6 scientific works.

Research interests: crimes committed using information and communication technologies.

Разделяем точку зрения ряда ученых [1, с. 31–32; 2, с. 54; 3, с. 10], которые к преступлениям в информационно-телекоммуникационной сфере относят не только противоправные посягательства, совершенные в глобальной сети Интернет, но и все виды уголовно наказуемых деяний, осуществленных с использованием информационно-телекоммуникационных технологий (далее – ИТТ), где информация, информационные ресурсы, информационная техника могут выступать предметом преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления.

Преступность в информационно-телекоммуникационной сфере включает в себя различные противоправные посягательства: мошенничество с использованием платежных карт и в сфере компьютерной информации, незаконные организация и проведение азартных игр, публичные призывы к осуществлению террористической и экстремистской деятельности, незаконный сбыт наркотиков, распространение порнографических материалов, неправомерный доступ к компьютерной информации, создание и распространение вредоносных компьютерных программ и др.

Определенная часть преступлений, совершаемых с использованием ИТТ, остается вне поля зрения правоохранительных органов. Латентная преступность в информационно-телекоммуникационном пространстве – это объективное социально-правовое явление, имеющее свои качественные и количественные характеристики, представляющее собой совокупность противоправных посягательств, совершенных с использованием ИТТ, не выявленных и (или) не учтенных правоохранительными органами на той или иной территории в определенный период времени [4, с. 121].

Наибольшей латентностью обладают преступления, связанные с неправомерным доступом к охраняемой законом компьютерной информации. По мнению экспертов [5, с. 66], латентность указанных противоправных посягательств составляет 80–85 %, а факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер.

Высокая латентность уголовно наказуемых деяний, совершаемых с использованием ИТТ, обусловлена различными причинами. Под детерминантами латентных преступлений, совершаемых с использованием ИТТ, следует понимать совокупность обстоятельств социального, организационного, правового, личностного, технического и иного характера, препятствующих выявлению (установлению), регистрации и учету преступных посягательств в сфере информационно-телекоммуникационных технологий.

Криминологами по механизму образования выделяются три вида латентных противоправных посягательств – преступлений, совершаемых с использованием ИТТ, представленных во всех разновидностях [6, с. 37]:

а) к естественно-латентным следует отнести совокупность преступлений, совершаемых с использованием ИТТ, не ставших известными (не выявленных) правоохранительным органам, соответственно, не учтенных в уголовной статистике, в отношении которых не приняты предусмотренные законом меры реагирования;

б) к искусственно-латентным следует отнести совокупность преступлений, совершаемых с использованием ИТТ, ставших известными правоохранительным органам, но в силу различных причин умышленно сокрытых от регистрации;

в) к третьей разновидности латентной преступности, совершаемой с использованием ИТТ, следует отнести совокупность противоправных посягательств, информация о которых стала известна правоохранительным органам, но которые оказались за рамками статистического учета в силу их добросовестно ошибочной или заведомо незаконной правовой оценки.

На основании предложенной классификации видов латентной преступности, совершаемой с использованием ИТТ, рассмотрим детерминанты (причины и условия), в силу которых часть противоправных посягательств в информационно-телекоммуникационном пространстве остается не охваченной правоохранительными органами.

Правоохранительные органы не могут обеспечить соответствующую правовую реакцию (не в состоянии надлежащим образом проверять все сообщения) на постоянно возрастающий объем оперативной информации о преступлениях, совершаемых с использованием ИТТ. Методы (инструменты) выявления и раскрытия преступлений, которые являются эффективными для правоохранительных органов на «земле», неэффективны в виртуальном мире [7, с. 285].

В ходе выявления преступлений, совершаемых с использованием ИТТ, возникают трудности, обусловленные отсутствием представителей правообладателей указанных контентов на территории

Российской Федерации и фактическим нахождением серверов, на которых хранится указанная выше информация на территории иностранных государств [8, с. 246]. Преступниками для совершения преступления одновременно могут использоваться несколько тысяч компьютеров, располагающихся в различных частях мира. Кроме того, правонарушители с помощью ботнэта получают доступ к большему числу компьютеров, поэтому в состоянии многократно увеличивать количество совершаемых в международном информационно-телекоммуникационном пространстве противоправных деяний.

Одной из причин естественной латентности преступлений, совершаемых с использованием ИТТ, является проблема установления конкретного лица, совершившего преступление в сети Интернет. Она связана с трансграничностью сети и наличием эффективных механизмов (например, использование анонимайзеров ToR, SRWare Iron, поддельных адресов электронной почты) обеспечения анонимности лица, являющегося участником информационного пространства: преступник может находиться в одном государстве, а результаты преступной деятельности проявляются на территориях других государств [9, с. 163–164]. Положение осложняется тем, что информация может храниться на web-сайтах и серверах в другой стране или на другом континенте, где по местному законодательству ответственность граждан за определенный вид противоправных посягательств (например, за хранение и распространение порнографических сайтов в отношении несовершеннолетних) отсутствует.

Преступления, совершаемые с использованием ИТТ, в силу их содержательной виртуальности и оформленной высокотехнологичности относятся к деяниям, где нет явно выраженной потерпевшей стороны, поэтому зачастую просто некому сообщать о преступлениях в компетентные органы. Пользователи сети Интернет нередко находятся в состоянии неведения, что в отношении них совершены противоправные посягательства в сфере ИТТ. Так, вирусные черви, являющиеся вредоносной компьютерной программой, проникают в устройство пользователей с целью сбора и передачи информации в интересах правонарушителя, но остаются скрытыми для владельцев устройств.

К одной из причин естественной латентности преступлений, совершаемых с использованием ИТТ, следует отнести наличие у участников информационного пространства правового нигилизма [10, с. 165; 11, с. 64]. С точки зрения определенного числа пользователей Всемирной паутины, пострадавших от отдельных видов преступлений, совершаемых с использованием ИТТ (например, несанкционированный доступ к сетевым ресурсам), причиненный им вред является незначительным, степень общественной опасности деяний невысока, следовательно, нет смысла тратить время и силы на подачу заявления в правоохранительные органы. Многие пользователи Сети не обращаются в правоохранительные органы, поскольку полагают, что сами виноваты в произошедшем: попадание в устройства вирусов «списывается» ими или на непреднамеренную личностную ошибку, или на неумение «отлавливать» вирусы при общении (работе) в информационном пространстве. Значительная часть преступлений, совершаемых в информационном пространстве, остаются без внимания в силу незнания пользователями сети Интернет своих прав и нежелания добиваться их защиты правовыми средствами. Часть пользователей, пострадавших от таких противоправных действий, считают, что полиция по их заявлениям ничего реально сделать не сможет.

В информационно-коммуникационном пространстве регулярно происходит повсеместное нарушение авторских и патентных прав производителей программных продуктов, обеспечивающих надлежащую работу компьютерных сетей: при этом «рядовой» пользователь может и не знать о том, что фактически незаконно пользуется «чужим» программным продуктом [12, с. 153]. Кроме того, нередко сами пользователи приобретают за небольшие деньги добытую заведомо незаконными способами информацию, продаваемую в виртуальном пространстве (например, базы данных ГИБДД, налоговой службы и т. п.).

Крупные компании (холдинги) и банки, ставшие жертвами преступников, нередко в правоохранительные органы не обращаются, предпочитая самостоятельно разобраться с проблемами собственной компьютерной безопасности. Таковая позиция обусловлена: нежеланием ставить под сомнение свою деловую репутацию с возможной потерей клиентов; желанием избежать потенциальных убытков от расследования (например, изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев), которые могут оказаться выше суммы причиненного ущерба; обеспечением коммерческой тайны; опасением, что в ходе проверки заявления могут быть выявлены факты неправомерной деятельности самих потерпевших. Кроме того, признание факта несанкционированного доступа в подведомственную систему не только ставит под сомнение профессиональную квалификацию должностных лиц, в обязанности которых входит обеспечение компьютерной безопасности, но и может вызвать серьезные внутренние осложнения в деятельности организации [13, с. 34–35].

О части преступлений, осуществленных с использованием ИТТ, правоохранительным органам становится известно только через определенный период времени после их совершения – от самого преступника, привлекаемого позже за аналогичные противоправные деяния.

В настоящее время новые защитные механизмы работы компьютерных систем и технологий начинают разрабатываться, как правило, после атаки на них со стороны злоумышленников без учета того, как они будут функционировать в условиях возрастающих угроз со стороны организованной

преступности в сфере ИТТ. Кроме того, регулярно появляющиеся новые способы совершения преступлений, совершаемых с использованием ИТТ, опережают не только процессы по улучшению защиты функционирующих информационных систем и сетей, но и существующие меры уголовно-процессуального и уголовно-правового реагирования [14, с. 67].

По мнению экспертов [15, с. 153], наличие защитных мер позволяет снижать риски от преступлений, совершаемых с использованием ИТТ, но анализ успешных атак на хорошо защищенные компьютерные системы показывает, что предпринимаемые пользователями мероприятия по технической защите не могут полностью предотвратить незаконные вторжения.

Внедрение систем 5G, с помощью которых можно создать новые типы и способы атак в информационно-телекоммуникационном пространстве, будет способствовать значительному росту преступлений, совершаемых с использованием ИТТ, определенная часть из которых не попадет в поле зрения правоохранительных органов.

О значительном числе «бытовых компьютерных» преступлений, совершаемых с использованием ИТТ (взлом социальных сетей или мессенджеров, вирусные атаки на домашние компьютеры и др.), потерпевшие узнают только через определенное количество времени и обращаются в правоохранительные органы с существенным опозданием, поэтому нередко получают от них незаконный отказ по заявленным противоправным фактам.

Есть негласное указание отдельных руководителей правоохранительных органов о необходимости сокращения количества регистрируемых в сфере ИТТ противоправных деяний, не имеющих реальной судебной перспективы, следовательно, «портящих» статистические показатели, что может привести к неблагоприятным последствиям как для отдельных сотрудников (например, смещение с должности), так и всей силовой структуры.

Определенное количество выявленных преступлений, совершаемых с использованием ИТТ, отдельными сотрудниками правоохранительных органов незаконно скрывается от регистрации из-за корыстных побуждений или иной личной заинтересованности.

Наличие противоречий между реальными потребностями граждан в информационных услугах и возможностью их удовлетворения легальными способами в силу низкого уровня жизни, а также монополизма разработчиков компьютерных программ, искусственно завышающих цены на свои продукты приводит к тому, что в большинстве случаев сотрудники правоохранительных органов «закрывают глаза» на ставшие им известные факты использования населением «дешевой» (нередко не уступающей по своим качественным характеристикам оригиналу) нелицензированной продукции [16, с. 98].

Часть преступлений, совершаемых с использованием ИТТ, остается латентными в силу того, что отдельные сотрудники правоохранительных органов за получение помощи (информации) со стороны «доверенных» хакеров «закрывают глаза» на совершаемые последними посягательства в информационно-телекоммуникационной сфере.

Возбуждение уголовных дел по ряду преступлений, совершаемых с использованием ИТТ (например, взлом аккаунтов социальных сетей, распространение вредоносных программ), связано с необходимостью проведения большого объема процессуальных действий, что «подталкивает» недобросовестных сотрудников правоохранительных органов к вынесению незаконных постановлений об отказе в их возбуждении.

По причине применяемых преступниками высокоразвитых технологий у сотрудников правоохранительных органов, осуществляющих проверку информации (например, хищение криптовалюты), возникают неопределенность и разумные сомнения как относительно наличия самого преступления, совершаемого с использованием ИТТ, так и предусмотренного законом основания для возбуждения уголовного дела.

Отсутствие своевременных апробированных на практике научно разработанных методик выявления (доказывания) преступных посягательств, совершаемых в информационно-телекоммуникационном пространстве, а также недостаточность системных обобщений материалов оперативной, следственной и судебной практики в указанной сфере затрудняют во многих случаях возможность установления события или состава преступления, совершаемого с использованием ИТТ, а следовательно, приводят к необоснованным отказам в возбуждении соответствующих уголовных дел [17, с. 96].

Существование латентной преступности, совершаемой в сфере ИТТ, отчасти обусловлено недостаточным опытом работы сотрудников правоохранительных органов со специфическими источниками доказательственной информации, находящейся в цифровой форме в виде электронных сообщений, страниц, сайтов [18, с. 85–86]. Так, выявлением преступлений, совершаемых с использованием ИТТ, занимаются сотрудники подразделения «К» МВД России, имеющие, как правило, юридическое образование, тогда как во многих странах мира это осуществляют прежде всего «технические» эксперты с дополнительным образованием в области юриспруденции. Поэтому у сотрудников правоохранительных органов возникают определенные сложности в осуществлении оперативно-розыскной деятельности по выявлению преступлений в сфере информационно-телекоммуникационных технологий, а также лиц (юридических и физических), причастных к их совершению.

Часть преступлений, совершаемых с использованием ИТТ, остаются латентными в силу существования проблем, связанных с нехваткой в штате экспертных подразделений правоохранительных органов (прежде всего на местах) квалифициро-

ванных специалистов в области компьютерной информации и (или) их недостаточной подготовленностью в области программного обеспечения и компьютерной техники; длительностью проведения экспертных исследований, а также трудностями в интерпретации результатов экспертизы. Заключения экспертов зачастую оказываются либо неконкретными, малоинформативными для следствия, либо же «легко» оспариваются адвокатом подозреваемого лица. [19, с. 66].

Латентности преступлений, совершаемых с использованием ИТТ, способствует то обстоятельство, что до настоящего времени не окончен процесс формирования договорной правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисов, в том числе социальных сетей. Также отсутствуют эффективные механизмы взаимодействия органов внутренних дел с заинтересованными ведомствами, коммерческими организациями, предусматривающие возможность оперативной блокировки сайтов интернет-пирамид, фишинговых сайтов и мошеннических колл-центров, а также номеров телефонов, с использованием которых осуществляются мошеннические действия. Кроме того, не разработан механизм блокирования вредоносного программного обеспечения для операционных систем мобильных устройств, используемого в целях хищения денежных средств со счетов через услугу «Мобильный банк» [20, с. 6].

Преступления, совершаемые с использованием ИТТ, остаются латентными в силу того, что законодательная деятельность правоохранительных органов по установлению «жесткого» государственного контроля над информационно-коммуникационным пространством наталкивается на активное сопротивление со стороны общественных институтов, представители которых усматривают в этом ущемление прав граждан и вмешательство в их частную жизнь.

Условиями, способствующими латентности преступлений, совершаемых с использованием ИТТ, являются также: доступ самых широких слоев населения к компьютерной технике и Интернету; трансграничность географии совершения преступлений, совершаемых с использованием ИТТ; отсутствие у значительного числа пользователи минимальных знаний о «компьютерной гигиене» и правилах безопасной работы в информационном пространстве; безконтактность и относительная доступность объекта преступного посягательства; относительная комфортность деятельности преступников, связанной с подготовкой и реализацией преступных замыслов [21, с. 77].

Вышесказанное позволяет сформулировать следующие выводы.

В ближайшие годы продолжится процесс усложнения способов совершения преступлений с использованием ИТТ, а также рост криминального профессионализма компьютерных преступников.

В связи с дальнейшим неизбежным развитием информационных и компьютерных технологий, а также расширением информационно-коммуникационного пространства количество (объем) преступлений в указанной сфере будут увеличиваться, а определенная часть из них останется латентными.

Детерминанты латентности преступности в сфере ИТТ носят разнообразный, разнонаправленный и разносторонний характер, что объясняется постоянным совершенствованием компьютерных технологий и расширением информационно-телекоммуникационного пространства.

Успешное воздействие на детерминанты латентных преступлений, совершаемых с использованием ИТТ, позволит вывести из «тени» определенную часть противоправных посягательств, а также реализовать на практике принцип неотвратимости уголовной ответственности и наказания.

Библиографический список

1. Состояние преступности в России за январь-декабрь 2019 года. ФКУ ГИАЦ МВД РФ. Москва, 2020. С. 30–31. URL: http://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf.

2. Саркисян А. Ж. Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий // Российский следователь. 2019. № 3. С. 54–59. URL: http://elibrary.ru/item.asp?id=37158345.

3. Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учебное пособие. Москва, 2018. 115 с. DOI: http://doi.org/10.12737/textbook_5c4ef6ec398dc8.00768597.

4. Иванова Е. О. Латентная преступность: понятие и критерии классификации // Современное право. 2015. № 5. С. 119–123. URL: http://elibrary.ru/item.asp?id=23501557.

5. Ki Hong (Steve) Chon. Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. 2018. № 1. С. 66–81. DOI: http://doi.org/10.25911/5D778A24D8836.

6. Джафарли В. Ф. Краткий криминологический анализ причин и условий киберпреступности и методы ее предупреждения // Ученые труды Российской Академии адвокатуры и нотариата. 2017. № 2. С. 54–58. URL: http://elibrary.ru/item.asp?id=30047906.

7. Арипшев А. М. Преступления в сфере информационных технологий: киберпреступность // Евразийский юридический журнал. 2019. № 1. С. 285–286. URL: http://elibrary.ru/item.asp?id=37084960.

8. Трофимцева С. Ю., Илюшин Д. А. Некоторые аспекты определения места и времени совершения киберпреступлений в Российской Федерации // Евразийский юридический журнал. 2016. № 9. С. 246–247. URL: http://elibrary.ru/item.asp?id=27316147.

9. Дремлюга Р. И., Крипакова А. В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. № 3. С. 161–169. DOI: http://doi.org/10.17803/1994-1471.2019.100.3.161-169.

10. Поляков В. В., Ширяев А. В. Криминалистические аспекты личности потерпевших от киберпреступлений // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий: сб. нвуч. ст. / отв. ред. С. И. Давыдов, В. В. Поляков. Вып. XV. Барнаул: Изд-во Алт. ун-та, 2018. С. 164–171. URL: http://www.elibrary.ru/item.asp?id=38581275&.

11. Пичугин В. Г., Годунова Л. А. Социально-психологические причины латентной преступности // Вопросы российского и международного права. 2019. Т. 9, № 2-А. С. 62–68. DOI: http://doi.org/10.25799/AR.2019.83.2.008.

12. Кравцов Д. А., Дворникова Т. А, Колесинская Ю. А. Латентная преступность в сети «Интернет» и ее детерминанты // Advanced Science: сб. ст. VIII Международной науч.-практ. конф.: в 2 ч. Пенза. 2019. С. 152–154. URL: http://www.elibrary.ru/item.asp?id=37605830.

13. Евдокимов К. Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37. URL: http://www.elibrary.ru/item.asp?id=23128290.

14. Пучков Д. В. Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации // Правовая политика и правовая жизнь. 2019. № 1. С. 63–71. URL: http://www.elibrary.ru/item.asp?id=37108446.

15. Айсханова Е. С. Причины и мотивы роста киберпреступности как глобального явления современности // Вестник Чеченского государственного университета. 2017. № 4 (28). С. 153–155. URL: http://www.elibrary.ru/item.asp?id=32274561.

16. Чекунов И. Г. Киберпреступность: проблемы и пути их решения // Вестник Академии права и управления. 2017. № 25 С. 97–103. URL: http://www.elibrary.ru/item.asp?id=17260696.

17. Кузора С. А. Проблемы проведения проверки по сообщению о киберпреступлении // Закон и право. 2018. № 2. С. 94–96. URL: http://www.elibrary.ru/item.asp?id=32432944.

18. Кумышева М. К. Кадровое обеспечение противодействия кибертерроризму в Российской Федерации // «Черные дыры» в Российском законодательстве. 2017. № 3. С. 85–86. URL: http://www.elibrary.ru/item.asp?id=29277185.

19. Крамаренко В. П., Осипова Е. В., Загоскин А. В. Проблемы раскрытия и расследования преступлений экстремистской направленности в сети Интернет // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2017. № 4 (50). С. 65–68. URL: http://www.elibrary.ru/item.asp?id=32260181.

20. Решение коллегии Министерства внутренних дел Российской Федерации от 01.11.2019. URL: http://сао.мск.мвд.рф/Dop/Pravovaja_informacija/документы/приказы-мвд-россии/item/19245266 (дата обращения: 05.01.2020)

21. Шаталов А. С. Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 68–83. DOI: http://doi.org/10.17323/2072-8166.2018.2.68.83.

References

1. *Sostoyanie prestupnosti v Rossii za yanvar'-dekabr' 2019 goda* [State of crime in Russia for January-December 2019]. Moscow: FKU GIATs MVD RF, 2020, pp. 30–31. Available at: http://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf [in Russian].

2. Sarkisyan A. Zh. *Kriminologicheskaya kharakteristika prestupleniy, sovershaemykh v sfere informatsionno-kommunikatsionnykh tekhnologiy* [Criminologic characteristics of committed crimes in the information and communication technology sphere]. *Rossiyskiy sledovatel'* [Russian Investigator], 2019, no. 3, pp. 54–59. Available at: http://elibrary.ru/item.asp?id=37158345 [in Russian].

3. Russkevich E. A. *Ugolovno-pravovoe protivodeystvie prestupleniyam, sovershaemym s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologiy: uchebnoe posobie* [Criminal law counteraction to crimes committed with the use of information and communication technologies: textbook]. Moscow, 2018, 115 p. DOI: http://doi.org/10.12737/textbook_5c4ef6ec398dc8.00768597 [in Russian].

4. Ivanova E. O. *Latentnaya prestupnost': ponyatie i kriterii klassifikatsii* [Latent crime: definition and criteria of classification]. *Sovremennoe pravo* [Modern Law], 2015, no. 5, pp. 119–123. Available at: http://elibrary.ru/item.asp?id=23501557 [in Russian].

5. Ki Hong (Steve) Chon. Cybercrime Precursors:Towards a Model of Offender Resources *The Australian National University Journal*, 2018, no. 1, pp. 66–81. DOI: http://doi.org/10.25911/5D778A24D8836 [in English].

6. Jafarli V. F. *Kratkiy kriminologicheskiy analiz prichin i usloviy kiberprestupnosti i metody ee preduprezhdeniya* [A brief criminological analysis of reasons and conditions of kiberprestupniki and methods of its prevention]. *Uchenye trudy Rossiyskoy Akademii advokatury i notariata* [Scientific Works of the Russian Academy of Advocacy and Notary], 2017, no. 2, pp. 54–58. Available at: http://elibrary.ru/item.asp?id=30047906 [in Russian].

7. Aripshev A. M. *Prestupleniya v sfere informatsionnykh tekhnologiy: kiberprestupnost'* [Crimes in the sphere of information technologies: cybercrime]. *Evraziyskiy yuridicheskiy zhurnal* [Eurasian Law Journal], 2019, no. 1, pp. 285–286. Available at: http://elibrary.ru/item.asp?id=37084960 [in Russian].

8. Trofimtseva S. Yu., Ilyushin D. A. *Nekotorye aspekty opredeleniya mesta i vremeni sovershenia kiberprestupleniy v Rossiyskoy Federatsii* [Some aspects of identification of the place and time of cybercrime committing in the Russian Federation]. *Evraziyskiy yuridicheskiy zhurnal* [Eurasian Law Journal], 2016, no. 9, pp. 246–247. Available at: http://elibrary.ru/item.asp?id=27316147 [in Russian].

9. Dremlyuga R. I., Kripakova A. V. *Prestupleniya v virtual'noy real'nosti: mif ili real'nost'?* [Crimes in virtual reality: myth or reality?]. *Aktual'nye problemy rossiyskogo prava* [Actual Problems of Russian Law], 2019, no. 3, pp. 161–169. DOI: http://doi.org/10.17803/1994-1471.2019.100.3.161-169 [in Russian].

10. Polyakov V. V., Shiryaev A. V. *Kriminalisticheskie aspekty lichnosti poterpevshikh ot kiberprestupleniy* [Forensic aspects of the identity of victims of cybercrimes]. In: *Ugolovno-protsessual'nye i kriminalisticheskie chteniya na Altae: problemy i perspektivy protivodeystviya prestupleniyam, sovershaemym s primeneniem informatsionnykh*

tekhnologiy:sbornik nauchnykh statey. Otv. red. S. I. Davydov, V. V. Polyakov. Vyp. XV [Davydov S. I., Polyakov V. V. (Eds.) Criminal procedural and forensic readings in Altai: problems and prospects of combating crimes committed with the use of information technology. Collection of scientific articles. Issue XV]. Barnaul: Izd-vo Alt. un-ta, 2018, pp. 164–171. Available at: http://www.elibrary.ru/item.asp?id=38581275& [in Russian].

11. Pichugin V. G., Godunova L. A. *Sotsial'no-psikhologicheskie prichiny latentnoy prestupnosti* [Socio-psychological reasons of latent crime]. *Voprosy rossiyskogo i mezhdunarodnogo prava*, 2019, vol. 9, no. 2-A, pp. 62–68. DOI: http://doi.org/10.25799/AR.2019.83.2.008 [in Russian].

12. Kravtsov D. A., Dvornikova T. A, Kolesinskaya Yu. A. *Latentnaya prestupnost' v seti «Internet» i ee determinanty* [Latent crime in a network «the Internet» and its determinants). In: *Advanced Science: sbornik statey VIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii: v 2 ch.* [Advanced Science: collection of articles of the VIII International research and practical conference: in 2 parts]. Penza, 2019, pp. 152–154. Available at: http://www.elibrary.ru/item.asp?id=37605830 [in Russian].

13. Evdokimov K. N. *Prichiny komp'yuternoy prestupnosti v sovremennoy Rossii* [Causes of cyber crime in modern Russia]. *Rossiyskiy sledovatel'* [Russian Investigator], 2015, no. 3, pp. 33–37. Available at: http://www.elibrary.ru/item.asp?id=23128290 [in Russian].

14. Puchkov D. V. *Sostoyanie ugolovno-pravovogo regulirovaniya kiberprestupleniy v ugolovnom zakonodatel'stve Rossiyskoy Federatsii* [The state of criminal law regulation of cybercrime in the criminal legislation of the Russian Federation]. *Pravovaya politika i pravovaya zhizn',* 2019, no. 1, pp. 63–71. Available at: http://www.elibrary.ru/item.asp?id=37108446 [in Russian].

15. Ayskhanova E.S. *Prichiny i motivy rosta kiberprestupnosti kak global'nogo yavleniya sovremennosti* [The reasons and motives for the growth of cybercrime as a global phenomenon of our time]. *Vestnik Chechenskogo gosudarstvennogo universiteta,* 2017, no. 4 (28), pp. 153–155. Available at: http://www.elibrary.ru/item.asp?id=32274561 [in Russian].

16. Chekunov I. G. *Kiberprestupnost': problemy i puti ikh resheniya* [Cybercrime: problems and ways of their solution]. *Vestnik Akademii prava i upravleniya,* 2017, no. 25, pp. 97–103. Available at: http://www.elibrary.ru/item.asp?id=17260696 [in Russian].

17. Kuzora S. A. *Problemy provedeniya proverki po soobshcheniyu o kiberprestuplenii* [The problem of verification of reported cybercrime]. *Zakon i pravo* [Law and Legislation], 2018, no. 2, pp. 94–96. Available at: http://www.elibrary.ru/item.asp?id=32432944 [in Russian].

18. Kumysheva M. K. *Kadrovoe obespechenie protivodeystviya kiberterrorizmu v Rossiyskoy Federatsii* [Staffing countering cyber terrorism in the Russian Federation]. *«Chernye dyry» v Rossiyskom zakonodatel'stve* [Black Holes in Russian Legislation], 2017, no. 3, pp. 85–86. Available at: http://www.elibrary.ru/item.asp?id=29277185 [in Russian].

19. Kramarenko V. P., Osipova E. V., Zagoskin A. V. *Problemy raskrytiya i rassledovaniya prestupleniy ekstremistskoy napravlennosti v seti Internet* [Issues of investigation of extremism related crimes committed in the Internet]. *Vestnik Kaliningradskogo filiala Sankt-Peterburgskogo universiteta MVD Rossii* [Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Interior Affairs of Russia], 2017, no. 4 (50), pp. 65–68. Available at: http://www.elibrary.ru/item.asp?id=32260181 [in Russian].

20. *Reshenie kollegii Ministerstva vnutrennikh del Rossiyskoy Federatsii ot 01.11.2019* [Decision of the collegium of the Ministry of Internal Affairs of the Russian Federation dated 01.01.2019). Available at: http://сао.мск.мвд.рф/Dop/Pravovaja_informacija/документы/приказы-мвд-россии/tem/19245266 (accessed 05.01.2020) [in Russian].

21. Shatalov A. S. *Fenomenologiya prestupleniy, sovershennykh s ispol'zovaniem sovremennykh informatsionnykh tekhnologiy* [Phenomenology of the computer-oriented crimes]. *Pravo. Zhurnal Vysshey shkoly ekonomiki* [Law. Journal of the Higher School of Economics], 2018, no. 2, pp. 68–83. DOI: http://doi.org/10.17323/2072-8166.2018.2.68.83 [in Russian].